ЧЕРКАСЬКИЙ ДЕРЖАВНИЙ ТЕХНОЛОГІЧНИЙ УНІВЕРСИТЕТ
МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

Кваліфікаційна наукова
праця на правах рукопису

БАБЕНКО Віра Григорівна

УДК 004.056.55:004.312.2

ДИСЕРТАЦІЯ

МЕТОДОЛОГІЯ СИНТЕЗУ ОПЕРАЦІЙ ПЕРЕТВОРЕННЯ ІНФОРМАЦІЇ ДЛЯ КОМП'ЮТЕРНОЇ КРИПТОГРАФІЇ

05.13.05 – комп'ютерні системи та компоненти
технічні науки

Подається на здобуття наукового ступеня доктора технічних наук

Дисертація містить результати власних досліджень. Використання ідей, результатів і текстів інших авторів мають посилання на відповідне джерело.

В.Г. Бабенко

Науковий консультант: **Рудницький Володимир Миколайович**
доктор технічних наук, професор

Черкаси - 2020

АНОТАЦІЯ

Бабенко В.Г. Методологія синтезу операцій перетворення інформації для комп'ютерної криптографії. – Кваліфікаційна наукова праця на правах рукопису.

Дисертація на здобуття наукового ступеня доктора технічних наук за спеціальністю 05.13.05 «Комп'ютерні системи та компоненти». – Черкаський державний технологічний університет, Черкаси, 2020.

Дисертаційна робота присвячена підвищенню ефективності функціонування систем комп'ютерної криптографії шляхом створення методології синтезу операцій перетворення інформації та побудови криптографічних примітивів на їх основі.

Перший розділ присвячений аналітичному огляду систем криптографічного захисту, стандартних вимог до криптографічних систем. Для здійснення аналізу розглянуто принципи побудови й схеми криптологічних систем. Особливу увагу приділено дослідженню основних властивостей функцій криптографічного перетворення для побудови стійких шифрів. Проведений аналіз сучасних криптосистем та виокремлені основні характеристики ефективності функціонування системи криптографічного захисту. Сформульовані мета та задачі дисертаційного дослідження. Наведена структурно-логічна схема проведення наукового дослідження.

Другий розділ присвячений розробці та узагальненню методів синтезу операцій криптографічного перетворення, а також побудові та формалізації методології синтезу логічних операцій для криптографічного перетворення інформації.

У третьому розділі проведена класифікація трирозрядних елементарних функцій для криптографічного перетворення інформації за складністю та функціональними особливостями перетворення. Розроблені такі методи: метод синтезу трьохрозрядних розширених матричних елементарних функцій в дискретному представленні; метод синтезу трьохрозрядних розширених матричних елементарних функцій в модульно-дискретному представленні; метод синтезу m-розрядних розширених матричних елементарних функцій; метод

побудови обернених операцій за наявності однієї чи двох замін, а також на більшу кількість змінних; метод синтезу операції оберненого розширеного матричного криптографічного перетворення на основі індексації рядків.

Четвертий розділ присвячений реалізації криптопримітивів ковзного шифрування на основі матричних операцій криптографічного перетворення. Одержано узагальнені рекурентні послідовності, що описують функції перетворення інформації при здійсненні багаторазового ковзного шифрування, що дало змогу побудувати алгоритми паралельної реалізації криптопримітивів багаторазового ковзного шифрування заданої кількості ітерацій. Ці результати забезпечили підвищення швидкості шифрування до двох разів та стійкість до лінійного криптоаналізу при реалізації багаторазового ковзного шифрування.

П’ятий розділ присвячений моделюванню операцій для мультиопераційних матричних криптографічних примітивів. Розроблено технологію синтезу операцій для мультиопераційних матричних криптографічних примітивів на основі побудови нових груп операцій з точністю до перестановки шляхом використання запропонованої табличної моделі операції криптоперетворення. Розроблено технологію синтезу двохоперандних матричних операцій для матричних моделей криптографічного перетворення з метою розширення кількості операцій криптографічного перетворення інформації в матричних операціях криптографічного перетворення. Побудовано узагальнені моделі рекурентних послідовностей, що описують реалізацію багаторазового криптопримітиву ковзного шифрування зі змінними операціями раунду на основі використанням операцій з синтезованої групи операцій криптографічного перетворення.

Шостий розділ присвячено синтезу криптоалгоритмів на основі синтезованих операцій криптографічного перетворення інформації шляхом їх дослідження на структурному рівні та апаратної реалізації. Здійснено дослідження способів забезпечення нелінійності перетворення матричними операціями криптоперетворення. Наведено розрахунки оцінки показників ефективності реалізації синтезованих операцій за наступними параметрами: розрядність операцій; складність операції; час виконання операції; складність

перетворення блоку інформації; час виконання перетворення блоку інформації, що дозволяють отримати показники ефективності криптоалгоритмів, побудованих на основі комбінації синтезованих груп операцій.

Висновки містять основні наукові та практичні результати дисертаційного дослідження.

Наукова новизна отриманих результатів:

1. Вперше запропонована методологія синтезу операцій криптографічного перетворення інформації на основі існуючих та розроблених методів синтезу операцій прямого, оберненого та взаємного криптографічного перетворення шляхом їх класифікації та узагальнення, що забезпечило можливість розширення бази операцій, використання яких дозволяє вдосконалювати існуючі та синтезувати нові криптоалгоритми і криптопримітиви.

2. Вперше розроблено технологію синтезу операцій для мультиопераційних матричних криптографічних примітивів на основі побудови нових груп операцій з точністю до перестановки шляхом використання запропонованої табличної моделі операції криптоперетворення, що дозволило за рахунок варіативності операцій підвищити криптостійкість існуючих криптопримітивів.

3. Удосконалено методи побудови криптографічних примітивів на прикладі примітивів ковзного шифрування на основі матричних операцій криптографічного перетворення та отриманих узагальнених рекурентних послідовностей для побудови моделей шляхом їх паралельної реалізації, що забезпечило підвищення швидкості шифрування (до двох разів) та стійкості до лінійного криптоаналізу.

4. Удосконалено методи синтезу та аналізу криптографічних алгоритмів на основі узагальненої моделі криптоалгоритму, шляхом послідовно-паралельної реалізації операцій криптографічного перетворення інформації на макро- та мікрорівнях, що забезпечило можливість вирішення протиріч між криптостійкістю, складністю та швидкістю для досягнення заданої ефективності, виходячи з задач проектування.

5. Отримали подальший розвиток математичні моделі та методи синтезу

елементарних функцій та операцій криптоперетворення на основі запропонованої методології та вибраної групи елементарних функцій розширеного матричного криптоперетворення шляхом вдосконалення математичного апарату для синтезу прямих та обернених матричних моделей не афінних дискретних перетворень, що в сукупності забезпечило можливість синтезу операцій нелінійних криптографічних перетворень.

Практичне значення отриманих результатів. Практична цінність роботи полягає в доведенні здобувачем отриманих наукових результатів до конкретних інженерних методик, алгоритмів, моделей та варіантів побудови криптографічних алгоритмів.

На підставі проведених досліджень одержано такі практичні результати: розроблено методологію синтезу операцій криптографічного перетворення інформації в рамках запропонованої концепції побудови алгоритмів захисту інформації на їх основі з можливістю підбору оптимальних показників криптостійкості та швидкодії, що дає змогу покращити ефективність функціонування системи криптографічного захисту в цілому; розроблено технологію побудови та використання криптопримітивів на основі синтезованих операцій криптографічного перетворення інформації з можливістю їх паралельного виконання, що дає виграш у швидкості та часі здійснення перетворення безпосередньо інформації; запропоновано варіанти реалізації на програмному та апаратному рівнях нових груп криптографічних операцій заданої розрядності, що володіють властивостями афінності та нелінійності, зокрема матричного та розширеного матричного перетворення. Застосування синтезованих операцій криптографічного перетворення на основі запропонованих варіантів комбінації використання матричного та розширеного матричного перетворення при конструюванні алгоритмів дає можливість збільшити криптостійкість (від 2^{166} до 2^{8157} разів) пропорційно відносно потокового шифрування при зменшенні часу шифрування (від 1,3 до 8 разів).

Реалізація. Результати дисертаційної роботи включені до звітів НДР: «Методи та засоби захисту інформації МНС України на основі операцій

криптографічного кодування» (ДР № 0112U003579), «Криптографічне кодування: методи та засоби реалізації (частина 2)» (ДР № 0113U001475), «Ефективність систем інформаційної безпеки», шифр НДР «Безпека» (ДРН 0113U004731), «Ефективність систем інформаційної безпеки» (Шифр «Перетворення»), «Синтез операцій криптографічного перетворення з заданим характеристиками» (ДР № 0116U008714), «Розробка методів та засобів оцінки ефективності соціоінжинірингу» (ДР № 0116U008715), при виконанні держбюджетної теми № 36Б115 «Розробка методів синтезу тестових моделей поведінки програмних об'єктів, підвищення оперативності передачі та захисту інформації у телекомунікаційних системах» (ДР № 0115U003103) (Кіровоградський національний технічний університет), в яких автор брав участь як виконавець.

Одержані в ній теоретичні й практичні результати використані та впроваджені у таких закладах: НВК «Фотоприлад», «Науково-дослідний інститут «Акорд» та ПП «Сенсорна електроніка» (м. Черкаси), ТОВ «Люменс-груп» (м. Кіровоград) та в освітній процес у навчальних закладах: Черкаському державному технологічному університеті, Черкаському національному університеті імені Б. Хмельницького, Національному аерокосмічному університеті імені М. Є. Жуковського «ХАІ», Кіровоградському національному технічному університеті.

Ключові слова: комп’ютерна криптографія, операції криптографічного перетворення, нелінійність, варіативність, паралельна реалізація, узагальнена модель, криптостійкість, швидкість перетворення.

ABSTRACT

Babenko V.G. The methodology for the synthesis of information transformation operations for computer cryptography. – Qualification scientific work with the manuscript copyright.

The thesis for a Doctor of Science Degree in speciality 05.13.05 – Computer Systems and Components. – Cherkasy State Technological University, Cherkasy, 2020.

The dissertation is devoted to increasing the functioning efficiency of the computer cryptosystems, based on the methodology creation for the synthesis of information's cryptographic transformation operations and the construction of cryptographic primitives based on them.

The first section is devoted to the analytical review of cryptographic protection systems, standard requirements for cryptographic systems. To carry out the analysis, the principles of construction and scheme of cryptological systems are considered. Particular attention is paid to the study of the cryptographic transformation functions basic properties for the construction of stable ciphers. The analysis of modern cryptosystems is carried out and the main functioning efficiency characteristics of system of cryptographic protection are allocated. The purpose and tasks of the dissertation research are formulated. The structural and logical scheme of scientific research is given.

The second section is devoted to the development and generalization of methods for the cryptographic transformation operations' synthesis, as well as the construction and formalization of the methodology for the synthesis of logical operations for cryptographic information transformation.

The classification of three-bit elementary functions for information's cryptographic transformation by complexity and functional features of transformation is performed in the third section. The following methods have been developed: a method for the synthesis of three-digit extended matrix elementary functions in a discrete representation; method of synthesis of three-bit extended matrix elementary functions in modular-discrete representation; method of synthesis m-bit extended matrix elementary functions; the method of constructing inverse operations in the presence of one or two

substitutions, as well as for a larger number of variables; method of synthesis of inverse extended matrix cryptographic transformation operation based on string indexing.

The fourth section is devoted to the implementation of crypto-primitives of sliding encryption based on matrix operations of cryptographic transformation. Generalized recurrent sequences describing the functions of information transformation in the multiple sliding encryption implementation are obtained, which allowed to build algorithms for parallel implementation of crypto primitives of multiple sliding encryption of a given number of iterations. These results provided an increase in the encryption speed up to twice and resistance to linear cryptanalysis in the implementation of multiple sliding encryption.

The fifth section is devoted to modeling operations for multi-operational matrix cryptographic primitives. The synthesizing technology of operations for multioperative matrix cryptographic primitives basing on constructing new groups of operations with accuracy to permutation by use of the offered tabular model of cryptotransformation operation is developed. The synthesizing technology of two - operand matrix operations for matrix models of cryptographic transformation to expanse the operations' number of cryptographic transformation of information in cryptographic transformation's matrix operations is developed. Generalized models of recurrent sequences are constructed, which describe the implementation of a multiple cryptoprimitive of sliding encryption with variable round operations based on the use of operations from the cryptographic transformation operations' synthesized group.

The sixth section is devoted to synthesizing the cryptoalgorithms based on synthesized operations of information's cryptographic transformation through their study at the structural level and hardware implementation. Researching the ways to provide the nonlinearity of transformation by matrix operations of cryptographic transformation is carried out. The calculations of the indicators' estimation of realization efficiency for the synthesized operations on the following parameters are resulted: bit size of operations; the complexity of the operation; operation execution time; the transformation complexity of the information block; the execution time of transforming

the information's block that allows to obtain performance indicators of cryptoalgorithms built on the basis of the operations' synthesized groups combination.

The conclusions contain the main scientific and practical results of the dissertation research.

Scientific novelty of the obtained results:

1. For the first time the synthesizing methodology of information's cryptographic transformation operations based on existing and developed methods of synthesizing the operations of direct, inverse and mutual cryptographic transformation by their classification and generalization is offered.

2. For the first time, the technology of operations synthesis for multioperative matrix cryptographic primitives was developed on the basis of constructing the new groups of operations with accuracy to permutation by using the proposed tabular model of cryptographic transformation operation, which allowed increasing the existing cryptoprimitives cryptostability due to the variability of operations.

3. Improved methods for constructing cryptographic primitives on the example of sliding encryption primitives based on matrix operations of cryptographic transformation and obtained generalized recurrent sequences for building models by their parallel implementation, which provided increased encryption speed (up to twice) and resistance to linear cryptanalysis.

4. Improved methods for synthesizing and analyzing the cryptographic algorithms based on a generalized model of cryptoalgorithm, by sequential parallel implementation of information's cryptographic transformation at the macro and micro levels, which provided the ability to resolve conflicts between cryptographic resistance, complexity and speed to achieve efficiency, based on design tasks.

5. Mathematical models and methods of synthesizing the elementary functions and crypto conversion operations were further developed based on the proposed methodology and the selected elementary functions group of extended matrix cryptographic transformation by improving the mathematical apparatus for synthesis of direct and inverse matrix models of non-affine discrete transformations which together

provided the possibility to synthesize the operations of nonlinear cryptographic transformations.

Practical significance of obtained results. The practical value of the work lies in bringing the applicant's scientific results to specific engineering techniques, algorithms, models and options for constructing cryptographic algorithms.

Based on the research, the following practical results were obtained: a methodology for synthesizing operations of cryptographic information transformation within the proposed concept of building information protection algorithms based on them with the possibility of selecting optimal indicators of cryptographic stability and speed, which improves the efficiency of cryptographic protection system as a whole; developed technology for constructing and using crypto-primitives based on synthesized operations of information' cryptographic transformation of with the possibility of their parallel execution, which gives a gain in the speed and time of conversion directly the information; variants of realization at the software and hardware implementation levels of new cryptographic operations groups of the set bit rate possessing properties of affinity and nonlinearity, in particular matrix and extended matrix transformation are offered.

Using the synthesized operations of cryptographic transformation based on the proposed options for combining the use of matrix and extended matrix transformations in the design of algorithms allows to increase the cryptographic security from 2166 to 28157 times in proportion to stream encryption while reducing the encryption time from 1.3 to 8 times.

Implementation. The results of the dissertation are included in the reports of research works: "Methods and means of information protection of the Ministry of Emergencies of Ukraine based on cryptographic coding operations" (DR № 0112U003579), "Cryptographic coding: methods and means of implementation (part 2)" (DR № 0113U001475), "Efficiency of information security systems", code research work "Security" (DRN 0113U004731), "Efficiency of information security systems" (Code "Transformation"), "Synthesis of cryptographic transformation operations with specified characteristics" (DR № 0116U008714), "Development of methods and tools evaluation of

the effectiveness of socio-engineering "(DR № 0116U008715), in the implementation of the state budget theme № 36B115" Development of methods for synthesis of test models of behavior of software objects, improving the efficiency of transmission and protection of information in telecommunications systems "(DR № 0115U003103), Kirovograd University in which the author participated as a performer.

The theoretical and practical results obtained in it were used and implemented in the following institutions: research and production complex "Fotoprilad", "Research Institute "Accord" and private enterprise "Sensor Electronics"(Cherkasy), limited liability company "Lumens- groups" (Kirovograd) and in the educational process in educational institutions: Cherkasy State Technological University, Cherkasy National University named after B. Khmelnytsky, National Aerospace University named after M.Y. Zhukovsky "KHAI ", Kirovograd National Technical University.

Keywords: computer cryptography, cryptographic transformation operations, nonlinearity, variability, parallel implementation, generalized model, cryptographic resistance, transformation speed.

Список публікацій здобувача:

1. Бабенко В. Г. Дослідження матричних операцій криптографічного перетворення на основі арифметичних операцій за модулем. *Системи управління, навігації та зв'язку*. 2012. Вип. 4 (24). С. 85–88.

2. Бабенко В. Г. Параллельная реализация скользящего шифрования. *Системи обробки інформації*. 2013. Вип. 9 (116). С. 131–134.

3. Бабенко В. Г. Оптимизация матричных операций скользящего шифрования. *Системи озброєння і військова техніка*. 2013. № 4 (36). С. 132–135.

4. Бабенко В. Г. Складності та особливості побудови ефективних криптоалгоритмів. *Вісник Черкаського державного технологічного університету*. 2014. № 3. С. 87–91.

5. Бабенко В. Г. Застосування операцій криптографічного перетворення для синтезу криптоалгоритмів. *Сучасна спеціальна техніка*. 2014. № 3 (38). С. 49–55.

6. Рудницький В. М., Миронець І. В., Бабенко В. Г. Обґрунтування можливості розширення набору функцій перекодування інформації для захисту конфіденційних інформаційних ресурсів. *Системи управління, навігації та зв'язку*. 2010. Вип. 2 (14). С. 118–122.

7. Рудницький В. М., Миронець І. В., Бабенко В. Г. Методологія підвищення оперативності доступу до конфіденційних інформаційних ресурсів. *Системи обробки інформації*. 2010. Вип. 5 (86). С. 15–19.

8. Рудницький В. М., Миронець І. В., Бабенко В. Г. Реалізація методу підвищення оперативності доступу до конфіденційних інформаційних ресурсів. *Вісник Черкаського державного технологічного університету.* 2010. № 3. С. 60–65.

9. Рудницький В. М., Бабенко В. Г., Жиляєв Д. А. Алгебраїчна структура множини логічних операцій кодування. *Наука і техніка Повітряних Сил Збройних Сил України*. 2011. Вип. 2 (6). С. 112–114.

10. Рудницький В. М., Миронець І. В., Бабенко В. Г. Систематизація повної множини логічних функцій для криптографічного перетворення інформації. *Системи обробки інформації*. 2011. Вип. 8 (98). С. 184–188.

11. Рудницький В. М., Миронець І. В., Бабенко В. Г. Технологія побудови пристрою реалізації методу підвищення оперативності доступу до конфіденційних інформаційних ресурсів. *Збірник наукових праць Харківського університету Повітряних Сил*. 2011. Вип. 3 (29). С. 145–150.

12. Бабенко В. Г., Миронець І. В., Рудницький С. В. Декодування інформації в групі дворозрядних операцій криптографічного перетворення. *Системи управління, навігації та зв'язку*. 2011. Вип. 4 (20). С. 208–212.

13. Бабенко В. Г., Рудницький С. В., Мельник Р. П. Визначення множини трирозрядних елементарних операцій криптографічного перетворення. *Вісник інженерної академії України*. 2012. Вип. 3 (4). С. 77–79.

14. Рудницький В. М., Бабенко В. Г., Рудницький С. В. Метод синтезу матричних моделей операцій криптографічного кодування та декодування інформації. *Збірник наукових праць Харківського університету Повітряних Сил*. 2012. Вип. 4 (33). С. 198–200.

15. Рудницький В. М., Бабенко В. Г., Рудницький С. В. Метод синтезу матричних моделей операцій криптографічного перекодування інформації. *Захист інформації*. 2012. № 3 (56). С. 50–56.

16. Голуб С. В., Бабенко В. Г., Рудницький С. В. Метод синтезу операцій криптографічного перетворення на основі додавання за модулем два. *Системи обробки інформації*. 2012. Вип. 3 (101). Т. 1. С. 119–122.

17. Бабенко В. Г., Мельник Р. П., Рудницький С. В. Дослідження способів запису трьохрозрядних криптографічних операцій. *Системи управління, навігації та зв'язку.* 2012. Вип. 1 (21). Т. 2. С. 170–173.

18. Бабенко В. Г., Рудницький С. В. Синтез функцій перекодування для групи трьохрозрядних криптографічних операцій. *Системи озброєння і військова техніка*. 2012. Вип. 1 (29). С. 84–87.

19. Вдосконалення методу синтезу операцій криптографічного перетворення на основі дискретно-алгебраїчного представлення операцій / С. В. Голуб, В. Г. Бабенко, С. В. Рудницький, Р. П. Мельник. *Системи управління, навігації та зв'язку.* 2012. Вип. 2 (22). С. 163–168.

20. Бабенко В. Г., Рудницький С. В. Реалізація методу захисту інформації на основі матричних операцій криптографічного перетворення. *Системи обробки інформації*. 2012. № 9 (107). С. 130–139.

21. Бабенко В. Г., Мельник Р. П., Рудницкий С. В. Синтез операций криптографического декодирования на основе элементарных операций расширенного матричного представления. *Информационные системы и технологии: управление и безопасность:* сб. ст. I междунар. заочной науч.-практ. конф. Тольятти: ПВГУС, 2012. С. 67–77.

22. Бабенко В., Мельник О., Мельник Р. Класифікація трирозрядних елементарних функцій для криптографічного перетворення інформації. *Безпека інформації*. 2013. Т. 19. № 1. С. 56–59.

23. Бабенко В. Г., Стабецька Т. А. Побудова моделі оберненої нелінійної операції матричного криптографічного перетворення. *Системи управління, навігації та зв'язку*. 2013. Вип. 3 (27). С. 117–119.

24. Параллельная реализация нелинейного расширенного матричного криптографического преобразования / В. Г. Бабенко, С. В. Пивнева, О. Г. Мельник, Р. П. Мельник. *Вектор науки Тольяттинского государственного университета*. 2014. № 3 (29). С. 17–19.

25. Синтез модели обратной нелинейной операции расширенного матричного криптографического преобразования / В. Н. Рудницкий, С. В. Пивнева, В. Г. Бабенко и др. *Вектор науки Тольяттинского государственного университета*. 2014. № 4 (30). С. 18–21.

26. Бабенко В. Г., Мельник Р. П., Гончар С. В. Оцінка ефективності використання операцій криптографічного перетворення. *Вісник Інженерної академії України*. 2014. Вип. 2. С. 39–41.

27. Метод захисту конфіденційної інформації як складова управління інформаційною безпекою ДСНС України / Р. П. Мельник, О. Г. Мельник, С. В. Гончар, В. Г. Бабенко. *Системи обробки інформації*. 2014. Вип. 4 (120). С. 145–148.

28. Рудницкий В. Н., Козлов Е. В., Бабенко В. Г. Способ параллельной реализации операций матричного криптографического преобразования. *Вектор науки Тольяттинского государственного университета*. 2014. № 2 (28). С. 11–15.

29. Бабенко В. Г., Лада Н. В. Синтез і аналіз операцій криптографічного додавання за модулем два. *Системи обробки інформації*. 2014. Вип. 2 (118). С. 116–118.

30. Бабенко В. Г., Мельник О. Г., Стабецька Т. А. Синтез нелінійних операцій криптографічного перетворення. *Безпека інформації*. 2014. Т. 20. № 2. С. 143–147.

31. Рудницький В. М., Бабенко В. Г., Стабецька Т. А. Узагальнений метод синтезу обернених нелінійних операцій розширеного матричного криптографічного перетворення. *Системи обробки інформації*. 2014. Вип. 6 (122). С. 118–121.

32. Бабенко В. Г., Козловська С. Г. Особливості використання матричних операцій криптографічного перетворення інформації. *Системи обробки інформації*. 2015. Вип. 3 (128). С. 84–87.

33. Бабенко В. Г., Ланських Є. В., Зажома В. М. Вбудовування даних в стеганоконтейнер на основі надлишкових позиційних систем числення. *Вісник Черкаського державного технологічного університету*. 2015. № 1. С. 111–115.

34. Бабенко В. Г., Мельник Р. П., Гончар С. В. Розробка методів синтезу трирозрядних розширених матричних елементарних функцій. *Наука і техніка Повітряних Сил Збройних Сил України*. 2015. Вип. 1 (18). С. 154–156.

35. Мельник Р. П., Бабенко В. Г., Гончар С. В. Удосконалений метод синтезу розширених матричних елементарних функцій для криптоперетворення даних. *Системи озброєння і військова техніка*. 2015. Вип. 1 (41). С. 132–134.

36. Бабенко В. Г., Мельник О. Г., Нестеренко О. Б. Моделювання примітивів ковзного шифрування на основі рекурентних послідовностей. *Наука і техніка Повітряних Сил Збройних Сил України*. 2015. Вип. 3 (20). С. 129–133.

37. Бабенко В. Г., Мельник О. Г., Мельник Р. П. Мультиопераційне багаторазове ковзне шифрування. *Системи озброєння і військова техніка*. 2015. Вип. 3 (43). С. 70–72.

38. Бабенко В. Г., Зажома В. М., Нестеренко О. Б. Метод вбудовування стегоповідомлення на основі ключового елементу. *Автоматизированные системы управления и приборы автоматики.* Харьков. 2014. Вып. 168. С. 53–58.

39. Бабенко В. Г., Лада Н. В., Лада С. В. Дослідження взаємозв'язків між операціями в матричних моделях криптографічного перетворення. *Вісник Черкаського державного технологічного університету.* 2016. № 1. С. 5–11.

40. Эффективное совмещенное мультиоперандное сложение в избыточной линейной рекуррентной системе счисления третьего порядка / И. Н. Федотова-Пивень, В. Г. Бабенко, О. Б. Пивень, С. Ю. Куницкая. *Wschodnioeuropejskie Czasopismo Naukowe:* East European sci. journ. 2016. No. 11 (15). Part 2. P. 19–24. (Варшава, Польща).

41. Реалізація вершинної мінімізації булевих функцій для моделювання процесів, що не формалізуються / В. М. Рудницький, І. В. Миронець, В. Г. Бабенко та ін. *Science and Education a New Dimension. Natural and Ttechnical Science:* міжнар. наук. журн. 2017. Vol. 14. Iss. 132. P. 85–88. (BUDAPEST) (Будапешт, Угорщина).

42. Особенности применения операций перестановок, управляемых информацией, для криптографического преобразования / Т. В. Миронюк, И. В. Миронец, В. Г. Бабенко, С. В. Сысоенко. *Wschodnioeuropejskie Czasopismo Naukowe:* East European sci. journ. 2017. No. 11 (27). Part 1. P. 85–93. (Варшава, Польща).

43. Сисоєнко С. В., Миронець І. В., Бабенко В. Г. Побудова узагальненої математичної моделі групового матричного криптографічного перетворення. *Сучасна спеціальна техніка*. 2018. № 4. С. 96–103.

44. Миронець І. В., Бабенко В. Г., Сисоєнко С. В. Метод мінімізації булевих функцій з великою кількістю змінних на основі направленого перебору. *Щомісячний науковий журнал «Smart and Young».* 2016. № 7. С. 63–71.

45. Бабенко В. Г., Лада Н. В. Технологія дослідження операцій за модулем два. *Щомісячний науковий журнал «Smart and Young»*. 2016. № 11–12. Ч. 1. С. 49–54.

46. Бабенко В. Г., Кучеренко С. Ю., Зажома В. М. Моделирование позиционных избыточных систем счисления. *Системи управління, навігації та зв'язку.* 2010. Вип. 4 (16). С. 51–54.

47. Бабенко В. Г., Кучеренко С. Ю., Зажома В. М. Синтез правил выполнения операций сложения на основе моделей позиционных систем счисления. *Системи обробки інформації*. 2010. Вип. 9 (90). С. 179–182.

48. Бабенко В. Г., Шадхін В. Ю., Шевченко О. О. Дослідження принципів організації передачі даних в TCP/IP-мережах. *Вісник Черкаського державного технологічного університету.* 2010. № 2. С. 3–6.

49. Бабенко В. Г., Шадхін В. Ю., Компанієць В. О. Оперативний розподіл навантаження на мережі передачі даних. *Вісник Хмельницького національного університету*. 2010. Вип. 3. С. 217–220.

50. Эвристические алгоритмы и распределённые вычисления в прикладных задачах (вып. 2): кол. монограф. / под ред. Б. Ф. Мельникова. Ульяновск, 2013. 202 с.

51. Наукоемкие технологии в инфокоммуникациях: обработка и защита информации: кол. монограф. / под ред. В. М. Безрука, В. В. Баранника. Харьков: Компания СМИТ, 2013. 398 с.

52. Криптографическое кодирование: методы и средства реализации: монография / В. Н. Рудницкий, С. В. Пивнева, В. Г. Бабенко и др.; Тольят. гос. ун-т. Тольятти, 2013. 196 с.

53. Криптографическое кодирование: методы и средства реализации (часть 2): монография / В. Н. Рудницкий, В. Я. Мильчевич, В. Г. Бабенко и др. Харьков: Щедрая усадьба плюс, 2014. 224 с.

54. Криптографическое кодирование: кол. монограф. / под ред. В. Н. Рудницкого, В. Я. Мильчевича. Харьков: Щедрая усадьба плюс, 2014. 240 с.

55. Рудницький В. М., Лада Н. В., Бабенко В. Г. Криптографічне кодування: синтез операцій потокового шифрування з точністю до перестановки: монографія. Харків: ДІСА ПЛЮС, 2018. 184 с.

56. Криптографічне кодування: обробка та захист інформації: кол. монографія / Бабенко В. Г., Лада Н. В. та ін.; під. ред. В. М. Рудницького. Харків: ДІСА ПЛЮС, 2018. 139 с.

57. Бабенко В. Г. Етапи реалізації технології підвищення швидкодії систем захисту інформації. *Методи та засоби кодування, захисту й ущільнення інформації:* тези доп. Третьої міжнар. наук.-практ. конф., (20–22 квіт. 2011 р.). Вінниця: ВНТУ, 2011. С. 80–81.

58. Бабенко В. Г. Використання матричних операцій криптографічного перетворення для ковзного шифрування. *Проблеми інформатизації:* тези доп. Першої міжнар. наук.-техн. конф., (19–20 груд. 2013 р.). Черкаси: ЧДТУ; Київ: ДУТ; Тольятті: ТДУ; Полтава: ПНТУ, 2013. С. 22.

59. Миронець І. В., Бабенко В. Г. Методика синтезу функцій декодування на основі спеціалізованих логічних функцій. *Проблеми інформатизації:* зб. тез доп. наук.-техн. семінару, (15–16 квіт. 2009 р.). Черкаси: ЧДТУ, 2009. Вип. 1 (3). С. 18–19.

60. Миронець І. В., Бабенко В. Г. Вдосконалена методика синтезу функцій декодування на основі спеціалізованих логічних функцій. *Інтегровані інтелектуальні робототехнічні комплекси:* зб. тез Другої міжнар. наук.-практ. конф., (25–28 трав. 2009 р.). Київ: НАУ, 2009. С. 228–229.

61. Бабенко В. Г., Рудницький С. В. Дослідження двохрозрядних операцій криптографічного перетворення. *Інтегровані комп'ютерні технології в машинобудуванні ІКТМ-2011:* тези доп. Всеукр. наук.-техн. конф. Харків: НАУ «ХАІ», 2011. Т. 3. С. 218.

62. Бабенко В. Г., Рудницький С. В. Синтез функцій декодування інформації в групі трьохрозрядних криптографічних операцій перетворення. *Моделювання, ідентифікація, синтез систем керування:* зб. тез П'ятнадцятої міжнар. наук.-техн. конф., (9–16 верес. 2012 р.). Донецьк: Вид-во Ін-ту прикл. математики і механіки НАН України, 2012. С. 190–191.

63. Бабенко В. Г., Рудницький С. В. Моделювання логічних функцій для систем захисту інформації. *Методи та засоби кодування, захисту й ущільнення*

інформації: тези доп. Третьої міжнар. наук.-практ. конф. Вінниця: ВНТУ, 2011. С. 82–83.

64. Бабенко В. Г., Рудницький С. В. Дослідження групи трьохрозрядних криптографічних операцій. *Новітні технології – для захисту повітряного простору:* тези доп. Восьмої наук. конф. Харків. ун-ту Повітр. Сил ім. І. Кожедуба, (18–19 квіт. 2012 р.). Харків: ХУПС ім. І. Кожедуба, 2012. С. 218.

65. Бабенко В. Г., Лада Н. В. Дослідження множини операцій криптографічного додавання. *Інформаційні технології в освіті, науці і техніці (ІТОНТ-2014):* тези доп. ІІ Міжнар. наук.-практ. конф., (м. Черкаси, Україна, 24–26 квіт. 2014 р.). Черкаси: ЧДТУ, 2014. Т. 1. С. 135–136.

66. Бабенко В. Г., Стабецька Т. А. Операції матричного криптографічного декодування на основі логічних визначників. *Методи та засоби кодування, захисту й ущільнення інформації:* тези доп. Четвертої міжнар. наук.-практ. конф., (м. Вінниця, Україна, 23–25 квіт. 2013 р.). Вінниця: ТД Едельвейс і К, 2013. С. 135–137.

67. Бабенко В. Г., Лада Н. В. Синтез і аналіз мікрооперацій для криптографічного перетворення. *Проблеми інформатизації:* тези доп. Другої міжнар. наук.-техн. конф., (м. Черкаси, Україна – м. Тольятті, Росія, 25–26 листоп. 2014 р.). Черкаси: ЧДТУ; Тольятті: ТДУ, 2014. С. 9–10.

68. Ланських Є. В., Бабенко В. Г., Зажома В. М. Алгоритми вбудовування повідомлення для LSB методу. *Інформаційні технології в освіті, науці і техніці (ІТОНТ-2014):* тези доп. ІІ Міжнар. наук.-практ. конф., (м. Черкаси, Україна, 24–26 квіт. 2014 р.). Черкаси: ЧДТУ, 2014. Т. 1. С. 141–142.

69. Ланських Є. В., Бабенко В. Г., Зажома В. М. Технологія застосування ключового елементу стеганоконтейнера для LSB методу. *Інтегровані інтелектуальні робототехнічні комплекси (ІІРТК-2014):* тези доп. Сьомої міжнар. наук.-практ. конф., (19–20 трав. 2014 р.). Київ: НАУ, 2014. С. 312–313.

70. Ланських Є. В., Бабенко В. Г., Зажома В. М. Використання надлишковості систем числення в стеганографічних системах. *Інформаційні технології та комп'ютерна інженерія (ІТКІ-2014):* тези доп. Четвертої міжнар. наук.-практ.

конф., (м. Вінниця, Україна, 27–30 трав. 2014 р.). Вінниця: ВНТУ, 2014. С. 161–162.

71. Гресько Є. І., Бабенко В. Г. Огляд стеганографічних методів приховування інформації. *Інформаційна безпека держави, суспільства та особистості:* зб. тез доп. Всеукр. наук.-практ. конф., (16 квіт. 2015 р.). Кіровоград: КНТУ, 2015. С. 87–89.

72. Бабенко В. Г., Рудницький С. В. Способи синтезу алгоритмів на основі операцій криптографічного перетворення інформації. *Проблеми інформатизації:* тези доп. Другої міжнар. наук.-техн. конф. (м. Черкаси, Україна – м. Тольятті, Росія, 25–26 листоп. 2014 р.). Черкаси: ЧДТУ; Тольятті: ТДУ, 2014. С. 10.

73. Бабенко В. Г. Синтез моделей реалізації багаторазового примітиву ковзного шифрування. *Сучасні напрями розвитку інформаційно-комунікаційних технологій та засобів управління:* матеріали П'ятої міжнар. наук.-техн. конф., (23–24 квіт. 2015 р.). Полтава: ПНТУ; Баку: ВА ЗС АР; Кіровоград: КЛА НАУ; Харків: ХНДІ ТМ, 2015. С. 59.

74. Бабенко В. Г., Лада Н. В. Аналіз результатів виконання модифікованих операцій додавання за модулем два з точністю до перестановки. *The Scientific Potential of the Present:* зб. наук. праць «ЛОГОΣ». 2016. С. 108–111.

75. Бабенко В. Г., Лада Н. В., Лада С. В. Взаємозв'язки між операціями в матричних моделях криптографічного перетворення. *Проблеми науково-технічного та правового забезпечення кібербезпеки у сучасному світі «ПНПЗК-2016»:* тези доп. Першої міжнар. наук.-практ. конф., (30 берез.–1 квіт. 2016 р.). Харків: Нац. техн. ун-т «ХПІ», 2016. С. 17.

76. Бабенко В. Г., Лада Н. В., Лада С. В. Аналіз множини операцій, синтезованих на основі додавання за модулем два. *Методи та засоби кодування, захисту й ущільнення інформації:* тези доп. П'ятої міжнар. наук.-практ. конф., (19–21 квіт. 2016 р.). Вінниця: ВНТУ, 2016. С. 54–57.

77. Бабенко В. Г., Висоцький С. В. Забезпечення захисту інформації для системи моніторингу та статистики web-ресурсів. *Інформаційні технології в*

освіті, науці й техніці (ІТОНТ-2016): тези доп. Третьої міжнар. наук.-практ. конф., (12–14 трав. 2016 р.). Черкаси: ЧДТУ, 2016. С. 85–86.

78. Бабенко В. Г., Ланських Є. В. Дослідження заміни операції для реалізації матричного криптографічного перетворення. *Інтегровані інтелектуальні робототехнічні комплекси (ІІРТК-2016):* тези доп. Дев'ятої міжнар. наук.-практ. конф., (17–18 трав. 2016 р.). Київ: НАУ, 2016. С. 246–248.

79. Бабенко В. Г., Стабецька Т. А. Синтез обернених операцій розширеного матричного криптографічного перетворення. *Проблеми інформатизації:* тези доп. Четвертої міжнар. наук.-техн. конф., (м. Черкаси, Україна, 3–4 листоп. 2016 р.). Черкаси: ЧДТУ; Баку: ВА ЗС АР; Бельсько-Бяла: УТіГН; Полтава: ПНТУ, 2016. С. 9.

80. Стабецька Т. А., Бабенко В. Г. Алгоритми побудови та застосування операцій розширеного матричного криптографічного перетворення. *Наукова думка інформаційного століття:* матеріали Міжнар. наук.-практ. конф., (м. Дніпропетровськ, Україна, 19 черв. 2017 р.). Одеса: Друкарня «Друкарик», 2017. Т. 6. С. 86–94.

81. Миронюк Т. В., Бабенко В. Г. Аналіз статистичних властивостей результатів криптографічного перетворення на основі операцій перестановок, керованих інформацією. *Інноваційні тенденції сьогодення у сфері природничих, гуманітарних та точних наук:* матеріали Міжнар. наук.-практ. конф., (м. Івано-Франківськ, Україна, 17 жовт. 2017 р.). Одеса: Друкарня «Друкарик», 2017. Т. 2. С. 41–47.

82. Бабенко В. Г., Лада Н. В. Потокові шифри з використанням групи модифікованих операцій криптографічного додавання за модулем два з точністю до перестановки. *Проблеми інформатизації:* тези доп. П'ятої міжнар. наук.-техн. конф., (м. Черкаси, Україна, 13–15 листоп. 2017 р.). Черкаси: ЧДТУ; Баку: ВА ЗС АР; Бельсько-Бяла: УТіГН; Полтава: ПНТУ, 2017. С. 12.

83. Стабецька Т. А., Бабенко В. Г. Порівняльна оцінка основних параметрів методу захисту інформації на основі операцій розширеного матричного криптографічного перетворення. *Наука у контексті сучасних глобалізаційних*

процесів: зб. наук. праць «*ΛΌГОΣ*» з *матеріалами Міжнар. наук.-практ. конф.*, (м. Полтава, Україна, 19 листоп. 2017 р.) / відп. за вип. М. А. Голденблат; ГО «Європейська наукова платформа». Одеса: Друкарня «Друкарик», 2017. Т. 10. С. 81–84.

84. Бабенко В. Г., Нестеренко О. Б., Пустовіт М. О. Дослідження результатів багатораундового шифрування, реалізованого на основі операцій строгого стійкого кодування. *Проблеми інформатизації:* тези доп. Шостої міжнар. наук.-техн. конф., (м. Черкаси, Україна, 14–16 листоп. 2018 р.). Черкаси: ЧДТУ; Баку: ВА ЗС АР; Бельсько-Бяла: УТіГН; Полтава: ПНТУ, 2018. С. 9–10.

85. Сисоєнко С. В., Бабенко В. Г. Аналіз складності реалізації моделей операцій групового матричного криптографічного перетворення. *Naukowy i innowacyjny potencjał prezentacji:* kolekcja prac naukowych «ΛΌГОΣ» z materiałami Międzynar. nauk.-prakt. konf., (Opole, 18 listopada 2018 r.). Równe: Volynsky Oberegi, 2018. T. 7. S. 5–53.

86. Sysoienko S., Myronets I., Babenko V. Practical implementation effectiveness of the speed increasing method of group matrix cryptographic transformation. *Second International Workshop on Computer Modeling and Proceedings of the Second International Workshop on Computer Modeling and Intelligent Systems (CMIS-2019),* (Zaporizhzhia, Ukraine, April 15–19, 2019). P. 402–412. URL: http://ceur-ws.org/Vol-2353/paper32.pdf

87. Пристрій для виконання логічних операцій криптографічного перетворення: декларац. пат. на корисну модель 45916 Україна, МПК H03M 13/00 / Рудницький В. М., Паціра Є. В., Миронець І. В., Бабенко В. Г. № u200907997; заявл. 29.07.2009; опубл. 25.11.2009, Бюл. № 22. 3 с.

88. Пристрій для виконання логічних операцій криптографічного перетворення: декларац. пат. на корисну модель 45917 Україна, МПК H03M 13/00 / Рудницький В. М., Паціра Є. В., Миронець І. В., Бабенко В. Г. № u200907998; заявл. 29.07.2009; опубл. 25.11.2009, Бюл. № 22. 3 с.

89. Пристрій для виконання логічних операцій криптографічного перетворення: деклара. пат. на корисну модель 46617 Україна, МПК H03M 13/00 /

Рудницький В. М., Паціра Є. В., Миронець І. В., Бабенко В. Г. № u200908000; заявл. 29.07.2009; опубл. 25.12.2009, Бюл. № 24. 3 с.

90. Пристрій для виконання логічних операцій криптографічного перетворення: декларац. пат. на корисну модель 46618 Україна, МПК H03M 13/00 / Рудницький В. М., Паціра Є. В., Миронець І. В., Бабенко В. Г. № u200908001; заявл. 29.07.2009; опубл. 25.12.2009, Бюл. № 24. 3 с.

ЗМІСТ

ВСТУП

Актуальність теми. Глобалізація інформаційних процесів й автоматизація їх обробки в усіх сферах людської діяльності зумовлені тенденцією постійного збільшення обсягів інформації, що циркулює в мережах та системах. Ці процеси не лише характеризуються позитивними наслідками, але водночас спричиняють появу нових негативних інформаційних впливів, зокрема – сприяють стрімкому розвитку кіберзлочинності. У зв'язку з цим зростає потреба захисту інформації, яка має відповідну цінність як для держави, так і для окремих користувачів, а також набувають особливої актуальності для сьогодення проблеми інформаційної безпеки та захисту інформаційних ресурсів.

Криптографічний захист інформації залишається одним із найважливіших способів забезпечення безпеки інформації в комп'ютерних мережах і системах.

Вагомий внесок у розвиток криптографічних методів захисту інформації зробили такі науковці, як А. А. Молдовян, І. Д. Горбенко, К. Є. Шеннон, Брюс Шнайєр, Р. А. Хаді, W. Diffie, M. E. Hellman, R. L. Rivest, A. Shamir, В. В. Ященко, О. А. Логачов, С. О. Шестаков, А. Н. Фіонов, Б. Я. Рябко, Дж. Л. Мессі, Чарльз Г. Беннет, Ж. Брассар, B. Chor, U. M. Maurer, N. Koblitz та ін.

Традиційні криптографічні алгоритми поділяють на високошвидкісні потокові та блокові шифри, які володіють високою стійкістю і складністю. На сьогоднішній день стандартизовані криптографічні алгоритми демонструють високу стійкість зашифрованої інформації, однак створення перших квантових комп'ютерів ставить під питання їх стійкість до постквантового криптографічного аналізу. Подальше збільшення стійкості за

рахунок ускладнення криптографічних алгоритмів зумовлює складнощі щодо їх застосування в системах реального часу.

Основним критерієм при виборі криптосистем є стійкість, проте для деяких задач, наприклад, для шифрування великого об'єму даних, захисту онлайнових платіжних систем та ін. ключову роль відіграє швидкість криптографічної обробки даних. Незважаючи на різноманітність сучасних криптографічних методів та систем, далеко не всі володіють необхідним рівнем ефективності (швидкодії та стійкості) для забезпечення захисту інформаційних ресурсів. Крім того, стрімкий розвиток обчислювальних засобів та їх одночасне здешевлення формулюють нові вимоги як до стійкості, так і до швидкодії систем криптографічного захисту, тому зростання криптостійкості має бути не меншим за ріст швидкодії. Отже, завжди існуватиме потреба підвищення стійкості та швидкодії криптографічних методів захисту інформації.

У багатьох наукових роботах було показано, що один із найперспективніших напрямків розвитку криптографії – у поєднанні криптології та комп'ютерної інженерії; він полягає в розширенні спектра операцій криптографічного перетворення, забезпечуючи на їх основі вдосконалення існуючих та побудову нових криптографічних алгоритмів. Сутність процесу криптографічного перетворення зводиться до перетворення блоку інформації за допомогою випадково вибраних таблиць підстановок, реалізованих на основі дискретних моделей кодування. Основна задача даного криптографічного перетворення полягає у випадковій генерації моделей таблиць підстановок, які відповідають заданим вимогам щодо якості криптоперетворень блоку даних. Основні переваги: велика варіативність при виборі таблиць підстановок (для одного байта існує 256! таблиць підстановок); висока швидкість генерації моделей таблиць підстановок; висока швидкість реалізації дискретних моделей пристроїв кодування. Саме таке криптографічне перетворення об'єднує сильні сторони потокового й

блочного шифрування і забезпечує протидію постквантовому криптоаналізу за рахунок збільшення варіативності криптографічних алгоритмів.

Переваги криптографічного кодування безпосередньо пов’язані з проблемами, які виникають при їх реалізації. Основна проблема полягає в тому, що через величезну кількість таблиць підстановок відсутні як загальні підходи, так і алгоритми для побудови множин груп дискретних моделей. Відсутні методи синтезу груп дискретних моделей операцій криптографічного кодування із заданими властивостями. Рішення даної проблеми стане підґрунтям для створення теоретичної бази побудови високоефективних систем комп’ютерної криптографії. Виходячи з цього можна стверджувати що тема дисертаційного дослідження є актуальною.

Зв’язок роботи з науковими програмами, планами, темами. Результати дисертаційної роботи включені до звітів НДР: «Методи та засоби захисту інформації МНС України на основі операцій криптографічного кодування» (ДР № 0112U003579), «Криптографічне кодування: методи та засоби реалізації (частина 2)» (ДР № 0113U001475), «Ефективність систем інформаційної безпеки», шифр НДР «Безпека» (ДРН 0113U004731), «Ефективність систем інформаційної безпеки» (Шифр «Перетворення»), «Синтез операцій криптографічного перетворення з заданим характеристиками» (ДР № 0116U008714), «Розробка методів та засобів оцінки ефективності соціоінжинірингу» (ДР № 0116U008715), при виконанні держбюджетної теми № 36Б115 «Розробка методів синтезу тестових моделей поведінки програмних об'єктів, підвищення оперативності передачі та захисту інформації у телекомунікаційних системах» (ДР № 0115U003103) (Кіровоградський національний технічний університет), в яких автор брав участь як виконавець.

Мета і задачі дослідження. Основною метою дисертаційної роботи є рішення науково-технічної проблеми підвищення ефективності функціонування систем комп’ютерної криптографії шляхом створення

методології синтезу операцій перетворення інформації та побудови криптографічних примітивів на їх основі.

Рішення даної наукової проблеми передбачає удосконалення теорії, спрямованої на подолання суперечностей і труднощів при проектуванні систем комп'ютерної криптографії. Тому в роботі поставлені та вирішені наступні проблемні задачі:

1. Розробити основні положення методології синтезу операцій перетворення інформації для систем комп'ютерної криптографії.

2. На основі застосування запропонованої методології розробити та вдосконалити методи синтезу й аналізу групи нелінійних операцій криптографічного перетворення інформації.

3. Вдосконалити існуючі примітиви комп'ютерної криптографії на основі застосування синтезованих операцій криптографічного перетворення інформації та оцінити їх ефективність.

4. Розробити технологію синтезу операцій для мультиопераційних матричних криптографічних примітивів.

5. Удосконалити методи застосування операцій криптографічного перетворення інформації та оцінити їх ефективність.

Об'єктом дослідження є процеси синтезу операцій перетворення інформації.

Предмет дослідження – методи та засоби синтезу операцій перетворення інформації для комп'ютерної криптографії.

Методи дослідження. Розробка принципів, методів і алгоритмів синтезу операцій криптографічного перетворення згідно з запропонованою методологією базується на положеннях теорії інформації, теорії множин, систем числення, криптографії, методів дискретної математики та комп'ютерного моделювання. Оцінка ефективності криптографічних примітивів базується на основі теорії алгоритмів, математичної статистики, лінійного та нелінійного криптоаналізу.

Наукова новизна одержаних результатів. У процесі вирішення поставлених задач автором одержано такі результати:

1. Вперше запропонована методологія синтезу операцій криптографічного перетворення інформації на основі існуючих та розроблених методів синтезу операцій прямого, оберненого та взаємного криптографічного перетворення шляхом їх класифікації та узагальнення, що забезпечило можливість розширення бази операцій, використання яких дозволяє вдосконалювати існуючі та синтезувати нові криптоалгоритми і криптопримітиви.

2. Вперше розроблено технологію синтезу операцій для мультиопераційних матричних криптографічних примітивів на основі побудови нових груп операцій з точністю до перестановки шляхом використання запропонованої табличної моделі операції криптоперетворення, що дозволило за рахунок варіативності операцій підвищити криптостійкість існуючих криптопримітивів.

3. Удосконалено методи побудови криптографічних примітивів на прикладі примітивів ковзного шифрування на основі матричних операцій криптографічного перетворення та отриманих узагальнених рекурентних послідовностей для побудови моделей шляхом їх паралельної реалізації, що забезпечило підвищення швидкості шифрування (до двох разів) та стійкості до лінійного криптоаналізу.

4. Удосконалено методи синтезу та аналізу криптографічних алгоритмів на основі узагальненої моделі криптоалгоритму, шляхом послідовно-паралельної реалізації операцій криптографічного перетворення інформації на макро- та мікрорівнях, що забезпечило можливість вирішення протиріч між криптостійкістю, складністю та швидкістю для досягнення заданої ефективності, виходячи з задач проектування.

5. Отримали подальший розвиток математичні моделі та методи синтезу елементарних функцій та операцій криптоперетворення на основі

запропонованої методології та вибраної групи нелінійних елементарних функцій шляхом вдосконалення математичного апарату для синтезу прямих та обернених матричних моделей не афінних дискретних перетворень, що в сукупності забезпечило можливість синтезу операцій нелінійних криптографічних перетворень.

Практичне значення одержаних результатів. Практична цінність роботи полягає в доведенні здобувачем отриманих наукових результатів до конкретних інженерних методик, алгоритмів, моделей та варіантів побудови криптографічних алгоритмів.

На підставі проведених досліджень одержано такі практичні результати: розроблено методологію синтезу операцій криптографічного перетворення інформації в рамках запропонованої концепції побудови алгоритмів захисту інформації на їх основі з можливістю підбору оптимальних показників криптостійкості та швидкодії, що дає змогу покращити ефективність функціонування системи криптографічного захисту в цілому; розроблено технологію побудови та використання криптопримітивів на основі синтезованих операцій криптографічного перетворення інформації з можливістю їх паралельного виконання, що дає виграш у швидкості та часі здійснення перетворення безпосередньо інформації; запропоновано варіанти реалізації на програмному та апаратному рівнях нових груп криптографічних операцій заданої розрядності, що володіють властивостями афінності та нелінійності, зокрема матричного та розширеного матричного перетворення. Застосування синтезованих операцій криптографічного перетворення на основі запропонованих варіантів комбінації використання матричного та розширеного матричного перетворення при конструюванні алгоритмів дає можливість збільшити криптостійкість (від 2^{166} до 2^{8157} разів) пропорційно відносно потокового шифрування при зменшенні часу шифрування (від 1,3 до 8 разів).

Практична цінність роботи підтверджена актами впровадження на підприємствах і організаціях: НВК «Фотоприлад», «Науково-дослідний інститут «Акорд» та ПП «Сенсорна електроніка» (м. Черкаси), ТОВ «Люменс-груп» (м. Кіровоград) та в освітній процес у навчальних закладах: Черкаському державному технологічному університеті, Черкаському національному університеті імені Б. Хмельницького, Національному аерокосмічному університеті імені М. Є. Жуковського «ХАІ», Кіровоградському національному технічному університеті (додаток А).

Особистий внесок здобувача. Усі нові результати дисертаційної роботи отримано автором самостійно. Роботи [1-5, 57, 58, 73] виконані без співавторів. У наукових працях, опублікованих у співавторстві, з питань, що стосуються даного дослідження, автору належать: розробка принципів та методів синтезу наборів функцій для криптографічного перетворення [6-8, 41, 44, 52, 59-61]; перевірка методу підвищення оперативності доступу до конфіденційних інформаційних ресурсів [9-11, 52, 64]; розробка методики формування груп операцій та реалізація побудови моделі процесу декодування або перекодування інформації [12, 13, 18, 52, 53, 61]; опис процесу реалізації методів синтезу матричних моделей операцій криптографічного кодування [14, 15, 53, 62]; основні підходи щодо розробки та реалізації методу синтезу базових операцій криптографічного перетворення, формулювання методу синтезу операцій криптографічного перетворення на основі додавання за модулем два, узагальнення та аналіз одержаних результатів [16-19, 45 ,53, 63, 74-76]; розробка методу захисту інформаційних ресурсів на основі матричних операцій криптографічного перетворення та алгоритмів їх застосування, оцінка статистичних властивостей результатів криптографічного перетворення [20-22, 24, 26, 34, 35, 50, 54-56, 82,83]; формулювання теореми про побудову оберненої матриці розширеного матричного криптографічного перетворення [23, 34, 50, 54]; модель синтезу нелінійної операції розширеного матричного

криптографічного перетворення та розробка правил побудови оберненої операції [25, 35, 54]; перевірка результатів застосування методу захисту конфіденційної інформації [27, 28, 54]; аналіз синтезованих та пошук базових операцій криптографічного перетворення [29, 39, 42, 54, 65, 81]; узагальнення методу синтезу обернених операцій нелінійного розширеного матричного криптографічного перетворення [30, 31, 51, 54]; аналіз властивостей результатів перетворення матричними операціями криптографічного перетворення та розробка технології їх використання [32, 84, 85]; способи застосування матричних операцій криптографічного перетворення для LSB методу [33]; опис особливостей застосування ключових елементів для здійснення процесу вбудовування повідомлення великої довжини з використанням декількох контейнерів [38, 68-71]; спосіб застосування матричних операцій криптографічного перетворення в примітивах ковзного шифрування [36, 37]; опис способів застосування операцій криптографічного перетворення для синтезу алгоритмів захисту [43, 55, 56, 67, 72, 86]; синтез моделей надлишкових позиційних систем числення [40, 46, 47]; аналіз сучасного стану мереж передачі даних [48, 49] та способів захисту систем моніторингу веб-ресурсів [77]; побудова матричних операцій декодування інформації за допомогою логічних визначників [66, 79, 80]; опис варіантів реалізації правил синтезу операцій криптографічного перетворення [78-80]; розробка математичних моделей пристроїв [87-90].

Із робіт, що опубліковані у співавторстві, у дисертаційній роботі використовуються результати, одержані особисто здобувачем.

Апробація результатів дисертації. Основні положення дисертаційної роботи доповідалися та обговорювалися більш ніж на 10 міжнародних та всеукраїнських наукових семінарах та конференціях, серед яких: міжнародна науково-практична конференція «Інтегровані інтелектуальні робототехнічні комплекси» (Київ, 2009, 2014); всеукраїнські науково-технічна та науково-практична конференції: «Інтегровані комп’ютерні технології в

машинобудуванні ІКТМ-2011» (Харків, 2011), «Інформаційна безпека держави, суспільства та особистості» (Кіровоград, 2015), восьма наукова конференція ХУПС ім. І. Кожедуба «Новітні технології – для захисту повітряного простору» (Харків, 2012); п'ятнадцята міжнародна науково-технічна конференція «Моделирование, идентификация, синтез систем управления (МИССУ-2012)» (Канака, Крим, 2012), перша міжнародна заочна науково-практична конференція «Информационные системы и технологии: управление и безопасность» (Тольятті-Русе, 2012), міжнародні науково-практичні конференції: «Методи та засоби кодування, захисту й ущільнення інформації» (Вінниця, 2013, 2016) та «Інформаційні технології та комп'ютерна інженерія» (ІТКІ-2014) (Вінниця, 2014); міжнародні науково-практичні конференції: «Проблеми інформатизації» (Черкаси, 2009, 2013, 2016-2019) та «Інформаційні технології в освіті, науці і техніці» (Черкаси, 2014, 2016); п'ята міжнародна науково-технічна конференція «Сучасні напрями розвитку інформаційно-комунікаційних технологій та засобів управління» (Харків, 2015); міжнародні науково-практичні конференції: «Проблеми науково-технічного та правового забезпечення кібербезпеки у сучасному світі «ПНПЗК-2016»» (Харків, 2016), «Наукова думка інформаційного століття» (Дніпро, 2017), «Інноваційні тенденції сьогодення у сфері природничих, гуманітарних та точних наук» (Івано-Франківськ, 2017), «Наука у контексті сучасних глобалізаційних процесів» (Полтава, 2017), «Науковий і інноваційний потенціал сьогодення» (Ополе, Польща, 2018), Second International Workshop on Computer Modeling and Intelligent Systems (CMIS-2019) (Запоріжжя, 2019).

Публікації. Основні результати дисертаційної роботи викладено в 90 друкованих працях, а саме: 49 наукових статтях у журналах, з них 40 – у фахових виданнях України, 6 статтях у наукових фахових виданнях за кордоном, 7 монографіях, з яких 2 видані за кордоном, 4 деклараційних патенти на корисну модель та 30 тезах доповідей на міжнародних та всеукраїнських наукових конференціях і семінарах.

Структура й обсяг дисертації. Дисертація складається зі вступу, шести розділів, висновків, списку використаних джерел з 258 найменувань на 30 сторінках та додатків на 76 сторінках. Загальний обсяг дисертації становить 474 сторінок, в тому числі 336 сторінок основної частини, 65 рисунків, 55 таблиць.

РОЗДІЛ 1
ПРЕДМЕТ ДОСЛІДЖЕННЯ ТА СУТНІСТЬ НАУКОВОЇ ПРОБЛЕМИ

1.1 Огляд основних проблемних задач реалізації криптографічних систем

У сучасному суспільстві все більшу роль відіграють комп'ютери, і взагалі електронні засоби передачі, зберігання, і обробки інформації. Для того, щоб інформаційні технології можна було використовувати в різних областях, необхідно забезпечити їх надійність і безпеку. Під безпекою (в широкому сенсі) розуміється здатність інформаційної системи зберігати свою цілісність і працездатність при випадкових або навмисних зовнішніх впливах. Тому широке використання інформаційних технологій призвело до бурхливого розвитку різних методів захисту інформації, з яких основними можна, мабуть, назвати, завадостійке кодування і криптографію [91-125].

Найпростіші способи шифрування з'явилися дуже давно, однак науковий підхід до дослідження і розробки криптографічних методів з'явився тільки в минулому (двадцятому) столітті. До теперішнього часу криптографія містить безліч результатів (теорем, алгоритмів), як фундаментальних, так і прикладних. Займатися криптографією неможливо без серйозної математичної підготовки. Особливо необхідні знання в області дискретної математики, теорії чисел, абстрактної алгебри та теорії алгоритмів. Разом з тим не слід забувати, що криптографічні методи призначені, в першу чергу, для практичного застосування, а теоретично стійкі алгоритми можуть виявитися незахищеними перед атаками, не передбаченими математичною моделлю. Тому після аналізу абстрактної математичної моделі завжди необхідний аналіз отриманого алгоритму з урахуванням ситуації, в якій він буде використовуватися на практиці [115-120].

1.1.1 Принципи побудови й схеми криптологічних систем

Хоча історія криптографії нараховує більш 2000 років, можна вважати, що першою теоретичною роботою можна назвати роботу голландського вченого Керкхоффа [142, 167, 202, 206, 227-229], у якій було сформульовано загальноприйняте зараз правило. Воно говорить про те, що стійкість шифру повинна визначатися тільки таємністю ключа. Це означає те, що алгоритм шифрування, текст криптограми відомі криптоаналітику.

Більшість учених уважає, що криптологія як наука виникла після опублікування К.Шенноном статті « Теорія зв'язку в секретних системах» в 1949 році [171]. Перш ніж приступитися до викладу теоретичного матеріалу, викладеного Шенноном у своїй статті, розглянемо сам предмет наших досліджень – криптологічну систему. Сам К.Шеннон використовував термін «секретна система».

Згідно Шеннону, є три загальні типи секретних систем [121, 137, 142, 171]:

1. системи маскування, які включають застосування таких методів, як невидиме чорнило, вистава повідомлення у формі невинного тексту або маскування криптограми, і інші методи, за допомогою яких факт наявності повідомлення ховається від супротивника (у цей час розробкою засобів і методів приховання фактів передачі повідомлення займається стеганографія);
2. таємні системи (наприклад, інвертування мови), у яких для розкриття повідомлення потрібно спеціальне устаткування;
3. «властиво» секретні системи, де зміст повідомлення ховається за допомогою шифру, коду й т.д., але саме існування повідомлення не ховається й передбачається, що супротивник має будь-яке спеціальне

устаткування, необхідний для перехоплення й запису переданих сигналів.

Далі буде розглянутий тільки третій тип систем, які називаються криптологичними системами. Найбільш загальна схема криптосистеми представлена на рис.1.1 [118, 121, 142, 155, 197, 198]

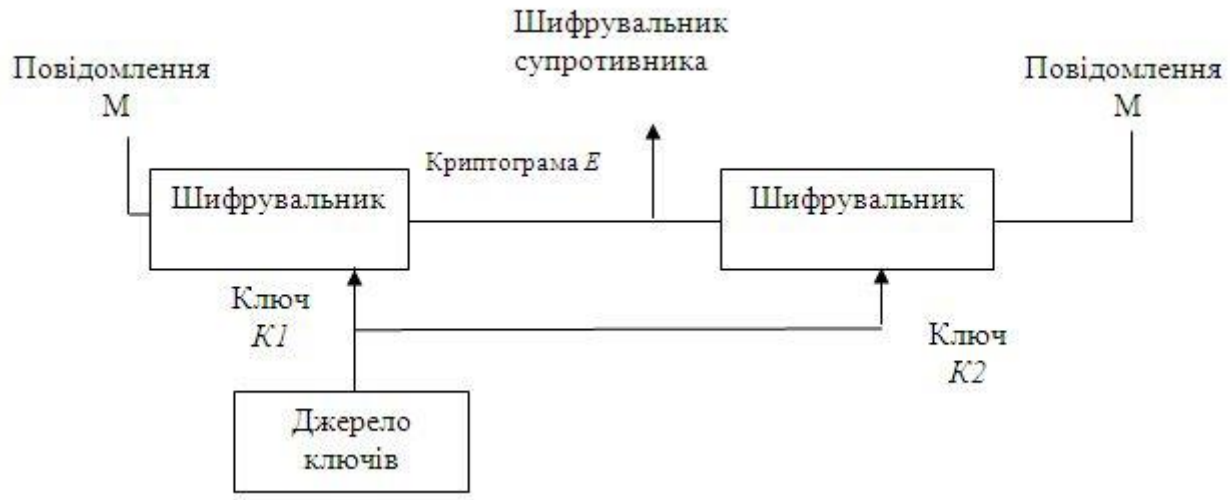


Рис 1.1 Загальна структура криптосистеми

Роботу криптосистеми найбільш загально можна описати в такий спосіб [142, 191, 197, 198, 206. 209]:

1. Передавальна сторона одержує із джерела ключів ключ для шифрування свого повідомлення.
2. Передавальна сторона зашифровує текст повідомлення й передає криптограму E в відкритий канал зв'язки в напрямку одержувача.
3. Одержувач повідомлення одержує із джерела ключів ключ, за допомогою якого можна розшифрувати отриману криптограму.
4. Одержувач розшифровує криптограму E.

1.1.2 Вимоги до криптографічних систем

Процес криптографічного закриття даних може здійснюватися як програмно, так і апаратно. Апаратна реалізація відрізняється суттєво більшою вартістю, однак їй властиві й переваги: висока продуктивність, простота, захищеність і т.д.. Програмна реалізація більш практична, допускає відому гнучкість у використанні [91, 92, 94, 96 98, 100, 104, 105, 108, 112-114, 123].

Для сучасних криптографічних систем захисту інформації сформульовані наступні загальноприйняті вимоги [124, 126, 130, 133-138, 142, 149-157]:

– зашифроване повідомлення повинне піддаватися читанню тільки при наявності ключа;

– число операції, необхідних для визначення використаного ключа шифрування по фрагменту шифрованого повідомлення й відповідного йому відкритого тексту, повинне бути не менше загального числа можливих ключів;

– число операцій, необхідних для розшифровування інформації шляхом перебору всіляких ключів, повинне мати строгу нижню оцінку й виходити за межі можливостей сучасних комп'ютерів (з урахуванням можливості використання мережних обчислень) або вимагати неприйнятно високих витрат на ці обчислення;

– знання алгоритму шифрування не повинне впливати на надійність захисту;

– незначна зміна ключа повинна приводити до істотної зміни виду зашифрованого повідомлення навіть при шифруванні того самого вихідного тексту;

– незначна зміна вихідного тексту повинне приводити до істотної зміни виду зашифрованого повідомлення навіть при використанні того самого ключа;

– структурні елементи алгоритму шифрування повинні бути незмінними;

– додаткові біти, що уводяться в повідомлення в процесі шифрування, повинні бути повністю й надійно сховані в шифрованому тексті;

– довжина шифрованого тексту не повинна перевершувати довжину вихідного тексту;

– не повинне бути простих і легко встановлюваних залежностей між ключами, послідовно використовуваними в процесі шифрування;

– будь-який ключ із множини можливих повинен забезпечувати надійний захист інформації;

– алгоритм повинен допускати як програмну, так і апаратну реалізацію, при цьому зміна довжини ключа не повинне вести до якісного погіршення алгоритму шифрування.

1.1.3 Шифрування великих повідомлень і потоків даних

Ця проблема з'явилася порівняно недавно з появою засобів *мультимедіа* і мереж з високою пропускною здатністю, що забезпечують передачу мультимедійних даних [124, 147-158].

Дотепер говорилося про захист повідомлень. При цьому під ними малася на увазі скоріше деяка текстова або символічна інформація. Однак у сучасних інформаційних системах починають застосовуватися технології, що вимагають передачі істотно великих обсягів даних. Серед таких технологій [211, 218-229]:

* факсимільний, відео і мовний зв'язок;

* голосова пошта;
* системи відеоконференцій.

Обсяг інформації, яка передається різних типів можна представити на умовній діаграмі рис.1.2 [147, 203-205].

Оскільки передача оцифрованої звукової, графічної і відеоінформації в багатьох випадках вимагає конфіденційності, то виникає проблема шифрування величезних інформаційних масивів. Для інтерактивних систем типу телеконференцій, ведення аудіо або відеозв'язку, таке шифрування повинне здійснюватися в реальному масштабі часу і по можливості бути “прозорим” для користувачів [203-205, 222, 223, 229, 231].

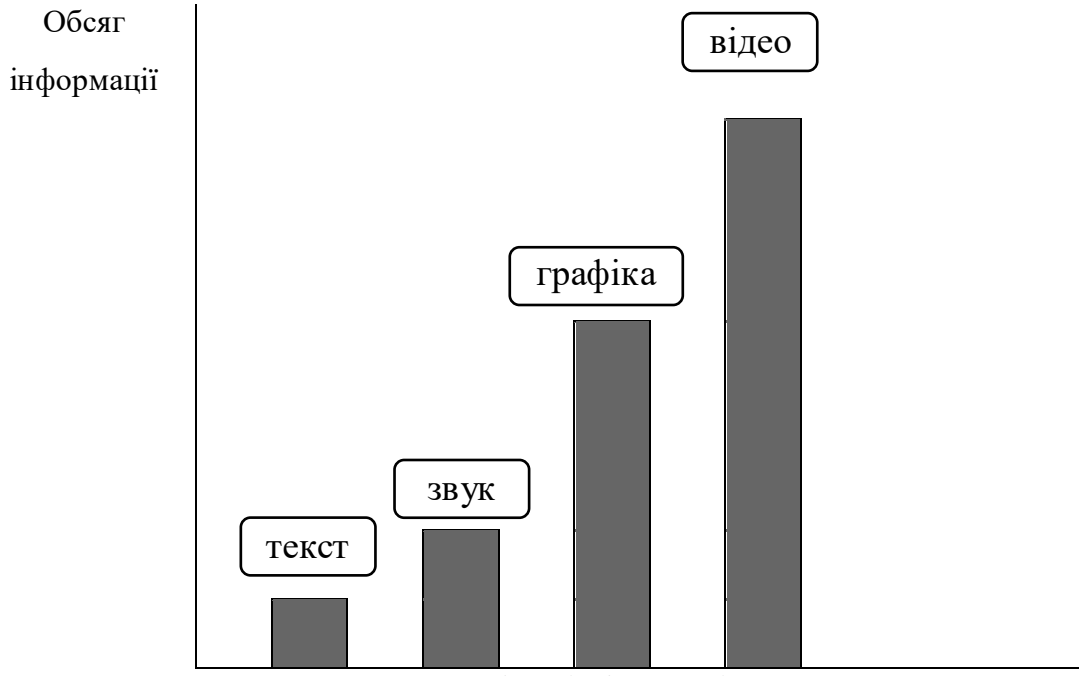


Рис. 1.2 – Обсяг інформації, що передається.

Це немислимо без використання сучасних технологій шифрування.

Найбільш розповсюдженим є потокове шифрування даних. Якщо в описаних раніше криптосистемах передбачалося, що на вході мається деяке кінцеве повідомлення, до якого і застосовується криптографічний алгоритм, то в системах з потоковим шифруванням принцип інший.

Система захисту не чекає, коли закінчиться передане повідомлення, а відразу ж здійснює його шифрування і передачу [149-151, 154, 156, 157].

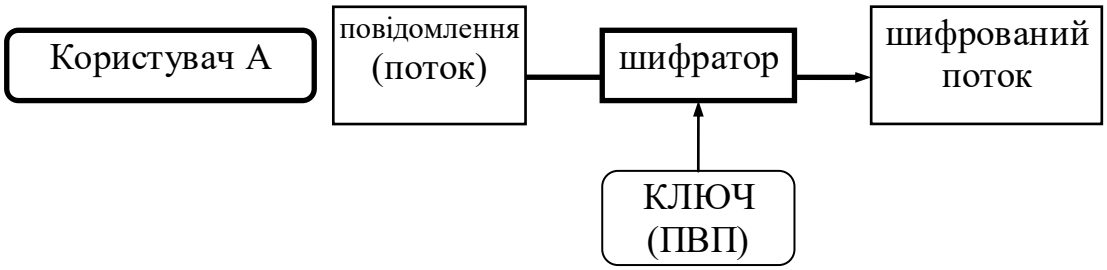


Рис. 1.3 - Потокове шифрування даних

Найбільш очевидним є побітове додавання вхідної послідовності (повідомлення) з деяким нескінченним або періодичним ключем, одержуваним наприклад від генератора ПВП [141, 142, 167, 168, 176, 185, 187, 213]. Прикладом стандарту потокового шифрування є RC4, розроблений Рівестом [142,190, 197, 199].

Іншим, іноді більш ефективним методом потокового шифрування є шифрування блоками. Тобто накопичується фіксований обсяг інформації (блок), а потім перетворений деяким криптографічним методом передається в канал зв'язку[124-126, 143-146, 190].

1.1.4 Використання “блукаючих ключів”

Як було неодноразово відзначене, проблема розподілу ключів є найбільш гострою у великих інформаційних системах [124, 134-136]. Частково ця проблема вирішується (а точніше знімається) за рахунок використання відкритих ключів. Але найбільш надійні криптосистеми з відкритим ключем типу RSA досить трудомісткі, а для шифрування мультимедиіних даних і зовсім не придатні [222].

Оригінальні рішення проблеми “блукаючих ключів” активно розробляються фахівцями. Ці системи є деяким компромісом між системами з відкритими ключами і звичайними алгоритмами, для яких потрібне наявність того самого ключа у відправника й одержувача. [120, 151, 154, 157]

Ідея методу досить проста.

Після того, як ключ використаний в одному сеансі за деяким правилом він змінюється іншим. Це правило повинне бути відомо і відправникові, і одержувачеві. Знаючи правило, після одержання чергового повідомлення одержувач теж змінює ключ. Якщо правила зміни ключів неухильно дотримується і відправник і одержувач, то в кожен момент часу вони мають однаковий ключ. Постійна зміна ключа ускладнює розкриття інформації зловмисником [112, 142, 148-151, 153-154].

Основна задача в реалізації цього методу - вибір ефективного правила зміни ключів. Найбільш простий шлях - генерація випадкового списку ключів. Зміна ключів здійснюється в порядку списку. Однак, очевидно список доведеться якимсь чином передавати.

Інший варіант - використання математичних алгоритмів, заснованих на так званих послідовностях, що перебирають. На множині ключів шляхом застосування однієї і тієї ж операції над елементом виходить інший елемент. Послідовність цих операцій дозволяє переходити від одного елемента до іншого, поки не буде перебрана вся множина [120,121, 125, 130-133].

Найбільш доступним є використання полів Галуа. За рахунок підведення до степеня елемента, що породжує, можна послідовно переходити від одного числа до іншого. Ці числа приймаються як ключі [120,121].

Ключовою інформацією в даному випадку є вихідний елемент, що перед початком зв'язку повинний бути відомий і відправникові й одержувачеві.

Надійність таких методів повинна бути забезпечена з урахуванням популярності зловмисникові використовуваного правила зміни ключів.

Цікавою і перспективною задачею є реалізація методу “блукаючих ключів” не для двох абонентів, а для досить великої мережі, коли повідомлення пересилаються між всіма учасниками.

1.1.5 Шифрування, кодування і стиснення інформації

Ці три види перетворення інформації використовуються в різних цілях, що можна представити в табл. 1.1 [141-147, 203-205, 211, 221, 222, 223, 231].

Як видно ці три види перетворення інформації почасти доповнюють один одного і їхнє комплексне використання допоможе ефективно використовувати канали зв'язку для надійного захисту переданої інформації [111-121, 124, 129].

Особливо цікавим представляється можливість об'єднання методів кодування і шифрування. Можна стверджувати, що по суті кодування - це елементарне шифрування, а шифрування - це елементарне завадостійке кодування.

Інша можливість - комбінування алгоритмів шифрування і стисненняи інформації. Завдання стиснення полягає в тому, щоб перетворити повідомлення в межах того самого алфавіту таким чином, щоб його довжина (кількість букв алфавіту) стала менше, але при цьому повідомлення можна було відновити без використання якоїсь додаткової інформації. Найбільш популярні алгоритми стиснення - RLE, коди Хаффмана, алгоритм Лемпеля-Зіва. Для стиснення графічної і відеоінформації використовуються алгоритми JPEG і MPEG [111, 176, 120, 130-132].

Головне достоїнство алгоритмів стиснення з погляду криптографії полягає в тому, що вони змінюють статистику вхідного тексту убік її вирівнювання. Так, у звичайному тексті, стиснутому за допомогою ефективного алгоритму всі символи мають однакові частотні характеристики

і навіть використання прості системи шифрування зроблять текст недоступним для криптоаналіза.

Таблиця 1.1

Перетворення інформації

Вид перетворення	**Ціль**	**Зміна обсягу інформації після перетворення.**
Шифрування	– передача конфіденційної інформації; – забезпечення аутентифікації і захисту від навмисних змін;	звичайно не змінюється, збільшується лише в цифрових сигнатурах і підписах
Завадостійке кодування	– захист від спотворення перешкодами в каналах зв'язку	збільшується
Стиснення (компресія)	– скорочення обсягу переданих або збережених даних	зменшується

Розробка і реалізація таких універсальних методів - перспектива сучасних інформаційних систем.

1.1.6 Реалізація криптографічних методів

Проблема реалізації методів захисту інформації має два аспекти [143-146, 156, 157, 194]:

– розробку засобів, що реалізують криптографічні алгоритми,

– методику використання цих засобів.

Кожний з розглянутих криптографічних методів може бути реалізований або програмними, або апаратним способом [143-146].

Можливість програмної реалізації обумовлюється тим, що всі методи криптографічного перетворення формальні і можуть бути представлені у вигляді кінцевої алгоритмічної процедури.

При апаратній реалізації всі процедури шифрування і розшифрування виконуються спеціальними електронними схемами. Найбільше поширення одержали модулі, що реалізують комбіновані методи.

При цьому неодмінним компонентом всіх апаратно реалізованих методів є гамування. Це обумовлюється тим, що метод гамування вдало сполучить у собі високу криптостійкість і простоту реалізації [121, 134, 154, 156].

Найбільше часто як генератор використовується широко відомий регістр зсуву зі зворотними зв'язками (лінійними або нелінійними). Мінімальний період породжуваної послідовності дорівнює 2^N-1 біт. Для підвищення якості послідовності, яка генерується, можна передбачити спеціальний блок керування роботою регістра зсуву. Таке керування може полягати, наприклад, у тім, що після шифрування визначеного обсягу інформації вміст регістра зсуву циклічно змінюється.

Інша можливість поліпшення якості гамування полягає у використанні нелінійних зворотних зв'язків. При цьому поліпшення досягається не за рахунок збільшення довжини гами, а за рахунок ускладнення закону її формування, що істотно ускладнює криптоаналіз.

Більшість закордонних серійних засобів шифрування засновано на американському стандарті DES. Вітчизняної ж розробки, такі як, наприклад, пристрій КРИПТОН, використовує вітчизняний стандарт шифрування [138, 195, 196].

Основним достоїнством програмних методів реалізації захисту є їхня гнучкість, тобто можливість швидкої зміни алгоритмів шифрування [167].

Основним же недоліком програмної реалізації є істотно менша швидкодія в порівнянні з апаратними засобами (приблизно в 10 разів).

Останнім часом стали з'являтися комбіновані засоби шифрування, так називані програмно-апаратні засоби. У цьому випадку в комп'ютері використовується своєрідний “криптографічний співпроцесор” - обчислювальний пристрій, орієнтований на виконання криптографічних операцій (додавання по модулі, зсуву і т.д.). Змінюючи програмне забезпечення для такого пристрою, можна вибирати той або інший метод шифрування. Такий метод поєднує в собі достоїнства програмних і апаратних методів.

Таким чином, вибір типу реалізації криптозахисту для конкретної інформаційної системи в істотній мірі залежить від її особливостей і повинний спиратися на всебічний аналіз вимог, пропонованих до системи захисту інформації.

1.2 Загальні алгоритмічні проблеми аналізу основних типів шифрів

1.2.1 Елементарні шифри

Шифр заміни (шифр підстановки) - метод шифрування, при якому кожен елемент вихідного тексту взаємнооднозначно заміняється одним, або декількома знаками деякого алфавіту. Шифр простої заміни заміняє кожен знак вхідного алфавіту на деякий знак з того ж алфавіту. Результат заміни не залежить від розташування знака у відкритому тексті. Ключами для шифрів заміни є таблиці заміни. [121, 134, 154, 156]

Можлива побудова шифру, аналогічного шифрові заміни, коли в такті шифрування можуть перетворюватися групи різної значності. Такою властивістю володіють шифрсистеми, називані кодами. Специфічною особливістю кодів є те, що вони оперують не з довільними комбінаціями

символів, а зі словами, складами і фразами. Перевагою кодів є стиснення інформації при зашифруванні, оскільки кодові групи, як правило, коротше величин, що вони заміняють, а недоліком те, що словниковий склад коду розрахований на визначений характер переписки, тобто спеціалізований.

Шифри заміни часто приводяться в спеціальній і популярній літературі як приклади слабких шифрів. Необхідно відзначити, що, як і для будь-якого іншого шифру, це може бути вірним лише в конкретних випадках. Наприклад, алгоритми DES, ГОСТ 28147-89 базуються на шифрі заміни, а алгоритм шифрування RSA реалізує цей шифр безпосередньо [121, 134, 154, 156].

Шифри перестановки відрізняються від шифрів заміни тим, що при зашифруванні буква відкритого тексту переходить не у фіксований знак алфавіту, а в іншу букву того ж відкритого тексту, у результаті чого букви розташовуються на нових місцях, тобто переставляються. Ключі для таких шифрів представляються у виді підстановок розмірності до довжини тексту включно. Шифри перестановки мають багато різновидів, що відрізняються в основному тим, яким способом породжуються ключі. У ручних системах, наприклад, для цієї мети використовуються різні варіанти розміщення відкритих текстів у площі різної конфігурації і виписки його за законом, що утримується в секреті [121, 134, 154, 156].

Шифри гамування. Широко розповсюджені приклади шифру даного типу засновані на т.зв. операції додавання чисел по деякому модулю.

Символи алфавіту відкритого тексту, попередньо замінні на числа, складаються з елементами деякої числової послідовності, що називається гамою. Процедура зашифрування називається модульним гамуванням, кількість знаків в алфавіті - модулем гамування.

У загальному випадку операція гамування не обов'язково є модульним додаванням: часто використовуються деякі оборотні табличні функції.

Оскільки можна дописувати будь-яке число алфавітів, то букви можна складати, множити, віднімати. Така арифметика називається модульною. У

загальному випадку порівнянність чисел a і b за модулем n записується у вигляді $a \equiv b(\mathrm{mod}\ n)$.

Ключем шифрсистеми є гама, довжина якої, узагалі говорячи, дорівнює довжині відкритого тексту. Оскільки послідовність знаків гами може породжуватися по деякому алгоритмі, то гама може бути задана допоміжним ключем, довжина якого істотно менше довжини відкритого тексту, зокрема, гама може мати малий період, а також іншими особливостями.

1.2.2 Основні типи шифрів

Особлива увага на одне з розходжень між шифром простої заміни і гамування: у шифрі простої заміни один і той же елемент відкритого тексту перейде у фіксований знак шифртекста в будь-якому такті шифрування, а в шифрі гамування це не так. Цей шифр перетворить елемент відкритого тексту в залежності від значення гами (тобто ключа) на кожнім такті шифрування. Можна сказати, що згаданий ключ задає послідовність шифроперетворень, на відміну від шифру простої заміни, де всі шифррперетворення однакові. Зазначене розходження приводить до понять основних типів шифрів: блокових і потокових шифрів відповідно.

1.2.3 Потокові шифри. Послідовність вибору шифроперетворень

Розглянемо пронумерований список Δ усіх різних шифроперетворень, що могли б виникнути в процесі шифрування повідомлень за допомогою даної криптосистеми. Процес шифрування можна записати як послідовність номерів шифроперетворень, обраних на відповідних тактах. Позначимо цю послідовність через Г и назвемо ключовим потоком. Послідовність Г аналогічна функції вибору станів деякого автомата. Вона залежить від ключів і номерів тактів шифрування.

Властивості цієї послідовності багато в чому відбивають якість шифру і визначають його класифікацію. Наприклад, якщо список Δ містить тільки шифроперетворення, що є додаванням по модулі n, кожне з фіксованим числом ci, (i = 0,1, … n-1), то шифр є шифром гамування по модулю n. Потоковим шифром називається система, у якій на кожнім такті використовується перемінний, обираний за допомогою елементів ключового потоку, алгоритм шифрування [115, 142, 154, 156].

Ключовий потік визначається вихідними ключовими даними і номерами тактів шифрування, аж до розглянутого.

Потокові шифри, мабуть, більш чуттєві до порушень синхронізації (вставка, пропуск), чим блокові. Для деякої компенсації даного недоліку використовуються потокові шифри зі зворотним зв'язком. У цих шифрах значення елемента ключового потоку на такті t обчислюється за допомогою фіксованої функції f від ключа і декількох знаків шифртекста, отриманих на т попередніх тактах.

У криптографічній літературі під потоковим шифром дуже часто розуміють так називаний двійковий аддитивний потоковий шифр, що представляє собою шифр гамування по модулі два з псевдовипадковою гамою. Для такого шифру ключовий потік можна записати за допомогою нулів і одиниць і безпосередньо використовувати для гамування відкритого тексту.

1.2.4 Якість гами

Очевидно, властивості потокового шифру залежать від властивостей ключового потоку (гами). Якщо в ключовому потоці виявляються закономірності, то аналіз шифру спрощується. Наприклад, якщо період гами короткий, то у випадку нерівноймовірного відкритого тексту класичний шифр гамування стає катастрофічно слабким. Небажаними є не тільки детерміновані, але і стохастичні залежності в гамі.

У 1926 році американський інженер Вернам запропонував для шифрування кожного біта відкритого тексту використовувати свій ключ. У системі Вернама потрібно, щоб джерело ключів виробляв випадкову раівноймовірну двійкову послідовність, знаки якої незалежні і щоб черговий біт відкритого тексту перешифровувався черговим бітом ключа (гами).

К.Шеннон [171] показав, що система Вернама є недешифрованою навіть при повному переборі усіх варіантів послідовності гами, унаслідок відсутності критерію відкритого тексту. На практиці застосовуються послідовності гами, по параметрах, що наближаються до вимог системи Вернама.

При великих витратах на проведення відповідних організаційних мір і побудова громіздкої системи технічного захисту інформації, за допомогою специфічних фізичних процесів, неземних джерел випромінювань і т.п., можна організувати систему нагромадження випадкової гами. Однак чисто випадкова послідовність може (у принципі) містити неякісні ділянки. Тому необхідно розробляти математичні алгоритми для її коректування, що приводить до необхідності формальної оцінки якості гами. Проте, криптосистеми, засновані на подібному підході, існують. Більш практичними є криптосистеми, що породжують гаму з дуже великим періодом. Періоди колосальної величини необхідні, але не достатні. Значення елементів на періоді повинні бути непередбачені, принаймні, зі значимою імовірністю. Розробка методів побудови й аналізу таких послідовностей є однієї з основних задач криптології.

1.2.5 Періодичність гами

В даний час у системах криптографічного захисту інформації широко використовуються так називані шифратори з внутрішнім носієм гами, що реалізують потокові шифри, що генерують послідовності з дуже великими періодами і гарними статистичними властивостями [5,30].

Ці шифратори засновані на комбінуванні т.зв. регістрів зсуву. Відповідні генератори гами, у переважній більшості випадків, складаються з типових вузлів, заснованих на комбінаціях регістрів зсуву і функціях ускладнення [9]. Найбільш простим вузлом є т.зв. регістр зсуву з лінійними зворотними зв'язками (РЗЛЗЗ), що генерує рекуррентную послідовність виду $x_{i+0} \oplus x_{i+k} \oplus ... \oplus x_{i+t} = x_{i+n}$, де $\oplus$ означає додавання по модулю два.

Наприклад, послідовність, яка генерується РЗЛЗЗ за рекурентним законом $x_{i+0} \oplus x_{i+2} = x_{i+5}$ і початковим станом 11000, має вигляд:

1100011011101010000100101100111110001101110101000010010.

Подібні послідовності є періодичними.

При відповідному виборі параметрів РЗЛЗЗ можна досягти максимально можливих значень періоду рівних $2^n - 1$.

У випадку короткого періоду гами d, виписка відрізків криптограми довжини d друг під другом дасть сукупність стовпчиків, для кожної з яких використовувався фіксований знак гами.

Якщо відкритий текст не є рівноймовірним, то кожен стовпчик дозволяє визначити один знак гами, з точністю до інверсії. У підсумку, визначається гама на всьому періоді.

Безпосередньо для генерації гами РЗЛЗЗ не підходять, тому що відповідні вихідні послідовності є передбачуваними. На практиці застосовуються комбінації залежних РЗЛЗЗ, що взаємно впливають на формування своїх послідовних заповнень, а гама формується за допомогою складних функцій від значень проміжних обчислень [122-157].

Для передбачуваної гами знання невеликого її відрізка (наприклад, при переборі значень відкритого тексту) дозволяє упорядкувати по імовірності варіанти можливого продовження гами. Це дозволяє різко звузити кількість можливих варіантів відкритого тексту і продовжувати послідовне розкриття тексту за значеннєвим критерієм. Одним із загальних підходів аналізу потокових шифрів є декомпозиція автомата на відповідні вузли й аналіз вихідних послідовностей вузлів і шифратора в цілому.

1.2.6 Блокові шифри

Необхідність застосування криптографічного захисту інформації в мережах ЕОМ, у базах даних, у системах електронних платежів привела до широкого використання програмних засобів шифрування. При цьому виявилося, що програмна реалізація потокових шифрів, у ряді випадків, уступає у швидкодії шифрам іншого типу, так називаним, блоковим шифрам.

Блоковим шифром називається система шифрування, що використовує на кожнім такті постійний, обраний до початку шифрування, у залежності від ключів, алгоритм [2,5,8].

Знаки алфавіту представляються у виді двійкових блоків даних фіксованої довжини. Наприклад, алгоритм ГОСТ 28147-89 призначений для роботи з блоками довжиною 64 біта. У режимі простої заміни цей шифр взаємооднозначно відображає множину потужності 264 на себе.

Існують потокові шифри, що використовують блоковий шифр як вузол генерації гами. У криптографії прийнято розглядати подібні шифри як режими роботи відповідного блокового шифру. Наприклад, у режимах шифрування алгоритм ДСТ 28147-89 працює як шифр гамування по модулю два, використовуючи двійкову гаму, вироблену в режимі, що відповідає блоковому шифрові.

1.2.7 Алгоритмічні проблеми, пов'язані зі стійкістю основних типів шифрів

Для блокових шифрів оцінка стійкості зв'язана з оцінкою якості т.зв. віртуальних таблиць заміни, тобто таблиць заміни, представити які цілком на носії неможливо через великий обсяг даних. Блоковий шифр є сукупністю віртуальних таблиць заміни. Ключ служить для вибору таблиці, що є незмінною в процесі шифрування окремого повідомлення [218-229].

Очевидно, що криптографічні властивості шифру простої заміни істотно залежать від ключів. Тому в блоковому шифрі ключі, узагалі говорячи, можуть бути нерівноцінні. Наприклад, віртуальні таблиці можуть здійснювати нестійкі перетворення над елементами (блоками) відкритого тексту. Крім того, не виключається, що вибір однієї і тієї ж віртуальної таблиці може бути здійснений за допомогою різних ключів.

Загальна проблема оцінки якості блокового шифру зводиться до задачі визначення великих областей ключів, яким відповідають підстановки, найбільш складні для розкриття шифру простої заміни. У ситуації, коли віртуальна таблиця заміни легко описується формулами, можуть бути сформульовані загальні задачі, рішення яких приводить до дешифрування відповідних криптосистем [218-229].

До подібним задач зводиться стійкість значного числа сучасних асиметричних криптоалгоритмів.

Розглянемо, наприклад, степеневу функцію виду $g(x) = x^e \bmod n$, де $n = p*q$, p, q - різні прості числа. Для обернення цієї функції досить вирішити задачу розкладання числа n на співмножники. Ця задача є алгоритмічною проблемою, на якій заснована стійкість розповсюдженої криптосистеми RSA.

Аналогічна ситуація має місце з дискретною експонентою, тобто функцією виду $f(x) = a^x \bmod p$, де p - велике просте число. Ця функція часто використовується в процедурах аутентифікації. Унаслідок кінцевості множиниі відрахувань по модулю p, послідовність $a^k \bmod p$, $k = 1,2\ldots$,періодична. Найменший період називається показником (порядком) числа a за модулем p [120, 138].

Відомо, що функція $f(x) = a^x \bmod p$ при великих значеннях x і ordpa поводиться як однобічна.

Зворотна функція (дискретний логарифм) обчислювально нереалізований і задача дискретного логарифмування також є алгоритмічною проблемою, на якій заснована стійкість ряду криптоалгоритмів. Що стосується якісних потокових шифрів, то фактично кожен такий шифр

зводиться до чергової, раніше невідомій математичній задачі, що піддається рішенню лише в окремих випадках [138].

Проте, можна сформулювати загальну алгоритмічну проблему, що лежить в основі стійкості шифрів модульного гамування. Очевидно, модульне гамування можна розглядати як процедуру перекручування гами знаками відкритого тексту. При нерівноймовірному відкритому тексті це дозволяє використовувати зв'язку в гамі для складання відповідних систем рівнянь, а потім розглядати отримані рівняння як виконуються для шифртекста, але з перекрученими правими частинами. Щодо перекручувань відомо лише розподіл імовірностей.

Даний підхід приводить до загальної проблеми рішення систем рівнянь з перекрученими параметрами. Так, для шифрів гамування, побудованих на використанні комбінацій регістрів зсуву, загальна проблема відновлення перекрученої (нелінійної) рекурентної послідовності є алгоритмічною проблемою, на якій ґрунтується стійкість шифру.

1.3 Підходи щодо оцінки надійності реальних криптосистем

Розвиток математичних методів і підвищення продуктивності обчислювальної техніки може згодом привести до ослаблення використовуваної криптосистеми. Таким чином, виникає необхідність криптологічного супроводу криптосистем протягом усього терміну їхньої дії.

Супровід криптосистем полягає в контролі за дотриманням порядку й умов її експлуатації, а також в ухваленні своєчасного рішення на зміну її параметрів. Основних причин, унаслідок яких варто прийняти теза про потенційну ненадійність діючих криптосистем дві: відсутності повних формальних критеріїв якості криптосистем, а також неможливість на практиці виконання в повному обсязі вимог, виходячи з яких висновок про достатній рівень захисту інформації обґрунтований теоретично. До того ж, оскільки в даний час має місце масове застосування криптосистем,

починають виявлятися малоймовірні ситуації, невраховані розроблювачем. Відповідно, виникають передумови до порушення захисту інформації. Ще одним джерелом потенційної ненадійності криптосистем є можливість створювати криптосистеми зі свідомо внесеними слабостями (лазівками). Відсутність формального критерію стійкості криптосистеми змушує використовувати для визначення рівня її надійності оцінку практичної стійкості, тобто, згідно К.Шеннону, оцінювати стійкість, виходячи з параметрів найкращого відомого методу дешифрування [138, 171].

1.3.1 Метод експертних оцінок

Суть методу експертних оцінок полягає у використанні усього криптологічного потенціалу, що мається в розпорядженні підприємства, фірми, держави, для одержання максимально об'єктивних висновків щодо якості розроблювальної або впроваджуваної криптосистеми. Як правило, застосовується багатоетапне обговорення проектів. На кожнім етапі обговорюються висновки експертів і приймається рішення про усунення виявлених недоліків, подальшому обговоренні, або про завершення роботи експертів. Остаточне рішення приймається відповідною комісією на основі експертних висновків. Рішення комісії затверджується керівником уповноваженого органа. Надійність криптосистеми залежить не тільки від математичних властивостей криптоалгоритмів. Вона залежить і від системи генерації ключів, і від психології персоналу, і навіть від стану системи електропостачання (якщо система непрацездатна, то вона марна). Таким чином, до оцінки надійності криптосистеми необхідно підходити комплексно. Комплексна оцінка якості засобів криптографічного захисту інформації передбачає розгляд питань стійкості алгоритмів, побудови ключової системи, тестування системи зв'язку і т.п. Особливу хибність являють собою проблеми технічного захисту інформації. Велике значення для ефективності комплексної оцінки мають повнота і коректність вимог,

висунутих до системи користувачами. Вибір засобів криптографічного захисту інформації і вихідних вимог до їхньої стійкості повинні бути адекватними тій конкретній задачі в області інформаційної безпеки, у якій ці засоби планується використовувати. Тому неправильно було б здобувати довільну криптосистему, а потім досліджувати її властивості. Насправді необхідно, виходячи з потреб, проробити і висунути вимоги щодо бажаних властивостей шифру і лише за тим оцінювати якість системи або її проекту. Фактично, оптимальна оцінка потреб у захисті інформації є головна задача при ухваленні рішення на використання криптозасобів. Особливо варто підкреслити, що після введення криптосистеми в експлуатацію, як правило, вона стає практично недоступної для спостереження і подальшого аналізу, хоча саме в процесі експлуатації недоліки виявляються найбільше повно і якісно [138].

1.3.2 Метод зведення до загальної алгоритмічної проблеми

Не існує універсальних засобів захисту інформації й окремих алгоритмів, що підходили б для рішення криптографічних задач без попередніх досліджень. Для кожної конкретної задачі необхідна адаптація відповідних алгоритмів. Навіть застосування стандартизованих методів захисту інформації вимагає кваліфікованого пророблення багатьох додаткових питань, насамперед, вибору конкретної конфігурації криптоалгоритма, що часто приводить до необхідності формального обґрунтування стійкості його параметрів. Одним з підходів до оцінки стійкості і виявленню наявності відомих типів слабостей для конкретної криптосистеми, є метод зведення оцінки стійкості до оцінки складності деякої загальної алгоритмічної проблеми. Типовим випадком є, наприклад, криптосистеми з відкритими ключами, оскільки вони створювалися таким чином, щоб задача їхнього дешифрування зводилася до тієї або іншої обчислювально нереалізованої процедури. Основні труднощі полягають у

тім, що для реальних систем згадані алгоритмічні проблеми вивчені недостатньо і мають велику кількість спеціальних значень параметрів, при яких системи стають слабкими. Цілком уникнути подібних випадків украй складно, оскільки, як уже відзначалося, масове використання криптосистем забезпечує можливість реального виникнення цих рідких ситуацій. Розробкою криптосистем і аналізом їхньої стійкості займаються багато фахівців у різних країнах світу. Методи, використовувані при аналізі криптоалгоритмів, багато в чому аналогічні тим, що застосовуються при їхньому синтезі. Тому велике значення має взаємозв'язок між підходами до дешифрування в окремих випадках і методами побудови стійких параметрів криптосистем. Характерним підходом є прагнення виділити деякі найбільш критичні особливості криптосистеми, висунути ряд вимог до криптоперетворень, а після побудувати параметри криптоперетворень, що найкраще задовольняють сукупності висунутих умов. Для усвідомлення необхідних вимог також дуже важливим є пошук окремих випадків ослаблення стійкості шифроперетворень або випадків дешифрування окремих повідомлень. Відповідні криптоаналітичні прийоми можуть бути як очевидними, так і дуже складними. Можна затверджувати, що рекомендації міжнародних стандартів в області криптографії створені так, щоб максимально врахувати усі відомі окремі випадки ослаблення відповідних криптоалгоритмів. До недоліків методу експертних оцінок і методу зведення до загальної алгоритмічної проблеми випливає, відповідно, віднести: по-перше, неможливість передбачення несприятливих ситуацій, коли користувачем порушуються вихідні посилки, що послужили базою для оцінки якості системи, по-друге, неможливість врахувати всі окремі випадки, коли рішення складної математичної проблеми може бути ефективно реалізовано. У той же час очевидно, що зведення до загальної алгоритмічної проблеми є природним підходом до оцінки параметрів криптоалгоритмів, що дозволяють виділити приватні задачі й оцінювати стійкість криптоалгоритма, виходячи зі складності підзадач [138].

1.4 Криптосистема як алгебраїчна модель. Аналіз властивостей.

Варто відзначити, що процес криптографічного захисту інформації виконується за заздалегідь визначеною схемою шифрування, яку можна представити у вигляді алгебраїчної моделі [163].

Нехай X, Y і Q – деякі скінченні множини відкритого тексту, зашифрованого тексту і ключів відповідно. Введемо такі $K1, K2 \in Q$, що на добутках $X \times Q$ і $Y \times Q$ множин X, Q і Y задано таку пару функції відображень $E_{K1} : X \times Q \to Y$ і $D_{K2} : Y \times Q \to X$ відповідно. При цьому, відображення E_{K1} визначає метод зашифрування відкритого тексту, а відображення D_{K2} – метод розшифрування зашифрованого тексту.

Алгебраїчною моделлю шифру є п’ятірка [115-144]:

$$\sum = (X, Y, Q, E_{K1}, D_{K2}),$$

якщо виконуються такі умови:

1) $\forall x \in X$, $\forall K1, K2 \in Q$: $D_{K2}(E_{K1}(x)) = x$.

2) $Y = \bigcup_{K1 \in Q} E_{K1}(X)$.

У симетричних блокових шифрах під час зашифрування та розшифрування використовують один і той же ключ $K = K1 = K2$, тому з урахуванням даного факту, алгебраїчна модель приймає такий вигляд

$$\sum = (X, Y, Q, E_K, D_K). \qquad (1.1)$$

До узагальненої алгебраїчної моделі симетричного блокового шифрування (1.1) інколи вводять ще множину керування станом процесу шифрування T, елементи якої можуть бути відкритими та вносити в блоковий

шифр властивість випадковості [164]. Таким чином, функції відображень, що визначають методи зашифрування та розшифрування приймають такий вигляд $E_K : X \times Q \times T \to Y$ і $D_K : Y \times Q \times T \to X$ відповідно, а алгебраїчна модель шифру приймає такий вигляд

$$\sum = (X, Y, Q, T, E_K, D_K). \quad (1.2)$$

За рахунок використання різних значень елементів множини T і одного й того ж незмінного секретного ключа K досягається можливість для однакових блоків відкритого тексту отримувати різні блоки зашифрованого тексту.

Огюст Керкгоффс був одним із перших, хто у своїй роботі, визначив базові принципи, які використовують під час розроблення шифрів [129]. По-перше, шифри необхідно розглядати з точки зору їх масового використання, коли один і той же метод шифрування використовують доволі багато користувачів. По-друге, коли складно довести теоретичну стійкість запропонованого криптографічного методу, то використовують емпіричні методи дослідження, які ґрунтуються на проведенні криптографічних атак, тобто використанні криптоаналізу. Якщо результати емпіричних досліджень є негативними, то шифр вважають стійким з урахуванням розвитку сучасних електронно-обчислювальних можливостей.

Криптографічна система згідно Керкгоффса має задовольняти таким вимогам, які і до сьогодні є актуальними [129]:

1) Система повинна володіти практичною стійкістю до атак, якщо не можливо довести її теоретичну стійкість.

2) Складність зламу системи не повинна базуватися на секретності її архітектури.

3) Процес зміни, передачі і зберігання секретного ключа має бути простим та відбуватися без фізичного запису на паперові носії інформації.

4) Захищена інформація повинна передаватися без додаткових складнощів через сучасні інформаційно-телекомунікаційні мережі.

5) Система має бути портативною та не вимагати багатьох операторів для обслуговування.

6) Система має бути простою у використанні.

Вагомий вклад у становлення принципів, на основі яких розробляють криптографічні методи захисту інформації вніс К. Шеннон. У своїй праці [171], він вводить класифікацію шифрів і поділяє їх на теоретично стійкі, практично стійкі і абсолютно стійкі.

Теоретично стійким є шифр виду (X, Y, Q, E_K, D_K), $Y = E_K(X \times Q)$, $X = D_K(Y \times Q)$ із заданими імовірнісними розподілами $p(x)$, $x \in X$ на X і $p(K)$, $K \in Q$, якщо він досконалий за Шенноном, тобто при будь-якому $y \in Y$ і x [142, 156, 171]

$$p(x/y) = p(x),$$

де $p(x/y)$ – апостеріорна імовірність отримання відкритого тексту x при умові, що обрано зашифрований текст y.

Окрім того, необхідною і достатньою умовою теоретичної стійкості шифру, при будь-якому $y \in Y$ і $x \in X$ є виконання такої рівності [138]

$$p(y/x) = p(y),$$

де $p(y/x)$ – умовна ймовірність отримання зашифрованого тексту y при умові, що обрано відкритий текст x;

$p(y)$ – імовірність отримання зашифрованого тексту y.

Також, відносно методів криптографічного аналізу *теоретично стійкими* є такі шифри, зашифровані тексти яких містять недостатню кількість інформації для однозначного визначення відповідних їм відкритих текстів або ключів [124, 126, 130].

Практично стійким є такий шифр, задача зламу якого або зводиться до протидії відомим методам криптографічного аналізу, або має достатньо велику обчислювальну складність на протязі якої інформація втратить свою цінність [124, 142, 130].

Під *абсолютно стійкими* розуміють такі шифри, в яких розмір ключової інформації рівний або більший за розмір відкритого тексту, що зашифровують та такі ключі використовують лише один раз [232]. Використання абсолютно стійких шифрів на практиці є неефективним, оскільки ключова інформація має достатньо великий розмір і необхідно дотримуватися достатньо високого рівня її захищеності під час зберігання.

К. Шеннон також встановив ряд критеріїв, що висуваються до блокових шифрів під час їх розроблення, які до сьогодні є актуальними вимоги [124, 126, 130, 133-138, 142, 149-157].

1) Секретний ключ має бути невеликого розміру, але при цьому забезпечувати достатній рівень криптографічної стійкості шифру.

2) Незначна зміна в секретному ключі або відкритому тексті повинна спричинювати суттєві зміни в зашифрованому тексті.

3) Будь-який секретний ключ має забезпечувати однаковий рівень криптографічної стійкості шифру.

4) Операції зашифрування та розшифрування мають бути простими, щоб забезпечити високу швидкість процесу шифрування.

5) Кількість помилок, які виникають під час виконання шифрування або передавання повідомлення необхідно мінімізувати, щоб вони не поширювалися на все повідомлення.

6) Обсяг повідомлення після виконання процесу зашифрування не повинен збільшуватися.

За останні десятиліття до симетричних блокових шифрів висувають додаткові вимоги, зокрема [230-232]:

− підтримка можливості використовувати секретні ключі змінної довжини;

− підтримка можливості розпаралелення обчислень;

− підтримка можливості використання шифрів на широкому колі апаратних засобів;

− вартість шифрування не має перевищувати вартості інформації, яка підлягає захисту.

Окрім того, криптографічні перетворення, що використовуються в симетричних шифрах повинні забезпечувати два основних принципи – розсіювання та перемішування для створення криптографічно стійких шифрів.

Принцип *перемішування* дозволяє встановити складні статистичні залежності між відкритим і зашифрованим текстом [223-229]. Метою такого перетворення є усунення зв'язку між відкритим і зашифрованим текстом.

Під *розсіюванням* розуміють таке криптографічне перетворення, яке дозволяє перерозподілити надлишковість відкритого тексту, шляхом поширення її на весь зашифрований текст з використанням секретного ключа за рахунок впливу одного символу відкритого тексту на значну кількість символів зашифрованого тексту [156, 157, 223-229].

Як вже згадувалося раніше, найбільш стійкими шифрами є абсолютно стійкі шифри, але оскільки в абсолютно стійких шифрах $|X| \le |Q|$, тому в симетричних блокових шифрах використовують секретні ключі K невеликого розміру (порядку 128-256 біт). Це у свою чергу спричинює використання повторювальних наборів операції перетворення даних у методах симетричного блокового шифрування. Шифри, що використовують такі

методи шифрування називають *ітераційними*. Ітераційні методи блокового шифрування будують на основі:

- мережі Фейстеля та її модифікаціях [156, 157];
- підстановочно-перестановочної мережі [112, 121, 123];
- еластичної мережі [124, 133];
- неортодоксальних структур [124, 126, 130, 133-138, 142, 149-157].

В основу ітераційних СБШ покладена ідея К. Шеннона [10], яка полягає в послідовному використанні простих криптографічних перетворень, які дозволяють найбільш швидко та ефективно реалізувати перемішування та розсіювання даних і складаються з однієї або декількох різних груп операцій для побудови криптографічно стійких функцій шифрування даних.

Одноразовий виклик функції шифрування даних називають *раундом шифрування*, в кожному з яких використовують різні підключі, які називають *раундовими ключами* [116, 156, 142]. Раундові ключі отримують внаслідок перетворення вхідного секретного ключа K в задану кількість підключів, меншої або такої ж самої розрядності, які використовують у процедурі шифрування даних, щоб забезпечити високий рівень перемішування. У загальному випадку на кожному раунді шифрування використовуються різні раундові ключі і розмір раундового ключа може бути набагато більшим за розмір секретного ключа K, через що, збільшується стійкість процесу шифрування даних.

До перетворень, які використовують під час формування раундових ключів, висувають такі вимоги [117-122, 125, 128].

1) Процес відновлення секретного ключа шифрування K із заданого підключа повинен бути достатньо складним, тобто необхідно уникати лінійних перетворень.

2) Кожен біт секретного ключа шифрування K повинен впливати на кожен підключ, тобто має забезпечуватися лавинний ефект.

В якості перетворень, які забезпечують високий рівень розсіювання та перемішування відкритого тексту і секретного ключа використовують операції підстановок і перестановок, ефективність яких була доведена К. Шенноном [171]. Окрім вище зазначених операцій використовують [117-122, 125, 128]:

- логічні операції (І, АБО, виключне-АБО, інверсія тощо);
- арифметичні операції (додавання і множення за модулем);
- операції зсувів (звичайного і циклічного);
- спеціалізовані логічні функції.

Виходячи з алгебраїчної структури симетричного блокового шифру, вище зазначених принципів побудови симетричних блокових шифрів, базових криптографічних перетворень та ітеративної схеми алгоритмів шифрування можна зробити такі висновки.

Характерним недоліком мережі Фейстеля та її модифікацій є те, що розмір оброблюваних блоків даних не може перевищувати максимальну розрядність процесора, внаслідок чого за один раунд шифруванню підлягає неповний блок відкритого тексту, що спричинює низький ступінь розсіювання.

При реалізації підстановочно-перестановочної мережі розробникам необхідно або розміщувати таблиці підстановок в оперативну пам’ять, часте звернення до якої уповільнюватиме процес шифрування, або обмежувати таблиці підстановок розміром кеша центрального процесора. Іншим підходом є використання математичних або логічних функцій, які імітують правила підстановок або перестановок [154-157]. Проте такі функції мають володіти високим ступенем нелінійності, а їхній пошук є достатньо складним. Тобто основним недоліком підстановочно-перестановочної мережі є неефективність її реалізації в сучасних комп`ютерних системах та мережах.

Еластична мережа забезпечує збільшення криптографічної стійкості шифру вдвічі, але при цьому збільшується час шифрування та розмір зашифрованого тексту порівняно з відкритим текстом [133, 138, 134-136].

Отже, актуальним є пошук нових методів шифрування, які б забезпечували достатньо високий рівень криптографічної стійкості та були б простими в апаратній та програмній реалізаціях, з урахуванням особливостей сучасних мікропроцесорів.

1.5 Формальна постановка наукової проблеми

Основні характеристики криптосистеми:

1. Криптостійкість (К).
2. Складність реалізації криптографічного перетворення (С).
3. Швидкість виконання криптографічного перетворення (Ш).
4. Статистичні властивості результатів криптографічного перетворення (Н).

На основі вибраних комплексних показників якості та ефективності функціонування системи комп'ютерної криптографії можливо проводити порівняльний аналіз методів та принципів, покладених в основу архітектури ефективних криптографічних алгоритмів для систем захисту інформаційних ресурсів.

Взаємозалежності ефективних систем комп'ютерної криптографії визначаються на основі описаних показників та можуть бути досягнуті за наступних умов:

1. Криптостійкість $K \to \max$.

$$K \to \max, \text{ якщо } \begin{cases} \mathrm{C} \to \max \\ \mathrm{V} \to \min \end{cases}.$$

2. Складність $C \to \min$.

$$C \to \min \text{, якщо } \begin{cases} \text{V} \to \max \\ \text{К} \to \min \end{cases}.$$

3. Швидкість $\text{V} \to \max$.

$$\text{V} \to \max \text{, якщо } \begin{cases} C \to \min \\ K \to \min \end{cases}.$$

4. Статистичні характеристики $H \to \max$.

$$\text{H} \to \max \text{, якщо } \begin{cases} \text{C} \to \max \\ \text{V} \to \min \\ \text{К} \to \max \end{cases}.$$

Оскільки швидкість та складність виконання криптографічного алгоритму напряму залежить від швидкості та складності виконання операцій перетворення інформації, які складають основу алгоритму $\text{V}_{\text{ALG}} \to \text{V}(\text{F}_\text{i})$ і $\text{C}_{\text{ALG}} \to \text{C}(\text{F}_\text{i})$, тоді швидкість виконання алгоритму напряму залежить від складності $\text{V}(\text{F}_\text{i}) \to \text{C}(\text{F}_\text{i})$ і $V_{ALG} \to C_{ALG}$. Звідси, якщо зростає складність, тоді знижується швидкість $\uparrow C_{ALG} \Rightarrow \downarrow V_{ALG}$ і навпаки.

Отже, виникає протиріччя між складністю, криптостійкістю та швидкістю: складність алгоритму повинна бути мінімальною, показники швидкості, криптостійкості та статистичні властивості – максимальними:

$$\begin{cases} C \to \min; \\ V \to \max; \\ K \to \max; \\ H \to \max. \end{cases}$$

На основі вибраних комплексних показників якості функціонування криптографічних алгоритмів можливо здійснювати порівняльний аналіз методів та принципів, що покладені в основу структури криптографічного алгоритму та синтезу і вибору операцій криптографічного перетворення інформації.

Виходячи з вище наведеного матеріалу, метою даної роботи є рішення науково-технічної проблеми підвищення ефективності функціонування систем комп'ютерної криптографії шляхом створення теоретичних та методологічних положень синтезу операцій криптографічного перетворення інформації та розробки концепції побудови криптографічних алгоритмів на основі них.

Рішення даної наукової проблеми передбачає удосконалення теорії, спрямованої на подолання суперечностей і труднощів при проектуванні систем комп'ютерної криптографії та розробці ефективних криптоалгоритмів. Тому в роботі поставлені та вирішені такі взаємозалежні задачі:

– розробити основні положення методології синтезу операцій перетворення інформації для систем комп'ютерної криптографії;

– на основі застосування запропонованої методології розробити та вдосконалити методи синтезу й аналізу групи нелінійних операцій криптографічного перетворення інформації;

– вдосконалити існуючі примітиви комп'ютерної криптографії на основі застосування синтезованих операцій криптографічного перетворення інформації та оцінити їх ефективність;

– розробити технологію синтезу операцій для мультиопераційних матричних криптографічних примітивів;

– удосконалити методи застосування операцій криптографічного перетворення інформації та оцінити їх ефективність.

Під час вирішення проблемних питань використовувались методи дослідження та математичний апарат, що базується на розділах теорії ймовірності, систем числення, дискретної математики, логіки та алгоритмів.

1.6 Висновки до першого розділу

Перший розділ присвячений аналітичному огляду стандартних вимог до криптографічних систем.

Для здійснення аналізу розглянуто базові принципи побудови й схеми криптологічних систем. Наведений огляд основних проблемних задач, що постають під час реалізації криптографічних систем.

Проведений аналіз сучасних криптосистем та виокремлені основні характеристики ефективності функціонування системи криптографічного захисту.

У першому розділі здійснена формальна постановка наукової проблеми, що підлягає вирішенню, та сформульовані основні задачі дисертаційного дослідження.

РОЗДІЛ 2
РОЗРОБКА ТА УЗАГАЛЬНЕННЯ МЕТОДІВ СИНТЕЗУ ОПЕРАЦІЙ КРИПТОГРАФІЧНОГО ПЕРЕТВОРЕННЯ

2.1 Розробка методів синтезу операцій матричного криптографічного перетворення

2.1.1 Узагальнення результатів дослідження двохрозрядних операцій криптографічного перетворення

У теорії захисту інформації існує два напрями: криптографія і кодування [139-148]. Проте по своїй сутності обидва напрями забезпечують криптографічне перетворення інформації і відрізняються складністю алгоритму кодування та практичною реалізацією. Криптографічні алгоритми, як правило, достатньо складні і реалізуються на програмному рівні, а алгоритми кодування – на апаратному, тому що мають меншу алгоритмічну складність. Криптографічне кодування інформації під управлінням криптосистеми дозволяє зменшити вимоги до криптографічного алгоритму, компенсувавши їх додатковим використанням операцій криптографічного кодування. Поєднання цих двох напрямів в єдиний дозволить підвищити оперативність доступу до конфіденційних інформаційних ресурсів [149-158].

У результаті попередніх досліджень [159, 160] визначено повну множину наборів спеціалізованих логічних функцій двох змінних для систем захисту інформації. Наведені в табл. 2.1 операції криптоперетворення забезпечують пряме та обернене криптографічне перетворення інформації.

Криптопримітиви мають більш складну структуру, ніж операції для криптоперетворення, такі як додавання за модулем, зсув, перестановка, підстановка та інші. Виявлення нових операцій придатних для ефективного криптоперетворення дозволить вдосконалити криптографічні примітиви.

Таблиця 2.1

Повна множина спеціалізованих логічних функцій двох змінних для прямого та оберненого перетворення інформації в криптосистемах

Функція кодування-декодування		Функція кодування-декодування		Функція кодування-декодування	
Кодування	Декодування	Кодування	Декодування	Кодування	Декодування
$\vec{F}_1 = \begin{pmatrix} x_1 \\ x_2 \end{pmatrix}$		$\vec{F}_9 = \begin{pmatrix} x_1 \oplus x_2 \\ x_2 \end{pmatrix}$		$\vec{F}_{17} = \begin{pmatrix} x_1 \\ x_1 \oplus x_2 \end{pmatrix}$	
$\vec{F}_2 = \begin{pmatrix} x_2 \\ x_1 \end{pmatrix}$		$\vec{F}_{10} = \begin{pmatrix} x_2 \\ x_1 \oplus x_2 \end{pmatrix}$	$\vec{F}_{18} = \begin{pmatrix} x_1 \oplus x_2 \\ x_1 \end{pmatrix}$	$\vec{F}_{18} = \begin{pmatrix} x_1 \oplus x_2 \\ x_1 \end{pmatrix}$	$\vec{F}_{10} = \begin{pmatrix} x_2 \\ x_1 \oplus x_2 \end{pmatrix}$
$\vec{F}_3 = \begin{pmatrix} x_1 \oplus 1 \\ x_2 \end{pmatrix}$		$\vec{F}_{11} = \begin{pmatrix} x_1 \oplus x_2 \oplus 1 \\ x_2 \oplus 1 \end{pmatrix}$	$\vec{F}_{13} = \begin{pmatrix} x_1 \oplus x_2 \\ x_2 \oplus 1 \end{pmatrix}$	$\vec{F}_{19} = \begin{pmatrix} x_1 \oplus 1 \\ x_1 \oplus x_2 \oplus 1 \end{pmatrix}$	$\vec{F}_{22} = \begin{pmatrix} x_1 \oplus 1 \\ x_1 \oplus x_2 \end{pmatrix}$
$\vec{F}_4 = \begin{pmatrix} x_1 \\ x_2 \oplus 1 \end{pmatrix}$		$\vec{F}_{12} = \begin{pmatrix} x_2 \oplus 1 \\ x_1 \oplus x_2 \oplus 1 \end{pmatrix}$	$\vec{F}_{23} = \begin{pmatrix} x_1 \oplus x_2 \\ x_1 \oplus 1 \end{pmatrix}$	$\vec{F}_{20} = \begin{pmatrix} x_1 \oplus x_2 \oplus 1 \\ x_1 \oplus 1 \end{pmatrix}$	$\vec{F}_{16} = \begin{pmatrix} x_2 \oplus 1 \\ x_1 \oplus x_2 \end{pmatrix}$
$\vec{F}_5 = \begin{pmatrix} x_1 \oplus 1 \\ x_2 \oplus 1 \end{pmatrix}$		$\vec{F}_{13} = \begin{pmatrix} x_1 \oplus x_2 \\ x_2 \oplus 1 \end{pmatrix}$	$\vec{F}_{11} = \begin{pmatrix} x_1 \oplus x_2 \oplus 1 \\ x_2 \oplus 1 \end{pmatrix}$	$\vec{F}_{21} = \begin{pmatrix} x_1 \\ x_1 \oplus x_2 \oplus 1 \end{pmatrix}$	
$\vec{F}_6 = \begin{pmatrix} x_2 \oplus 1 \\ x_1 \oplus 1 \end{pmatrix}$		$\vec{F}_{14} = \begin{pmatrix} x_1 \oplus x_2 \oplus 1 \\ x_2 \end{pmatrix}$		$\vec{F}_{22} = \begin{pmatrix} x_1 \oplus 1 \\ x_1 \oplus x_2 \end{pmatrix}$	$\vec{F}_{19} = \begin{pmatrix} x_1 \oplus 1 \\ x_1 \oplus x_2 \oplus 1 \end{pmatrix}$
$\vec{F}_7 = \begin{pmatrix} x_2 \\ x_1 \oplus 1 \end{pmatrix}$	$\vec{F}_8 = \begin{pmatrix} x_2 \oplus 1 \\ x_1 \end{pmatrix}$	$\vec{F}_{15} = \begin{pmatrix} x_2 \\ x_1 \oplus x_2 \oplus 1 \end{pmatrix}$	$\vec{F}_{14} = \begin{pmatrix} x_1 \oplus x_2 \oplus 1 \\ x_1 \end{pmatrix}$	$\vec{F}_{23} = \begin{pmatrix} x_1 \oplus x_2 \\ x_1 \oplus 1 \end{pmatrix}$	$\vec{F}_{12} = \begin{pmatrix} x_2 \oplus 1 \\ x_1 \oplus x_2 \oplus 1 \end{pmatrix}$
$\vec{F}_8 = \begin{pmatrix} x_2 \oplus 1 \\ x_1 \end{pmatrix}$	$\vec{F}_7 = \begin{pmatrix} x_2 \\ x_1 \oplus 1 \end{pmatrix}$	$\vec{F}_{16} = \begin{pmatrix} x_2 \oplus 1 \\ x_1 \oplus x_2 \end{pmatrix}$	$\vec{F}_{20} = \begin{pmatrix} x_1 \oplus x_2 \oplus 1 \\ x_1 \oplus 1 \end{pmatrix}$	$\vec{F}_{24} = \begin{pmatrix} x_1 \oplus x_2 \oplus 1 \\ x_1 \end{pmatrix}$	$\vec{F}_{15} = \begin{pmatrix} x_2 \\ x_1 \oplus x_2 \oplus 1 \end{pmatrix}$

Для криптографічних операцій двох змінних було сформульовано і доведено ряд теорем, які стали теоретичним підґрунтям для побудови моделей пристроїв прямого, оберненого та взаємного криптографічного перетворення. Отримані результати дали змогу спростити процес побудови функцій криптографічного перетворення інформації. Забезпечення конфіденційності інформації при реалізації даних операцій базується на забезпеченні криптостійкості стандартними алгоритмами, а також збільшенням кількості перетворень, які використовуються.

На основі проведених теоретичних розрахунків та експериментальних досліджень було доведено, що метод підвищення оперативності криптографічного перетворення інформації на основі використання запропонованих спеціалізованих логічних функцій для систем захисту інформації, зокрема комп'ютерної криптографії, дозволяє збільшити швидкість обробки інформації від 1,57 до 2,92 разів залежно від часу отримання ключа та розрядності перетворення [161, 162].

З метою проведення узагальнення результатів для подальшого дослідження двохрозрядних логічних функцій криптографічного перетворення введемо наступні означення.

Означення 2.1. Елементарна функція – це функція криптографічного перетворення множини вхідних значень в одне вихідне значення.

Інакше, кожна елементарна функція відображає правило-залежність перетвореного значення розряду від всіх N початкових значень розрядів інформації [13, 52].

Елементарні функції:

$$f_1^{(1)}(x_1, x_2, \ldots, x_N),$$

$$f_2^{(2)}(x_1, x_2, \ldots, x_N),$$

$$f_m^{(N)}(x_1, x_2, \ldots, x_N),$$

де N – кількість розрядів інформації, що беруть участь у процесі

криптографічного перетворення, а m – це номер функції перетворення, що застосовується, $m = 1..M$, де M – загальна можлива кількість N-розрядних функцій криптографічного перетворення; $x_1, x_2, ..., x_N$ – значення першого, другого, N-го розрядів інформації відповідно.

Оскільки $x_1, x_2, x_N \in \{0;1\}$, а відповідно і значення дискретних елементарних функцій $f_1^{(1)}, f_2^{(2)}, ..., f_m^N \in \{0;1\}$.

Означення 2.2. Під композицією двох логічних операцій будемо розуміти їх послідовне виконання [9].

Означення 2.3. Криптографічна операція – це понумерований набір елементарних функцій, які в сукупності забезпечують виконання криптографічного перетворення [52].

Іншими словами, криптографічні операції є композицією відповідних елементарних функцій перетворення [19]:

$$F_{1,2,...,m} = (f_1^{(1)}, f_2^{(2)}, ..., f_m^N).$$

Криптографічні операції утворюють групу [12, 61]. Виходячи з цього, як для криптографічних операцій, так і для елементарних функцій виконується властивість суперпозиції: серед множини основних елементарних функцій можна знайти відповідні набори пар функцій таких, що $f_1^N(f_2^N(x_1, x_2, ..., x_N)) = (x_1, x_2, ..., x_N)$.

Тобто, множину основних елементарних функцій, з яких формуються криптографічні операції, можливо використовувати як для безпосередньо перетворення, так і для оберненого перетворення відповідно. Надалі будемо називати такі відповідні пари як криптографічна операція перетворення F^k та криптографічна операція оберненого перетворення F^d інформації відповідно.

Під час проведення досліджень двохрозрядних операцій криптографічного перетворення ми встановили, що операції криптографічного перетворення можуть бути поділені на групи [12, 61]:

– базова група операцій криптографічного перетворення;
– група операцій перестановки;
– група операцій інверсії.

Повний набір двохрозрядних базових операцій та операцій інверсії представлено в табл. 2.2., а операцій перестановки в табл. 2.3.

Таблиця 2.2

Повний набір базових операцій та операцій інверсії

Порядковий номер	Матричне представлення
Базові операції $\vec{F}_a\begin{pmatrix} x_1 \\ x_2 \end{pmatrix}$	
1	$\vec{F}_a\begin{pmatrix} x_1 \\ x_2 \end{pmatrix}$
2	$\vec{F}_a\begin{pmatrix} x_1 \oplus x_2 \\ x_2 \end{pmatrix}$
3	$\vec{F}_a\begin{pmatrix} x_1 \\ x_2 \oplus x_1 \end{pmatrix}$
Операції інверсії $\vec{F}_b\begin{pmatrix} b_1 \\ b_2 \end{pmatrix}$	
1	$\vec{F}_b\begin{pmatrix} b_1 \\ b_2 \end{pmatrix}$, де $b_1 = b_2 = 0$
2	$\vec{F}_b\begin{pmatrix} b_1 \\ b_2 \end{pmatrix}$, де $b_1 = b_2 = 1$
3	$\vec{F}_b\begin{pmatrix} b_1 \\ b_2 \end{pmatrix}$, де $b_1 = 1$ і $b_2 = 0$
4	$\vec{F}_b\begin{pmatrix} b_1 \\ b_2 \end{pmatrix}$, де $b_1 = 0$ і $b_2 = 1$

Для двохрозрядних операцій криптографічного перетворення базова група операцій криптографічного перетворення включає в себе три

операції, група операцій перестановки – дві операції, група операцій інверсії – чотири операції. Загальна кількість двохрозрядних операцій криптографічного перетворення буде дорівнювати 24 (добутку кількостей операцій у кожній групі).

Таблиця 2.3

Повний набір операцій перестановки

Порядковий номер	Матричне представлення	
	Базова операція $\vec{F}_a\begin{pmatrix} x_1 \\ x_2 \end{pmatrix}$	Операція перестановки $\vec{F}_p\begin{pmatrix} x_2 \\ x_1 \end{pmatrix}$
1	$\vec{F}_a\begin{pmatrix} x_1 \\ x_2 \end{pmatrix}$	$\vec{F}_p\begin{pmatrix} x_2 \\ x_1 \end{pmatrix}$
2	$\vec{F}_a\begin{pmatrix} x_1 \oplus x_2 \\ x_2 \end{pmatrix}$	$\vec{F}_p\begin{pmatrix} x_2 \\ x_2 \oplus x_1 \end{pmatrix}$
3	$\vec{F}_a\begin{pmatrix} x_1 \\ x_2 \oplus x_1 \end{pmatrix}$	$\vec{F}_p\begin{pmatrix} x_1 \oplus x_2 \\ x_1 \end{pmatrix}$

Загальна кількість операцій криптографічного перетворення утворюється поєднанням базових операцій, операцій перестановки та операцій інверсії [63]:

$$N = N_б \cdot N_n \cdot N_i, \tag{2.1}$$

де $N_б$ – кількість базових операцій, N_n – кількість операцій перестановки, N_i – кількість операцій інверсії.

Визначимо кількість базових операцій криптографічного перетворення:

$$N_б = \frac{N}{N_n \cdot N_i}.$$

Подамо отримані за результатами обчислювального експерименту в [6, 8] двохрозрядні елементарні функції згідно прийнятих нами позначень:

$$f_3 = x_1, \tag{2.2}$$

$$f_5 = x_2, \tag{2.3}$$

$$f_{12} = \bar{x}_1, \tag{2.4}$$

$$f_{10} = \bar{x}_2, \tag{2.5}$$

$$f_6 = x_1 \oplus x_2, \tag{2.6}$$

$$f_9 = x_1 \oplus x_2 \oplus 1. \tag{2.7}$$

Отримані двохрозрядні елементарні функції для криптографічного перетворення інформації мають одну спільну особливість – однакова кількість нулів та одиниць.

Виходячи з цього, можна припустити, що кількість елементарних функцій для криптографічного перетворення визначається через кількість сполучень як:

$$K_{eo} = C_{2^n}^{2^{n-1}}, \tag{2.8}$$

де n – розрядність елементарних функцій для криптографічного перетворення.

Для проведення подальших досліджень введемо наступні означення і твердження [6, 8, 52].

Означення 2.4. Вектор-функцією $\bar{F}$ будемо називати деяке перетворення двох сусідніх байтів (бітів) і позначимо $\bar{F}: \begin{pmatrix} x_1 \\ x_2 \end{pmatrix} \to \begin{pmatrix} x_1^* \\ x_2^* \end{pmatrix}$ – деяке відображення множини (повідомлення) самої на себе.

Крім того, відомо, що бінарне перетворення можна записати у вигляді системи алгебраїчних рівнянь:

$$\begin{cases} x_1^* = a_{11}x_1 \oplus a_{12}x_2 \oplus b_1, \\ x_2^* = a_{21}x_1 \oplus a_{22}x_2 \oplus b_2. \end{cases}$$

Щоб забезпечити невиродженість перетворення, накладаються обмеження: $a_{ij} = \{0; 1\}$, $b_i = \{0; 1\}$, $i = \overline{1,2}$, $j = \overline{1,2}$, $a_{11} \cdot a_{22} - a_{12} \cdot a_{21} \neq 0$.

Означення 2.5. Якщо існує хоча б один розв'язок системи лінійних рівнянь, то така система називається сумісною, в протилежному випадку – несумісною.

Означення 2.6. Сумісна система лінійних рівнянь називається визначеною, якщо вона має єдиний розв'язок, і невизначеною, якщо вона має множину розв'язків.

Означення 2.7. Системи лінійних рівнянь називають еквівалентними, якщо довільний розв'язок однієї з них є розв'язком другої, і навпаки (тобто, якщо вони мають одну і ту ж множину розв'язків).

У загальному вигляді операції криптографічного перетворення, побудовані на основі додавання за модулем два, описуються такою моделлю:

$$\vec{F} = \begin{pmatrix} a_{11}x_1 \oplus a_{12}x_2 \oplus b_1 \\ a_{21}x_1 \oplus a_{22}x_2 \oplus b_2 \end{pmatrix}, \qquad (2.9)$$

де $a_{ij} \in [0,1]$; $b_i \in [0,1]$; x_1, x_2 – операнди-розряди відповідно; $\oplus$ – операція «сума за mod 2».

Зведемо вектор-функцію до загального матричного вигляду логічної функції як добутку двох матриць, тоді одержимо [6, 8]:

$$\vec{F}\begin{pmatrix} x_1 \\ x_2 \end{pmatrix} = \begin{pmatrix} a_{11}x_1 \oplus a_{12}x_2 \oplus b_1 \\ a_{21}x_1 \oplus a_{22}x_2 \oplus b_2 \end{pmatrix} = \begin{pmatrix} a_{11}x_1 \oplus a_{12}x_2 \\ a_{21}x_1 \oplus a_{22}x_2 \end{pmatrix} * \begin{pmatrix} b_1 \\ b_2 \end{pmatrix} = \vec{F}_a \begin{pmatrix} x_1 \\ x_2 \end{pmatrix} * \vec{F}_b \begin{pmatrix} b_1 \\ b_2 \end{pmatrix}, \quad (2.10)$$

де $a_{ij} = \overline{0,1}$, $b_i = \overline{0,1}$, $\oplus -$ операція суми за модулем два.

Подання (2.10) дає можливість довести, що вектор-функція утворена з поєднання двох логічних операцій: базової логічної операції, що позначається як матриця-стовпець $\vec{F}_a \begin{pmatrix} x_1 \\ x_2 \end{pmatrix}$, та операції інверсії з позначенням як $\vec{F}_b \begin{pmatrix} b_1 \\ b_2 \end{pmatrix}$.

Подання (2.10) теоретично обґрунтовує можливість розглядати базову операцію та операцію інверсії окремо. Крім цього, додатково можна ввести дворозрядну логічну операцію перестановки. Зрозуміло, що для двох розрядів існують лише дві перестановки: $\overline{F}_p : \begin{pmatrix} x_1 \\ x_2 \end{pmatrix} \to \begin{pmatrix} x_2 \\ x_1 \end{pmatrix}$. Використовуючи матричне подання та застосовуючи перестановку відносно базової операції в поєднанні з операціями інверсії, отримаємо повний набір операцій (табл. 2.2 та табл. 2.3).

Таким чином, загальна кількість операцій, що утворюються поєднанням базової операції, операцій перестановки та інверсії, визначається як загальна кількість комбінацій таких операцій:

$$Count(\vec{F}_a, \vec{F}_p, \vec{F}_b,) = \vec{F}_a \times \vec{F}_p \times \vec{F}_b = 3 \times 2 \times 4 = 24.$$

Доведено, що дворозрядні логічні операції утворюють групу. Для цього було введено в множині криптографічних операцій бінарну алгебраїчну операцію композиції [6].

Теорема 2.1. Множина двохрозрядних криптографічних операцій утворює групу відносно операції композиції. Ця група ізоморфна групі S^4 [9].

Доведення. При композиції двох двохрозрядних криптографічних операцій відбувається послідовне переставляння елементів повідомлення, тобто виконується композиція 4-елементних перестановок. Відомо, що 4-елементні перестановки відносно операції композиції утворюють групу S^4. Таким чином, оскільки ми встановили пряму відповідність між елементами множини криптографічних операцій і елементами групи S^4, показали еквівалентність операції композиції для обох множин, то множина двохрозрядних логічних операцій відносно операції композиції ізоморфна групі S^4, а отже, і сама є групою. Теорему доведено.

А це означає, що будь-яке поєднання базових операцій, операцій перестановок та операцій інверсії теж утворюватиме групу.

За аналогією може бути доведено, що:

- множина трьохрозрядних криптографічних операцій утворює групу відносно операції композиції. Ця група ізоморфна групі S^8;
- множина чотирьох розрядних криптографічних операцій утворює групу відносно операції композиції. Ця група ізоморфна групі S^{16}, і т.д..

Виходячи з вище наведеного, можна визначити залежність кількості операцій криптографічного перетворення від їх розрядності [6]:

$$K_{on} = 2^n!. \qquad (2.11)$$

Оскільки елементарних функцій та операцій криптографічного перетворення досить багато, то базуючись лише на одно- та двохрозрядних операціях криптографічного перетворення, не можливо проводити синтез таких операцій.

Результати дослідження показали, що отримана можливість використовувати в алгоритмах потокового шифрування разом з операціями повтору та рівнозначності додатково 22 двохрозрядні операції. Під час розробки алгоритмів блокового шифрування також можливо використання всіх 24 операцій.

Подальші дослідження будуть направлені на виявлення нових операцій криптографічного перетворення. Дані дослідження також повинні базуватися на результатах обчислювального експерименту в ході розширення розрядності елементарних функцій.

2.1.2 Дослідження множини трирозрядних елементарних функцій для криптоперетворення інформації

З метою дослідження трирозрядних елементарних функцій для криптоперетворення на основі вдосконалення існуючого програмного забезпечення було проведено обчислювальний експеримент, результатом якого є 70 елементарних функцій [6, 8]. Отриманий результат підтвердив коректність гіпотези, що елементарні функції для криптоперетворення представляють собою логічні функції, в таблиці істинності яких однакова кількість нулів і одиниць.

Отримані табличні елементарні функції для криптоперетворення за допомогою методів мінімізації логічних функцій [163, 164] було формалізовано та відображено в табл. 2.4.

За результатами проведення обчислювального експерименту було отримано 40320 операцій криптографічного перетворення, які включають 70 елементарних функцій.

Результати обчислювального експерименту підтвердили коректність виразу (2.11), оскільки $K_{on} = 2^3! = 8! = 40320$.

Таблиця 2.4

Трирозрядні елементарні функції для криптографічного перетворення інформації

Основні елементарні функції					
Код функції		Опис функції	Код функції		Опис функції
00001111	15	$f_{15} = x_1$	10000111	135	$f_{135} = x_1 \cdot x_2 \vee x_1 \cdot x_3 \vee \vee \bar{x}_1 \cdot \bar{x}_2 \cdot \bar{x}_3$
00010111	23	$f_{23} = x_1 \cdot x_2 \vee x_1 \cdot x_3 \vee x_2 \cdot x_3$	10001011	139	$f_{139} = x_1 \cdot x_2 \vee \bar{x}_2 \cdot \bar{x}_3$
00011011	27	$f_{27} = x_1 \cdot \bar{x}_3 \vee x_2 \cdot x_3$	10001101	141	$f_{141} = x_1 \cdot x_3 \vee \bar{x}_2 \cdot \bar{x}_3$
00011101	29	$f_{29} = x_1 \cdot \bar{x}_2 \vee x_2 \cdot x_3$	10001110	142	$f_{142} = x_1 \cdot \bar{x}_2 \vee x_1 \cdot \bar{x}_3 \vee \bar{x}_2 \cdot \bar{x}_3$
00011110	30	$f_{30} = x_1 \cdot \bar{x}_2 \vee x_1 \cdot \bar{x}_3 \vee \vee \bar{x}_1 \cdot x_2 \cdot x_3$	10010011	147	$f_{147} = x_1 \cdot x_2 \vee x_2 \cdot \bar{x}_3 \vee \vee \bar{x}_1 \cdot \bar{x}_2 \cdot \bar{x}_3$
00100111	39	$f_{39} = x_1 \cdot x_3 \vee x_2 \cdot \bar{x}_3$	10010101	149	$f_{149} = x_1 \cdot x_3 \vee x_2 \cdot x_3 \vee \vee \bar{x}_1 \cdot \bar{x}_2 \cdot \bar{x}_3$
00101011	43	$f_{43} = x_1 \cdot x_2 \vee x_1 \cdot \bar{x}_3 \vee \vee x_2 \cdot \bar{x}_3$	10010110	150	$f_{150} = x_1 \oplus x_2 \oplus x_3 \oplus 1$
00101101	45	$f_{45} = x_1 \cdot \bar{x}_2 \vee x_1 \cdot x_3 \vee \vee \bar{x}_1 \cdot x_2 \cdot \bar{x}_3$	10011001	153	$f_{153} = \bar{x}_2 \cdot \bar{x}_3 \vee x_2 \cdot x_3$
00101110	46	$f_{46} = x_1 \cdot \bar{x}_2 \vee x_2 \cdot \bar{x}_3$	10011010	154	$f_{154} = x_1 \cdot \bar{x}_3 \vee \bar{x}_2 \cdot \bar{x}_3 \vee \vee \bar{x}_1 \cdot x_2 \cdot x_3$
00110011	51	$f_{51} = x_2$	10011100	156	$f_{156} = x_1 \cdot \bar{x}_2 \vee \bar{x}_2 \cdot \bar{x}_3 \vee \vee \bar{x}_1 \cdot x_2 \cdot x_3$
00110101	53	$f_{53} = \bar{x}_1 \cdot x_2 \vee x_1 \cdot x_3$	10100011	163	$f_{163} = x_1 \cdot x_2 \vee \bar{x}_1 \cdot \bar{x}_3$
00110110	54	$f_{54} = \bar{x}_1 \cdot x_2 \vee x_2 \cdot \bar{x}_3 \vee \vee x_1 \cdot \bar{x}_2 \cdot x_3$	10100101	165	$f_{165} = \bar{x}_1 \cdot \bar{x}_3 \vee x_1 \cdot x_3$
00111001	57	$f_{57} = \bar{x}_1 \cdot x_2 \vee x_2 \cdot x_3 \vee \vee x_1 \cdot \bar{x}_2 \cdot \bar{x}_3$	10100110	166	$f_{166} = \bar{x}_1 \cdot \bar{x}_3 \vee x_2 \cdot \bar{x}_3 \vee \vee x_1 \cdot \bar{x}_2 \cdot x_3$
00111010	58	$f_{58} = \bar{x}_1 \cdot x_2 \vee x_1 \cdot \bar{x}_3$	10101001	169	$f_{169} = \bar{x}_1 \cdot \bar{x}_3 \vee \bar{x}_2 \cdot \bar{x}_3 \vee \vee x_1 \cdot x_2 \cdot x_3$
00111100	60	$f_{60} = \bar{x}_1 \cdot x_2 \vee x_1 \cdot \bar{x}_2$	10101010	170	$f_{170} = \bar{x}_3$
01000111	71	$f_{71} = x_1 \cdot x_2 \vee \bar{x}_2 \cdot x_3$	10101100	172	$f_{172} = x_1 \cdot \bar{x}_2 \vee \bar{x}_1 \cdot \bar{x}_3$
01001011	75	$f_{75} = x_1 \cdot x_2 \vee x_1 \cdot \bar{x}_3 \vee \vee \bar{x}_1 \cdot \bar{x}_2 \cdot x_3$	10110001	177	$f_{177} = \bar{x}_1 \cdot \bar{x}_3 \vee x_2 \cdot x_3$
01001101	77	$f_{77} = x_1 \cdot \bar{x}_2 \vee x_1 \cdot x_3 \vee \vee \bar{x}_2 \cdot x_3$	10110010	178	$f_{178} = \bar{x}_1 \cdot x_2 \vee \bar{x}_1 \cdot \bar{x}_3 \vee \vee x_2 \cdot \bar{x}_3$
01001110	78	$f_{78} = x_1 \cdot \bar{x}_3 \vee \bar{x}_2 \cdot x_3$	10110100	180	$f_{180} = \bar{x}_1 \cdot x_2 \vee \bar{x}_1 \cdot \bar{x}_3 \vee \vee x_1 \cdot \bar{x}_2 \cdot \bar{x}_3$
01010011	83	$f_{83} = x_1 \cdot x_2 \vee \bar{x}_1 \cdot x_3$	10111000	184	$f_{184} = \bar{x}_1 \cdot x_2 \vee \bar{x}_2 \cdot \bar{x}_3$
01010101	85	$f_{85} = x_3$	11000011	195	$f_{195} = \bar{x}_1 \cdot \bar{x}_2 \vee x_1 \cdot x_2$
01010110	86	$f_{86} = \bar{x}_1 \cdot x_3 \vee \bar{x}_2 \cdot x_3 \vee \vee x_1 \cdot x_2 \cdot \bar{x}_3$	11000101	197	$f_{197} = \bar{x}_1 \cdot \bar{x}_2 \vee x_1 \cdot x_3$
01011001	89	$f_{89} = \bar{x}_1 \cdot x_3 \vee x_2 \cdot x_3 \vee \vee x_1 \cdot \bar{x}_2 \cdot \bar{x}_3$	11000110	198	$f_{198} = \bar{x}_1 \cdot \bar{x}_2 \vee \bar{x}_2 \cdot x_3 \vee \vee x_1 \cdot x_2 \cdot \bar{x}_3$
01011010	90	$f_{90} = \bar{x}_1 \cdot x_3 \vee x_1 \cdot \bar{x}_3$	11001001	201	$f_{201} = \bar{x}_1 \cdot \bar{x}_2 \vee \bar{x}_2 \cdot \bar{x}_3 \vee \vee x_1 \cdot x_2 \cdot \bar{x}_3$

Продовження табл. 2.4

Основні елементарні функції					
Код функції		Опис функції	Код функції		Опис функції
01011100	92	$f_{92} = x_1 \cdot \bar{x}_2 \vee \bar{x}_1 \cdot x_3$	11001010	202	$f_{202} = \bar{x}_1 \cdot \bar{x}_2 \vee x_1 \cdot \bar{x}_3$
01100011	99	$f_{99} = x_1 \cdot x_2 \vee x_2 \cdot \bar{x}_3 \vee \vee \bar{x}_1 \cdot \bar{x}_2 \cdot x_3$	11001100	204	$f_{204} = \bar{x}_2$
01100101	101	$f_{101} = x_1 \cdot x_3 \vee \bar{x}_2 \cdot x_3 \vee \vee \bar{x}_1 \cdot x_2 \cdot \bar{x}_3$	11010001	209	$f_{209} = \bar{x}_1 \cdot \bar{x}_2 \vee x_2 \cdot x_3$
01100110	102	$f_{102} = \bar{x}_2 \cdot x_3 \vee x_2 \cdot \bar{x}_3$	11010010	210	$f_{210} = \bar{x}_1 \cdot \bar{x}_2 \vee \bar{x}_1 \cdot x_3 \vee \vee x_1 \cdot x_2 \cdot \bar{x}_3$
01101010	106	$f_{106} = x_1 \cdot \bar{x}_3 \vee x_2 \cdot \bar{x}_3 \vee \vee \bar{x}_1 \cdot \bar{x}_2 \cdot x_3$	11010100	212	$f_{212} = \bar{x}_1 \cdot \bar{x}_2 \vee \bar{x}_1 \cdot x_3 \vee \bar{x}_2 \cdot x_3$
01101100	108	$f_{108} = x_1 \cdot \bar{x}_2 \vee \bar{x}_2 \cdot x_3 \vee \vee \bar{x}_1 \cdot x_2 \cdot \bar{x}_3$	11011000	216	$f_{216} = \bar{x}_1 \cdot x_3 \vee \bar{x}_2 \cdot \bar{x}_3$
01101001	105	$f_{105} = x_1 \oplus x_2 \oplus x_3$	11100001	225	$f_{225} = \bar{x}_1 \cdot \bar{x}_2 \vee \bar{x}_1 \cdot \bar{x}_3 \vee \vee x_1 \cdot x_2 \cdot x_3$
01110001	113	$f_{113} = \bar{x}_1 \cdot x_2 \vee \bar{x}_1 \cdot x_3 \vee \vee x_2 \cdot x_3$	11100010	226	$f_{226} = \bar{x}_1 \cdot \bar{x}_2 \vee x_2 \cdot \bar{x}_3$
01110010	114	$f_{114} = \bar{x}_1 \cdot x_3 \vee x_2 \cdot \bar{x}_3$	11100100	228	$f_{228} = \bar{x}_1 \cdot \bar{x}_3 \vee \bar{x}_2 \cdot x_3$
01110100	116	$f_{116} = \bar{x}_1 \cdot x_2 \vee \bar{x}_2 \cdot x_3$	11101000	232	$f_{232} = \bar{x}_1 \cdot \bar{x}_2 \vee \bar{x}_1 \cdot \bar{x}_3 \vee \bar{x}_2 \cdot \bar{x}_3$
01111000	120	$f_{120} = \bar{x}_1 \cdot x_2 \vee \bar{x}_1 \cdot x_3 \vee \vee x_1 \cdot \bar{x}_2 \cdot \bar{x}_3$	11110000	240	$f_{240} = \bar{x}_1$

Запропонований підхід поділу операцій на базову групу операцій криптографічного перетворення, групу операцій перестановки та групу операцій інверсії (2.1) дозволяє зменшити кількість операцій, які потрібно дослідити, в 48 разів, оскільки для трирозрядних операцій криптографічного перетворення група операцій перестановки становитиме 3! = 6, а група операцій інверсії становитиме $2^3 = 8$.

Виходячи з (2.1), кількість трьохрозрядних базових операцій криптографічного перетворення становить $N_б = \frac{40320}{31 \cdot 2^3} = 840$. Тому постає задача виокремлення групи елементарних функцій та, як наслідок, групи операцій криптографічного перетворення для подальших досліджень.

Під час проведення досліджень на наступному етапі обмежимося операціями криптографічного перетворення, що побудовані на основі додавання за модулем два.

За аналогією з (2.9) у загальному вигляді операції криптографічного перетворення, що побудовані на основі додавання за модулем два, описуються такою моделлю:

$$\vec{F} = \begin{pmatrix} a_{11}x_1 \oplus a_{12}x_2 \oplus ... \oplus a_{1n}x_n \oplus b_1 \\ a_{21}x_1 \oplus a_{22}x_2 \oplus ... \oplus a_{2n}x_n \oplus b_2 \\ . \quad . \quad . \quad . \quad . \quad . \quad . \quad . \quad . \quad . \quad . \\ a_{n1}x_1 \oplus a_{n2}x_2 \oplus ... \oplus a_{n\,n}x_n \oplus b_n \end{pmatrix}, \tag{2.11}$$

де $a_{ij} \in [0,1]$; $b_i \in [0,1]$; $x_1 ... x_n$ – операнди-розряди відповідно; $\oplus$ – операція «сума за mod 2».

У [16, 64] доведено, що для синтезу трирозрядних операцій криптографічного перетворення на основі моделі (2.11), можуть використовуватися такі елементарні логічні операції:

$$f_{15} = x_1, \tag{2.12}$$

$$f_{51} = x_2, \tag{2.13}$$

$$f_{85} = x_3, \tag{2.14}$$

$$f_{60} = \bar{x}_1 \cdot x_2 \vee x_1 \cdot \bar{x}_2 = x_1 \oplus x_2, \tag{2.15}$$

$$f_{90} = \bar{x}_1 \cdot x_3 \vee x_1 \cdot \bar{x}_3 = x_1 \oplus x_3, \tag{2.16}$$

$$f_{102} = \bar{x}_2 \cdot x_3 \vee x_2 \cdot \bar{x}_3 = x_2 \oplus x_3, \tag{2.17}$$

$$f_{105} = x_1 \oplus x_2 \oplus x_3, \tag{2.18}$$

$$f_{240} = \bar{x}_1,$$

$$f_{204} = \bar{x}_2,$$

$$f_{170} = \bar{x}_3,$$

$$f_{195} = \bar{x}_1 \cdot \bar{x}_2 \vee x_1 \cdot x_2 = x_1 \oplus x_2 \oplus 1,$$

$$f_{165} = \bar{x}_1 \cdot \bar{x}_3 \vee x_1 \cdot x_3 = x_1 \oplus x_3 \oplus 1,$$

$$f_{153} = \bar{x}_2 \cdot \bar{x}_3 \vee x_2 \cdot x_3 = x_2 \oplus x_3 \oplus 1,$$

$$f_{150} = x_1 \oplus x_2 \oplus x_3 \oplus 1.$$

Під час проведення дослідження обмежимося лише групою базових операцій та групою операцій перестановок. Серед 14 елементарних логічних операцій виберемо сім прямих елементарних логічних операцій, які представлені виразами (2.12–2.18).

Відповідно до нашого обмеження матриця криптографічного перетворення, побудована на основі додавання за модулем два, описуватиметься моделлю [16]:

$$\vec{F} = \begin{pmatrix} a_{11}x_1 \oplus a_{12}x_2 \oplus \ldots \oplus a_{1n}x_n \\ a_{21}x_1 \oplus a_{22}x_2 \oplus \ldots \oplus a_{2n}x_n \\ . \quad . \quad . \quad . \quad . \quad . \quad . \quad . \quad . \\ a_{n1}x_1 \oplus a_{n2}x_2 \oplus \ldots \oplus a_{n\,n}x_n \end{pmatrix} . \qquad (2.19)$$

Дослідимо трирозрядні операції криптографічного перетворення, побудовані на основі додавання за модулем два, та розширимо отримані результати на довільну кількість розрядів.

За результатами обчислювального експерименту кількість операцій криптографічного перетворення, що побудовані на основі моделі (2.19), становить 168 операцій.

Визначимо кількість трирозрядних базових операцій криптографічного перетворення. Оскільки для трирозрядних $N_i = 2^3$, а $N_n = 3!$, то враховуючи, що $N = N_б \cdot N_n \cdot N_i = N_б \cdot 3! \cdot 2^3 = 1344$, отримаємо $N_б = 28$.

Під час проведення подальших досліджень необхідно побудувати 28 базових операцій криптографічного перетворення.

Оскільки вираз (2.11) представляє собою матрицю, то отримані на його основі операції криптоперетворення будемо називати матричними операціями криптографічного перетворення.

2.1.3 Розробка методів синтезу матричних операцій криптографічного перетворення

Для синтезу дворозрядних операцій криптографічного перетворення було використано операцію заміщення [52, 53], на основі якої розроблено метод синтезу базових операцій криптографічного перетворення на основі заміщення. За аналогією з алгоритмом реалізації методу синтезу базових операцій криптографічного перетворення на основі заміщення [16] виберемо операцію повторення інформації (нульову операцію) [53]. Дана операція має подання:

$$F^{k}_{15,51,85} = F^{d}_{15,51,85} = (f^{1}_{15},\ f^{2}_{51},\ f^{3}_{85}) = \begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix} . \qquad (2.20)$$

Здійснюючи синтез базових операцій, кожній отриманій операції криптографічного перетворення наведемо відповідну їй операцію оберненого криптографічного перетворення, що буде необхідно для розробки методу синтезу операцій оберненого криптографічного перетворення [53].

Під час реалізації заміни необхідно враховувати збереження інформативності при виконанні операції криптографічного перетворення. Так, елементарна функція $f_{60} = x_1 \oplus x_2$ може заміняти $f_{15} = x_1$ та $f_{51} = x_2$, а елементарну функцію $f_{85} = x_3$ заміняти не може, інакше має місце випадок, коли при перетворенні втрачається значення x_3, чого допустити ні в якому разі не можна.

Провівши заміну елементарних функцій в операції (2.20) однією з елементарних функцій (2.15)–(2.18), отримаємо [53]:

$$F^k_{60,51,85} = F^d_{60,51,85} = (f^1_{60},\ f^2_{51},\ f^3_{85}) = \begin{pmatrix} x_1 \oplus x_2 \\ x_2 \\ x_3 \end{pmatrix}; \tag{2.21}$$

$$F^k_{15,60,85} = F^d_{15,60,85} = (f^1_{15},\ f^2_{60},\ f^3_{85}) = \begin{pmatrix} x_1 \\ x_1 \oplus x_2 \\ x_3 \end{pmatrix}; \tag{2.22}$$

$$F^k_{90,51,85} = F^d_{90,51,85} = (f^1_{90},\ f^2_{51},\ f^3_{85}) = \begin{pmatrix} x_1 \oplus x_3 \\ x_2 \\ x_3 \end{pmatrix}; \tag{2.23}$$

$$F^k_{15,51,90} = F^d_{15,51,90} = (f^1_{15},\ f^2_{51},\ f^3_{90}) = \begin{pmatrix} x_1 \\ x_2 \\ x_1 \oplus x_3 \end{pmatrix}; \tag{2.24}$$

$$F^k_{15,102,85} = F^d_{15,102,85} = (f^1_{15},\ f^2_{102},\ f^3_{85}) = \begin{pmatrix} x_1 \\ x_2 \oplus x_3 \\ x_3 \end{pmatrix}; \tag{2.25}$$

$$F^k_{15,51,102} = F^d_{15,51,102} = (f^1_{15},\ f^2_{51},\ f^3_{102}) = \begin{pmatrix} x_1 \\ x_2 \\ x_2 \oplus x_3 \end{pmatrix}; \tag{2.26}$$

$$F^k_{105,51,85} = F^d_{105,51,85} = (f^1_{105},\ f^2_{51},\ f^3_{85}) = \begin{pmatrix} x_1 \oplus x_2 \oplus x_3 \\ x_2 \\ x_3 \end{pmatrix}; \tag{2.27}$$

$$F^k_{15,105,85} = F^d_{15,105,85} = (f^1_{15},\ f^2_{105},\ f^3_{85}) = \begin{pmatrix} x_1 \\ x_1 \oplus x_2 \oplus x_3 \\ x_3 \end{pmatrix}; \tag{2.28}$$

$$F^k_{15,51,105} = F^d_{15,51,105} = (f^1_{15},\ f^2_{51},\ f^3_{105}) = \begin{pmatrix} x_1 \\ x_2 \\ x_1 \oplus x_2 \oplus x_3 \end{pmatrix}. \tag{2.29}$$

Провівши заміну двох елементарних функцій в операції (2.20) двома елементарними функціями (2.15)–(2.18) та вилучивши з базових операцій поєднання базових операцій та операцій перестановки, отримаємо [53]:

$$F^k_{15,60,105} = \begin{pmatrix} x_1 \\ x_1 \oplus x_2 \\ x_1 \oplus x_2 \oplus x_3 \end{pmatrix} \qquad F^d_{15,60,102} = \begin{pmatrix} x_1 \\ x_1 \oplus x_2 \\ x_2 \oplus x_3 \end{pmatrix}, \tag{2.30}$$

$$F^k_{15,90,105} = \begin{pmatrix} x_1 \\ x_1 \oplus x_3 \\ x_1 \oplus x_2 \oplus x_3 \end{pmatrix} \qquad F^d_{15,102,60} = \begin{pmatrix} x_1 \\ x_2 \oplus x_3 \\ x_1 \oplus x_2 \end{pmatrix}, \tag{2.31}$$

$$F^k_{105,51,60} = \begin{pmatrix} x_1 \oplus x_2 \oplus x_3 \\ x_2 \\ x_1 \oplus x_2 \end{pmatrix} \qquad F^d_{102,51,90} = \begin{pmatrix} x_2 \oplus x_3 \\ x_2 \\ x_1 \oplus x_3 \end{pmatrix}, \tag{2.32}$$

$$F^k_{105,51,102}=\begin{pmatrix} x_1\oplus x_2\oplus x_3\\ x_2\\ x_2\oplus x_3\end{pmatrix}\qquad F^d_{90,51,102}=\begin{pmatrix} x_1\oplus x_3\\ x_2\\ x_2\oplus x_3\end{pmatrix}, \tag{2.33}$$

$$F^k_{105,102,85}=\begin{pmatrix} x_1\oplus x_2\oplus x_3\\ x_2\oplus x_3\\ x_3\end{pmatrix}\qquad F^d_{60,102,85}=\begin{pmatrix} x_1\oplus x_2\\ x_2\oplus x_3\\ x_3\end{pmatrix}, \tag{2.34}$$

$$F^k_{105,90,85}=\begin{pmatrix} x_1\oplus x_2\oplus x_3\\ x_1\oplus x_3\\ x_3\end{pmatrix}\qquad F^d_{102,60,85}=\begin{pmatrix} x_2\oplus x_3\\ x_1\oplus x_2\\ x_3\end{pmatrix}, \tag{2.35}$$

$$F^k_{15,60,102}=\begin{pmatrix} x_1\\ x_1\oplus x_2\\ x_2\oplus x_3\end{pmatrix}\qquad F^d_{15,60,105}=\begin{pmatrix} x_1;\\ x_1\oplus x_2\\ x_1\oplus x_2\oplus x_3\end{pmatrix}, \tag{2.36}$$

$$F^k_{15,102,90}=\begin{pmatrix} x_1\\ x_2\oplus x_3\\ x_1\oplus x_3\end{pmatrix}\qquad F^d_{15,105,90}=\begin{pmatrix} x_1\\ x_1\oplus x_2\oplus x_3\\ x_1\oplus x_3\end{pmatrix}, \tag{2.37}$$

$$F^k_{15,60,90}=F^d_{15,60,90}=\begin{pmatrix} x_1\\ x_1\oplus x_2\\ x_1\oplus x_3\end{pmatrix}, \tag{2.38}$$

$$F^k_{60,51,102}=\begin{pmatrix} x_1\oplus x_2\\ x_2\\ x_2\oplus x_3\end{pmatrix}\qquad F^d_{60,51,105}=\begin{pmatrix} x_1\oplus x_2\\ x_2\\ x_1\oplus x_2\oplus x_3\end{pmatrix}, \tag{2.39}$$

$$F^k_{90,51,102}=\begin{pmatrix} x_1\oplus x_3\\ x_2\\ x_2\oplus x_3\end{pmatrix}\qquad F^d_{105,51,102}=\begin{pmatrix} x_1\oplus x_2\oplus x_3\\ x_2\\ x_2\oplus x_3\end{pmatrix}, \tag{2.40}$$

$$F^k_{60,51,90}=\begin{pmatrix} x_1\oplus x_2\\ x_2\\ x_1\oplus x_3\end{pmatrix}\qquad F^d_{60,51,105}=\begin{pmatrix} x_1\oplus x_2\\ x_2\\ x_1\oplus x_2\oplus x_3\end{pmatrix}, \tag{2.41}$$

$$F^k_{60,102,85}=\begin{pmatrix} x_1\oplus x_2\\ x_2\oplus x_3\\ x_3\end{pmatrix}\qquad F^k_{105,102,85}=\begin{pmatrix} x_1\oplus x_2\oplus x_3\\ x_2\oplus x_3\\ x_3\end{pmatrix}, \tag{2.42}$$

$$F^k_{90,102,85}=F^k_{90,102,85}=\begin{pmatrix} x_1\oplus x_3\\ x_2\oplus x_3\\ x_3\end{pmatrix}, \tag{2.43}$$

$$F^k_{90,60,85}=\begin{pmatrix} x_1\oplus x_3\\ x_1\oplus x_2\\ x_3\end{pmatrix}\qquad F^d_{90,105,85}=\begin{pmatrix} x_1\oplus x_3\\ x_1\oplus x_2\oplus x_3\\ x_3\end{pmatrix}. \tag{2.44}$$

Провівши заміну трьох елементарних функцій в операції (2.20) трьома елементарними функціями (2.15)–(2.18) та вилучивши з базових операцій

поєднання базових операцій та операцій перестановки, отримаємо [53]:

$$F^{k}_{90,60,105}=\begin{pmatrix} x_1 \oplus x_3 \\ x_1 \oplus x_2 \\ x_1 \oplus x_2 \oplus x_3 \end{pmatrix} \quad F^{d}_{105,90,102}=\begin{pmatrix} x_1 \oplus x_2 \oplus x_3 \\ x_1 \oplus x_3 \\ x_2 \oplus x_3 \end{pmatrix}, \tag{2.45}$$

$$F^{k}_{90,102,105}=\begin{pmatrix} x_1 \oplus x_3 \\ x_2 \oplus x_3 \\ x_1 \oplus x_2 \oplus x_3 \end{pmatrix} \quad F^{d}_{102,90,105}=\begin{pmatrix} x_2 \oplus x_3 \\ x_1 \oplus x_3 \\ x_1 \oplus x_2 \oplus x_3 \end{pmatrix}, \tag{2.46}$$

$$F^{k}_{60,102,105}=\begin{pmatrix} x_1 \oplus x_2 \\ x_2 \oplus x_3 \\ x_1 \oplus x_2 \oplus x_3 \end{pmatrix} \quad F^{d}_{102,105,90}=\begin{pmatrix} x_2 \oplus x_3 \\ x_1 \oplus x_2 \oplus x_3 \\ x_1 \oplus x_3 \end{pmatrix}. \tag{2.47}$$

У результаті заміни однієї, двох або трьох елементарних функцій в операції (2.20) функціями (2.15)–(2.18) та, вилучивши з базових операцій поєднання базових операцій та операцій перестановки, ми отримали всі 28 базових операцій.

У результаті проведеного дослідження можна сформулювати метод синтезу операцій криптографічного перетворення на основі додавання за модулем два, який полягає в наступному [53]:

1. в операції повтору інформації заміною однієї або декількох елементарних функцій отримати розширену базову групу операцій криптографічного перетворення;
2. вибракувавши з розширеної групи базових операцій поєднання базових операцій та операцій перестановки, отримати базову групу операцій криптографічного перетворення;
3. виконавши над кожною операцією базової групи операції перестановки елементарних функцій, отримати групу операцій заміщення та перестановки;
4. виконавши над кожною операцією групи операцій заміщення та перестановки операції інверсії елементарних функцій, отримати повну групу операцій криптографічного перетворення на основі додавання за модулем два.

За результатами обчислювального експерименту група операцій заміщення та перестановки, а також група операцій криптографічного перетворення на основі додавання за модулем два є математичними групами операцій [53].

2.1.4 Аналіз способів запису елементарних функцій та криптографічних операцій

Оскільки логічні функції мають різноманітні способи запису, то й криптографічні операції теж можна подавати по-різному. Розглянемо основні способи запису трьохрозрядних криптографічних операцій [17].

Наведемо деякі можливі способи запису основних елементарних функцій та криптографічних операцій на основі них.

Деякі з основних елементарних функцій наведені нижче в дискретному представленні [17]:

1. 00011110 (30) – $f_{30} = x_1 \cdot \bar{x}_3 \vee x_1 \cdot \bar{x}_2 \vee \bar{x}_1 \cdot x_2 \cdot x_3$;
2. 00101101 (45) – $f_{45} = x_1 \cdot \bar{x}_2 \vee x_1 \cdot x_3 \vee \bar{x}_1 \cdot x_2 \cdot \bar{x}_3$;
3. 00110110 (54) – $f_{54} = \bar{x}_1 \cdot x_2 \vee x_2 \cdot \bar{x}_3 \vee x_1 \cdot \bar{x}_2 \cdot x_3$;
4. 00111001 (57) – $f_{57} = \bar{x}_1 \cdot x_2 \vee x_2 \cdot x_3 \vee x_1 \cdot \bar{x}_2 \cdot \bar{x}_3$;
5. 01001011 (75) – $f_{57} = x_1 \cdot x_2 \vee x_1 \cdot \bar{x}_3 \vee \bar{x}_1 \cdot \bar{x}_2 \cdot x_3$;
6. 01010110 (86) – $f_{86} = \bar{x}_1 \cdot x_3 \vee \bar{x}_2 \cdot \bar{x}_3 \vee x_1 \cdot x_2 \cdot \bar{x}_3$;
7. 00111001 (106) – $f_{106} = x_1 \cdot \bar{x}_3 \vee x_2 \cdot \bar{x}_3 \vee \bar{x}_1 \cdot \bar{x}_2 \cdot x_3$.

На основі даних функцій будуються операції прямого та оберненого перетворення інформації. Наприклад:

$$F^k_{30,57,106} = (f^{(1)}_{30}, f^{(2)}_{57}, f^{(3)}_{106}) \quad \Rightarrow \quad F^d_{45,54,106} = (f^{(1)}_{45}, f^{(2)}_{54}, f^{(3)}_{106})$$

$$F^k_{30,89,108} = (f^{(1)}_{30}, f^{(2)}_{89}, f^{(3)}_{108}) \quad \Rightarrow \quad F^d_{45,106,54} = (f^{(1)}_{45}, f^{(2)}_{106}, f^{(3)}_{54})$$

Якщо розписати кожну основну елементарну функцію, то отримаємо розширене дискретне представлення криптографічних операцій, що матиме вигляд [17]:

– операція прямого перетворення $F^{k}_{30,57,106} = \begin{pmatrix} x_1 \cdot \bar{x}_3 \vee x_1 \cdot \bar{x}_2 \vee \bar{x}_1 \cdot x_2 \cdot x_3, \\ \bar{x}_1 \cdot x_2 \vee x_2 \cdot x_3 \vee x_1 \cdot \bar{x}_2 \cdot \bar{x}_3, \\ x_1 \cdot \bar{x}_3 \vee x_2 \cdot \bar{x}_3 \vee \bar{x}_1 \cdot \bar{x}_2 \cdot x_3 \end{pmatrix}$;

– операція оберненого перетворення $F^{d}_{45,54,106} = \begin{pmatrix} x_1 \cdot \bar{x}_2 \vee x_1 \cdot x_3 \vee \bar{x}_1 \cdot x_2 \cdot \bar{x}_3, \\ \bar{x}_1 \cdot x_2 \vee x_2 \cdot \bar{x}_3 \vee x_1 \cdot \bar{x}_2 \cdot x_3, \\ x_1 \cdot \bar{x}_3 \vee x_2 \cdot \bar{x}_3 \vee \bar{x}_1 \cdot \bar{x}_2 \cdot x_3 \end{pmatrix}$.

Для проведення досліджень може бути доцільним використання різних способів запису криптографічних операцій.

Наведемо деякі можливі способи запису основних елементарних функцій та криптографічних операцій на основі них.

За допомогою повної системи булевих функцій $\langle \wedge, \oplus, 1 \rangle$ можливо побудувати функції у вигляді полінома Жегалкіна [17]:

$$P(X_1 \ldots X_n) = a \oplus a_1 X_1 \oplus a_2 X_2 \oplus \ldots \oplus a_n X_n \oplus a_{12} X_1 X_2 \oplus a_{13} X_1 X_3 \oplus \ldots \oplus a_{1..n} X_1 \ldots X_n,$$
$$a \ldots a_{1..n} \in \{0,1\}.$$

Для цього потрібно використати еквівалентні перетворення ДНФ. У порівнянні з ДНФ в поліномі Жегалкіна відсутні операції «АБО» та «ЗАПЕРЕЧЕННЯ». Таким чином, поліном Жегалкіна можна отримати із ДНФ, записавши операції «АБО» та «ЗАПЕРЕЧЕННЯ» через операції «ВИКЛЮЧНЕ АБО», «І» та константу 1. Для цього застосовують наступні відношення [140]:

$$A \vee B = A \oplus B \oplus AB;$$
$$\bar{A} = A \oplus 1.$$

Наведемо приклад перетворення ДНФ в поліном Жегалкіна [166]:

$$XY \vee \bar{X}\bar{Y} = XY \oplus \bar{X}\bar{Y} \oplus XY\bar{X}\bar{Y} = XY \oplus \bar{X}\bar{Y} = XY \oplus (X \oplus 1)(Y \oplus 1) = XY \oplus XY \oplus X \oplus Y \oplus 1 = X \oplus Y \oplus 1.$$

При перетвореннях використані відношення [166]:

$$A \oplus A = 0;$$
$$(A \oplus B)C = AC \oplus BC.$$

Отримані нами основні елементарні функції теж можуть мати подання поліномами Жегалкіна:

– 00011110 (30) – $f_{30} = x_1 \oplus x_2 \cdot x_3$;

– 00111001 (57) – $f_{57} = x_1 \oplus x_2 \oplus x_1 \cdot x_3$;

– 00111001 (106) – $f_{106} = x_1 \oplus x_2 \oplus x_3 \oplus x_1 \cdot x_2$;

– 00101101 (45) – $f_{45} = x_1 \oplus x_2 \oplus x_2 \cdot x_3$;

– 00110110 (54) – $f_{54} = x_2 \oplus x_1 \cdot x_3$.

Тоді можна записати і подання криптографічних операцій поліномами Жегалкіна, яке набуде наступного виду [17]:

– операція прямого перетворення $F^k_{30,57,106} = \begin{cases} x_1 \oplus x_2 \cdot x_3 \\ x_1 \oplus x_2 \oplus x_1 \cdot x_3 \\ x_1 \oplus x_2 \oplus x_3 \oplus x_1 \cdot x_2 \end{cases}$;

– операція оберненого перетворення $F^d_{45,54,106} = \begin{pmatrix} x_1 \oplus x_2 \oplus x_2 \cdot x_3, \\ x_2 \oplus x_1 \cdot x_3, \\ x_1 \oplus x_2 \oplus x_3 \oplus x_1 \cdot x_2 \end{pmatrix}$.

Інше поліноміальне подання основних елементарних функцій у базисі $\langle \wedge, \oplus, HE \rangle$ матиме вигляд [17]:

– 00011110 (30) – $f_{30} = x_1 \oplus (x_2 \cdot x_3)$;

– 00111001 (57) – $f_{57} = x_2 \oplus (x_1 \cdot \bar{x}_3)$;

– 00111001 (106) – $f_{106} = x_3 \oplus (\bar{x}_1 \cdot \bar{x}_2) \oplus 1$;

– 00101101 (45) – $f_{45} = x_1 \oplus (x_2 \cdot \bar{x}_3)$;

– 00110110 (54) – $f_{54} = x_2 \oplus (x_1 \cdot x_3)$.

Відповідно подання криптографічних операцій:

– операція прямого перетворення $F^{k}_{30,57,106} = \begin{pmatrix} x_1 \oplus (x_2 \cdot x_3), \\ x_2 \oplus (x_1 \cdot \bar{x}_3), \\ x_3 \oplus (\bar{x}_1 \cdot \bar{x}_2) \oplus 1 \end{pmatrix}$;

– операція оберненого перетворення $F^{d}_{45,54,106} = \begin{pmatrix} x_1 \oplus (x_2 \cdot \bar{x}_3), \\ x_2 \oplus (x_1 \cdot x_3), \\ x_3 \oplus (\bar{x}_1 \cdot \bar{x}_2) \oplus 1 \end{pmatrix}$.

Крім цього, від поліноміального подання можливо перейти до дискретно-алгебраїчного подання основних елементарних функцій [17]:

– 00011110 (30) – $f_{30} = \begin{cases} x_1, \ якщо \ x_2 \cdot x_3 = 0 \\ \bar{x}_1, \ якщо \ x_2 \cdot x_3 = 1 \end{cases}$;

– 00111001 (57) – $f_{57} = \begin{cases} x_2, \ якщо \ x_1 \cdot \bar{x}_3 = 0 \\ \bar{x}_2, \ якщо \ x_1 \cdot \bar{x}_3 = 1 \end{cases}$;.

– 00111001 (106) –. $f_{106} = \begin{cases} \bar{x}_3, \ якщо \ \bar{x}_1 \cdot \bar{x}_2 = 0 \\ x_3, \ якщо \ \bar{x}_1 \cdot \bar{x}_2 = 1 \end{cases}$;

– 00101101 (45) – $f_{45} = \begin{cases} x_1, \ якщо \ x_2 \cdot \bar{x}_3 = 0 \\ \bar{x}_1, \ якщо \ x_2 \cdot \bar{x}_3 = 1 \end{cases}$;

– 00110110 (54) – $f_{54} = \begin{cases} x_2, \ якщо \ x_1 \cdot x_3 = 0 \\ \bar{x}_2, \ якщо \ x_1 \cdot x_3 = 1 \end{cases}$.

Тоді представлення криптографічних операцій запишеться як вектор-система:

$$F^{k}_{30,57,106} = \begin{pmatrix} \begin{cases} x_1, \ якщо \ x_2 \cdot x_3 = 0 \\ \bar{x}_1, \ якщо \ x_2 \cdot x_3 = 1 \end{cases}, \\ \begin{cases} x_2, \ якщо \ x_1 \cdot \bar{x}_3 = 0 \\ \bar{x}_2, \ якщо \ x_1 \cdot \bar{x}_3 = 1 \end{cases}, \\ \begin{cases} \bar{x}_3, \ якщо \ \bar{x}_1 \cdot \bar{x}_2 = 0 \\ x_3, \ якщо \ \bar{x}_1 \cdot \bar{x}_2 = 1 \end{cases} \end{pmatrix},$$

$$F^{d}_{45,54,106} = \begin{pmatrix} \begin{cases} x_1, \ якщо \ x_2 \cdot \bar{x}_3 = 0 \\ \bar{x}_1, \ якщо \ x_2 \cdot \bar{x}_3 = 1 \end{cases}, \\ \begin{cases} x_2, \ якщо \ x_1 \cdot x_3 = 0 \\ \bar{x}_2, \ якщо \ x_1 \cdot x_3 = 1 \end{cases}, \\ \begin{cases} \bar{x}_3, \ якщо \ \bar{x}_1 \cdot \bar{x}_2 = 0 \\ x_3, \ якщо \ \bar{x}_1 \cdot \bar{x}_2 = 1 \end{cases} \end{pmatrix}.$$

Наведене дискретно-алгебраїчне подання основних елементарних функцій [17] можна трактувати по-іншому, а саме:

– 00011110 (30) – $f_{30} = \begin{cases} x_2 \cdot x_3, & якщо \ \ x_1 = 0 \\ \overline{x_2 \cdot x_3}, & якщо \ \ x_1 = 1 \end{cases}$;

– 00111001 (57) – $f_{57} = \begin{cases} x_1 \cdot \bar{x}_3, & якщо \ \ x_2 = 0 \\ \overline{x_1 \cdot \bar{x}_3}, & якщо \ \ x_2 = 1 \end{cases}$;

– 00111001 (106) –. $f_{106} = \begin{cases} \bar{x}_1 \cdot \bar{x}_2, якщо \ \ x_3 = 0 \\ \overline{\bar{x}_1 \cdot \bar{x}_2}, & якщо \ \ x_3 = 1 \end{cases}$;

– 00101101 (45) – $f_{45} = \begin{cases} x_2 \cdot \bar{x}_3, & якщо \ \ x_1 = 0 \\ \overline{x_2 \cdot \bar{x}_3}, & якщо \ \ x_1 = 1 \end{cases}$;

– 00110110 (54) – $f_{54} = \begin{cases} x_1 \cdot x_3, & якщо \ \ x_2 = 0 \\ \overline{x_1 \cdot x_3}, & якщо \ \ x_2 = 1 \end{cases}$.

Звідси подання криптографічних операцій прямого та оберненого перетворення відповідно:

$$F^{k}_{30,57,106} = \left(\begin{cases} \underline{x_2 \cdot x_3}, якщо \ \ x_1 = 0 \\ x_2 \cdot x_3, \ \ якщо \ \ x_1 = 1 \end{cases}; \begin{cases} \underline{x_1 \cdot \bar{x}_3}, \ \ якщо \ \ x_2 = 0 \\ x_1 \cdot \bar{x}_3, якщо \ \ x_2 = 1 \end{cases}; \begin{cases} \underline{\bar{x}_1 \cdot \bar{x}_2}, \ \ якщо \ \ x_3 = 0 \\ \bar{x}_1 \cdot \bar{x}_2, \ \ якщо \ \ x_3 = 1 \end{cases} \right),$$

$$F^{d}_{45,54,106} = \left(\begin{cases} \underline{x_2 \cdot \bar{x}_3}, \ \ якщо \ \ x_1 = 0 \\ x_2 \cdot \bar{x}_3, \ \ якщо \ \ x_1 = 1 \end{cases}; \begin{cases} \underline{x_1 \cdot x_3}, \ \ якщо \ \ x_2 = 0 \\ x_1 \cdot x_3, \ \ якщо \ \ x_2 = 1 \end{cases}; \begin{cases} \underline{\bar{x}_1 \cdot \bar{x}_2}, \ \ якщо \ \ x_3 = 0 \\ \bar{x}_1 \cdot \bar{x}_2, \ \ якщо \ \ x_3 = 1 \end{cases} \right).$$

Наведені подання криптографічних операцій у перспективі дають можливість зрозуміти логіку роботи дискретних пристроїв перетворення інформації на основі криптографічних операцій. А представлені способи запису дозволяють виокремити структурні блоки для реалізації схемотехнічних рішень синтезованих криптографічних операцій.

У результаті дослідження способів запису криптографічних операцій перетворення інформації було встановлено, що всі способи запису мають право на існування і використовуються відповідно до задач дослідження [17].

Завдяки представленим різним способам запису криптографічних операцій перетворення інформації виникла можливість побудови різноваріантних дискретних пристроїв на основі однотипних схемотехнічних конструкцій, що в подальшому дозволяє контролювати та обмежувати складність пристроїв.

На основі отриманих результатів можна зробити висновок, що кожному способу запису можна поставити у відповідність структурні блоки, що реалізують логічні перетворення над даними за правилом описаним криптографічними операціями.

Використання запропонованих способів запису операцій криптоперетворення дає змогу спростити процеси синтезу та дослідження базових операцій [17, 53]. Наприклад, у методі синтезу матричних операцій криптоперетворення синтез базових операцій проводиться на першому та другому етапах. З них найбільш трудомістким є другий етап, оскільки вимагає проведення скорочення розширеної групи базових операцій на основі видалення поєднання базових операцій та операцій перестановки.

Запис операцій криптографічного перетворення в дискретно-алгебраїчному поданні дає змогу виявити явні логічні залежності між значеннями розрядів інформації, що беруть участь у процесі криптографічного перетворення інформації [16, 17].

Крім цього, дискретно-алгебраїчне подання операцій криптографічного перетворення дає змогу уникнути інваріантності побудови базової групи операцій криптографічного перетворення інформації, що дає можливість зменшити кількість етапів та спростити складність реалізації методу синтезу матричних операцій криптоперетворення [53].

Наведемо фрагменти синтезу базових операцій:

$$F^{k}_{15,51,85}=\begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix};\qquad F^{d}_{15,51,85}=\begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix}.$$

$$F^{k}_{15,51,90}=\begin{pmatrix} x_1 \\ x_2 \\ \begin{cases} x_3 & якщо\ \ x_1=0 \\ \bar{x}_3 & якщо\ \ x_1=1 \end{cases} \end{pmatrix};\qquad F^{d}_{15,51,90}=\begin{pmatrix} x_1 \\ x_2 \\ \begin{cases} x_3 & якщо\ \ x_1=0 \\ \bar{x}_3 & якщо\ \ x_1=1 \end{cases} \end{pmatrix}.$$

$$F^{k}_{15,105,85}=\begin{pmatrix} x_1 \\ \begin{cases} x_2 & якщо\ \ x_1\oplus x_3=0 \\ \bar{x}_2 & якщо\ \ x_1\oplus x_3=1 \end{cases} \\ x_3 \end{pmatrix};\qquad F^{d}_{15,105,85}=\begin{pmatrix} x_1 \\ \begin{cases} x_2 & якщо\ \ x_1\oplus x_3=0 \\ \bar{x}_2 & якщо\ \ x_1\oplus x_3=1 \end{cases} \\ x_3 \end{pmatrix}.$$

$$F^{k}_{105,51,60}=\begin{pmatrix} \begin{cases} x_3 & якщо\ \ x_1\oplus x_2=0 \\ \bar{x}_3 & якщо\ \ x_1\oplus x_2=1 \end{cases} \\ x_2 \\ \begin{cases} x_1 & якщо\ \ x_2=0 \\ \bar{x}_1 & якщо\ \ x_2=1 \end{cases} \end{pmatrix};\qquad F^{d}_{102,51,90}=\begin{pmatrix} \begin{cases} x_3 & якщо\ \ x_2=0 \\ \bar{x}_3 & якщо\ \ x_2=1 \end{cases} \\ x_2 \\ \begin{cases} x_3 & якщо\ \ x_1=0 \\ \bar{x}_3 & якщо\ \ x_1=1 \end{cases} \end{pmatrix}.$$

$$F^{k}_{15,102,90}=\begin{pmatrix} x_1 \\ \begin{cases} x_2 & якщо\ \ x_3=0 \\ \bar{x}_2 & якщо\ \ x_3=1 \end{cases} \\ \begin{cases} x_3 & якщо\ \ x_1=0 \\ \bar{x}_3 & якщо\ \ x_1=1 \end{cases} \end{pmatrix};\qquad F^{d}_{15,105,90}=\begin{pmatrix} x_1 \\ \begin{cases} x_2 & якщо\ \ x_1\oplus x_3=0 \\ \bar{x}_2 & якщо\ \ x_1\oplus x_3=1 \end{cases} \\ \begin{cases} x_3 & якщо\ \ x_1=0 \\ \bar{x}_3 & якщо\ \ x_1=1 \end{cases} \end{pmatrix}.$$

$$F^{k}_{90,60,105}=\begin{pmatrix} \begin{cases} x_1 & якщо\ \ x_3=0 \\ \bar{x}_1 & якщо\ \ x_3=1 \end{cases} \\ \begin{cases} x_2 & якщо\ \ x_1=0 \\ \bar{x}_2 & якщо\ \ x_1=1 \end{cases} \\ \begin{cases} x_3 & якщо\ \ x_1\oplus x_2=0 \\ \bar{x}_3 & якщо\ \ x_1\oplus x_2=1 \end{cases} \end{pmatrix};\qquad F^{d}_{105,90,102}=\begin{pmatrix} \begin{cases} x_1 & якщо\ \ x_2\oplus x_3=0 \\ \bar{x}_1 & якщо\ \ x_2\oplus x_3=1 \end{cases} \\ \begin{cases} x_3 & якщо\ \ x_1=0 \\ \bar{x}_3 & якщо\ \ x_1=1 \end{cases} \\ \begin{cases} x_2 & якщо\ \ x_3=0 \\ \bar{x}_2 & якщо\ \ x_3=1 \end{cases} \end{pmatrix}.$$

Розроблений метод дає можливість зменшити складність алгоритмів побудови базових операцій криптографічного перетворення інформації та автоматизувати процес подальших досліджень [9, 53].

2.1.5 Метод синтезу матричних операцій оберненого криптографічного перетворення інформації

Синтез операцій оберненого криптографічного перетворення інформації в групі трирозрядних криптографічних операцій перетворення відповідно до заданої функції прямого перетворення [62, 64], базується на

використанні методу синтезу операцій криптографічного перетворення на основі додавання за модулем два зі збереженням інформативності [16]. Багато публікацій присвячено питанням синтезу криптографічних примітивів [142, 149, 156, 167, 168], проте не існує математичного апарату для побудови операцій перетворення інформації, а також відсутні методи обчислення криптографічної двійкової матриці оберненого перетворення з заданої криптографічної двійкової матриці прямого перетворення.

Задача синтезу операцій оберненого криптографічного перетворення в загальному випадку не вирішена.

У загальному вигляді операції криптографічного перетворення, що побудовані на основі додавання за модулем два, описуються моделлю (2.11) [14].

Якщо операція криптографічного прямого перетворення без урахування групи операцій інверсії задана виразом

$$\vec{F}_k = \begin{pmatrix} a_{11}x_1 \oplus a_{12}x_2 \oplus ... \oplus a_{1n}x_n \\ a_{21}x_1 \oplus a_{22}x_2 \oplus ... \oplus a_{2n}x_n \\ . \quad . \quad . \quad . \quad . \quad . \quad . \quad . \quad . \quad . \quad . \\ a_{n1}x_1 \oplus a_{n2}x_2 \oplus ... \oplus a_{n\,n}x_n \end{pmatrix}, \qquad (2.48)$$

де $a_{ij} \in [0,1]$; $b_i \in [0,1]$; $x_1 ... x_n$ – операнди-розряди відповідно; $\oplus$ – операція «сума за mod 2», тоді операція криптографічного оберненого перетворення буде задана виразом

$$\vec{F}_d = \begin{pmatrix} b_{11}y_1 \oplus b_{12}y_2 \oplus ... \oplus b_{1n}y_n \\ b_{21}y_1 \oplus b_{22}y_2 \oplus ... \oplus b_{2n}y_n \\ . \quad . \quad . \quad . \quad . \quad . \quad . \quad . \quad . \quad . \quad . \\ b_{n1}y_1 \oplus b_{n2}y_2 \oplus ... \oplus b_{n\,n}y_n \end{pmatrix}, \qquad (2.49)$$

де b_i – коефіцієнти матриці оберненого перетворення, y_i – операнди-розряди інформації, які отримані в результаті застосування операції прямого перетворення ($y_i = \vec{F}_k(x_i)$) відповідно.

Отже, результатом виконання операції оберненого перетворення повинен бути вираз, що відповідає такому запису:

$$\vec{F}_r = \begin{pmatrix} a_{11}x_1 & & & & \\ & a_{22}x_2 & & & \\ . & . & . & . & . \\ & & & & a_{nn}x_n \end{pmatrix}, \qquad (2.50)$$

де $\vec{F}_r$ – еталонна матриця або матриця-результат, $x_1 ... x_n$ – початкові операнди-розряди інформації; $a_{ij} = 1$ при $i = j$, тому що потрібно забезпечити невиродженість перетворення, тобто повинна виконуватись умова $a_{11} \cdot a_{22} - a_{12} \cdot a_{21} \neq 0$, а також відсутні перестановки рядків матриці.

Розглянемо докладніше процес знаходження операції (матриці) оберненого перетворення [14, 53, 169]:

$$\vec{F}_d = \begin{pmatrix} b_{11}(a_{11}x_1 \oplus a_{12}x_2 \oplus ... \oplus a_{1n}x_n) \oplus b_{12}(a_{21}x_1 \oplus a_{22}x_2 \oplus ... \oplus a_{2n}x_n) \oplus ... \oplus \\ \oplus b_{1n}(a_{n1}x_1 \oplus a_{n2}x_2 \oplus ... \oplus a_{nn}x_n) \\ b_{21}(a_{11}x_1 \oplus a_{12}x_2 \oplus ... \oplus a_{1n}x_n) \oplus b_{22}(a_{21}x_1 \oplus a_{22}x_2 \oplus ... \oplus a_{2n}x_n) \oplus ... \oplus \\ \oplus b_{2n}(a_{n1}x_1 \oplus a_{n2}x_2 \oplus ... \oplus a_{nn}x_n) \\ . \quad . \quad . \quad . \quad . \quad . \quad . \quad . \quad . \quad . \quad . \quad . \\ b_{n1}(a_{11}x_1 \oplus a_{12}x_2 \oplus ... \oplus a_{1n}x_n) \oplus b_{n2}(a_{21}x_1 \oplus a_{22}x_2 \oplus ... \oplus a_{2n}x_n) \oplus ... \oplus \\ \oplus b_{nn}(a_{n1}x_1 \oplus a_{n2}x_2 \oplus ... \oplus a_{nn}x_n) \end{pmatrix} = \qquad (2.51)$$

$$= \begin{pmatrix} a_{11}x_1 & & & & \\ & a_{22}x_2 & & & \\ . & . & . & . & . \\ & & & & a_{nn}x_n \end{pmatrix}.$$

Цей процес можна зобразити такими етапами реалізації [14]:

1. Знайдемо перший рядок матриці оберненого перетворення:

$$\begin{aligned} &b_{11}(a_{11}x_1 \oplus a_{12}x_2 \oplus ... \oplus a_{1n}x_n) \oplus \\ &\oplus b_{12}(a_{21}x_1 \oplus a_{22}x_2 \oplus ... \oplus a_{2n}x_n) \oplus ... \oplus \\ &\oplus b_{1n}(a_{n1}x_1 \oplus a_{n2}x_2 \oplus ... \oplus a_{nn}x_n) = a_{11}x_1 \end{aligned}. \qquad (2.52)$$

Оскільки $x_1 = 1$, а $x_j = 0$ при $j \neq 1$, тоді b_{1i} є рішенням системи рівнянь:

$$\begin{cases} b_{11}a_{11} \oplus b_{12}a_{21} \oplus ... \oplus b_{1n}a_{n1} = 1 \\ b_{11}a_{12} \oplus b_{12}a_{22} \oplus ... \oplus b_{1n}a_{n2} = 0 \\ . \quad . \quad . \quad . \quad . \quad . \quad . \quad . \quad . \quad . \\ b_{11}a_{1n} \oplus b_{12}a_{2n} \oplus ... \oplus b_{1n}a_{nn} = 0 \end{cases}. \qquad (2.53)$$

2. Знайдемо другий рядок матриці оберненого перетворення:

$$\begin{aligned} & b_{21}(a_{11}x_1 \oplus a_{12}x_2 \oplus ... \oplus a_{1n}x_n) \oplus \\ & \oplus b_{22}(a_{21}x_1 \oplus a_{22}x_2 \oplus ... \oplus a_{2n}x_n) \oplus ... \oplus \\ & \oplus b_{2n}(a_{n1}x_1 \oplus a_{n2}x_2 \oplus ... \oplus a_{nn}x_n) = a_{22}x_2 \end{aligned}. \qquad (2.54)$$

Оскільки $x_2 = 1$, а $x_j = 0$ при $j \neq 2$, тоді b_{2i} є рішенням системи рівнянь:

$$\begin{cases} b_{21}a_{11} \oplus b_{22}a_{21} \oplus ... \oplus b_{2n}a_{n1} = 0 \\ b_{21}a_{12} \oplus b_{22}a_{22} \oplus ... \oplus b_{2n}a_{n2} = 1 \\ . \quad . \quad . \quad . \quad . \quad . \quad . \quad . \quad . \quad . \\ b_{21}a_{1n} \oplus b_{22}a_{2n} \oplus ... \oplus b_{2n}a_{nn} = 0 \end{cases}. \qquad (2.55)$$

3. Знайдемо n-й рядок матриці оберненого перетворення:

$$\begin{aligned} & b_{n1}(a_{11}x_1 \oplus a_{12}x_2 \oplus ... \oplus a_{1n}x_n) \oplus \\ & \oplus b_{n2}(a_{21}x_1 \oplus a_{22}x_2 \oplus ... \oplus a_{2n}x_n) \oplus ... \oplus \\ & \oplus b_{nn}(a_{n1}x_1 \oplus a_{n2}x_2 \oplus ... \oplus a_{nn}x_n) = a_{nn}x_n \end{aligned}. \qquad 2.56)$$

Оскільки $x_n = 1$, а $x_j = 0$ при $j \neq n$, тоді b_{ni} є рішенням системи рівнянь:

$$\begin{cases} b_{n1}a_{11} \oplus b_{n2}a_{21} \oplus ... \oplus b_{nn}a_{n1} = 0 \\ b_{n1}a_{12} \oplus b_{n2}a_{22} \oplus ... \oplus b_{nn}a_{n2} = 0 \\ . \quad . \quad . \quad . \quad . \quad . \quad . \quad . \quad . \quad . \quad . \quad . \\ b_{n1}a_{1n} \oplus b_{n2}a_{2n} \oplus ... \oplus b_{nn}a_{nn} = 1 \end{cases} \qquad (2.57)$$

Вирази (2.48)–(2.57) можна розглядати як метод синтезу матричних операцій криптографічного оберненого перетворення [14, 53].

На основі проведених досліджень було сформовано вимоги щодо існування операцій (матриць) перетворення [53]:

Вимога 2.1. Матриця повинна бути невиродженою (відсутні нульові рядки $\sum_{j=1}^{n} a_{ij} > 0$ чи нульові стовбці $\sum_{i=1}^{n} a_{ij} > 0$).

Вимога 2.2. Сума за модулем два двох чи декількох рядків не повторює існуючий рядок матриці: $\sum_{j=1}^{n} (a_{ij} \oplus a_{lj} \oplus a_{hj} \oplus ... \oplus a_{uj}) > 0$.

Відповідність цим вимогам забезпечує наявність розв'язку виразу (2.51) і, як наслідок, існування для кожної операції (матриці) прямого перетворення операції (матриці) оберненого перетворення.

Приклади використання методу синтезу матричних операцій оберненого криптографічного перетворення інформації наведені в [51].

Для операцій криптографічного перетворення обернені операції можуть бути знайдені на основі логічних визначників [66].

Розглянемо двійкове поле, яке складається з 0 і 1. Ці елементи є відповідно одиничними елементами відносно логічного додавання $\oplus$ і логічного множення $\otimes$ за модулем 2, які визначаються правилами [166, 170]:

$0 \oplus 0 = 1 \oplus 1 = 0$; $0 \otimes 0 = 0$, $1 \otimes 1 = 1$;

$1 \oplus 0 = 0 \oplus 1 = 1$; $0 \otimes 1 = 1 \otimes 0 = 0$.

Оскільки $-1 \equiv 1(\mathrm{mod}\,2)$, то операції додавання і віднімання у двійковому полі співпадають, а так як $1^{-1} = 1$, також співпадають операції множення і ділення.

Позначимо це поле $K = \langle \{0,1\}, \oplus, \otimes \rangle$. Над цим полем розглянемо визначники і матриці, які називатимемо логічними [66].

Означення 2.8. Логічним визначником другого порядку називається вираз:

$$\Delta = \begin{vmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{vmatrix} = a_{11}a_{22} \oplus a_{12}a_{21}, \tag{2.58}$$

де $a_{ij} \in K$.

Означення 2.9. Логічним визначником третього порядку називається вираз:

$$\Delta = \begin{vmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \end{vmatrix} = a_{11}a_{22}a_{33} \oplus a_{13}a_{21}a_{32} \oplus a_{12}a_{23}a_{31} \oplus a_{13}a_{22}a_{31} \oplus a_{12}a_{21}a_{33} \oplus a_{11}a_{23}a_{32}, \tag{2.59}$$

де $a_{ij} \in K$.

Далі наведемо розклад логічного визначника за елементами рядка або стовпця.

Нехай задано логічний визначник третього порядку:

$$\Delta = \begin{vmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \end{vmatrix}. \tag{2.60}$$

Означення 2.10. Логічним доповненням L_{ij} елемента a_{ij} логічного визначника називається логічний визначник, який утворюється з даного визначника в результаті викреслення i-го рядка та j-го стовпця.

Наприклад, для визначника (2.60) логічним доповненням елемента a_{32} є такий визначник:

$$L_{32} = \begin{vmatrix} a_{11} & a_{13} \\ a_{21} & a_{23} \end{vmatrix}.$$

Теорема 2.2. Визначник дорівнює логічній сумі добутків елементів якого-небудь рядка (стовпця) на їхні логічні доповнення:

$$\begin{aligned} &\Delta = a_{11}L_{11} \oplus a_{12}L_{12} \oplus a_{13}L_{13}; && \Delta = a_{11}L_{11} \oplus a_{21}L_{21} \oplus a_{31}L_{31}; \\ &\Delta = a_{21}L_{21} \oplus a_{22}L_{22} \oplus a_{23}L_{23}; && \Delta = a_{12}L_{12} \oplus a_{22}L_{22} \oplus a_{32}L_{32}; \\ &\Delta = a_{31}L_{31} \oplus a_{32}L_{32} \oplus a_{33}L_{33}; && \Delta = a_{13}L_{13} \oplus a_{23}L_{23} \oplus a_{33}L_{33}. \end{aligned} \qquad (2.61)$$

Доведення. Спочатку доведемо, наприклад, першу з рівностей. Для цього розкриваємо визначник (2.60) за формулою (2.59) і, групуючи доданки, що містять елементи першого рядка, маємо:

$$\Delta = a_{11}(a_{22}a_{33} \oplus a_{23}a_{32}) \oplus a_{12}(a_{23}a_{31} \oplus a_{21}a_{33}) \oplus a_{13}(a_{21}a_{32} \oplus a_{22}a_{31}).$$

За означенням (2.60) вирази, що стоять у дужках, відповідно дорівнюють логічним доповненням L_{11}, L_{12}, L_{13}, тому $\Delta = a_{11}L_{11} \oplus a_{12}L_{12} \oplus a_{13}L_{13}$.

Аналогічно доводяться й інші рівності.

Запис визначника за будь-якою з формул (2.61) називають розкладом визначника за елементами відповідного рядка чи стовпця.

Теорема 2.3. Сума добутків елементів будь-якого рядка (стовпця) визначника на логічні доповнення відповідних елементів іншого рядка (стовпця) дорівнює нулю.

Доведення. Розглянемо, наприклад, логічну суму добутків елементів першого рядка визначника (2.60) на логічні доповнення елементів другого рядка:

$$a_{11}L_{21} \oplus a_{12}L_{22} \oplus a_{13}L_{23} = a_{11}(a_{12}a_{33} \oplus a_{13}a_{32}) \oplus a_{12}(a_{11}a_{33} \oplus a_{13}a_{31}) \oplus a_{13}(a_{11}a_{32} \oplus a_{12}a_{31}) =$$

$$= a_{11}a_{12}a_{33} \oplus a_{11}a_{13}a_{32} \oplus a_{12}a_{11}a_{33} \oplus a_{12}a_{13}a_{31} \oplus a_{13}a_{11}a_{32} \oplus a_{13}a_{12}a_{31}.$$

Оскільки, однакові пари доданків взаємно знищуються, то цей вираз дорівнює нулю.

Означення 2.11. Логічною матрицею називається квадратна таблиця чисел $a_{ij} \in K$, $(i, j = 1,...,n)$, складена з n рядків та n стовпців і записана у вигляді:

$$A = \begin{pmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ a_{21} & a_{22} & \dots & a_{2n} \\ \dots & \dots & \dots & \dots \\ a_{n1} & a_{n2} & \dots & a_{nn} \end{pmatrix}.$$

Поняття діагональної та одиничної логічних матриць аналогічні поняттям звичайних матриць.

Відомо, що будь-якій квадратній матриці можна поставити у відповідність певне число, яке називається визначником матриці. Визначники логічних матриць можуть набувати лише двох значень 0 або 1. [169]

Поняття оберненої логічної матриці аналогічне поняттю алгебраїчної оберненої матриці.

Нехай A - логічна матриця. Матриця A^{-1} називається оберненою до матриці A, якщо виконується умова [169]:

$$AA^{-1} = A^{-1}A = E.$$

Якщо визначник логічної матриці дорівнює нулю, то матриця називається виродженою, а якщо дорівнює 1, то невиродженою. Відомо, що лише для невироджених матриць існують обернені матриці [169].

Теорема про обернену матрицю. Якщо логічна $(n \times n)$ матриця A оборотна, то елементи оберненої логічної матриці A^{-1} знаходяться як логічні доповнення елементів транспонованої матриці A^T [23]:

$$A^{-1} = \begin{pmatrix} L_{11} & L_{21} & L_{31} \\ L_{12} & L_{22} & L_{32} \\ L_{13} & L_{23} & L_{33} \end{pmatrix}.$$

Доведення. Розглянемо логічну матрицю A. Нехай оберненою до неї є матриця B. Знайдемо логічний добуток матриць $A \otimes B = C$ і покажемо, що матриця $C = E$.

Нехай матриця $A = \begin{pmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \end{pmatrix}$, матриця $B = \begin{pmatrix} L_{11} & L_{21} & L_{31} \\ L_{12} & L_{22} & L_{32} \\ L_{13} & L_{23} & L_{33} \end{pmatrix}$.

Покажемо, що діагональні елементи матриці C дорівнюють 1.

Дійсно, застосовуючи правило знаходження добутку матриць і теорему 1 про розклад визначника за елементами його рядка, матимемо:

$$c_{11} = a_{11}L_{11} \oplus a_{12}L_{12} \oplus a_{13}L_{13} = |A| = 1.$$

Аналогічно доводяться рівності $c_{22} = c_{33} = 1$.

Покажемо, що всі поза діагональні елементи матриці C дорівнюють нулю.

Знайдемо, наприклад c_{12}:

$$c_{12} = a_{11}L_{21} \oplus a_{12}L_{22} \oplus a_{13}L_{23}.$$

За теоремою 2.3, така сума дорівнює нулю. Тому $c_{12} = a_{11}L_{21} \oplus a_{12}L_{22} \oplus a_{13}L_{23} = 0$.

Аналогічно доводиться рівність нулю решти поза діагональних елементів.

Таким чином доведено: $C = E$. Тому $B = \begin{pmatrix} L_{11} & L_{21} & L_{31} \\ L_{12} & L_{22} & L_{32} \\ L_{13} & L_{23} & L_{33} \end{pmatrix}$ є оберненою матрицею для матриці A. Теорему доведено.

Розроблені методи синтезу прямих та обернених матричних операцій криптографічного перетворення створюють теоретичне підґрунтя для вдосконалення існуючих та розробки нових криптографічних алгоритмів.

2.2 Розробка методу синтезу операцій матричного криптографічного взаємного перетворення

У роботі «Теорія зв'язку в секретних системах» Шеннон довів, що повторне використання криптоалгоритмів, які створюють групу, не забезпечує підвищення криптостійкості [171]. Спробуємо використати дане обмеження для підвищення оперативності доступу до конфіденційних інформаційних ресурсів на основі використання синтезованих операцій матричного криптографічного перетворення. На даний час в доступних джерелах науково-технічної інформації відсутні дані про підвищення оперативності доступу до конфіденційних інформаційних ресурсів на основі використання широкого спектру операцій криптографічного перетворення інформації.

Сутність методу підвищення оперативності доступу до конфіденційних інформаційних ресурсів полягає в наступному:

Нехай справедливі операції криптографічного перетворення: $y = F_1^k(x), \quad y = F_2^k(x)$ такі, що $F_1^k(F_2^k(x)) = y$. Також, нехай справедливі операції криптографічного перетворення: $y = F_3^k(x), \quad y = F_4^k(x)$, такі, що

$F_3^k(F_4^k(x)) = y$. Тоді існує функція $y = F_*^k(x)$, яка забезпечує перетворення інформації:

$$y = F_*^k(F_1^k(x)) = F_3^k(x). \qquad (2.58)$$

Іншими словами: існує операція криптографічного перетворення $y = F_*^k(x)$, яка забезпечує перетворення результату виконання однієї операції у результат виконання іншої операції без етапу виконання оберненої операції. Дані операції будемо називати операціями взаємного криптографічного перетворення.

Наступні дослідження проводилися з метою визначення $y = F_*^k(x)$, в залежності від відомих $y = F_1^k(x)$ та $y = F_3^k(x)$ [8, 14].

Отримати вихідну (початкову) інформацію про операції взаємного криптографічного перетворення можна лише за допомогою проведення обчислювального експерименту. Без даної інформації неможливо проводити узагальнення та розробляти методи синтезу операцій взаємного криптоперетворення.

Для проведення обчислювального експерименту в процесі проведення дослідження нами створено спеціалізоване програмне забезпечення.

Основні задачі та цілі створення спеціалізованого програмного забезпечення є такими [14]:

– визначення елементарних логічних функцій заданої кількості змінних, які можуть використовуватися в криптоперетвореннях;

– визначення можливих варіантів поєднання елементарних логічних функцій в операції криптографічного перетворення;

– визначення груп операцій криптографічного перетворення, для яких виконується правило суперпозиції, що створює умову реалізації взаємного криптографічного перетворення;

– визначення операцій взаємного криптографічного перетворення на всій множині операцій в групі.

За результатами обчислювального експерименту нами отримані дані для узагальнення та подальшої розробки методу підвищення оперативності доступу до конфіденційних інформаційних ресурсів на основі використання операцій взаємного криптографічного перетворення.

Мета дослідження полягає у проведенні систематизації операцій криптоперетворення придатних для підвищення оперативності доступу до конфіденційних інформаційних ресурсів.

Подальші дослідження проведемо на прикладі двохрозрядних операцій криптографічного перетворення заданих табл. 2.1.

2.2.1 Систематизація повної множини логічних функцій для криптографічного перетворення інформації

Результатами обчислювального експерименту щодо визначення повної множини двохрозрядних операцій криптографічного перетворення, придатних для здійснення взаємного криптоперетворення, стали 576 функцій, використання яких дає можливість підвищення оперативності доступу до конфіденційних інформаційних ресурсів. Збільшення кількості спеціалізованих логічних функцій дозволяє підвищити захищеність конфіденційної інформації. Також проведений експеримент створює теоретичну базу для подальших досліджень, що направлені на доведення доцільності використання елементарних функцій криптоперетворення будь-якої складності.

За результатами досліджень нами отримано логічні функції взаємного криптоперетворення, які можуть бути використані в системах комп'ютерної криптографії на етапі криптографічного додавання [87-90].

Для аналізу одержаних результатів використаємо векторне подання функцій взаємного криптоперетворення (2.9) та позначимо кодами наступні елементарні функції:

$$f = x_1 \rightarrow 10; \qquad f = x_1 \oplus 1 \rightarrow 11;$$

$$f = x_2 \rightarrow 20; \qquad f = x_2 \oplus 1 \rightarrow 21;$$

$$f = x_1 \oplus x_2 \rightarrow 30; \qquad f = x_1 \oplus x_2 \oplus 1 \rightarrow 31.$$

Дане позначення стало необхідним для компактного подання результатів експерименту.

Структуровані результати обчислювального експерименту наведено в таблиці 2.5 [53].

Таблиця 2.5

Структуровані результати обчислювального експерименту

Vh \ Vmh	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24
	10	20	11	10	11	21	20	21	30	20	31	21	30	31	20	21	10	30	11	31	10	11	30	31
	20	10	20	21	21	11	11	10	20	30	21	31	21	20	31	30	30	10	31	11	31	30	11	10
1	10	20	11	10	11	21	20	21	30	20	31	21	30	31	20	21	10	30	11	31	10	11	30	31
2	20	10	21	20	21	11	10	11	30	10	31	11	30	31	10	11	20	30	21	31	20	21	30	31
3	11	20	10	11	10	21	20	21	31	20	30	21	31	30	20	21	11	31	10	30	11	10	31	30
4	10	21	11	10	11	20	21	20	31	21	30	20	31	30	21	20	10	31	11	30	10	11	31	30
5	11	21	10	11	10	20	21	20	30	21	31	20	30	31	21	20	11	30	10	31	11	10	30	31
6	21	11	20	21	20	10	11	10	30	11	31	10	30	31	11	10	21	30	20	31	21	20	30	31
7	20	21	10	20	21	11	10	11	31	10	30	11	31	30	10	11	21	31	20	30	21	20	31	30
8	21	20	11	21	20	21	10	11	10	31	11	30	10	31	30	11	10	20	31	21	30	20	21	31	30
9	30	30	20	31	30	31	21	20	21	10	20	11	21	10	11	20	21	30	10	31	11	30	31	10	11
10	20	30	10	31	30	31	11	10	11	20	10	21	11	20	21	10	11	30	20	31	21	30	31	20	21
11	31	30	21	31	30	31	20	21	20	11	21	10	20	11	10	21	20	30	11	31	10	30	31	11	10
12	21	30	11	31	30	31	10	11	10	21	11	20	10	21	20	11	10	30	21	31	20	30	31	21	20
13	30	31	21	30	31	30	20	21	20	10	21	11	20	10	11	21	20	31	10	30	11	31	30	10	11
14	31	31	20	30	31	30	21	20	21	11	20	10	21	11	10	20	21	31	11	30	10	31	30	11	10
15	20	31	10	30	31	30	11	10	11	21	10	20	11	21	20	10	11	31	21	30	20	31	30	21	20
16	21	31	11	30	31	30	10	11	10	20	11	21	10	20	21	11	10	31	20	30	21	31	30	20	21
17	10	10	30	11	10	11	31	30	31	20	30	21	31	20	21	30	31	10	20	11	21	10	11	20	21
18	30	20	30	21	20	21	31	30	31	10	30	11	31	10	11	30	31	20	10	21	11	20	21	10	11
19	11	30	10	11	10	31	30	31	21	30	20	31	21	20	30	31	11	21	10	20	11	10	21	20	11
20	31	21	30	20	21	20	31	30	31	11	30	10	31	11	10	30	31	21	11	20	10	21	20	11	10
21	10	10	31	11	10	11	30	31	30	21	31	20	30	21	20	31	30	10	21	11	20	10	11	21	20
22	11	11	31	10	11	10	30	31	30	20	31	21	30	20	21	31	30	11	20	10	21	11	10	20	21
23	30	21	31	20	21	20	30	31	30	10	31	11	30	10	11	31	30	21	10	20	11	21	20	10	11
24	31	20	31	21	20	21	30	31	30	11	31	10	30	11	10	31	30	20	11	21	10	20	21	11	10
	10	20	11	10	11	21	20	21	30	20	31	21	30	31	20	21	10	30	11	31	10	11	30	31
	20	10	20	21	21	11	11	10	20	30	21	31	21	20	31	30	30	10	31	11	31	30	11	10

Здійснивши дослідження структурованої таблиці отриманих результатів експерименту (табл. 2.5), нами виявлено, що всі логічні функції взаємного криптоперетворення можливо умовно об’єднати в три великі блоки.

Класифікуємо функції взаємного криптоперетворення на основі представлення вхідної та вихідної логічної функції.

– Проста логічна функція (функції з номерами 1-8);
– Складна логічна функція (функції з номерами 9-24), враховуючи, що:
  – складна логічна функція першої заміни (функції з номерами 9-16);
  – складна логічна функція другогї заміни (функції з номерами 17-24).

Перший блок логічних функцій взаємного криптоперетворення включає в себе лише прості логічні функції, одержані на основі перестановок та інверсій −це 8 спеціалізованих функцій [6, 7, 89]:

$$\vec{F}_1 = \begin{pmatrix} x_1 \\ x_2 \end{pmatrix}, \vec{F}_2 = \begin{pmatrix} x_2 \\ x_1 \end{pmatrix}, \vec{F}_3 = \begin{pmatrix} x_1 \oplus 1 \\ x_2 \end{pmatrix}, \vec{F}_4 = \begin{pmatrix} x_1 \\ x_2 \oplus 1 \end{pmatrix},$$

$$\vec{F}_5 = \begin{pmatrix} x_1 \oplus 1 \\ x_2 \oplus 1 \end{pmatrix}, \vec{F}_6 = \begin{pmatrix} x_2 \oplus 1 \\ x_1 \oplus 1 \end{pmatrix}, \vec{F}_7 = \begin{pmatrix} x_2 \\ x_1 \oplus 1 \end{pmatrix}, \vec{F}_8 = \begin{pmatrix} x_2 \oplus 1 \\ x_1 \end{pmatrix}.$$

Другий блок логічних функцій взаємного криптоперетворення включає в себе лише складні логічні функції першої заміни, одержані на основі перестановок та інверсій−це 8 спеціалізованих функцій [6, 7, 90]:

$$\vec{F}_9 = \begin{pmatrix} x_1 \oplus x_2 \\ x_2 \end{pmatrix}, \quad \vec{F}_{10} = \begin{pmatrix} x_2 \\ x_1 \oplus x_2 \end{pmatrix}, \quad \vec{F}_{11} = \begin{pmatrix} x_1 \oplus x_2 \oplus 1 \\ x_2 \oplus 1 \end{pmatrix}, \quad \vec{F}_{12} = \begin{pmatrix} x_2 \oplus 1 \\ x_1 \oplus x_2 \oplus 1 \end{pmatrix},$$

$$\vec{F}_{13} = \begin{pmatrix} x_1 \oplus x_2 \\ x_2 \oplus 1 \end{pmatrix}, \quad \vec{F}_{14} = \begin{pmatrix} x_1 \oplus x_2 \oplus 1 \\ x_2 \end{pmatrix}, \quad \vec{F}_{15} = \begin{pmatrix} x_2 \\ x_1 \oplus x_2 \oplus 1 \end{pmatrix}, \quad \vec{F}_{16} = \begin{pmatrix} x_2 \oplus 1 \\ x_1 \oplus x_2 \end{pmatrix}.$$

Третій блок логічних функцій взаємного криптоперетворення включає в себе лише складні логічні функції другої заміни, одержані на основі перестановок та інверсій −це 8 спеціалізованих функцій [6, 7, 90]:

$$\vec{F}_{17}=\begin{pmatrix} x_1 \\ x_1 \oplus x_2 \end{pmatrix},\quad \vec{F}_{18}=\begin{pmatrix} x_1 \oplus x_2 \\ x_1 \end{pmatrix},\quad \vec{F}_{19}=\begin{pmatrix} x_1 \oplus 1 \\ x_1 \oplus x_2 \oplus 1 \end{pmatrix},\quad \vec{F}_{20}=\begin{pmatrix} x_1 \oplus x_2 \oplus 1 \\ x_1 \oplus 1 \end{pmatrix},$$

$$\vec{F}_{21}=\begin{pmatrix} x_1 \\ x_1 \oplus x_2 \oplus 1 \end{pmatrix},\quad \vec{F}_{22}=\begin{pmatrix} x_1 \oplus 1 \\ x_1 \oplus x_2 \end{pmatrix},\quad \vec{F}_{23}=\begin{pmatrix} x_1 \oplus x_2 \\ x_1 \oplus 1 \end{pmatrix},\quad \vec{F}_{24}=\begin{pmatrix} x_1 \oplus x_2 \oplus 1 \\ x_1 \end{pmatrix}.$$

Повна множина варіантів взаємного криптоперетворення у кожній множині визначає 64 функції взаємного перетворення [10].

Шляхом аналізу структурного табличного подання результатів експерименту нами проведено систематизацію операцій криптографічного перетворення, яка дала змогу спростити подальший аналіз та виявлення взаємозв’язків між відомими вхідними та вихідними операціями.

Отримані результати дослідження експериментальних даних на основі їх векторного подання дозволили забезпечили достатнє наукове обґрунтування правильності одержаних результатів та коректності використання двохрозрядних операцій криптографічного перетворення для підвищення оперативності доступу до конфіденційних інформаційних ресурсів.

2.2.2. Синтез математичних моделей операцій взаємного криптографічного перетворення

Розглянемо один із варіантів створення алгоритму побудови функцій взаємного криптоперетворення. Він буде ґрунтуватися на виконанні логічних операцій над рядками вхідної та вихідної функцій [53].

Виходячи із матричного подання логічний функцій (2.10), введемо загальний вигляд відповідно вхідної та вихідної функцій [53]:

$$\vec{F}_{Vh} = \begin{pmatrix} x_1 & x_2 \\ x_3 & x_4 \end{pmatrix}, \quad \vec{F}_{Vuh} = \begin{pmatrix} x_5 & x_6 \\ x_7 & x_8 \end{pmatrix}, \tag{2.59}$$

та функції взаємного перетворення, яку маємо отримати в результаті проведених досліджень:

$$\vec{F}_{Pk} = \begin{pmatrix} f_1 & f_2 \\ f_3 & f_4 \end{pmatrix}. \tag{2.60}$$

Оскільки, розглядаються лише не інвертовані логічні функції, одержимо наступну таблицю 2.6 для створення математичної моделі функції взаємного перетворення.

Таблиця 2.6

Таблиця даних для отримання математичної моделі функції взаємного перетворення

Вхідна логічна функція F_{Vh}				**Вихідна логічна функція** F_{Vuh}				**Функція взаємоперетворення** F_{Pk}			
перший розряд		**другий розряд**		**перший розряд**		**другий розряд**		**перший розряд**		**другий розряд**	
x1	**x2**	**x3**	**x4**	**x5**	**x6**	**x7**	**x8**	**f1**	**f2**	**f3**	**f4**
1	0	0	1	1	0	0	1	1	0	0	1
0	1	1	0	1	0	0	1	0	1	1	0
1	1	0	1	1	0	0	1	1	1	0	1
1	0	1	1	1	0	0	1	1	0	1	1
1	1	1	0	1	0	0	1	0	1	1	1
0	1	1	1	1	0	0	1	1	1	1	0
1	0	0	1	0	1	1	0	0	1	1	0
0	1	1	0	0	1	1	0	1	0	0	1
1	1	0	1	0	1	1	0	0	1	1	1

Продовження табл. 2.6

Вхідна логічна функція F_{Vh}				**Вихідна логічна функція** F_{Vuh}				**Функція взаємоперетворення** F_{Pk}			
перший розряд		**другий розряд**		**перший розряд**		**другий розряд**		**перший розряд**		**другий розряд**	
x1	**x2**	**x3**	**x4**	**x5**	**x6**	**x7**	**x8**	**f1**	**f2**	**f3**	**f4**
1	0	1	1	0	1	1	0	1	1	1	0
1	1	1	0	0	1	1	0	1	1	0	1
0	1	1	1	0	1	1	0	1	0	1	1
1	0	0	1	1	1	0	1	1	1	0	1
0	1	1	0	1	1	0	1	1	1	1	0
1	1	0	1	1	1	0	1	1	0	0	1
1	0	1	1	1	1	0	1	0	1	1	1
1	1	1	0	1	1	0	1	1	0	1	1
0	1	1	1	1	1	0	1	0	1	1	0
1	0	0	1	0	1	1	1	0	1	1	1
0	1	1	0	0	1	1	1	1	0	1	1
1	1	0	1	0	1	1	1	0	1	1	0
1	0	1	1	0	1	1	1	1	1	0	1
1	1	1	0	0	1	1	1	1	1	1	0
0	1	1	1	0	1	1	1	1	0	0	1
1	0	0	1	1	0	1	1	1	0	1	1
0	1	1	0	1	0	1	1	0	1	1	1
1	1	0	1	1	0	1	1	1	1	1	0
1	0	1	1	1	0	1	1	1	0	0	1
1	1	1	0	1	0	1	1	0	1	1	0
0	1	1	1	1	0	1	1	1	1	0	1
1	0	0	1	1	1	1	0	1	1	1	0
0	1	1	0	1	1	1	0	1	1	0	1
1	1	0	1	1	1	1	0	1	0	1	1
1	0	1	1	1	1	1	0	0	1	1	0
1	1	1	0	1	1	1	0	1	0	0	1
0	1	1	1	1	1	1	0	0	1	1	1

Аналізуючи дані таблиці 2.6 та використовуючи стандартні методи мінімізації логічних функцій, нами отримано такі функції [10]:

$$
\begin{aligned}
f_1 &= (x_3\bar{x}_5 \vee \bar{x}_3x_5) \vee (x_4\bar{x}_6 \vee \bar{x}_4x_6),\\
f_2 &= (x_1\bar{x}_5 \vee \bar{x}_1x_5) \vee (x_2\bar{x}_6 \vee \bar{x}_2x_6),\\
f_3 &= (x_3\bar{x}_7 \vee \bar{x}_3x_7) \vee (x_4\bar{x}_8 \vee \bar{x}_4x_8),\\
f_4 &= (x_1\bar{x}_7 \vee \bar{x}_1x_7) \vee (x_2\bar{x}_8 \vee \bar{x}_2x_8).
\end{aligned}
\qquad (2.61)
$$

Вирази (2.61) подамо як:

$$\begin{aligned} f_1 &= (x_3 \oplus x_5) \vee (x_4 \oplus x_6), \\ f_2 &= (x_1 \oplus x_5) \vee (x_2 \oplus x_6), \\ f_3 &= (x_3 \oplus x_7) \vee (x_4 \oplus x_8), \\ f_4 &= (x_1 \oplus x_7) \vee (x_2 \oplus x_8). \end{aligned} \tag{2.62}$$

У результаті проведеного дослідження та, виходячи із загального вигляду функції взаємоперетворення (2.60), одержимо загальне правило побудови функції взаємного криптоперетворення без урахування інверсій:

$$\vec{F}_{Pk} = \begin{pmatrix} f_1 & f_2 \\ f_3 & f_4 \end{pmatrix} = \begin{pmatrix} (x_3 \oplus x_5) \vee (x_4 \oplus x_6) & (x_1 \oplus x_5) \vee (x_2 \oplus x_6) \\ (x_3 \oplus x_7) \vee (x_4 \oplus x_8) & (x_1 \oplus x_7) \vee (x_2 \oplus x_8) \end{pmatrix}. \tag{2.63}$$

Повний аналіз множини логічних функцій взаємного перетворення на основі критерію даного підходу показав, що саме цей підхід дає максимальні можливості для створення алгоритму побудови функції взаємоперетворення.

Алгоритм побудови функцій взаємоперетворення для базових вхідних та вихідних логічних функцій (2.63) нам уже відомий, тому спробуємо поширити критерії даного підходу на всю множину логічних функцій взаємного криптоперетворення.

Виходячи із матричного подання загального вигляду логічної функції (2.10), проведемо дослідження алгоритму побудови математичної моделі функції інверсій, використовуючи запис:

$$\vec{F}\begin{pmatrix} x_1 \\ x_2 \end{pmatrix} = \begin{pmatrix} a_{11}x_1 \oplus a_{12}x_2 \oplus b_1 \\ a_{21}x_1 \oplus a_{22}x_2 \oplus b_2 \end{pmatrix} = \begin{pmatrix} a_{11}x_1 \oplus a_{12}x_2 \\ a_{21}x_1 \oplus a_{22}x_2 \end{pmatrix} * \begin{pmatrix} b_1 \\ b_2 \end{pmatrix} = \vec{F}_a \begin{pmatrix} x_1 \\ x_2 \end{pmatrix} * \vec{F}_b^{\,i} \begin{pmatrix} b_1 \\ b_2 \end{pmatrix}. \tag{2.64}$$

Введемо позначення матричного вигляду інверсних логічних функцій згідно формул (2.10) та(2.64), (2.59) та (2.60) відповідно вхідної $\vec{F}_{Vh}$, вихідної $\vec{F}_{Vuh}$ та функції взаємоперетворення $\vec{F}_{Pk}$:

$$\vec{F}_{Vh}^{\,i} = \begin{pmatrix} x_9 \\ x_{10} \end{pmatrix}, \tag{2.65}$$

$$\vec{F}_{Vuh}^{\,i} = \begin{pmatrix} x_{11} \\ x_{12} \end{pmatrix}, \tag{2.66}$$

$$\vec{F}_{Pk}^{\,i} = \begin{pmatrix} f_5 \\ f_6 \end{pmatrix}. \tag{2.67}$$

Тоді, враховуючи формулу (2.64), вхідна $\vec{F}_{Vh}$ логічна функція, вихідна $\vec{F}_{Vuh}$ логічна функція та функція взаємоперетворення $\vec{F}_{Pk}$ разом з функцією інверсій набудуть наступного матричного вигляду:

$$\vec{F}_{Vh} = \begin{pmatrix} x_1 & x_2 \\ x_3 & x_4 \end{pmatrix} * \begin{pmatrix} x_9 \\ x_{10} \end{pmatrix} = \begin{pmatrix} x_1 & x_2 & x_9 \\ x_3 & x_4 & x_{10} \end{pmatrix}, \tag{2.68}$$

$$\vec{F}_{Vuh} = \begin{pmatrix} x_5 & x_6 \\ x_7 & x_8 \end{pmatrix} * \begin{pmatrix} x_{11} \\ x_{12} \end{pmatrix} = \begin{pmatrix} x_5 & x_6 & x_{11} \\ x_7 & x_8 & x_{12} \end{pmatrix}, \tag{2.69}$$

$$\vec{F}_{Pk} = \begin{pmatrix} f_1 & f_2 \\ f_3 & f_4 \end{pmatrix} * \begin{pmatrix} f_5 \\ f_6 \end{pmatrix} = \begin{pmatrix} f_1 & f_2 & f_5 \\ f_3 & f_4 & f_6 \end{pmatrix}. \tag{2.70}$$

Оскільки, інверсні функції вхідної та вихідної логічних функцій є відомими, то наступні дослідження направлені на знаходження інверсного вигляду функції взаємного криптоперетворення.

Для дослідження формування функцій взаємного перетворення на табл. 2.5 нами виділено відтінками варіанти можливих інверсій, які показали існування певної залежності для визначення функцій взаємоперетворення.

Для підвищення наочності виявлення залежностей переставимо деякі стовпці та рядки табл. 2.5 у межах кожної з множин відповідно класифікатора результатів обчислювального експерименту [10, 53].

У результаті перетворення табл. 2.5 було отримано нову таблицю результатів, яка чітко відображає отриману симетрію. Перший блок таблиці операцій взаємного перетворення представлено в табл. 2.8.

Таблиця 2.8

Функції взаємоперетворення першого блоку модифікованої таблиці

№ п/п		**1**	**2**	**5**	**6**	**3**	**7**	**4**	**8**
	Vuh / Vh	**10 20**	**20 10**	**11 21**	**21 11**	**11 20**	**20 11**	**10 21**	**21 10**
1	**10**	10	20	11	21	11	20	10	21
	20	20	10	21	11	20	11	21	10
2	**20**	20	10	21	11	21	10	20	11
	10	10	20	11	21	10	21	11	20
5	**11**	11	21	10	20	10	21	11	20
	21	21	11	20	10	21	10	20	11
6	**21**	21	11	20	10	20	11	21	10
	11	11	21	10	20	11	20	10	21
3	**11**	11	20	10	21	10	20	11	21
	20	20	11	21	10	20	10	21	11
7	**20**	21	10	20	11	20	10	21	11
	11	10	21	11	20	10	20	11	21
4	**10**	10	21	11	20	11	21	10	20
	21	21	10	20	11	21	11	20	10
8	**21**	20	11	21	10	21	11	20	10
	10	11	20	10	21	11	21	10	20

Оскільки досліджуються лише інверсії функцій взаємоперетворення, то для подання повної множини цих функцій введемо два додаткових параметри [10, 53]:

1. вхідна логічна функція $\vec{F}_{Vh}$ є: $x_{13} = \begin{cases} 0 - \textit{правильно розміщеною}, \\ 1 - \textit{неправильно розміщеною}. \end{cases}$

2. вихідна логічна функція $\vec{F}_{Vuh}$ є: $x_{14} = \begin{cases} 0 - \textit{правильно розміщеною}, \\ 1 - \textit{неправильно розміщеною}. \end{cases}$

На основі вище зазначеного нами створено таблиці істинності та карти Карно для побудови інверсної функції взаємоперетворення $\vec{F}_{Pk}^{\,i} = \begin{pmatrix} f_5 \\ f_6 \end{pmatrix}$ множини M_1 (табл. 2.9 і табл. 2.10).

Під час аналізу таблиць 2.8, 2.9 та 2.10 нами отримано інверсні функції згідно формули (2.67) для першого блоку модифікованої таблиці у вигляді:

$$f_5 = (x_{13} \oplus x_{14})(x_{10} \oplus x_{11}) \vee (x_{13} \equiv x_{14})(x_9 \oplus x_{11}), \tag{2.71}$$

$$f_6 = (x_{13} \oplus x_{14})(x_9 \oplus x_{12}) \vee (x_{13} \equiv x_{14})(x_{10} \oplus x_{12}). \tag{2.72}$$

Для спрощення знаходження закономірностей використання операцій інверсії застосуємо опис блоків за допомогою множин, що наведений в роботах [10, 53].

Таблиця 2.9

Карта Карно для отримання функції інверсії f_5

	000	**001**	**011**	**010**	**110**	**111**	**101**	**100**
000	0	0	1	1	1	1	0	0
001	0	0	1	1	0	0	1	1
011	1	1	0	0	0	0	1	1
010	1	1	0	0	1	1	0	0
110	0	0	1	1	0	0	1	1
111	1	1	0	0	0	0	1	1
101	1	1	0	0	1	1	0	0
100	0	0	1	1	1	1	0	0

Таблиця 2.10

Карта Карно для отримання функції інверсії f_6

	000	**001**	**011**	**010**	**110**	**111**	**101**	**100**
000	0	1	1	0	0	1	1	0
001	1	0	0	1	0	1	1	0
011	1	0	0	1	1	0	0	1
010	0	1	1	0	1	0	0	1
110	1	0	0	1	0	1	1	0
111	1	0	0	1	1	0	0	1
101	0	1	1	0	1	0	0	1
100	0	1	1	0	0	1	1	0

Застосовуючи закони мінімізації до одержаних функції інверсій та, враховуючи формули (2.67), (2.68), (2.69) і додатково введені параметри x_{13}, x_{14}, нами отримано наступний алгоритм побудови функцій взаємного криптоперетворення для першого блоку B_1 класифікатора результатів обчислювального експерименту (для множин M_1, M_5, M_9 [10]):

$$F_{Pk}^{i(1,5,9)} = \begin{pmatrix} f_5 \\ f_6 \end{pmatrix} = \begin{pmatrix} f_5^{1,5,9} \\ f_6^{1,5,9} \end{pmatrix} = \\ = \begin{pmatrix} (x_2x_3x_5x_8 \vee x_1x_4x_6x_7)(x_{10} \oplus x_{11}) \vee (x_2x_3x_6x_7 \vee x_1x_4x_5x_8)(x_9 \oplus x_{11}) \\ (x_2x_3x_5x_8 \vee x_1x_4x_6x_7)(x_9 \oplus x_{12}) \vee (x_2x_3x_6x_7 \vee x_1x_4x_5x_8)(x_{10} \oplus x_{12}) \end{pmatrix}. \quad (2.73)$$

Провівши аналогічні дослідження над логічними функціями множин M_5 та M_9, які теж є складовими першого умовного блоку B_1 класифікатора функцій взаємного перетворення, було встановлено, що інверсна функція (2.73) є загальним виглядом інверсних функцій першого та другого розрядів для всіх складових множин функцій взаємоперетворення першого блоку B_1 класифікатора результатів обчислювального експерименту.

Отже, згідно формули (2.70), було створено загальний алгоритм побудови математичної моделі функції взаємного перетворення з

урахуванням інверсій для логічних функцій першого умовного блоку B_1 класифікатора результатів обчислювального експерименту (множини $M_1,\ M_5, M_9$):

$$\vec{F}_{Pk}^{1,5,9} = \begin{pmatrix} f_1 & f_2 & f_5 \\ f_3 & f_4 & f_6 \end{pmatrix} = \begin{pmatrix} (x_3 \oplus x_5) \vee (x_4 \oplus x_6) & (x_1 \oplus x_5) \vee (x_2 \oplus x_6) & (x_2x_3x_5x_8 \vee x_1x_4x_6x_7)(x_{10} \oplus x_{11}) \vee (x_2x_3x_6x_7 \vee x_1x_4x_5x_8)(x_9 \oplus x_{11}) \\ (x_3 \oplus x_7) \vee (x_4 \oplus x_8) & (x_1 \oplus x_7) \vee (x_2 \oplus x_8) & (x_2x_3x_5x_8 \vee x_1x_4x_6x_7)(x_9 \oplus x_{12}) \vee (x_2x_3x_6x_7 \vee x_1x_4x_5x_8)(x_{10} \oplus x_{12}) \end{pmatrix} \quad (2.74)$$

Продовжуючи аналізувати далі табл. 2.9, нами виявлено, що функції взаємоперетворення другого B_2 та третього B_3 блоків класифікатора результатів обчислювального експерименту мають також ідентичні функції інверсій множинно-симетричні відносно першого блоку B_1 класифікатора, множини якого $M_1,\ M_5, M_9$ утворюють головну діагональ даної таблиці.

Тому, виходячи із результатів досліджень логічних функцій першого блоку класифікатора та, провівши аналогічні дослідження логічних функцій решти множин другого B_2 та третього B_3 блоків класифікатора функцій взаємного перетворення відповідно, нами одержано алгоритми побудови математичної моделі функції взаємного перетворення для інших симетричних множин.

Оскільки, функції інверсій $\vec{F}_{Pk}^{\,i} = \begin{pmatrix} f_5 \\ f_6 \end{pmatrix}$ функцій взаємоперетворення множини M_2 другого B_2 блоку класифікатора результатів обчислювального експерименту збігаються з функціями інверсій множини M_4 третього B_3 блоку класифікатора, то одержуємо алгоритм побудови математичної моделі функції взаємного криптоперетворення з урахуванням інверсії для множин M_2 та M_4:

$$\vec{F}_{Pk}^{2,4} = \begin{pmatrix} f_1 & f_2 & f_5 \\ f_3 & f_4 & f_6 \end{pmatrix} = \begin{pmatrix} (x_3 \oplus x_5) \vee (x_4 \oplus x_6) & (x_1 \oplus x_5) \vee (x_2 \oplus x_6) & x_6x_7(x_9 \oplus x_{10} \oplus x_{11}) \vee x_5x_8(x_2x_3(x_{10} \oplus x_{11}) \vee x_1x_4(\bar{x}_{10}x_{11} \vee x_9x_{11})) \\ (x_3 \oplus x_7) \vee (x_4 \oplus x_8) & (x_1 \oplus x_7) \vee (x_2 \oplus x_8) & x_6x_7(x_2x_3(x_{10}\bar{x}_{12} \vee x_{10}x_{12}) \vee x_1x_4(x_9 \oplus x_{12})) \vee x_5x_8(x_9 \oplus x_{10} \oplus x_{12}) \end{pmatrix} \quad (2.75)$$

Функції інверсій $\vec{F}^{i}_{Pk} = \begin{pmatrix} f_5 \\ f_6 \end{pmatrix}$ функцій взаємоперетворення множини M_3 другого B_2 блоку класифікатора результатів обчислювального експерименту збігаються з функціями інверсій множини M_7 третього B_3 блоку класифікатора. Тоді, згідно формули (2.70), одержуємо алгоритм побудови математичної моделі функції взаємного перетворення з урахуванням інверсії для множин M_3 та M_7:

$$\vec{F}^{3,7}_{Pk} = \begin{pmatrix} f_1 & f_2 & f_5 \\ f_3 & f_4 & f_6 \end{pmatrix} = \\ = \begin{pmatrix} (x_3 \oplus x_5) \vee (x_4 \oplus x_6) & (x_1 \oplus x_5) \vee (x_2 \oplus x_6) & x_6x_7(x_2x_3(x_9 \oplus x_{11})) \vee x_{11}(\bar{x}_{10}x_1x_4 \vee x_{10}x_2x_3)) \vee x_5x_8(x_9 \oplus x_{10} \oplus x_{11}) \\ (x_3 \oplus x_7) \vee (x_4 \oplus x_8) & (x_1 \oplus x_7) \vee (x_2 \oplus x_8) & x_5x_8(x_2x_3(x_{10} \oplus x_{12}) \vee x_1x_4\bar{x}_{10}x_{12} \vee x_2x_3x_{10}\bar{x}_{12}) \vee x_6x_7(x_9 \oplus x_{10} \oplus x_{12}) \end{pmatrix} \quad (2.76)$$

Функції інверсій $\vec{F}^{i}_{Pk} = \begin{pmatrix} f_5 \\ f_6 \end{pmatrix}$ функцій взаємоперетворення множини M_6 другого B_2 блоку класифікатора результатів обчислювального експерименту збігаються з функціями інверсій множини M_8 третього B_3 блоку класифікатора. Тоді, згідно формули (2.70), одержуємо алгоритм побудови математичної моделі функції взаємного перетворення з врахуванням інверсії для множин M_6 та M_8:

$$\vec{F}^{6,8}_{Pk} = \begin{pmatrix} f_1 & f_2 & f_5 \\ f_3 & f_4 & f_6 \end{pmatrix} = \\ = \begin{pmatrix} (x_3 \oplus x_5) \vee (x_4 \oplus x_6) & (x_1 \oplus x_5) \vee (x_2 \oplus x_6) & x_6x_7(x_2x_3(x_{10} \oplus x_{11}) \vee x_1x_4(x_9 \oplus x_{11})) \vee x_5x_8(x_9 \oplus x_{10} \oplus x_{11}) \\ (x_3 \oplus x_7) \vee (x_4 \oplus x_8) & (x_1 \oplus x_7) \vee (x_2 \oplus x_8) & x_5x_8(x_2x_3(x_{10} \oplus x_{12}) \vee x_1x_4(x_9 \oplus x_{12})) \vee x_6x_7(x_9 \oplus x_{10} \oplus x_{12}) \end{pmatrix} \quad (2.77)$$

Крім того, для достовірності побудови функцій взаємного перетворення, кожна отримана математична модель (2.74), (2.75), (2.76) та (2.77) повинна враховувати істинність вибору множини логічних функцій. Для цього необхідно враховувати так звану функцію варіанту вибору

множини класифікатора логічних функцій взаємного перетворення y_n, де n – позначення номеру множини класифікатора.

Провівши відповідні дослідження та аналіз табл. 2.9, нами отримано наступні функції варіанту вибору множини:

$$y_{1,5,9} = (\bar{x}_7\bar{x}_6 \vee \bar{x}_8\bar{x}_5)(\bar{x}_1\bar{x}_4 \vee \bar{x}_2\bar{x}_3) \vee x_2x_4x_6(\bar{x}_7 \vee x_8) \vee x_1x_3x_5x_7, \quad (2.78)$$

$$y_{2,4} = x_2x_4\bar{x}_8(\bar{x}_5 \vee \bar{x}_7) \vee x_6x_8(\bar{x}_1\bar{x}_4 \vee \bar{x}_2\bar{x}_3), \quad (2.79)$$

$$y_{3,7} = x_1x_3(\bar{x}_5\bar{x}_8 \vee \bar{x}_6\bar{x}_7) \vee x_5x_7(\bar{x}_2\bar{x}_3 \vee \bar{x}_1\bar{x}_4), \quad (2.80)$$

$$y_{6,8} = \bar{x}_1x_3x_6x_8 \vee x_2x_4x_5x_7. \quad (2.81)$$

Отже, згідно функцій варіанту вибору множини (2.78-2.81), функція інверсій відповідно кожної множини класифікатора набуде наступного вигляду:

$$\vec{F}_{Pk}^{\,i(1,5,9)} = \begin{pmatrix} y_{1,5,9} * f_5^{1,5,9} \\ y_{1,5,9} * f_6^{1,5,9} \end{pmatrix}, \quad (2.82)$$

$$\vec{F}_{Pk}^{\,i(2,4)} = \begin{pmatrix} y_{2,4} * f_5^{2,4} \\ y_{2,4} * f_6^{2,4} \end{pmatrix}, \quad (2.83)$$

$$\vec{F}_{Pk}^{\,i(3,7)} = \begin{pmatrix} y_{3,7} * f_5^{3,7} \\ y_{3,7} * f_6^{3,7} \end{pmatrix}, \quad (2.84)$$

$$\vec{F}_{Pk}^{\,i(6,8)} = \begin{pmatrix} y_{6,8} * f_5^{6,8} \\ y_{6,8} * f_6^{6,8} \end{pmatrix}. \quad (2.85)$$

Аналізуючи повну множину функцій взаємного перетворення, їхні функції інверсій та згідно формули (2.70), запишемо загальний вигляд

функції інверсій для повної множини функцій взаємного перетворення з урахуванням усіх можливих варіантів:

$$\vec{F}_{Pk} = \begin{pmatrix} f_1 & f_2 & f_5 \\ f_3 & f_4 & f_6 \end{pmatrix} = \begin{pmatrix} f_1 & f_2 & f_5^* \\ f_3 & f_4 & f_6^* \end{pmatrix}, \quad (2.86)$$

де функції f_5^* та f_6^* одержані згідно (2.82-2.85):

$$f_5^* = y_{1,5,9} * f_5^{1,5,9} \vee y_{2,4} * f_5^{2,4} \vee y_{3,7} * f_5^{3,7} \vee y_{6,8} * f_5^{6,8}, \quad (2.87)$$

$$f_6^* = y_{1,5,9} * f_6^{1,5,9} \vee y_{2,4} * f_6^{2,4} \vee y_{3,7} * f_6^{3,7} \vee y_{6,8} * f_6^{6,8}. \quad (2.88)$$

Отже, нами було одержано алгоритм побудови математичної моделі функції взаємного перетворення з врахуванням інверсій цих функцій. Але, виходячи із (2.86-2.88), його практичне застосування до повної множини результатів обчислювального експерименту є досить громіздким в обрахунках і не дає можливості побудувати дискретний пристрій придатний для практичної реалізації.

Використаємо підхід, який полягає в тому, що перетворення інформації є рознесеним у часі на перетворення базової функції взаємного перетворення та функції інверсії відповідно щодо (2.10).

Оскільки, загальне правило побудови базової функції взаємного перетворення вже є відомим згідно (2.63), тому дослідимо функцію перетворення $\vec{F}_{Pk}^{\,i} = \begin{pmatrix} f_5 \\ f_6 \end{pmatrix}$ для вхідної $\vec{F}_{Vh}^{\,i} = \begin{pmatrix} x_9 \\ x_{10} \end{pmatrix}$ та вихідної $\vec{F}_{Vuh}^{\,i} = \begin{pmatrix} x_{11} \\ x_{12} \end{pmatrix}$ функції інверсії на основі таблиць істинності.

Проаналізувавши можливі чотири варіанти інверсій для вхідної $\vec{F}_{Vh}^{\,i}$ та вихідної $\vec{F}_{Vuh}^{\,i}$ логічних функцій, нами складено таблицю істинності, під час мінімізації результатів якої одержали наступне твердження: функцією перекодування для логічних вхідної $\vec{F}_{Vh}^{\,i}$ та вихідної $\vec{F}_{Vuh}^{\,i}$ функцій інверсій є

логічна функція $\vec{F}_{Pk}^{\,i} = \begin{pmatrix} f_5 \\ f_6 \end{pmatrix}$, розряди якої це сума за модулем відповідних розрядів вище названих логічних функцій.

Виходячи із вище викладеного матеріалу та, враховуючи (2.65-2.67), отримаємо:

$$\vec{F}_{Pk}^{\,i} = \begin{pmatrix} f_5 \\ f_6 \end{pmatrix} = \begin{pmatrix} x_9 \bar{x}_{11} \vee \bar{x}_9 x_{11} \\ x_{10} \bar{x}_{12} \vee \bar{x}_{10} x_{12} \end{pmatrix} = \begin{pmatrix} x_9 \oplus x_{11} \\ x_{10} \oplus x_{12} \end{pmatrix}. \qquad (2.89)$$

Отже, лише розмежувавши в часі перетворення інформації на обробку базової функції та обробку функції інверсії, можливо отримати алгоритм побудови функцій взаємного перетворення наведений у (2.63) та (2.89), що є придатним стосовно застосування до повної їх множини і практичним стосовно простоти реалізації у подальших дослідженнях.

Отримані теоретичні результати дозволяють перейти до розробки методу підвищення оперативності доступу до конфіденційних інформаційних ресурсів.

2.2.3 Технологія підвищення швидкості доступу до конфіденційних інформаційних ресурсів на основі застосування операцій взаємного криптографічного перетворення

Виходячи з вище сказаного, технологія доступу до інформації полягає в наступному (рис. 2.3).

Отримані в дослідженнях результати дозволяють вдосконалити дану технологію. Враховуючи результати, структурна організація доступу до інформаційних ресурсів набуде нового відображення із врахуванням реалізації методу підвищення оперативності доступу до конфіденційних інформаційних ресурсів (рис. 2.4).

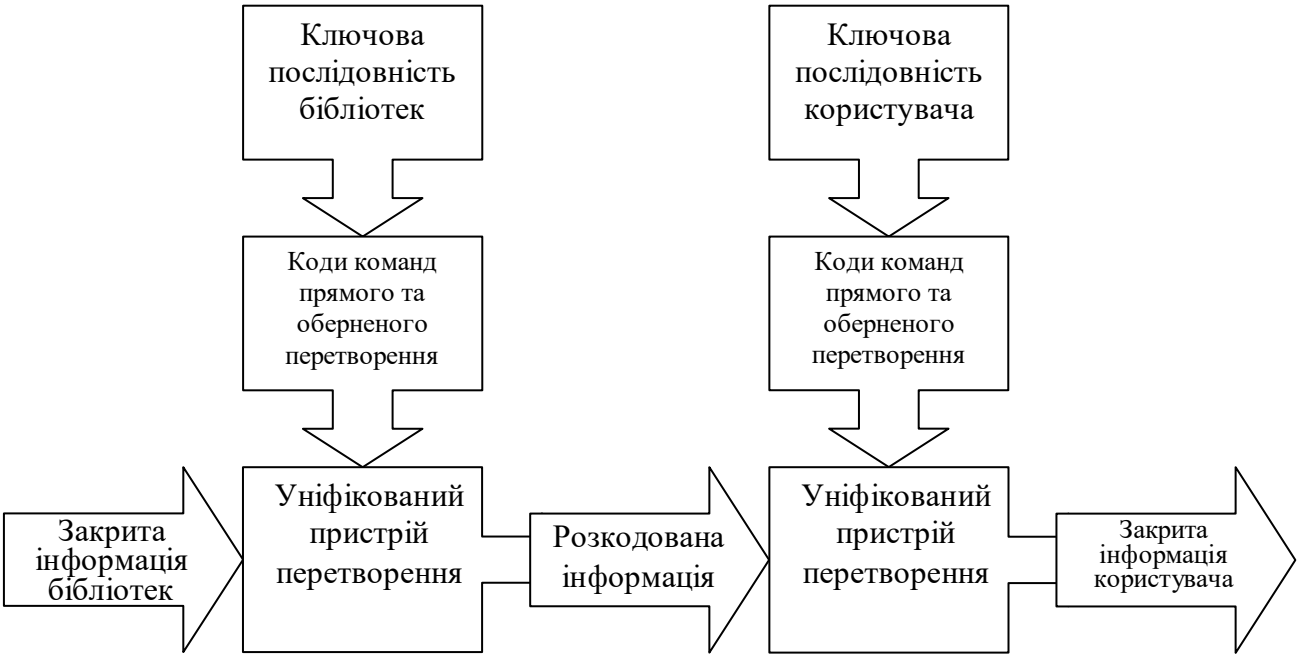


Рис. 2.3. Структурна організація удосконаленого доступу до інформаційних ресурсів

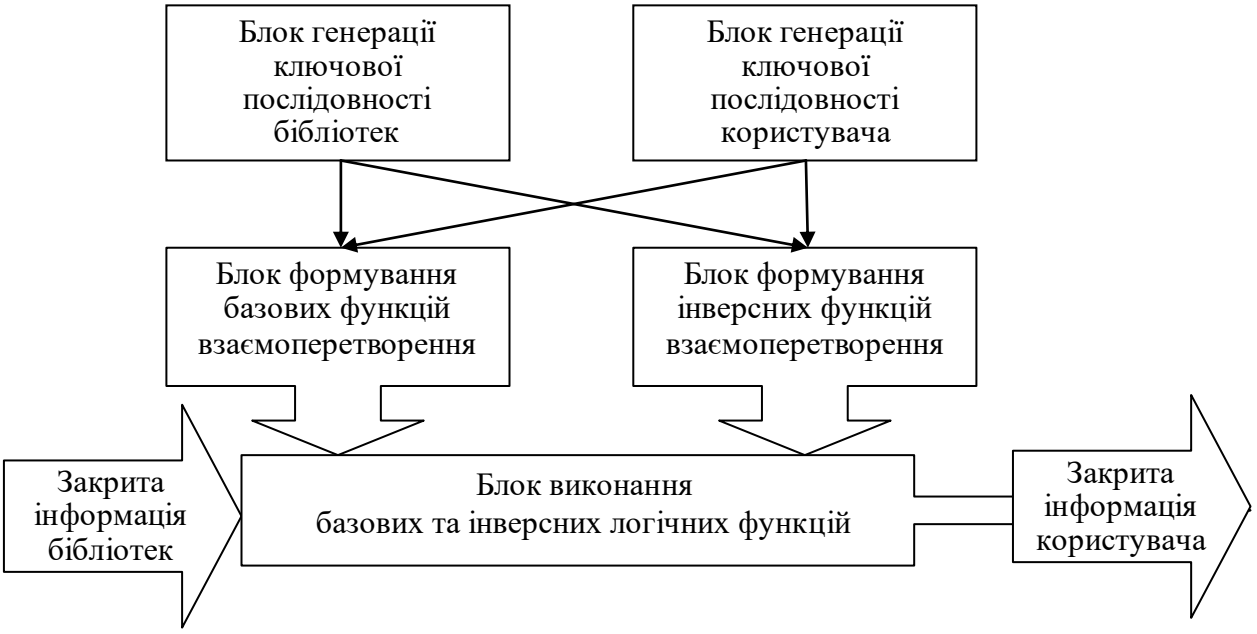


Рис. 2.4. Технологія підвищення оперативності доступу до конфіденційних інформаційних ресурсів в комп’ютерних системах

Узагальнивши отримані результати в підрозділі 2.2, сформулюємо алгоритм, який реалізує метод підвищення оперативності доступу до

конфіденційних інформаційних ресурсів в комп'ютерних системах [11, 52, 57]:

1) аналізуючи ключову послідовність бібліотеки, визначити матрицю вхідної логічної функції, на основі якої виконано пряме перетворення інформації;

2) аналізуючи ключову послідовність користувача, визначити матрицю вихідної логічної функції, на основі якої виконано пряме перетворення інформації користувача;

3) виділити базові вхідну $\vec{F}_{Vh}$ та вихідну $\vec{F}_{Vuh}$ матриці із матриць логічних функцій, що одержані в пунктах 1 і 2:

$$\vec{F}_{Vh} = \begin{pmatrix} x_1 & x_2 \\ x_3 & x_4 \end{pmatrix}, \quad \vec{F}_{Vuh} = \begin{pmatrix} x_5 & x_6 \\ x_7 & x_8 \end{pmatrix};$$

4) на основі виразу (2.64) отримати базову функцію взаємного перетворення інформації:

$$\vec{F}_{Pk} = \begin{pmatrix} f_1 & f_2 \\ f_3 & f_4 \end{pmatrix} = \begin{pmatrix} (x_3 \oplus x_5) \vee (x_4 \oplus x_6) & (x_1 \oplus x_5) \vee (x_2 \oplus x_6) \\ (x_3 \oplus x_7) \vee (x_4 \oplus x_8) & (x_1 \oplus x_7) \vee (x_2 \oplus x_8) \end{pmatrix};$$

5) виділити матриці інверсних вхідної $\vec{F}^{i}_{Vh}$ та вихідної $\vec{F}^{i}_{Vuh}$ функцій із матриць логічних функцій, які одержані в пунктах 1 і 2:

$$\vec{F}^{\,i}_{Vh} = \begin{pmatrix} x_9 \\ x_{10} \end{pmatrix}, \quad \vec{F}^{\,i}_{Vuh} = \begin{pmatrix} x_{11} \\ x_{12} \end{pmatrix};$$

6) на основі виразу (2.89) отримати інверсну функцію взаємного перетворення для логічних вхідної $\vec{F}^{i}_{Vh}$ та вихідної $\vec{F}^{i}_{Vuh}$ функцій інверсій:

$$\vec{F}_{Pk}^{\,i} = \begin{pmatrix} f_5 \\ f_6 \end{pmatrix} = \begin{pmatrix} x_9 \oplus x_{11} \\ x_{10} \oplus x_{12} \end{pmatrix};$$

7) перетворити функцію подану в коді бібліотеки у функцію користувача.

Порівняно з рис. 2.3, отриманий метод підвищує оперативність доступу до конфіденційних інформаційних ресурсів за рахунок заміни операцій оберненого та прямого перетворення на операцію взаємоперетворення.

Отримані математичні моделі синтезу операцій взаємного криптографічного перетворення дозволяють створити програно-апаратні засоби, які забезпечать підвищення швидкості доступу до конфіденційних інформаційних ресурсів [11].

Поряд з цим, використання даних моделей дозволили спростити процес синтезу двохрозрядних операцій оберненого криптографічного перетворення.

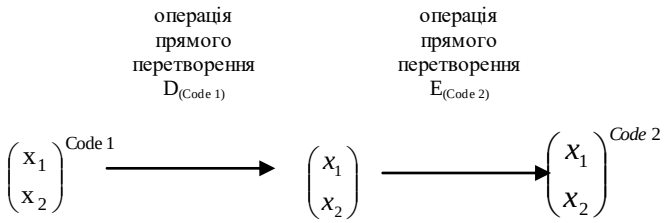
Розглянемо даний результат більш детально.

2.2.4 Дослідження моделей оберненого та взаємного криптографічних перетворень

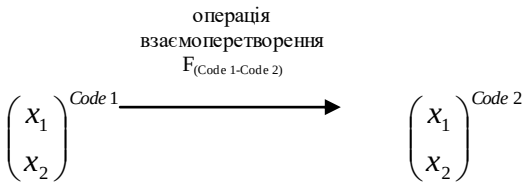
Зрозуміло, що при поєднанні операцій базової, перестановки та інверсії важливе значення відіграє їх порядок застосування. Наприклад, якщо для процесу прямого перетворення названі операції виконувались в заданому порядку, то для процесу оберненого перетворення потрібно їх виконувати відповідно в зворотному.

Розроблений раніше метод підвищення оперативності доступу до конфіденційних інформаційних ресурсів на основі використання логічних операцій для криптографічного перетворення шляхом введення логічних операцій взаємоперетворення дозволив зменшити час доступу до інформації за рахунок заміни процесу «обернене перетворення-пряме перетворення». Адже, якщо процес взаємоперетворення записати двома варіантами

(рис. 2.5), то бачимо, що дійсно застосування операції взаємоперетворення зменшує кількість перетворень, що потрібно виконати:



Варіант 1.



Варіант 2.

Рис. 2.5. Процес перекодування

Аналізуючи схему рис. 2.5 та пам’ятаючи, що операція взаємного перетворення – це бінарне перетворення, яке, в свою чергу, є відображенням множини (повідомлення) самої на себе, то можливий випадок, коли операція оберненого перетворення співпаде з операцією взаємоперетворення, а це означає, що $\begin{pmatrix} x_1 \\ x_2 \end{pmatrix}$ дорівнюватиме $\begin{pmatrix} x_1 \\ x_2 \end{pmatrix}^{Code\ 2}$.

Тобто, наведене вище дає змогу стверджувати, що обернене перетворення – це частковий випадок взаємоперетворення.

Для спрощення отримання математичної моделі побудови операцій взаємного перетворення ми розглядали поєднання логічних операцій без врахування інверсії.

У результаті проведення досліджень нами одержано модель синтезу групи операцій взаємного криптоперетворення без урахування інверсій відповідно матричного подання вхідної та вихідної логічних операцій.

На початку ми поставили, що бінарне перетворення можна записати у вигляді системи алгебраїчних рівнянь (2.9) з умовою виконання

невиродженості. Якщо виключити операцію інверсії, то система рівнянь перепишеться як:

$$\begin{cases} x_1^* = a_{11}x_1 \oplus a_{12}x_2, \\ x_2^* = a_{21}x_1 \oplus a_{22}x_{22}. \end{cases}, \text{ де } a_{ij} = \{0; 1\},\ i = \overline{1,2},\ j = \overline{1,2}.$$

Система називається невиродженою, якщо визначник системи лінійних рівнянь відмінний від нуля, тобто $a_{11} \cdot a_{22} - a_{12} \cdot a_{21} \neq 0$. А враховуючи, що $a_{ij} = \{0; 1\}$, то дана умова виконуватиметься в двох випадках:

1) якщо перший добуток дорівнюватиме одиниці $a_{11} \cdot a_{22} = 1$, тоді $a_{11} = a_{22} = 1$, а другий - нулю $a_{12} \cdot a_{21} = 0$, тоді:

- $a_{12} = a_{21} = 0$ або
- $a_{12} = 0, a_{21} = 1$ або
- $a_{12} = 1, a_{21} = 0$;

2) якщо другий добуток дорівнюватиме одиниці $a_{12} \cdot a_{21} = 1$, тоді $a_{12} = a_{21} = 1$, а перший - нулю $a_{11} \cdot a_{22} = 0$, тоді:

- $a_{11} = a_{22} = 0$ або
- $a_{11} = 0, a_{22} = 1$ або
- $a_{11} = 1, a_{22} = 0$;

Для того, щоб визначити модель операції взаємного перетворення, потрібно визначити перетворення f_1 над першим елементом x_1 та перетворення f_2 над другим x_2. Якщо зобразити це системою, то дана умова виконуватиметься для першого випадку при $a_{12} = a_{21} = 0$. Тобто, система матиме вигляд:

$$\begin{cases} x_1^{**} = a_{11}x_1^{*} \\ x_2^{**} = a_{22}x_2^{*} \end{cases}, \text{ де } \begin{cases} x_1^{*} = a_{11}x_1 \\ x_2^{*} = a_{22}x_2 \end{cases}, \quad \text{де } a_{ij} = \{0; 1\},\ i = \overline{1,2},\ j = \overline{1,2}.$$

Значить, можна записати, що операція взаємного перетворення визначається, коли $x_i^{**} = f_i(x_i^*)$, *де* $i \in \{0,1\}$, тобто можна зобразити як:

Таблиця 2.10

Значення коефіцієнтів a_{ij}		Операція перетворення
1	0	f_1
0	1	f_2

У роботі [18] проведений синтез функції взаємоперетворення на основі функції оберненого перетворення шести функцій без врахування інверсій. Узагальнений результат з позначенням входів – виходів для моделювання наведений в табл. 2.11.

Таблиця 2.11

Базова функція (без врахування інверсії)

Вхідна		**Вихідна**		**Перетворення**	
a_{11}	a_{12}	a_{11}^*	a_{12}^*	$f_1(a_1) = (a_{21} \oplus a_{11}^*) \vee (a_{22} \oplus a_{12}^*)$	$f_1(a_2) = (a_{11} \oplus a_{11}^*) \vee (a_{12} \oplus a_{12}^*)$
a_{21}	a_{22}	a_{21}^*	a_{22}^*	$f_2(a_1) = (a_{21} \oplus a_{21}^*) \vee (a_{22} \oplus a_{22}^*)$	$f_2(a_2) = (a_{11} \oplus a_{21}^*) \vee (a_{12} \oplus a_{22}^*)$

За умови коли коефіцієнти набудуть значення згідно табл. 2.10, перетворення видозміняться таким чином як показано в (2.90):

$$
\begin{aligned}
&f_1(a_2) = (a_{11} \oplus a_{11}^*) \vee (a_{12} \oplus a_{12}^*) = (a_{11} \oplus 1) \vee (a_{12} \oplus 0) = \bar{a}_{11} \vee a_{12};\\
&f_1(a_1) = (a_{21} \oplus a_{11}^*) \vee (a_{22} \oplus a_{12}^*) = (a_{21} \oplus 1) \vee (a_{22} \oplus 0) = \bar{a}_{21} \vee a_{22};\\
&f_2(a_1) = (a_{21} \oplus a_{21}^*) \vee (a_{22} \oplus a_{22}^*) = (a_{21} \oplus 0) \vee (a_{22} \oplus 1) = a_{21} \vee \bar{a}_{22};\\
&f_2(a_2) = (a_{11} \oplus a_{21}^*) \vee (a_{12} \oplus a_{22}^*) = (a_{11} \oplus 0) \vee (a_{12} \oplus 1) = a_{11} \vee \bar{a}_{12}.
\end{aligned}
\qquad (2.90)
$$

Враховуючи виключну ситуацію, коли функція взаємного перетворення співпадає з функцією оберненого перетворення можна

записати результат синтезу моделей функції оберненого перетворення для шести операцій, тобто набору базових операцій з урахуванням перестановок (табл. 2.12).

Таблиця 2.12

Результат синтеза функції оберненого перетворення з урахуванням перестановок

Пряме перетворення		**Обернене (взаємоперетворення)**	
a_{11}	a_{12}	$f_1(a_1) = \bar{a}_{21} \vee a_{22}$	$f_1(a_2) = \bar{a}_{11} \vee a_{12}$
a_{21}	a_{22}	$f_2(a_1) = a_{21} \vee \bar{a}_{22}$	$f_2(a_2) = a_{11} \vee \bar{a}_{12}$

Якщо виключити перестановки, то функція прямого перетворення співпадатиме з функцією оберненого перетворення, а це означає, що коефіцієнти не підлягають перетворенню (табл. 2.13).

Таблиця 2.13

Результат синтеза функції оберненого перетворення без перестановки

Пряме перетворення		**Обернене**	
a_{11}	a_{12}	$f_1(a_1) = a_{11}$	$f_1(a_2) = a_{12}$
a_{21}	a_{22}	$f_2(a_1) = a_{21}$	$f_2(a_2) = a_{22}$

Як бачимо з табл. 2.13 функція взаємного перетворення співпадає з функцією оберненого, а та, в свою чергу, повністю співпадає з функцією прямого перетворення.

Тобто, всі коефіцієнти, що отримали під час процесу прямого перетворення дорівнюватимуть коефіцієнтам, що потрібно знайти під час оберненого перетворення.

Отже, у даному дослідженні подано у матричному та алгебраїчному видах двохрозрядні операції криптографічного перетворення інформації.

Розглянуто методику формування груп операцій на основі поєднання базових операцій з перестановкою та інверсією. Виокремлено основний критерій знаходження функції оберненого перетворення для кожної логічної функції прямого перетовврення. Реалізовано побудову моделі процесу оберненого перетворення для групи двохрозрядних операцій криптографічного перетворення інформації. Отримано модель побудови операцій оберненого криптоперетворення, що є найбільш придатними для реалізації на практиці.

2.2.5 Формалізація методу синтезу матричних операцій взаємного криптографічного перетворення інформації

Результати дослідження були формалізовані і представлені наступним алгоритмом [51, 53].

Якщо операції криптографічного прямого перетворення без урахування групи операцій інверсії задані виразами:

$$\vec{F}_{k1} = \begin{pmatrix} a_{11}x_1 \oplus a_{12}x_2 \oplus ... \oplus a_{1n}x_n \\ a_{21}x_1 \oplus a_{22}x_2 \oplus ... \oplus a_{2n}x_n \\ . \quad . \quad . \quad . \quad . \quad . \quad . \quad . \quad . \quad . \\ a_{n1}x_1 \oplus a_{n2}x_2 \oplus ... \oplus a_{n\,n}x_n \end{pmatrix}, \tag{2.91}$$

де $a_{ij} \in [0,1]$; $x_1 ... x_n$ – операнди-розряди відповідно; $\oplus$ – операція «сума за mod 2»;

$$\vec{F}_{k2} = \begin{pmatrix} c_{11}x_1 \oplus c_{12}x_2 \oplus ... \oplus c_{1n}x_n \\ c_{21}x_1 \oplus c_{22}x_2 \oplus ... \oplus c_{2n}x_n \\ . \quad . \quad . \quad . \quad . \quad . \quad . \quad . \quad . \quad . \\ c_{n1}x_1 \oplus c_{n2}x_2 \oplus ... \oplus c_{n\,n}x_n \end{pmatrix}, \tag{2.92}$$

де $c_{ij} \in [0,1]$; $x_1 ... x_n$ – операнди-розряди відповідно, тоді операція криптографічного взаємного перетворення буде задана виразом:

$$\vec{F}_p = \begin{pmatrix} d_{11}y_1 \oplus d_{12}y_2 \oplus ... \oplus d_{1n}y_n \\ d_{21}y_1 \oplus d_{22}y_2 \oplus ... \oplus d_{2n}y_n \\ . \quad . \quad . \quad . \quad . \quad . \quad . \quad . \quad . \quad . \quad . \quad . \\ d_{n1}y_1 \oplus d_{n2}y_2 \oplus ... \oplus d_{n\,n}y_n \end{pmatrix}, \tag{2.93}$$

де $d_{ij} \in [0,1]$; $x_1 ... x_n$ – операнди-розряди відповідно.

Наведемо детальний опис процесу знаходження операції (матриці) взаємного перетворення [53].

$$\vec{F}_p = \begin{pmatrix} d_{11}(a_{11}x_1 \oplus a_{12}x_2 \oplus ... \oplus a_{1n}x_n) \oplus d_{12}(a_{21}x_1 \oplus a_{22}x_2 \oplus ... \oplus a_{2n}x_n) \oplus ... \oplus \\ \oplus d_{1n}(a_{n1}x_1 \oplus a_{n2}x_2 \oplus ... \oplus a_{n\,n}x_n) \\ d_{21}(a_{11}x_1 \oplus a_{12}x_2 \oplus ... \oplus a_{1n}x_n) \oplus d_{22}(a_{21}x_1 \oplus a_{22}x_2 \oplus ... \oplus a_{2n}x_n) \oplus ... \oplus \\ \oplus d_{2n}(a_{n1}x_1 \oplus a_{n2}x_2 \oplus ... \oplus a_{n\,n}x_n) \\ . \quad . \quad . \quad . \quad . \quad . \quad . \quad . \quad . \quad . \quad . \quad . \quad . \\ d_{n1}(a_{11}x_1 \oplus a_{12}x_2 \oplus ... \oplus a_{1n}x_n) \oplus d_{n2}(a_{21}x_1 \oplus a_{22}x_2 \oplus ... \oplus a_{2n}x_n) \oplus ... \oplus \\ \oplus d_{nn}(a_{n1}x_1 \oplus a_{n2}x_2 \oplus ... \oplus a_{n\,n}x_n) \end{pmatrix} = \tag{2.94}$$

$$= \begin{pmatrix} c_{11}x_1 \oplus c_{12}x_2 \oplus ... \oplus c_{1n}x_n \\ c_{21}x_1 \oplus c_{22}x_2 \oplus ... \oplus c_{2n}x_n \\ . \quad . \quad . \quad . \quad . \quad . \quad . \quad . \quad . \quad . \quad . \quad . \\ c_{n1}x_1 \oplus c_{n2}x_2 \oplus ... \oplus c_{n\,n}x_n \end{pmatrix},$$

Цей процес можна представити у вигляді таких етапів:

1. Знайдемо перший рядок матриці взаємного перетворення. Оскільки

$$\begin{aligned} &d_{11}(a_{11}x_1 \oplus a_{12}x_2 \oplus ... \oplus a_{1n}x_n) \oplus d_{12}(a_{21}x_1 \oplus a_{22}x_2 \oplus ... \oplus a_{2n}x_n) \oplus \\ &\oplus ... \oplus d_{1n}(a_{n1}x_1 \oplus a_{n2}x_2 \oplus ... \oplus a_{n\,n}x_n) = c_{11}x_1 \oplus c_{12}x_2 \oplus ... \oplus c_{1n}x_n \end{aligned}, \tag{2.95}$$

тоді d_{1i} є рішенням системи рівнянь:

$$\begin{cases} d_{11}a_{11} \oplus d_{12}a_{21} \oplus ... \oplus d_{1n}a_{n1} = c_{11} \\ d_{11}a_{12} \oplus d_{12}a_{22} \oplus ... \oplus d_{1n}a_{n2} = c_{12} \\ . \quad . \quad . \quad . \quad . \quad . \quad . \quad . \quad . \quad . \quad . \\ d_{11}a_{1n} \oplus d_{12}a_{2n} \oplus ... \oplus d_{1n}a_{nn} = c_{1n} \end{cases}. \tag{2.96}$$

2. Знайдемо другий рядок матриці взаємного перетворення. Оскільки

$$\begin{array}{l} d_{21}(a_{11}x_1 \oplus a_{12}x_2 \oplus ... \oplus a_{1n}x_n) \oplus d_{22}(a_{21}x_1 \oplus a_{22}x_2 \oplus ... \oplus a_{2n}x_n) \oplus \\ \oplus ... \oplus d_{2n}(a_{n1}x_1 \oplus a_{n2}x_2 \oplus ... \oplus a_{nn}x_n) = c_{21}x_1 \oplus c_{22}x_2 \oplus ... \oplus c_{2n}x_n \end{array}, \tag{2.97}$$

тоді d_{2i} є рішенням системи рівнянь:

$$\begin{cases} d_{21}a_{11} \oplus d_{22}a_{21} \oplus ... \oplus d_{2n}a_{n1} = c_{21} \\ d_{21}a_{12} \oplus d_{22}a_{22} \oplus ... \oplus d_{2n}a_{n2} = c_{22} \\ . \quad . \quad . \quad . \quad . \quad . \quad . \quad . \quad . \quad . \quad . \\ d_{21}a_{1n} \oplus d_{22}a_{2n} \oplus ... \oplus d_{2n}a_{nn} = c_{2n} \end{cases}. \tag{2.98}$$

3. Знайдемо n-й рядок матриці взаємного перетворення. Оскільки

$$\begin{array}{l} d_{n1}(a_{11}x_1 \oplus a_{12}x_2 \oplus ... \oplus a_{1n}x_n) \oplus d_{n2}(a_{21}x_1 \oplus a_{22}x_2 \oplus ... \oplus a_{2n}x_n) \oplus \\ \oplus ... \oplus d_{nn}(a_{n1}x_1 \oplus a_{n2}x_2 \oplus ... \oplus a_{nn}x_n) = c_{n1}x_1 \oplus c_{n2}x_2 \oplus ... \oplus c_{nn}x_n \end{array}, \tag{2.99}$$

тоді d_{ni} є рішенням системи рівнянь:

$$\begin{cases} d_{n1}a_{11} \oplus d_{n2}a_{21} \oplus ... \oplus d_{nn}a_{n1} = c_{n1} \\ d_{n1}a_{12} \oplus d_{n2}a_{22} \oplus ... \oplus d_{nn}a_{n2} = c_{n2} \\ . \quad . \quad . \quad . \quad . \quad . \quad . \quad . \quad . \quad . \quad . \\ d_{n1}a_{1n} \oplus d_{n2}a_{2n} \oplus ... \oplus d_{nn}a_{nn} = c_{nn} \end{cases}. \tag{2.100}$$

Вирази (2.91)–(2.100) можна розглядати як метод синтезу матричних операцій криптографічного взаємного перетворення [15].

Приклади побудови матричної операції взаємного перетворення за модулем два при відомих матричних операціях перетворення наведені в [53]. На основі наведених прикладів можна зробити висновок про коректність розробленого методу синтезу матричних операцій криптографічного взаємного перетворення [15].

Теоретична база, побудована на основі розроблених методів синтезу матричних операцій криптографічного прямого та взаємного перетворення, дає можливість перейти до реалізації швидкодіючих систем комп'ютерної криптографії для здійснення захисту інформації шляхом розробки спеціалізованих програмних та апаратних засобів.

Розроблений метод синтезу операцій взаємного криптографічного перетворення дає можливість [6, 8]:

1) зменшити час доступу до конфіденційних інформаційних ресурсів за рахунок заміни етапів перетворення у форматі користувача на етап взаємного перетворення;

2) підвищити конфіденційність збереження інформації за рахунок обмеження доступу технічних працівників електронних бібліотек до конфіденційних інформаційних ресурсів;

3) цей підхід дозволяє використовувати для побудови систем захисту конфіденційних інформаційних ресурсів будь-які спеціалізовані логічні функції, придатні для криптографії.

У процесі дисертаційного дослідження було встановлено ряд закономірностей, які дають змогу аналітично побудувати матричну операцію взаємного перетворення при відомих матричних операціях перетворення [15].

2.3 Побудова та формалізація методології синтезу і аналізу логічних операцій для криптографічного перетворення інформації

Розроблені та узагальнені методи синтезу елементарних функцій, а також методи синтезу операцій прямого, оберненого та взаємного криптографічного перетворення, на прикладі матричних операцій криптографічного перетворення, дозволяють сформулювати основні положення методології синтезу і аналізу логічних операцій для криптографічного перетворення інформації.

Необхідність розробки даної методології полягає в створенні технології побудови методів синтезу операцій криптографічного перетворення інформації, яка в свою чергу, забезпечить розробників криптографічних алгоритмів новими можливостями для побудови як криптопримітивів так і криптосистем в цілому.

Вирішення даної проблеми «в лоб» на основі обчислювального експерименту з послідуючим узагальненням результатів не може бути реалізовано із-за комбінаторного збільшення кількості як розрахунків та і їх результатів.

Наприклад, для байта інформації існує 258! таблиць підстановки, кожна з яких може бути представлена за допомогою 8 елементарних функцій криптографічного перетворення. Як наслідок, можливо побудувати 258! операцій криптографічного перетворення [53]. Для двох байтів інформації (16 біт) існує 65536! таблиць підстановок, кожна з яких може бути представлена за допомогою 16 елементарних функцій криптографічного перетворення. Побудувати дану множину підстановок на даний час не є технічно можливим, тим більше неможливо провести аналіз та визначення кращих таблиць підстановок. У даний час відсутня можливість збереження та використання сукупності множини таблиць підстановок у криптографічних алгоритмах.

Основна концепція побудови методології синтезу операцій криптографічного перетворення інформації полягає у класифікації операцій криптографічного перетворення та їх невід'ємної складової – елементарних функцій на групи, що дозволяє проводити паралельно дослідження кожної з груп окремо. Крім того, класифікувати операції криптоперетворення на базові операції, операції перестановки та операції інверсії, а елементарні функції класифікувати на прямі та обернені, що забезпечить необхідність та можливість синтезу і дослідження лише базових операцій криптографічного перетворення.

Розглянемо кількісні характеристики для моделювання n–розрядних операцій криптографічного перетворення операцій.

Якщо $M_f = \{f_1, f_2, f_3, \ldots f_m\}$ – множина елементарних функцій, тоді $m = 2^{2^n}$.

Якщо $M_f = \{f_1, f_2, f_3, \ldots f_p\}$ – множина елементарних функцій для безнадлишкового криптографічного перетворення, тоді $p = C_{2^n}^{2^{n-1}}$.

Якщо відібрана на основі класифікації підмножина елементарних функцій криптографічного перетворення складає, наприклад, k частину від загальної кількості елементарних функцій для криптографічного перетворення, тоді на попередньому етапі дослідження аналізується підмножина $M_f^* = \{f_1, f_2, f_3, \ldots f_v\}$, де $v = \frac{1}{k} C_{2^n}^{2^{n-1}}$, а в процесі моделювання буде використано $g = \frac{1}{2k} C_{2^n}^{2^{n-1}}$ елементарних функцій.

Якщо $M_F = \{F_1, F_2, F_3, \ldots F_p\}$ – множина n–розрядних операцій криптографічного перетворення, тоді $p = 2^n!$. Тому в процесі моделювання необхідно побудувати лише множину базових операцій, яка

складає $M_F^* = \{F_1, F_2, F_3, \ldots F_v\}$, де $v = \frac{2^n!}{2^n \cdot n!}$.

Виходячи з наведеного, можна стверджувати, що при проведенні моделювання і дослідженні кількість елементарних функцій для криптографічного перетворення зменшується в $2k$ разів, а кількість операцій криптографічного перетворення зменшується в $2^n \cdot n!$ разів.

Якщо підмножина елементарних функцій для криптографічного перетворення M_f^* вибрана і поділена на прямі та обернені операції правильно, тоді отримана в процесі моделювання на її основі підмножина M_F^* забезпечує реалізацію прямого, оберненого та взаємного криптографічного перетворення.

Наведені вирази для кількісних характеристик показують, що при значеннях n 3, 4 та 5 дані множини операцій криптоперетворення можуть бути отримані на основі обчислювального експерименту як таблиці підстановок.

Проте таблична реалізація операцій криптоперетворення, як щодо швидкості реалізації, так і щодо об’єму необхідної пам’яті, значно поступається аналітичній реалізації на основі моделей операцій прямого, оберненого та взаємного криптоперетворення.

Для практичної реалізації операцій криптографічного перетворення необхідно:

1. Класифікувати елементарні функції заданої розрядності на групи, виходячи із складності мінімальних диз'юнктивно нормальних форм подання. Складність операції будемо оцінювати кількістю операцій в її поданні.

2. Визначити групу елементарних функцій, яка не досліджувалася раніше.

3. На основі різних форм подання спростити сприйняття процесу реалізації функції, встановити логічні взаємозв’язки, та основну логічну

змінну, на основі якої побудована елементарна функція.

4. Побудувати модель елементарної функції, на основі якої розробити методи синтезу груп прямих та обернених елементарних функцій, а також повної групи вибраних елементарних функцій. Для кожної групи елементарних функцій вдосконалюються існуючі або розробляються нові методи синтезу для забезпечення простоти та швидкості їх реалізації.

5. На основі синтезованої групи прямих елементарних функцій записуються отримані за результатами моделювання базові операції криптографічного перетворення в аналітичному поданні. Розробляється новий або вдосконалюється існуючий метод синтезу базових операцій криптографічного перетворення для даної групи операцій.

6. З урахуванням особливостей побудованої групи операцій будується узагальнена аналітична модель операції даної групи, на основі якої розробляється метод синтезу операцій криптографічного перетворення, що придатний для практичної реалізації.

7. У синтезованій групі операцій встановлюються взаємозв’язки між операціями для забезпечення оберненого та взаємного перетворення. Розробляються методи синтезу операцій оберненого та взаємного криптографічного перетворення.

8. Проводиться аналіз можливості використання розроблених моделей та методів для синтезу аналогічних груп операцій (побудованих на основі аналогічних елементарних функцій за своїм фізичним чи математичним змістом) більшої розрядності. За позитивних результатів аналізу проводиться вдосконалення розроблених методів для синтезу груп операцій криптографічного перетворення заданої розрядності.

Запропонована методологія структурована і представлена на рис. 2.6, де відображені основні етапи синтезу операцій прямого оберненого та взаємного криптоперетворення, а також відображені логічні зв’язки між даними етапами.

Рис. 2.6. Методологія синтезу і аналізу логічних операцій для криптографічного перетворення інформації

Синтезувавши нові елементарні функції та побудовані на їх основі операції криптоперетворення, будуть отримані нові можливості для вдосконалення криптопримітивів. Зрозумівши фізичний зміст даних елементарних функції та операції криптоперетворення, будуть отримані можливості для побудови нових криптопримітивів.

2.4 Висновки до другого розділу

Вперше розроблена методологія синтезу операцій криптографічного перетворення інформації на основі існуючих та розроблених методів синтезу операцій прямого, оберненого та взаємного криптографічного перетворення шляхом їх класифікації та узагальнення, що забезпечило теоретичну можливість побудови нових операцій для конструювання алгоритмів комп'ютерної криптографії з покращеними показниками ефективності.

1. Шляхом аналізу та узагальнення існуючих, вдосконалених і розроблених методів синтезу елементарних функцій, методів синтезу операцій прямого та оберненого криптографічного перетворення побудовано методи синтезу груп матричних операцій криптографічного перетворення за рахунок збільшення кількості елементарних функцій на основі додавання за модулем два від більшої кількості змінних, шляхом побудови правил синтезу обернених операцій та модифікації операції з забезпеченням збереження інформативності перетворення, що дало змогу розширити множину операцій криптографічного перетворення для побудови систем комп'ютерної криптографії підвищеної криптостійкості.

2. Для забезпечення підвищення оперативності доступу до конфіденційних інформаційних ресурсів на основі матричних операцій криптографічного перетворення розроблено метод синтезу операцій матричного криптографічного взаємного перетворення шляхом побудови правил синтезу операцій взаємного перетворення в групах матричних операцій.

3. Застосування розробленої методології синтезу і аналізу операцій криптографічного перетворення інформації забезпечує теоретичну базу побудови нових операцій для конструювання алгоритмів захисту з покращеними показниками ефективності.

Результати розділу опубліковані в [6-16, ,18, 19, 23, 51, 52, 61-63, 64, 66, 87-90].

РОЗДІЛ 3
СИНТЕЗ ЛОГІЧНИХ ФУНКЦІЙ ТА ОПЕРАЦІЙ КРИПТОГРАФІЧНОГО ПЕРЕТВОРЕННЯ ІНФОРМАЦІЇ НА ОСНОВІ ЗАПРОПОНОВАНОЇ МЕТОДОЛОГІЇ

3.1 Класифікація множини трирозрядних основних елементарних функцій

Перевіримо коректність розробленої методології синтезу операцій криптографічного перетворення на прикладі однієї з груп трьохрозрядних операцій. Для цього проведемо класифікацію результатів обчислювального експерименту,що подані в табл. 2.4 за складністю. Складність елементарної функції криптографічного перетворення визначається як сума операцій диз'юнкції та кон'юнкції в мінімізованій формі запису моделі функції [166, 170, 172].

Класифікація формалізованих результатів обчислювального експерименту за складністю наведена в табл. 3.1 [23].

Проведемо детальний аналіз елементарних функцій, які подані в табл. 3.1. Класифікація трирозрядних елементарних функцій в залежності від способів їх побудови наведена на рис. 3.1.

Дослідження форм представлення трирозрядних основних елементарних функцій та криптографічних операцій на їх основі [18] дає можливість вивчити дані функції та способи їх реалізації, а також провести їх класифікацію відповідно до функціональних особливостей.

Виходячи з аналізу математичних моделей елементарних функцій, можна виділити групу елементарних функцій, які забезпечують перестановки розрядів. Тобто на основі цих елементарних функцій будуються операції криптографічного перетворення, які забезпечують виконання перестановок розрядів інформації, що кодуємо.

Таблиця 3.1

Класифікація трирозрядних елементарних функцій для криптографічного перетворення інформації за складністю

Пряма елементарна функція			Обернена елементарна функція		
Код функції		Опис функції	Код функції		Опис функції
00001111	15	$f_{15} = x_1$	11110000	240	$f_{240} = \bar{x}_1$
00110011	51	$f_{51} = x_2$	11001100	204	$f_{204} = \bar{x}_2$
01010101	85	$f_{85} = x_3$	10101010	170	$f_{170} = \bar{x}_3$
00111100	60	$f_{60} = \bar{x}_1 \cdot x_2 \vee x_1 \cdot \bar{x}_2$	11000011	195	$f_{195} = \bar{x}_1 \cdot \bar{x}_2 \vee x_1 \cdot x_2$
01011010	90	$f_{90} = \bar{x}_1 \cdot x_3 \vee x_1 \cdot \bar{x}_3$	10100101	165	$f_{165} = \bar{x}_1 \cdot \bar{x}_3 \vee x_1 \cdot x_3$
01100110	102	$f_{102} = \bar{x}_2 \cdot x_3 \vee x_2 \cdot \bar{x}_3$	10011001	153	$f_{153} = \bar{x}_2 \cdot \bar{x}_3 \vee x_2 \cdot x_3$
00011011	27	$f_{27} = x_1 \cdot \bar{x}_3 \vee x_2 \cdot x_3$	11100100	228	$f_{228} = \bar{x}_1 \cdot \bar{x}_3 \vee \bar{x}_2 \cdot x_3$
00011101	29	$f_{29} = x_1 \cdot \bar{x}_2 \vee x_2 \cdot x_3$	11100010	226	$f_{226} = \bar{x}_1 \cdot \bar{x}_2 \vee x_2 \cdot \bar{x}_3$
00100111	39	$f_{39} = x_1 \cdot x_3 \vee x_2 \cdot \bar{x}_3$	11011000	216	$f_{216} = \bar{x}_1 \cdot x_3 \vee \bar{x}_2 \cdot \bar{x}_3$
00101110	46	$f_{46} = x_1 \cdot \bar{x}_2 \vee x_2 \cdot \bar{x}_3$	11010001	209	$f_{209} = \bar{x}_1 \cdot \bar{x}_2 \vee x_2 \cdot x_3$
00110101	53	$f_{53} = \bar{x}_1 \cdot x_2 \vee x_1 \cdot x_3$	11001010	202	$f_{202} = \bar{x}_1 \cdot \bar{x}_2 \vee x_1 \cdot \bar{x}_3$
00111010	58	$f_{58} = \bar{x}_1 \cdot x_2 \vee x_1 \cdot \bar{x}_3$	11000101	197	$f_{197} = \bar{x}_1 \cdot \bar{x}_2 \vee x_1 \cdot x_3$
01000111	71	$f_{71} = x_1 \cdot x_2 \vee \bar{x}_2 \cdot x_3$	10111000	184	$f_{184} = \bar{x}_1 \cdot x_2 \vee \bar{x}_2 \cdot \bar{x}_3$
01001110	78	$f_{78} = x_1 \cdot \bar{x}_3 \vee \bar{x}_2 \cdot x_3$	10110001	177	$f_{177} = \bar{x}_1 \cdot \bar{x}_3 \vee x_2 \cdot x_3$
01010011	83	$f_{83} = x_1 \cdot x_2 \vee \bar{x}_1 \cdot x_3$	10101100	172	$f_{172} = x_1 \cdot \bar{x}_2 \vee \bar{x}_1 \cdot \bar{x}_3$
01011100	92	$f_{92} = x_1 \cdot \bar{x}_2 \vee \bar{x}_1 \cdot x_3$	10100011	163	$f_{163} = x_1 \cdot x_2 \vee \bar{x}_1 \cdot \bar{x}_3$
01110010	114	$f_{114} = \bar{x}_1 \cdot x_3 \vee x_2 \cdot \bar{x}_3$	10001101	141	$f_{141} = x_1 \cdot x_3 \vee \bar{x}_2 \cdot \bar{x}_3$
01110100	116	$f_{116} = \bar{x}_1 \cdot x_2 \vee \bar{x}_2 \cdot x_3$	10001011	139	$f_{139} = x_1 \cdot x_2 \vee \bar{x}_2 \cdot \bar{x}_3$
00010111	23	$f_{23} = x_1 \cdot x_2 \vee x_1 \cdot x_3 \vee x_2 \cdot x_3$	11101000	232	$f_{232} = \bar{x}_1 \cdot \bar{x}_2 \vee \bar{x}_1 \cdot \bar{x}_3 \vee \bar{x}_2 \cdot \bar{x}_3$
00101011	43	$f_{43} = x_1 \cdot x_2 \vee x_1 \cdot \bar{x}_3 \vee x_2 \cdot \bar{x}_3$	11010100	212	$f_{212} = \bar{x}_1 \cdot \bar{x}_2 \vee \bar{x}_1 \cdot x_3 \vee \bar{x}_2 \cdot x_3$
01001101	77	$f_{77} = x_1 \cdot \bar{x}_2 \vee x_1 \cdot x_3 \vee \bar{x}_2 \cdot x_3$	10110010	178	$f_{178} = \bar{x}_1 \cdot x_2 \vee \bar{x}_1 \cdot \bar{x}_3 \vee x_2 \cdot \bar{x}_3$
01110001	113	$f_{113} = \bar{x}_1 \cdot x_2 \vee \bar{x}_1 \cdot x_3 \vee x_2 \cdot x_3$	10001110	142	$f_{142} = x_1 \cdot \bar{x}_2 \vee x_1 \cdot \bar{x}_3 \vee \bar{x}_2 \cdot \bar{x}_3$
00011110	30	$f_{30} = x_1 \cdot \bar{x}_2 \vee x_1 \cdot \bar{x}_3 \vee \bar{x}_1 \cdot x_2 \cdot x_3$	11100001	225	$f_{225} = \bar{x}_1 \cdot \bar{x}_2 \vee \bar{x}_1 \cdot \bar{x}_3 \vee x_1 \cdot x_2 \cdot x_3$
00110110	54	$f_{54} = \bar{x}_1 \cdot x_2 \vee x_2 \cdot \bar{x}_3 \vee x_1 \cdot \bar{x}_2 \cdot x_3$	11001001	201	$f_{201} = \bar{x}_1 \cdot \bar{x}_2 \vee \bar{x}_2 \cdot \bar{x}_3 \vee x_1 \cdot x_2 \cdot \bar{x}_3$
00111001	57	$f_{57} = \bar{x}_1 \cdot x_2 \vee x_2 \cdot x_3 \vee x_1 \cdot \bar{x}_2 \cdot \bar{x}_3$	11000110	198	$f_{198} = \bar{x}_1 \cdot \bar{x}_2 \vee \bar{x}_2 \cdot x_3 \vee x_1 \cdot x_2 \cdot \bar{x}_3$
01001011	75	$f_{75} = x_1 \cdot x_2 \vee x_1 \cdot \bar{x}_3 \vee \bar{x}_1 \cdot \bar{x}_2 \cdot x_3$	10110100	180	$f_{180} = \bar{x}_1 \cdot x_2 \vee \bar{x}_1 \cdot \bar{x}_3 \vee x_1 \cdot \bar{x}_2 \cdot \bar{x}_3$
01010110	86	$f_{86} = \bar{x}_1 \cdot x_3 \vee \bar{x}_2 \cdot x_3 \vee x_1 \cdot x_2 \cdot \bar{x}_3$	10101001	169	$f_{169} = \bar{x}_1 \cdot \bar{x}_3 \vee \bar{x}_2 \cdot \bar{x}_3 \vee x_1 \cdot x_2 \cdot x_3$
01011001	89	$f_{89} = \bar{x}_1 \cdot x_3 \vee x_2 \cdot x_3 \vee x_1 \cdot \bar{x}_2 \cdot \bar{x}_3$	10100110	166	$f_{166} = \bar{x}_1 \cdot \bar{x}_3 \vee x_2 \cdot \bar{x}_3 \vee x_1 \cdot \bar{x}_2 \cdot x_3$
01100011	99	$f_{99} = x_1 \cdot x_2 \vee x_2 \cdot \bar{x}_3 \vee \bar{x}_1 \cdot \bar{x}_2 \cdot x_3$	10011100	156	$f_{156} = x_1 \cdot \bar{x}_2 \vee \bar{x}_2 \cdot \bar{x}_3 \vee \bar{x}_1 \cdot x_2 \cdot x_3$
01100101	101	$f_{101} = x_1 \cdot x_3 \vee \bar{x}_2 \cdot x_3 \vee \bar{x}_1 \cdot x_2 \cdot \bar{x}_3$	10011010	154	$f_{154} = x_1 \cdot \bar{x}_3 \vee \bar{x}_2 \cdot \bar{x}_3 \vee \bar{x}_1 \cdot x_2 \cdot x_3$
01101010	106	$f_{106} = x_1 \cdot \bar{x}_3 \vee x_2 \cdot \bar{x}_3 \vee \bar{x}_1 \cdot \bar{x}_2 \cdot x_3$	10010101	149	$f_{149} = x_1 \cdot x_3 \vee x_2 \cdot x_3 \vee \bar{x}_1 \cdot \bar{x}_2 \cdot \bar{x}_3$
01101100	108	$f_{108} = x_1 \cdot \bar{x}_2 \vee \bar{x}_2 \cdot x_3 \vee \bar{x}_1 \cdot x_2 \cdot \bar{x}_3$	10010011	147	$f_{147} = x_1 \cdot x_2 \vee x_2 \cdot \bar{x}_3 \vee \bar{x}_1 \cdot \bar{x}_2 \cdot \bar{x}_3$
01111000	120	$f_{120} = \bar{x}_1 \cdot x_2 \vee \bar{x}_1 \cdot x_3 \vee x_1 \cdot \bar{x}_2 \cdot \bar{x}_3$	10000111	135	$f_{135} = x_1 \cdot x_2 \vee x_1 \cdot x_3 \vee \bar{x}_1 \cdot \bar{x}_2 \cdot \bar{x}_3$
00101101	45	$f_{45} = x_1 \cdot \bar{x}_2 \vee x_1 \cdot x_3 \vee \bar{x}_1 \cdot x_2 \cdot \bar{x}_3$	11010010	210	$f_{210} = \bar{x}_1 \cdot \bar{x}_2 \vee \bar{x}_1 \cdot x_3 \vee x_1 \cdot x_2 \cdot \bar{x}_3$
01101001	105	$f_{105} = x_1 \oplus x_2 \oplus x_3$	10010110	150	$f_{150} = x_1 \oplus x_2 \oplus x_3 \oplus 1$

До цієї групи функцій відносяться:

$$f_{15} = x_1, \tag{3.1}$$

$$f_{51} = x_2, \tag{3.2}$$

$$f_{85} = x_3, \tag{3.3}$$

$$f_{240} = \bar{x}_1, \tag{3.4}$$

$$f_{204} = \bar{x}_2, \tag{3.5}$$

$$f_{170} = \bar{x}_3. \tag{3.6}$$

Елементарні функції (3.1) – (3.3) є прямими, а елементарні функції (3.4) – (3.6) є оберненими. Основні результати дослідження цих функцій опубліковані в роботі [173]. Слід відмітити, що номери прямих елементарних функцій є меншими за номери обернених елементарних функцій.

Розглянемо наступну групу елементарних функцій. До цієї групи відносяться елементарні функції з блоку № 2 та блоку № 6 (табл. 3.1), а саме:

$$f_{60} = \bar{x}_1 \cdot x_2 \vee x_1 \cdot \bar{x}_2 = x_1 \oplus x_2, \tag{3.7}$$

$$f_{90} = \bar{x}_1 \cdot x_3 \vee x_1 \cdot \bar{x}_3 = x_1 \oplus x_3, \tag{3.8}$$

$$f_{102} = \bar{x}_2 \cdot x_3 \vee x_2 \cdot \bar{x}_3 = x_2 \oplus x_3, \tag{3.9}$$

$$f_{105} = x_1 \oplus x_2 \oplus x_3,, \tag{3.10}$$

$$f_{195} = \bar{x}_1 \cdot \bar{x}_2 \vee x_1 \cdot x_2 = x_1 \equiv x_2 = x_1 \oplus x_2 \oplus 1 \tag{3.11}$$

$$f_{165} = \bar{x}_1 \cdot \bar{x}_3 \vee x_1 \cdot x_3 = x_1 \equiv x_3 = x_1 \oplus x_3 \oplus 1, \tag{3.12}$$

$$f_{153} = \bar{x}_2 \cdot \bar{x}_3 \vee x_2 \cdot x_3 = x_2 \equiv x_3 = x_2 \oplus x_3 \oplus 1, \tag{3.13}$$

$$f_{150} = x_1 \equiv x_2 \equiv x_3 = x_1 \oplus x_2 \oplus x_3 \oplus 1. \tag{3.14}$$

Як видно з представлених виразів, елементарні функції (3.7) – (3.10) є прямими, а елементарні функції (3.11) – (3.14) є оберненими. Слід відмітити, що

номери прямих елементарних функцій є меншими за номери обернених елементарних функцій.

Дану групу представляють елементарні функції, побудовані на основі додавання за модулем 2 (елементарні функції для операцій матричного криптографічного перетворення, або матричні функції) [17]. Типова схема реалізації даних елементарних функцій показана на рис. 3.1.

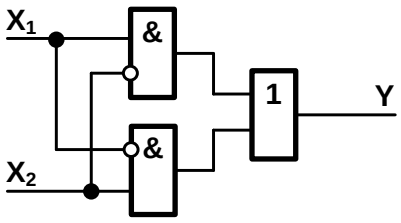


Рис. 3.1. Типова схема реалізації елементарних функцій на основі додавання за модулем 2 (матричні елементарні функції)

На основі дослідження даної групи елементарних функцій була сформульована методологія синтезу операцій криптографічного перетворення, що описана у попередньому розділі (розділ 2).

До наступної групи елементарних функцій відносяться функції з блоку № 3 (табл. 3.1):

$$f_{27} = x_1 \cdot \bar{x}_3 \vee x_2 \cdot x_3 = \begin{cases} x_1 & якщо \quad x_3 = 0 \\ x_2 & якщо \quad x_3 = 1 \end{cases}, \tag{3.15}$$

$$f_{29} = x_1 \cdot \bar{x}_2 \vee x_2 \cdot x_3 = \begin{cases} x_1 & якщо \quad x_2 = 0 \\ x_3 & якщо \quad x_2 = 1 \end{cases}, \tag{3.16}$$

$$f_{39} = x_1 \cdot x_3 \vee x_2 \cdot \bar{x}_3 = \begin{cases} x_2 & якщо \quad x_3 = 0 \\ x_1 & якщо \quad x_3 = 1 \end{cases}, \tag{3.17}$$

$$f_{46} = x_1 \cdot \bar{x}_2 \vee x_2 \cdot \bar{x}_3 = \begin{cases} x_1 & якщо \quad x_2 = 0 \\ \bar{x}_3 & якщо \quad x_2 = 1 \end{cases}, \tag{3.18}$$

$$f_{53} = \bar{x}_1 \cdot x_2 \vee x_1 \cdot x_3 = \begin{cases} x_2 & якщо \quad x_1 = 0 \\ x_3 & якщо \quad x_1 = 1 \end{cases}, \tag{3.19}$$

$$f_{58} = \bar{x}_1 \cdot x_2 \vee x_1 \cdot \bar{x}_3 = \begin{cases} x_2 & якщо \quad x_1 = 0 \\ \bar{x}_3 & якщо \quad x_1 = 1 \end{cases}, \tag{3.20}$$

$$f_{71} = x_1 \cdot x_2 \vee \bar{x}_2 \cdot x_3 = \begin{cases} x_3 & якщо \quad x_2 = 0 \\ x_1 & якщо \quad x_3 = 1 \end{cases}, \tag{3.21}$$

$$f_{78} = x_1 \cdot \bar{x}_3 \vee \bar{x}_2 \cdot x_3 = \begin{cases} x_1 & якщо \quad x_3 = 0 \\ \bar{x}_2 & якщо \quad x_3 = 1 \end{cases}, \tag{3.22}$$

$$f_{83} = x_1 \cdot x_2 \vee \bar{x}_1 \cdot x_3 = \begin{cases} x_3 & якщо \quad x_1 = 0 \\ x_2 & якщо \quad x_1 = 1 \end{cases}, \tag{3.23}$$

$$f_{92} = x_1 \cdot \bar{x}_2 \vee \bar{x}_1 \cdot x_3 = \begin{cases} x_3 & якщо \quad x_1 = 0 \\ \bar{x}_2 & якщо \quad x_1 = 1 \end{cases}, \tag{3.24}$$

$$f_{114} = \bar{x}_1 \cdot x_3 \vee x_2 \cdot \bar{x}_3 = \begin{cases} x_2 & якщо \quad x_3 = 0 \\ \bar{x}_1 & якщо \quad x_3 = 1 \end{cases}, \tag{3.25}$$

$$f_{116} = \bar{x}_1 \cdot x_2 \vee \bar{x}_2 \cdot x_3 = \begin{cases} x_3 & якщо \quad x_2 = 0 \\ \bar{x}_1 & якщо \quad x_3 = 1 \end{cases}, \tag{3.26}$$

$$f_{228} = \bar{x}_1 \cdot \bar{x}_3 \vee \bar{x}_2 \cdot x_3 = \begin{cases} \bar{x}_1 & якщо \quad x_3 = 0 \\ \bar{x}_2 & якщо \quad x_3 = 1 \end{cases}, \tag{3.27}$$

$$f_{226} = \bar{x}_1 \cdot \bar{x}_2 \vee x_2 \cdot \bar{x}_3 = \begin{cases} \bar{x}_1 & якщо \quad x_2 = 0 \\ \bar{x}_3 & якщо \quad x_2 = 1 \end{cases}, \tag{3.28}$$

$$f_{216} = \bar{x}_1 \cdot x_3 \vee \bar{x}_2 \cdot \bar{x}_3 = \begin{cases} \bar{x}_2 & якщо \quad x_3 = 0 \\ \bar{x}_1 & якщо \quad x_3 = 1 \end{cases}, \tag{3.29}$$

$$f_{209} = \bar{x}_1 \cdot \bar{x}_2 \vee x_2 \cdot x_3 = \begin{cases} \bar{x}_1 & якщо \quad x_2 = 0 \\ x_3 & якщо \quad x_2 = 1 \end{cases}, \tag{3.30}$$

$$f_{202} = \bar{x}_1 \cdot \bar{x}_2 \vee x_1 \cdot \bar{x}_3 = \begin{cases} \bar{x}_2 & якщо \quad x_1 = 0 \\ \bar{x}_3 & якщо \quad x_1 = 1 \end{cases}, \tag{3.31}$$

$$f_{197} = \bar{x}_1 \cdot \bar{x}_2 \vee x_1 \cdot x_3 = \begin{cases} \bar{x}_2 & якщо \quad x_1 = 0 \\ x_3 & якщо \quad x_1 = 1 \end{cases}, \tag{3.32}$$

$$f_{184} = \bar{x}_1 \cdot x_2 \vee \bar{x}_2 \cdot \bar{x}_3 = \begin{cases} \bar{x}_3 & якщо \quad x_2 = 0 \\ \bar{x}_1 & якщо \quad x_2 = 1 \end{cases}, \tag{3.33}$$

$$f_{177} = \bar{x}_1 \cdot \bar{x}_3 \vee x_2 \cdot x_3 = \begin{cases} \bar{x}_1 & якщо \quad x_3 = 0 \\ x_2 & якщо \quad x_3 = 1 \end{cases}, \tag{3.34}$$

$$f_{172} = x_1 \cdot \bar{x}_2 \vee \bar{x}_1 \cdot \bar{x}_3 = \begin{cases} x_3 & якщо \quad x_1 = 0 \\ \bar{x}_2 & якщо \quad x_1 = 1 \end{cases}, \tag{3.35}$$

$$f_{163} = x_1 \cdot x_2 \vee \bar{x}_1 \cdot \bar{x}_3 = \begin{cases} \bar{x}_3 & якщо \quad x_1 = 0 \\ x_2 & якщо \quad x_1 = 1 \end{cases}, \tag{3.36}$$

$$f_{141} = x_1 \cdot x_3 \vee \bar{x}_2 \cdot \bar{x}_3 = \begin{cases} \bar{x}_2 & якщо \quad x_3 = 0 \\ x_1 & якщо \quad x_3 = 1 \end{cases}, \tag{3.37}$$

$$f_{139} = x_1 \cdot x_2 \vee \bar{x}_2 \cdot \bar{x}_3 = \begin{cases} \bar{x}_3 & якщо \quad x_2 = 0 \\ x_1 & якщо \quad x_2 = 1 \end{cases}. \tag{3.38}$$

Типова схема реалізації елементарних функцій (3.15) – (3.38) показана на рис. 3.2. Як видно з функціональної схеми, результатом виконання елементарної функції в залежності від значення керуючого входу (вхід два), є встановлення на виході значення сигналу, яке надійшло на перший чи третій входи. Іншими словами, в залежності від значення входу на виході буде встановлено значення одного з двох інших входів у прямому чи інверсному стані. Виходячи з цього, дана група нами названа групою елементарних функцій, в яких інформація керує перестановками [23].

Слід відмітити, що прямі і обернені елементарні функції ні на основі моделей, ні на основі типової реалізації, визначити не вдалося. Встановлено, що кожній елементарній функції є їй обернена, яка з них пряма невідомо. Тому, за аналогією на даному етапі дослідження будемо вважати, що для пари елементарних функцій прямою є та, у якої менший порядковий номер.

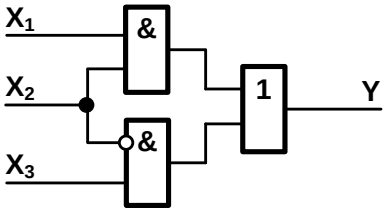


Рис. 3.2. Типова схема реалізації елементарних функцій, в яких інформація керує перестановками

На основі елементарних функцій (3.15) – (3.38) побудовані функції криптографічного перетворення інформації, у яких результат перетворення залежить не лише від операції, а й від самої інформації, що перетворюється. Тобто, інформація керує процесом перетворення на основі перестановок. Результати дослідження цих функцій опубліковані в [3.6 – 3.9].

Наступну групу елементарних функцій представляють функції, що входять до блоку № 4 (табл. 3.1):

$$
\begin{aligned}
f_{23} &= x_1 \cdot x_2 \vee x_1 \cdot x_3 \vee x_2 \cdot x_3 = \\
&= x_1 \cdot x_2 \vee x_1 \cdot x_3 \vee \bar{x}_1 \cdot x_2 \cdot x_3 = \begin{cases} x_2 \cdot x_3 & якщо \quad x_1 = 0 \\ x_2 \vee x_3 & якщо \quad x_1 = 1 \end{cases} = \\
&= x_1 \cdot x_2 \vee x_1 \cdot \bar{x}_2 \cdot x_3 \vee x_2 \cdot x_3 = \begin{cases} x_1 \cdot x_3 & якщо \quad x_2 = 0 \\ x_1 \vee x_3 & якщо \quad x_2 = 1 \end{cases} = \\
&= x_1 \cdot x_2 \cdot \bar{x}_3 \vee x_1 \cdot x_3 \vee x_2 \cdot x_3 = \begin{cases} x_1 \cdot x_2 & якщо \quad x_3 = 0 \\ x_1 \vee x_2 & якщо \quad x_3 = 1 \end{cases}
\end{aligned}
\tag{3.39}
$$

$$
\begin{aligned}
f_{43} &= x_1 \cdot x_2 \vee x_1 \cdot \bar{x}_3 \vee x_2 \cdot \bar{x}_3 = \\
&= x_1 \cdot x_2 \vee x_1 \cdot \bar{x}_3 \vee \bar{x}_1 \cdot x_2 \cdot \bar{x}_3 = \begin{cases} x_2 \cdot \bar{x}_3 & якщо \quad x_1 = 0 \\ x_2 \vee \bar{x}_3 & якщо \quad x_1 = 1 \end{cases} = \\
&= x_1 \cdot x_2 \vee x_1 \cdot \bar{x}_3 \vee \bar{x}_1 \cdot x_2 \cdot \bar{x}_3 = \begin{cases} x_1 \cdot \bar{x}_3 & якщо \quad x_2 = 0 \\ x_1 \vee \bar{x}_3 & якщо \quad x_2 = 1 \end{cases} = \\
&= x_1 \cdot x_2 \cdot x_3 \vee x_1 \cdot \bar{x}_3 \vee \cdot x_2 \cdot \bar{x}_3 = \begin{cases} x_1 \vee x_2 & якщо \quad x_3 = 0 \\ x_1 \cdot x_2 & якщо \quad x_3 = 1 \end{cases}
\end{aligned}
\tag{3.40}
$$

$$
\begin{aligned}
f_{77} &= x_1 \cdot \bar{x}_2 \vee x_1 \cdot x_3 \vee \bar{x}_2 \cdot x_3 = \\
&= x_1 \cdot \bar{x}_2 \vee x_1 \cdot x_3 \vee \bar{x}_1 \cdot \bar{x}_2 \cdot x_3 = \begin{cases} \bar{x}_2 \cdot x_3 & якщо \quad x_1 = 0 \\ \bar{x}_2 \vee x_3 & якщо \quad x_1 = 1 \end{cases} = \\
&= x_1 \cdot \bar{x}_2 \vee x_1 \cdot x_2 \cdot x_3 \vee \bar{x}_2 \cdot x_3 = \begin{cases} x_1 \vee x_3 & якщо \quad x_2 = 0 \\ x_1 \cdot x_3 & якщо \quad x_2 = 1 \end{cases} = \\
&= x_1 \cdot \bar{x}_2 \cdot \bar{x}_3 \vee x_1 \cdot x_3 \vee \bar{x}_2 \cdot x_3 = \begin{cases} x_1 \cdot \bar{x}_2 & якщо \quad x_3 = 0 \\ x_1 \vee \bar{x}_2 & якщо \quad x_3 = 1 \end{cases}
\end{aligned}
\tag{3.41}
$$

$$
\begin{aligned}
f_{113} &= \bar{x}_1 \cdot x_2 \vee \bar{x}_1 \cdot x_3 \vee x_2 \cdot x_3 = \\
&= \bar{x}_1 \cdot x_2 \vee \bar{x}_1 \cdot x_3 \vee x_1 \cdot x_2 \cdot x_3 = \begin{cases} x_2 \vee x_3 & якщо \quad x_1 = 0 \\ x_2 \cdot x_3 & якщо \quad x_1 = 1 \end{cases} = \\
&= \bar{x}_1 \cdot x_2 \vee \bar{x}_1 \cdot \bar{x}_2 \cdot x_3 \vee x_2 \cdot x_3 = \begin{cases} \bar{x}_1 \cdot x_3 & якщо \quad x_2 = 0 \\ \bar{x}_1 \vee x_3 & якщо \quad x_2 = 1 \end{cases} = \\
&= \bar{x}_1 \cdot x_2 \cdot \bar{x}_3 \vee \bar{x}_1 \cdot x_3 \vee x_2 \cdot x_3 = \begin{cases} x_1 \vee \bar{x}_2 & якщо \quad x_3 = 0 \\ x_1 \cdot \bar{x}_2 & якщо \quad x_3 = 1 \end{cases}
\end{aligned}
\tag{3.42}
$$

$$
\begin{aligned}
f_{232} &= \bar{x}_1 \cdot \bar{x}_2 \vee \bar{x}_1 \cdot \bar{x}_3 \vee \bar{x}_2 \cdot \bar{x}_3 = \\
&= \bar{x}_1 \cdot \bar{x}_2 \vee \bar{x}_1 \cdot \bar{x}_3 \vee x_1 \cdot \bar{x}_2 \cdot \bar{x}_3 = \begin{cases} \bar{x}_2 \vee \bar{x}_3 & якщо \quad x_1 = 0 \\ \bar{x}_2 \cdot \bar{x}_3 & якщо \quad x_1 = 1 \end{cases} = \\
&= \bar{x}_1 \cdot \bar{x}_2 \vee \bar{x}_1 \cdot x_2 \cdot \bar{x}_3 \vee \bar{x}_2 \cdot \bar{x}_3 = \begin{cases} \bar{x}_1 \vee \bar{x}_3 & якщо \quad x_2 = 0 \\ \bar{x}_1 \cdot \bar{x}_3 & якщо \quad x_2 = 1 \end{cases} = \\
&= \bar{x}_1 \cdot \bar{x}_2 \cdot x_3 \vee \bar{x}_1 \cdot \bar{x}_3 \vee \bar{x}_2 \cdot \bar{x}_3 = \begin{cases} \bar{x}_1 \vee \bar{x}_2 & якщо \quad x_3 = 0 \\ \bar{x}_1 \cdot \bar{x}_2 & якщо \quad x_3 = 1 \end{cases}
\end{aligned}
\tag{3.43}
$$

$$
\begin{aligned}
f_{232} &= \bar{x}_1 \cdot \bar{x}_2 \vee \bar{x}_1 \cdot x_3 \vee \bar{x}_2 \cdot x_3 = \\
&= \bar{x}_1 \cdot \bar{x}_2 \vee \bar{x}_1 \cdot x_3 \vee x_1 \cdot \bar{x}_2 \cdot x_3 = \begin{cases} \bar{x}_2 \vee x_3 & якщо \quad x_1 = 0 \\ \bar{x}_2 \cdot x_3 & якщо \quad x_1 = 1 \end{cases} = \\
&= \bar{x}_1 \cdot \bar{x}_2 \vee \bar{x}_1 \cdot x_2 \cdot x_3 \vee \bar{x}_2 \cdot x_3 = \begin{cases} \bar{x}_1 \vee x_3 & якщо \quad x_2 = 0 \\ \bar{x}_1 \cdot x_3 & якщо \quad x_2 = 1 \end{cases} = \\
&= \bar{x}_1 \cdot \bar{x}_2 \cdot \bar{x}_3 \vee \bar{x}_1 \cdot x_3 \vee \bar{x}_2 \cdot x_3 = \begin{cases} \bar{x}_1 \cdot \bar{x}_2 & якщо \quad x_3 = 0 \\ \bar{x}_1 \vee \bar{x}_2 & якщо \quad x_3 = 1 \end{cases}
\end{aligned}
\tag{3.44}
$$

$$
\begin{aligned}
f_{178} &= \bar{x}_1 \cdot x_2 \vee \bar{x}_1 \cdot \bar{x}_3 \vee x_2 \cdot \bar{x}_3 = \\
&= \bar{x}_1 \cdot x_2 \vee \bar{x}_1 \cdot \bar{x}_3 \vee x_1 \cdot x_2 \cdot \bar{x}_3 = \begin{cases} x_2 \vee \bar{x}_3 & якщо \quad x_1 = 0 \\ x_2 \cdot \bar{x}_3 & якщо \quad x_1 = 1 \end{cases} = \\
&= \bar{x}_1 \cdot x_2 \vee \bar{x}_1 \cdot \bar{x}_2 \cdot \bar{x}_3 \vee x_2 \cdot \bar{x}_3 = \begin{cases} \bar{x}_1 \cdot \bar{x}_3 & якщо \quad x_2 = 0 \\ \bar{x}_1 \vee \bar{x}_3 & якщо \quad x_2 = 1 \end{cases} = \\
&= \bar{x}_1 \cdot x_2 \cdot x_3 \vee \bar{x}_1 \cdot \bar{x}_3 \vee x_2 \cdot \bar{x}_3 = \begin{cases} \bar{x}_1 \vee x_2 & якщо \quad x_3 = 0 \\ \bar{x}_1 \cdot x_2 & якщо \quad x_3 = 1 \end{cases}
\end{aligned}
\tag{3.45}
$$

$$
\begin{aligned}
f_{142} &= x_1 \cdot \bar{x}_2 \vee x_1 \cdot \bar{x}_3 \vee \bar{x}_2 \cdot \bar{x}_3 = \\
&= x_1 \cdot \bar{x}_2 \vee x_1 \cdot \bar{x}_3 \vee \bar{x}_1 \cdot \bar{x}_2 \cdot \bar{x}_3 = \begin{cases} \bar{x}_2 \cdot \bar{x}_3 & якщо \quad x_1 = 0 \\ \bar{x}_2 \vee \bar{x}_3 & якщо \quad x_1 = 1 \end{cases} = \\
&= x_1 \cdot \bar{x}_2 \vee x_1 \cdot x_2 \cdot \bar{x}_3 \vee \bar{x}_2 \cdot \bar{x}_3 = \begin{cases} x_1 \vee \bar{x}_3 & якщо \quad x_2 = 0 \\ x_1 \cdot \bar{x}_3 & якщо \quad x_2 = 1 \end{cases} = \\
&= x_1 \cdot \bar{x}_2 \cdot x_3 \vee x_1 \cdot \bar{x}_3 \vee \bar{x}_2 \cdot \bar{x}_3 = \begin{cases} x_1 \vee \bar{x}_2 & якщо \quad x_3 = 0 \\ x_1 \cdot \bar{x}_2 & якщо \quad x_3 = 1 \end{cases}
\end{aligned}
\tag{3.46}
$$

Аналогічно попередньому, на даному етапі дослідження будемо вважати, що для пари елементарних функцій прямою є та, у якої менший порядковий номер.

На основі елементарних функцій (3.39) – (3.46) побудовані операції криптографічного перетворення інформації, у яких керування процесом перетворення на основі зміни логічної операції залежить від значення третього розряду [23].

Типова схема реалізації елементарних функцій, що керуються інформацією приведена на рис. 3.3.

На основі цих елементарних функцій побудовані операції криптографічного перетворення інформації, у яких керування процесом перетворення на основі перестановок залежить від значення третього розряду.

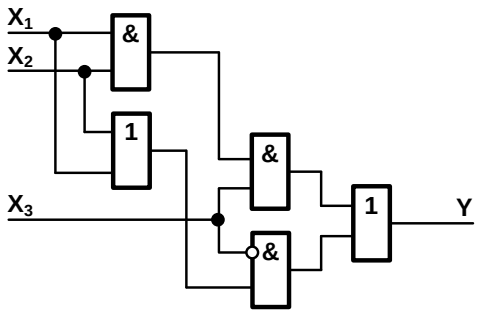


Рис. 3.3. Схема реалізації елементарних функцій, що керуються інформацією

Останню групу елементарних функцій представляють елементарні функції блоку № 5 (табл. 3.1):

$$f_{30} = x_1 \cdot \bar{x}_2 \vee x_1 \cdot \bar{x}_3 \vee \bar{x}_1 \cdot x_2 \cdot x_3 = x_1 \oplus (x_2 \cdot x_3) \quad (3.47)$$

$$f_{45} = x_1 \cdot \bar{x}_2 \vee x_1 \cdot x_3 \vee \bar{x}_1 \cdot x_2 \cdot \bar{x}_3 = x_1 \oplus (x_1 \cdot \bar{x}_3) \quad (3.48)$$

$$f_{54} = \bar{x}_1 \cdot x_2 \vee x_2 \cdot \bar{x}_3 \vee x_1 \cdot \bar{x}_2 \cdot x_3 = x_2 \oplus (x_1 \cdot x_3) \quad (3.49)$$

$$f_{57} = \bar{x}_1 \cdot x_2 \vee x_2 \cdot x_3 \vee x_1 \cdot \bar{x}_2 \cdot \bar{x}_3 = x_2 \oplus (x_1 \cdot \bar{x}_3) \quad (3.50)$$

$$f_{75} = x_1 \cdot x_2 \vee x_1 \cdot \bar{x}_3 \vee \bar{x}_1 \cdot \bar{x}_2 \cdot x_3 = x_1 \oplus (\bar{x}_2 \cdot x_3) \quad (3.51)$$

$$f_{86} = \bar{x}_1 \cdot x_3 \vee \bar{x}_2 \cdot x_3 \vee x_1 \cdot x_2 \cdot \bar{x}_3 = x_3 \oplus (x_1 \cdot x_2) \quad (3.52)$$

$$f_{89} = \bar{x}_1 \cdot x_3 \vee x_2 \cdot x_3 \vee x_1 \cdot \bar{x}_2 \cdot \bar{x}_3 = x_3 \oplus (x_1 \cdot \bar{x}_2) \quad (3.53)$$

$$f_{99} = x_1 \cdot x_2 \vee x_2 \cdot \bar{x}_3 \vee \bar{x}_1 \cdot \bar{x}_2 \cdot x_3 = x_2 \oplus (\bar{x}_1 \cdot x_3) \quad (3.54)$$

$$f_{101} = x_1 \cdot x_3 \vee \bar{x}_2 \cdot x_3 \vee \bar{x}_1 \cdot x_2 \cdot \bar{x}_3 = x_3 \oplus (\bar{x}_1 \cdot x_2) \quad (3.55)$$

$$f_{135} = x_1 \cdot x_2 \vee x_1 \cdot x_3 \vee \bar{x}_1 \cdot \bar{x}_2 \cdot \bar{x}_3 = x_1 \oplus (\bar{x}_2 \cdot \bar{x}_3) \quad (3.56)$$

$$f_{147} = x_1 \cdot x_2 \vee x_2 \cdot x_3 \vee \bar{x}_1 \cdot \bar{x}_2 \cdot \bar{x}_3 = x_2 \oplus (\bar{x}_1 \cdot \bar{x}_3) \quad (3.57)$$

$$f_{149} = x_1 \cdot x_3 \vee x_2 \cdot x_3 \vee \bar{x}_1 \cdot \bar{x}_2 \cdot \bar{x}_3 = x_3 \oplus (\bar{x}_1 \cdot \bar{x}_2) \quad (3.58)$$

$$f_{106} = x_1 \cdot \bar{x}_3 \vee x_2 \cdot \bar{x}_3 \vee \bar{x}_1 \cdot \bar{x}_2 \cdot x_3 = x_3 \equiv (\bar{x}_1 \cdot \bar{x}_2) = x_3 \oplus (\bar{x}_1 \cdot \bar{x}_2) \oplus 1 \quad (3.59)$$

$$f_{108} = x_1 \cdot \bar{x}_2 \vee \bar{x}_2 \cdot x_3 \vee \bar{x}_1 \cdot x_2 \cdot \bar{x}_3 = x_2 \equiv (\bar{x}_1 \cdot \bar{x}_3) = x_2 \oplus (\bar{x}_1 \cdot \bar{x}_3) \oplus 1 \quad (3.60)$$

$$f_{120} = \bar{x}_1 \cdot x_2 \vee \bar{x}_1 \cdot x_3 \vee x_1 \cdot \bar{x}_2 \cdot \bar{x}_3 = x_1 \equiv (\bar{x}_2 \cdot \bar{x}_3) = x_1 \oplus (\bar{x}_2 \cdot \bar{x}_3) \oplus 1 \quad (3.61)$$

$$f_{154} = x_1 \cdot \bar{x}_3 \vee \bar{x}_2 \cdot \bar{x}_3 \vee \bar{x}_1 \cdot x_2 \cdot x_3 = x_3 \equiv (\bar{x}_1 \cdot x_2) = x_3 \oplus (\bar{x}_1 \cdot x_2) \oplus 1 \quad (3.62)$$

$$f_{156} = x_1 \cdot \bar{x}_2 \vee \bar{x}_2 \cdot \bar{x}_3 \vee \bar{x}_1 \cdot x_2 \cdot x_3 = x_2 \equiv (\bar{x}_1 \cdot x_3) = x_2 \oplus (\bar{x}_1 \cdot x_3) \oplus 1 \quad (3.63)$$

$$f_{166} = \bar{x}_1 \cdot \bar{x}_3 \vee x_2 \cdot \bar{x}_3 \vee x_1 \cdot \bar{x}_2 \cdot x_3 = x_3 \equiv (x_1 \cdot \bar{x}_2) = x_3 \oplus (x_1 \cdot \bar{x}_2) \oplus 1 \quad (3.64)$$

$$f_{169} = \bar{x}_1 \cdot \bar{x}_3 \vee \bar{x}_2 \cdot \bar{x}_3 \vee x_1 \cdot x_2 \cdot x_3 = x_3 \equiv (x_1 \cdot x_2) = x_3 \oplus (x_1 \cdot x_2) \oplus 1 \quad (3.65)$$

$$f_{180} = \bar{x}_1 \cdot x_2 \vee \bar{x}_1 \cdot \bar{x}_3 \vee x_1 \cdot \bar{x}_2 \cdot x_3 = x_1 \equiv (\bar{x}_2 \cdot x_3) = x_1 \oplus (\bar{x}_2 \cdot x_3) \oplus 1 \quad (3.66)$$

$$f_{198} = \bar{x}_1 \cdot \bar{x}_2 \vee \bar{x}_2 \cdot x_3 \vee x_1 \cdot x_2 \cdot \bar{x}_3 = x_2 \equiv (x_1 \cdot \bar{x}_3) = x_2 \oplus (x_1 \cdot \bar{x}_3) \oplus 1 \quad (3.67)$$

$$f_{201} = \bar{x}_1 \cdot \bar{x}_2 \vee \bar{x}_2 \cdot \bar{x}_3 \vee x_1 \cdot x_2 \cdot x_3 = x_2 \equiv (x_1 \cdot x_3) = x_2 \oplus (x_1 \cdot x_3) \oplus 1 \quad (3.68)$$

$$f_{210} = \bar{x}_1 \cdot \bar{x}_2 \vee \bar{x}_1 \cdot x_3 \vee x_1 \cdot x_2 \cdot \bar{x}_3 = x_1 \equiv (x_1 \cdot \bar{x}_3) = x_1 \oplus (x_1 \cdot \bar{x}_3) \oplus 1 \quad (3.69)$$

$$f_{225} = \bar{x}_1 \cdot \bar{x}_2 \vee \bar{x}_1 \cdot \bar{x}_3 \vee x_1 \cdot x_2 \cdot x_3 = x_1 \equiv (x_2 \cdot x_3) = x_1 \oplus (x_2 \cdot x_3) \oplus 1 \quad (3.70)$$

Елементарні функції (3.47) – (3.58) є прямими, а (3.59) – (3.70) – оберненими. Класифікувати елементарні функції на прямі і обернені вдалося на основі поліноміального подання.

На основі поліноміального подання видно, що представлені елементарні функції є матричні елементарні функції з додатковою нелінійною умовою. Застосування даної умови призводить до збільшення кількості (розширення) матричних операцій. Виходячи з цього, дані операції нами названо операціями розширеного матричного криптоперетворення, а елементарні функції, з яких вони побудовані – елементарними функціями розширеного матричного перетворення [17]. Типова схема реалізації елементарних функцій розширеного матричного перетворення наведена на рис. 3.4 [23].

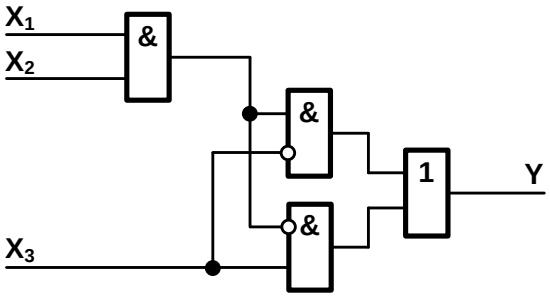


Рис. 3.4. Схема реалізації розширених матричних елементарних функцій

Наведені результати послужили основою для проведення класифікації трирозрядних елементарних функцій на основі функціональних особливостей (фізичного змісту) перетворення. Дана класифікація наведена на рис.3.5 [23].

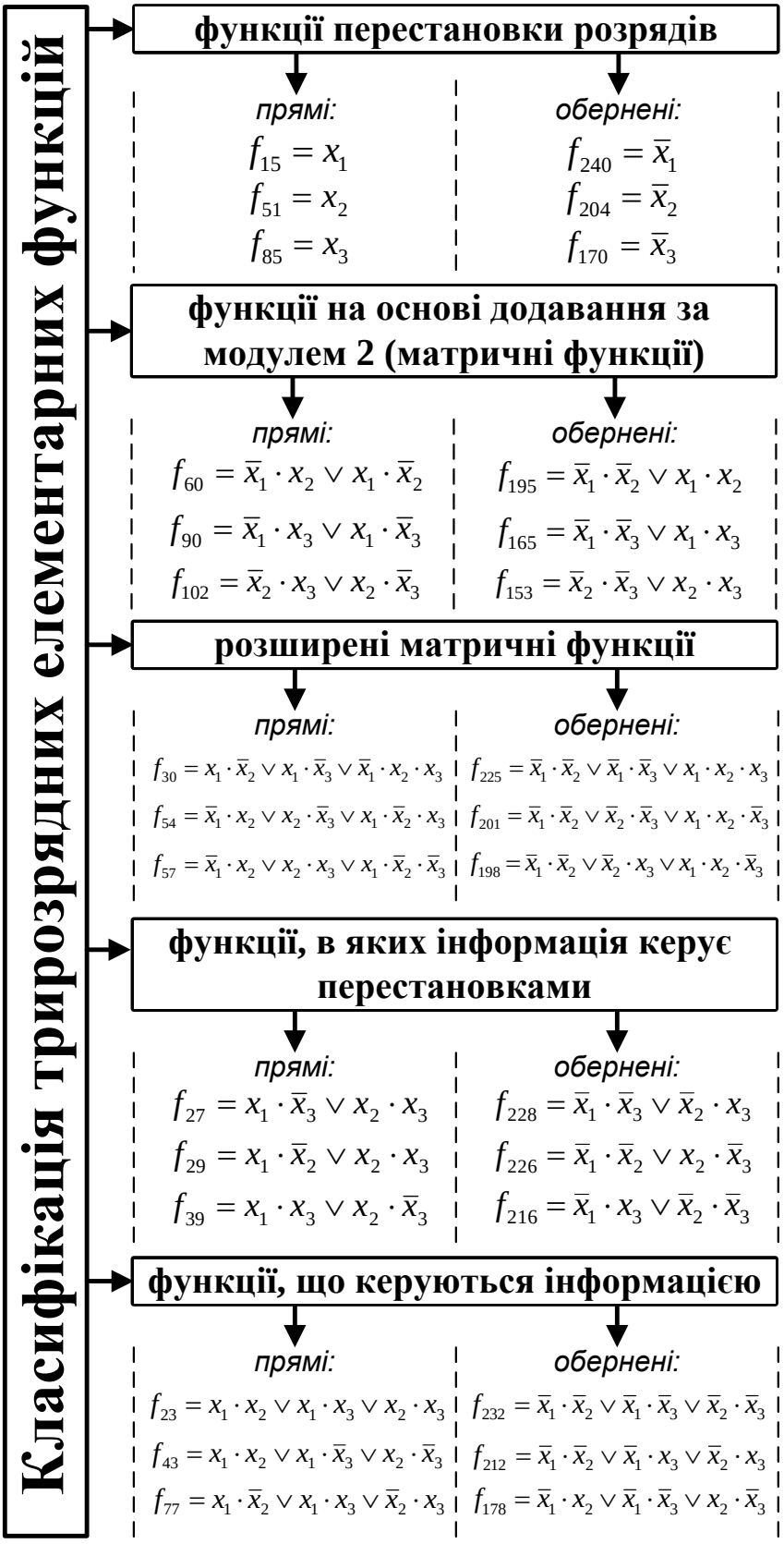


Рис. 3.5 Класифікація трирозрядних елементарних функцій

Для перевірки коректності розробленої методології синтезу операцій криптографічного перетворення виберемо трьохрозрядну групу розширених матричних елементарних функцій.

3.2 Синтез елементарних функцій для розширеного матричного криптографічного перетворення

Проведемо дослідження та систематизацію трьохрозрядних розширених матричних елементарних функцій (3.47 – 3.70) [13].

Лише один аргумент у дискретному представленні елементарних функцій входить до складу всіх трьох логічних доданків. Класифікуємо ці елементарні функції за даною ознакою та виокремемо серед них прямі та обернені:

1. Елементарні функції на основі x_1:
   - прямі елементарні функції: (3.47), (3.48), (3.51), (3.56);
   - обернені елементарні функції: (3.61), (3.66), (3.69), (3.70).
2. Елементарні функції на основі x_2:
   - прямі елементарні функції: (3.49), (3.50), (3.54), (3.57);
   - обернені елементарні функції: (3.60), (3.63), (3.67), (3.68).
3. Елементарні функції на основі x_3:
   - прямі елементарні функції: (3.52), (3.53), (3.55), (3.58);
   - обернені елементарні функції: (3.59), (3.62), (3.64), (3.65).

Розглянемо більш детально групу прямих елементарних функцій на основі x_1 [17]:

$$f_{30} = x_1 \cdot \bar{x}_2 \vee x_1 \cdot \bar{x}_3 \vee \bar{x}_1 \cdot x_2 \cdot x_3$$

$$f_{45} = x_1 \cdot \bar{x}_2 \vee x_1 \cdot x_3 \vee \bar{x}_1 \cdot x_2 \cdot \bar{x}_3$$

$$f_{75} = x_1 \cdot x_2 \vee x_1 \cdot \bar{x}_3 \vee \bar{x}_1 \cdot \bar{x}_2 \cdot x_3$$

$$f_{135} = x_1 \cdot x_2 \vee x_1 \cdot x_3 \vee \bar{x}_1 \cdot \bar{x}_2 \cdot \bar{x}_3$$

Як видно з наведеного подання:

– перший логічний доданок $x_1 \cdot x_2$;

– другий логічний доданок $x_2 \cdot x_3$;

– третій логічний доданок $x_1 \cdot x_2 \cdot x_3$;

– x_1 у першому та другому доданках має пряме значення, а у третьому доданку – інверсне;

– x_2 у першому і третьому доданках має різні знаки інверсії;

– x_3 у другому і третьому доданках має різні знаки інверсії.

Формалізуємо наведені правила:

$$f = x_1 \cdot \hat{x}_2 \vee x_1 \cdot \hat{x}_3 \vee \bar{x}_1 \cdot \bar{\hat{x}}_2 \cdot \bar{\hat{x}}_3, \qquad (3.71)$$

де x – пряме значення аргументу; $\bar{x}$ – інверсне значення аргументу; $\hat{x}$ – будь-яке значення аргументу; $\bar{\hat{x}}$ – інверсне щодо будь-якого значення аргументу.

Розглянемо більш детально групу обернених елементарних функцій на основі x_1 [17]:

$$f_{120} = \bar{x}_1 \cdot x_2 \vee \bar{x}_1 \cdot x_3 \vee x_1 \cdot \bar{x}_2 \cdot \bar{x}_3;$$

$$f_{180} = \bar{x}_1 \cdot x_2 \vee \bar{x}_1 \cdot \bar{x}_3 \vee x_1 \cdot \bar{x}_2 \cdot x_3;$$

$$f_{210} = \bar{x}_1 \cdot \bar{x}_2 \vee \bar{x}_1 \cdot x_3 \vee x_1 \cdot x_2 \cdot \bar{x}_3;$$

$$f_{225} = \bar{x}_1 \cdot \bar{x}_2 \vee \bar{x}_1 \cdot \bar{x}_3 \vee x_1 \cdot x_2 \cdot x_3.$$

Правила побудови обернених елементарних функцій на основі x_1 від побудови прямих елементарних функцій відрізняються лише тим, що x_1 у першому та другому доданках представлені інверсним значенням, а у третьому доданку представлено прямим значенням.

Формалізовані правила синтезу обернених елементарних функцій на основі x_1 будуть представлені моделлю:

$$f = \bar{x}_1 \cdot \hat{x}_2 \vee \bar{x}_1 \cdot \hat{x}_3 \vee x_1 \cdot \bar{\hat{x}}_2 \cdot \bar{\hat{x}}_3. \quad (3.72)$$

Об’єднавши вирази (3.71) і (3.72), ми отримали правила синтезу прямих і обернених елементарних функцій на основі x_1:

$$f = \hat{x}_1 \cdot \hat{x}_2 \vee \hat{x}_1 \cdot \hat{x}_3 \vee \bar{\hat{x}}_1 \cdot \bar{\hat{x}}_2 \cdot \bar{\hat{x}}_3. \quad (3.73)$$

Аналогічно можна отримати формалізовані правила прямих елементарних функцій на основі x_2 [17, 21]:

$$f = \hat{x}_1 \cdot x_2 \vee x_2 \cdot \hat{x}_3 \vee \bar{\hat{x}}_1 \cdot \bar{x}_2 \cdot \bar{\hat{x}}_3. \quad (3.74)$$

Формалізовані правила синтезу обернених елементарних функцій на основі x_2 будуть описані виразом:

$$f = \hat{x}_1 \cdot \bar{x}_2 \vee \bar{x}_2 \cdot \hat{x}_3 \vee \bar{\hat{x}}_1 \cdot x_2 \cdot \bar{\hat{x}}_3. \quad (3.75)$$

Об’єднавши вирази (3.74) і (3.75), ми отримали правила синтезу прямих і обернених елементарних функцій на основі x_2:

$$f = \hat{x}_1 \cdot \hat{x}_2 \vee \hat{x}_2 \cdot \hat{x}_3 \vee \bar{\hat{x}}_1 \cdot \bar{\hat{x}}_2 \cdot \bar{\hat{x}}_3. \quad (3.76)$$

Результати формалізації правил синтезу елементарних функцій на основі x_3 наступні [17]:

– прямі елементарні функції на основі x_3

$$f = \hat{x}_1 \cdot x_3 \vee \hat{x}_2 \cdot x_3 \vee \hat{\bar{x}}_1 \cdot \hat{\bar{x}}_2 \cdot \bar{x}_3; \quad (3.77)$$

– обернені елементарні функції на основі x_3

$$f = \hat{x}_1 \cdot \bar{x}_3 \vee \hat{x}_2 \cdot \bar{x}_3 \vee \hat{\bar{x}}_1 \cdot \hat{\bar{x}}_2 \cdot x_3; \quad (3.78)$$

– прямі і обернені елементарні функції на основі x_3

$$f = \hat{x}_1 \cdot \hat{x}_3 \vee \hat{x}_2 \cdot \hat{x}_3 \vee \hat{\bar{x}}_1 \cdot \hat{\bar{x}}_2 \cdot \hat{\bar{x}}_3. \quad (3.79)$$

Узагальнимо на основі виразів (3.71), (3.74), (3.77) правила синтезу прямих елементарних функцій:

$$f = x_i \cdot \hat{x}_j \vee x_i \cdot \hat{x}_l \vee \bar{x}_i \cdot \hat{\bar{x}}_j \cdot \hat{\bar{x}}_l, \quad (3.80)$$

де x – пряме значення аргументу; $\bar{x}$ – інверсне значення аргументу; $\hat{x}$ – будь-яке значення аргументу; $\hat{\bar{x}}$ – інверсне щодо будь-якого значення аргументу, за умови: $i, j, l \in [1,2,3]$; $i \neq j \neq l$.

На основі виразів (3.72), (3.75), (3.78) формалізуємо правила синтезу прямих елементарних функцій:

$$f = \bar{x}_i \cdot \hat{x}_j \vee \bar{x}_i \cdot \hat{x}_l \vee x_i \cdot \hat{\bar{x}}_j \cdot \hat{\bar{x}}_l. \quad (3.81)$$

Синтез повної множини прямих та обернених елементарних функцій базується на виразах (3.73), (3.76), (3.79) та у загальному випадку може бути описаний:

$$f = \hat{x}_i \cdot \hat{x}_j \vee \hat{x}_i \cdot \hat{x}_l \vee \hat{\bar{x}}_i \cdot \hat{\bar{x}}_j \cdot \hat{\bar{x}}_l. \quad (3.82)$$

Вирази (3.80) – (3.82) створюють основу методу синтезу трьохрозрядних розширених матричних елементарних функцій у дискретному представленні, сутність якого полягає в наступному:

1. Виходячи із задач проектування, визначити, які формалізовані правила необхідно використати:

– синтез множини прямих трьохрозрядних розширених матричних елементарних функцій необхідно здійснювати згідно виразу (3.80);

– синтез множини обернених трьохрозрядних розширених матричних елементарних функцій необхідно здійснювати використовуючи вираз (3.81);

– синтез повної множини трьохрозрядних розширених матричних елементарних функцій необхідно здійснювати згідно виразу (3.82).

2. На основі перебору значень i, j, l, де $i, j, l \in [1,2,3]$ за умови:

- $i \neq j \neq l$;
- $j < l$

отримати три основні трьохрозрядні розширені матричні елементарні функції:

– на основі виразу (3.80) $f = x_i \cdot \widehat{x}_j \vee x_i \cdot \widehat{x}_l \vee \overline{x}_i \cdot \overline{\widehat{x}}_j \cdot \overline{\widehat{x}}_l$;

$f = x_j \cdot \widehat{x}_i \vee x_j \cdot \widehat{x}_l \vee \overline{x}_j \cdot \overline{\widehat{x}}_i \cdot \overline{\widehat{x}}_l$;

$f = x_l \cdot \widehat{x}_j \vee x_l \cdot \widehat{x}_i \vee \overline{x}_l \cdot \overline{\widehat{x}}_j \cdot \overline{\widehat{x}}_i$;

– на основі виразу (3.81) $f = \overline{x}_i \cdot \widehat{x}_j \vee \overline{x}_i \cdot \widehat{x}_l \vee x_i \cdot \overline{\widehat{x}}_j \cdot \overline{\widehat{x}}_l$;

$f = \overline{x}_j \cdot \widehat{x}_i \vee \overline{x}_j \cdot \widehat{x}_l \vee x_j \cdot \overline{\widehat{x}}_i \cdot \overline{\widehat{x}}_l$;

$f = \overline{x}_l \cdot \widehat{x}_j \vee \overline{x}_l \cdot \widehat{x}_i \vee x_l \cdot \overline{\widehat{x}}_j \cdot \overline{\widehat{x}}_i$;

– на основі виразу (3.82) $f = \widehat{x}_i \cdot \widehat{x}_j \vee \overline{\widehat{x}}_i \cdot \widehat{x}_l \vee \overline{\widehat{x}}_i \cdot \overline{\widehat{x}}_j \cdot \overline{\widehat{x}}_l$;

$f = \widehat{x}_j \cdot \widehat{x}_i \vee \widehat{x}_j \cdot \widehat{x}_l \vee \overline{\widehat{x}}_j \cdot \overline{\widehat{x}}_i \cdot \overline{\widehat{x}}_l$;

$f = \widehat{x}_l \cdot \widehat{x}_j \vee \widehat{x}_l \cdot \widehat{x}_i \vee \overline{\widehat{x}}_l \cdot \overline{\widehat{x}}_j \cdot \overline{\widehat{x}}_i$.

3. На основі перебору значень інверсії $\widehat{x}_i$, $\widehat{x}_j$, $\widehat{x}_l$, де $\widehat{x}_i \in [x_i, \overline{x}_i]$, $\widehat{x}_j \in [x_j, \overline{x}_j]$, $\widehat{x}_l \in [x_l, \overline{x}_l]$, підставивши отримані набори в три основні трьохрозрядні розширені матричні елементарні функції, отримати повну множину трьохрозрядних розширених матричних елементарних функцій відповідно до задачі синтезу.

Приклади використання методу синтезу трьохрозрядних розширених матричних елементарних функцій наведені в роботі [27].

Аналогічно синтезу елементарних функцій в дискретному представленні розглянемо синтез операцій криптографічного перетворення на основі модульно-дискретного представлення елементарних функцій.

Як видно з елементарних функцій розширеного матричного перетворення (3.47)-(3.70), лише один аргумент входить до першого доданку за модулем.

Класифікуємо ці елементарні функції за даною ознакою та виділимо із них прямі та обернені:

1. Елементарні функції на основі x_1:

– прямі елементарні функції: (3.47), (3.48), (3.51), (3.56);

– обернені елементарні функції: (3.61), (3.66), (3.69), (3.70).

2. Елементарні функції на основі x_2:

– прямі елементарні функції: (3.49), (3.50), (3.54), (3.57);

– обернені елементарні функції: (3.60), (3.63), (3.67), (3.68).

3. Елементарні функції на основі x_3:

– прямі елементарні функції: (3.52), (3.53), (3.55), (3.58);

– обернені елементарні функції: (3.59), (3.62), (3.64), (3.65).

Класифікація елементарних функцій в дискретному і модульно-дискретному представленні повністю співпали. Виходячи з цього, можна стверджувати, що класифікації елементарних функцій не залежать від способів запису та представлення.

Розглянемо більш детально групу прямих елементарних функцій на основі x_1 [53]:

$$f_{30} = x_1 \oplus (x_2 \cdot x_3);$$
$$f_{45} = x_1 \oplus (x_2 \cdot \bar{x}_3);$$
$$f_{75} = x_1 \oplus (\bar{x}_2 \cdot x_3);$$
$$f_{135} = x_1 \oplus (\bar{x}_2 \cdot \bar{x}_3).$$

Формалізовані правила синтезу прямих елементарних функцій на основі x_1 описуються виразом [53]:

$$f = x_1 \oplus (\hat{x}_2 \cdot \hat{x}_3), \tag{3.83}$$

де x – пряме значення аргументу; $\bar{x}$ – інверсне значення аргументу; $\hat{x}$ – будь-яке значення аргументу; $\bar{\hat{x}}$ – інверсне щодо будь-якого значення аргументу.

Формалізовані правила синтезу обернених елементарних функцій на основі x_1 описуються виразом [53]:

$$f = x_1 \oplus (\hat{x}_2 \cdot \hat{x}_3) \oplus 1.$$

Аналогічно формалізовані правила синтезу прямих елементарних функцій на основі x_2 та x_3 описуються відповідно виразами [53]:

$$f = x_2 \oplus (\hat{x}_1 \cdot \hat{x}_3); \tag{3.84}$$
$$f = x_3 \oplus (\hat{x}_1 \cdot \hat{x}_2). \tag{3.85}$$

Правила синтезу обернених елементарних функцій на основі x_2 та x_3 описуються відповідно виразами:

$$f = x_2 \oplus (\hat{x}_1 \cdot \hat{x}_3) \oplus 1;$$
$$f = x_3 \oplus (\hat{x}_1 \cdot \hat{x}_2) \oplus 1.$$

Узагальнені правила синтезу прямих трьохрозрядних розширених матричних елементарних функцій описуються виразом [53]:

$$f = x_i \oplus (\hat{x}_j \cdot \hat{x}_l), \qquad (3.86)$$

де x – пряме значення аргументу; $\bar{x}$ – інверсне значення аргументу; $\hat{x}$ – будь-яке значення аргументу; $\bar{\hat{x}}$ – інверсне щодо будь-якого значення аргументу, $i, j, l \in [1,2,3]$ за умови $i \neq j \neq l$.

Узагальнені правила синтезу обернених трьохрозрядних розширених матричних елементарних функцій описуються виразом:

$$f = x_i \oplus (\hat{x}_j \cdot \hat{x}_l) \oplus 1. \qquad (3.87)$$

Вирази (3.86), (3.87) дозволяють розробити метод синтезу трьохрозрядних розширених матричних елементарних функцій у модульно-дискретному представленні.

Сутність розробленого методу полягає в наступному:

1. На основі виразу (3.86) шляхом перебору значень i, j, l, де $i, j, l \in [1,2,3]$ за умови

– $i \neq j \neq l$;

– $j < l$;

отримати три основні трьохрозрядні розширені матричні елементарні функції;

2. На основі перебору значень інверсії $\widehat{x}_j$, $\widehat{x}_l$, де $\widehat{x}_j \in [x_j, \bar{x}_j]$, $\widehat{x}_l \in [x_l, \bar{x}_l]$, підставивши отримані набори в три основні трьохрозрядні розширені матричні елементарні функції, отримати повну множину із 12 прямих трьохрозрядних розширених матричних елементарних функцій;

3. На основі виразу (3.87), інвертувавши множину прямих трьохрозрядних розширених матричних елементарних функцій, шляхом додавання по модулю два отримати множину обернених розширених матричних елементарних функцій;

4. Об'єднавши множини прямих і обернених елементарних функцій, отримуємо повну множину із 24 трьохрозрядних розширених матричних елементарних функцій.

Приклади використання методу синтезу трьохрозрядних розширених матричних елементарних функцій наведені у роботі [17].

Аналогічно можливо отримати метод синтезу трьохрозрядних розширених матричних елементарних функцій для криптоперетворення даних більшої розрядності. Для цього необхідно модифікувати розроблений метод синтезу до наступної редакції:

1. На основі виразу (3.86) шляхом перебору значень i, j, l, де $i, j, l \in [1, 2, \ldots, n]$ за умови

– $i \neq j \neq l$;

– $j < l$

отримати n основних трьохрозрядних розширених матричних елементарних функцій;

2. На основі перебору значень інверсії $\widehat{x}_j$, $\widehat{x}_l$, де $\widehat{x}_j \in [x_j, \bar{x}_j]$, $\widehat{x}_l \in [x_l, \bar{x}_l]$, підставивши отримані набори у три основні трьохрозрядні розширені матричні елементарні функції, отримати повну множину прямих трьохрозрядних розширених матричних елементарних функцій;

3. На основі виразу (3.87), інвертувавши множину прямих трьохрозрядних розширених матричних елементарних функцій, шляхом додавання по модулю два, отримати множину обернених розширених матричних елементарних функцій;

4. Об'єднавши множини прямих і обернених елементарних функцій, отримати повну множину трьохрозрядних розширених матричних елементарних функцій.

Визначимо кількість елементарних функцій розширеного матричного перетворення будь-якої розрядності [53].

Кількість елементарних функцій розширеного матричного перетворення визначається:

$$K_{П} = K_{O} = 12 \cdot C_{n}^{3} = \frac{12n!}{3!(n-3)!}, \tag{3.88}$$

де $K_{П}$ – кількість прямих елементарних функцій, K_{O} – кількість обернених елементарних функцій, С – кількість сполучень із n по 3, n – кількість розрядів, 3 – розрядність функцій.

Загальна кількість трирозрядних елементарних функцій розширеного матричного перетворення визначається:

$$K_{\Sigma} = K_{П} + K_{O} = 24 \cdot C_{n}^{3}. \tag{3.89}$$

Розширені матричні елементарні функції можуть бути не лише трирозрядними.

Метод синтезу m –розрядних розширених матричних елементарних функцій полягає в наступному:

1. На основі виразу

$$f = x_i \oplus (\hat{x}_j \cdot \hat{x}_l \cdot \ldots \cdot \hat{x}_q) \tag{3.90}$$

шляхом перебору значень i, j, l, …, q, де $i, j, l \in [1, 2, \ldots, n]$, …, $q \in [1, 2, \ldots, n]$ за умови

– $i \neq j \neq l \neq \ldots \neq q$;

– $j < l < \ldots < q$

отримати основні n –розрядні розширені матричні елементарні функції;

2. На основі перебору значень інверсії $\hat{x}_j$, $\hat{x}_l$, … , $\hat{x}_q$ де, $\hat{x}_j \in [x_j, \bar{x}_j]$, $\hat{x}_l \in [x_l, \bar{x}_l]$, …, $\hat{x}_q \in [x_q, \bar{x}_q]$, підставивши отримані набори в основні трьохрозрядні розширені матричні елементарні функції, отримати повну множину прямих трьохрозрядних розширених матричних елементарних функцій;

3. На основі виразу

$$f = x_i \oplus (\hat{x}_j \cdot \hat{x}_l \cdot \ldots \cdot \hat{x}_q) \oplus 1, \qquad (3.91)$$

інвертувавши множину прямих трьохрозрядних розширених матричних елементарних функцій, шляхом додавання по модулю два, отримати множину обернених розширених матричних елементарних функцій;

4. Об’єднавши множини прямих і обернених елементарних функцій, отримати повну множину трьохрозрядних розширених матричних елементарних функцій.

Кожна із синтезованих m –розрядних елементарних функцій розширеного матричного перетворення може бути використана в комп'ютерній криптографії, тому що для (3.90) та (3.91) виконується умова (2.8) і справедливі співвідношення:

$$\sum_{x=0}^{2^m-1} (x_i \oplus (\hat{x}_j \cdot \hat{x}_l \cdot \ldots \cdot \hat{x}_q)) = C_{2^m}^{2^{m-1}}$$

$$\sum_{x=0}^{2^m-1}(x_i \oplus (\widehat{x}_j \cdot \widehat{x}_l \cdot \ldots \cdot \widehat{x}_q) \oplus 1) = C_{2^m}^{2^{m-1}}$$

Виходячи з виразу (3.90), можливо синтезувати модель прямої m –розрядної елементарної функції розширеного матричного перетворення в дискретному представленні:

$$f = x_i \cdot \widehat{x}_j \vee x_i \cdot \widehat{x}_l \vee \ldots \vee x_i \cdot \widehat{x}_q \vee (\overline{x}_i \cdot \overline{\widehat{x}}_j \cdot \overline{\widehat{x}}_l \cdot \ldots \cdot \overline{\widehat{x}}_q), \quad (3.92)$$

де $i, j, l \in [1, 2, \ldots, n]$, …, $q \in [1, 2, \ldots, n]$ за умов $i \neq j \neq l \neq \ldots \neq q$ та $j < l < \ldots < q$.

Виходячи з виразів (3.80) і (3.90), можна синтезувати модель оберненої m –розрядної елементарної функції розширеного матричного перетворення в дискретному представленні:

$$f = \overline{x}_i \cdot \widehat{x}_j \vee \overline{x}_i \cdot \widehat{x}_l \vee \ldots \vee \overline{x}_i \cdot \widehat{x}_q \vee (x_i \cdot \overline{\widehat{x}}_j \cdot \overline{\widehat{x}}_l \cdot \ldots \cdot \overline{\widehat{x}}_q).$$

Кількість прямих m –розрядних елементарних функцій розширеного матричного перетворення визначається як:

$$K_{П} = K_{O} = 2^{m-1} \cdot m \cdot C_n^m = \frac{2^{m-1} \cdot m \cdot n!}{m!(n-m)!}, \quad (3.92)$$

Загальна кількість m –розрядних елементарних функцій розширеного матричного перетворення (прямих та обернених) на основі виразу (3.92) визначається як:

$$K_{\Sigma} = K_{П} + K_{O} = 2 \cdot 2^{m-1} \cdot m \cdot C_n^m = \frac{2^m \cdot m \cdot n!}{m!(n-m)!} \quad (3.93)$$

Для криптографічного перетворення n –розрядної інформації можуть бути використані елементарні функції розрядності від 3 до n.

Кількість n –розрядних елементарних функцій розширеного матричного перетворення можна отримати на основі виразу (3.93):

$$K_{\Sigma} = \sum_{m=3}^{n} \frac{2^m \cdot m \cdot n!}{m!(n-m)!} \tag{3.93}$$

Аналіз виразу (3.93) показує значний ріст кількості елементарних функцій розширеного матричного перетворення в залежності від розрядності моделі криптоперетворення.

3.3 Розробка методів синтезу операцій розширеного матричного криптографічного перетворення

3.3.1 Синтез моделі базової операції на основі трирозрядних елементарних функцій розширеного матричного представлення

Виходячи з методології синтезу операцій криптографічного перетворення, після розробки методів побудови групи елементарних функцій для криптоперетворення необхідно визначити модель операції для криптоперетворення. Тобто визначити систему обмежень, які будуть визначати правила об’єднання елементарних функцій в операції.

Оскільки операції розширеного матричного криптографічного перетворення за аналогією з операціями матричного криптографічного перетворення можуть бути поділені на базову групу операцій, групу операцій перестановки і групу операцій інверсії, то при побудові моделі операції обмежимося лише дослідженням базових операцій.

Для визначення моделі операції криптографічного перетворення використаємо результати обчислювального експерименту, в результаті якого на основі групи елементарних функцій розширеного матричного криптографічного перетворювання шляхом перебору моделювалися операції криптоперетворення.

Для аналізу на даному етапі дослідження обмежимося лише прямими елементарними функціями (3.47) – (3.58). Це дало можливість зменшити групу операцій, яка досліджується, за рахунок обмеження на синтез операцій, які включають у себе додаткові інверсії.

Синтез базових матричних операцій криптоперетворення методом заміщення базується на використанні в якості основної операції – операції повторення інформації (нульову операцію) (2.20). У даній операції першою елементарною функцією є x_1, другою – x_2, а третьою – x_3. Використавши в якості першої елементарної функції, елементарну функцію на основі x_1: (3.47), (3.48), (3.51), (3.56); в якості другої елементарної функції – елементарну функцію на основі x_2: (3.49), (3.50), (3.54), (3.57); в якості третьої елементарної функції – елементарну функцію на основі x_3: (3.52), (3.53), (3.55), (3.58); отримаємо можливість обмежити результати експерименту лише базовими операціями, в яких усі елементарні функції є розширеними матричними.

За результатами обчислювального експерименту нами отримані наступні прямі та їм обернені базові трирозрядні операції розширеного матричного криптографічного перетворення.

$$F^{k}_{30,57,149} = \begin{pmatrix} x_1 \oplus (x_2 \cdot x_3) \\ x_2 \oplus (x_1 \cdot \bar{x}_3) \\ x_3 \oplus (\bar{x}_1 \cdot \bar{x}_2) \end{pmatrix} \qquad F^{d}_{30,57,149} = \begin{pmatrix} x_1 \oplus (x_2 \cdot x_3) \\ x_2 \oplus (x_1 \cdot \bar{x}_3) \\ x_3 \oplus (\bar{x}_1 \cdot \bar{x}_2) \end{pmatrix} \tag{3.94}$$

$$F^{k}_{30,147,89} = \begin{pmatrix} x_1 \oplus (x_2 \cdot x_3) \\ x_2 \oplus (\bar{x}_1 \cdot \bar{x}_3) \\ x_3 \oplus (x_1 \cdot \bar{x}_2) \end{pmatrix} \qquad F^{d}_{30,147,89} = \begin{pmatrix} x_1 \oplus (x_2 \cdot x_3) \\ x_2 \oplus (\bar{x}_1 \cdot \bar{x}_3) \\ x_3 \oplus (x_1 \cdot \bar{x}_2) \end{pmatrix} \tag{3.95}$$

$$F^{k}_{45,54,149} = \begin{pmatrix} x_1 \oplus (x_2 \cdot \bar{x}_3) \\ x_2 \oplus (x_1 \cdot x_3) \\ x_3 \oplus (\bar{x}_1 \cdot \bar{x}_2) \end{pmatrix} \qquad F^{d}_{45,54,149} = \begin{pmatrix} x_1 \oplus (x_2 \cdot \bar{x}_3) \\ x_2 \oplus (x_1 \cdot x_3) \\ x_3 \oplus (\bar{x}_1 \cdot \bar{x}_2) \end{pmatrix} \tag{3.96}$$

$$F^{k}_{45,99,89} = \begin{pmatrix} x_1 \oplus (x_2 \cdot \bar{x}_3) \\ x_2 \oplus (\bar{x}_1 \cdot x_3) \\ x_3 \oplus (x_1 \cdot \bar{x}_2) \end{pmatrix} \qquad F^{d}_{45,99,89} = \begin{pmatrix} x_1 \oplus (x_2 \cdot \bar{x}_3) \\ x_2 \oplus (\bar{x}_1 \cdot x_3) \\ x_3 \oplus (x_1 \cdot \bar{x}_2) \end{pmatrix} \tag{3.98}$$

$$F^{k}_{75,57,101} = \begin{pmatrix} x_1 \oplus (\bar{x}_2 \cdot x_3) \\ x_2 \oplus (x_1 \cdot \bar{x}_3) \\ x_3 \oplus (\bar{x}_1 \cdot x_2) \end{pmatrix} \qquad F^{d}_{75,57,101} = \begin{pmatrix} x_1 \oplus (\bar{x}_2 \cdot x_3) \\ x_2 \oplus (x_1 \cdot \bar{x}_3) \\ x_3 \oplus (\bar{x}_1 \cdot x_2) \end{pmatrix} \tag{3.99}$$

$$F^{k}_{75,51,86} = \begin{pmatrix} x_1 \oplus (\bar{x}_2 \cdot x_3) \\ x_2 \oplus (\bar{x}_1 \cdot \bar{x}_3) \\ x_3 \oplus (x_1 \cdot x_2) \end{pmatrix} \qquad F^{d}_{75,51,86} = \begin{pmatrix} x_1 \oplus (\bar{x}_2 \cdot x_3) \\ x_2 \oplus (\bar{x}_1 \cdot \bar{x}_3) \\ x_3 \oplus (x_1 \cdot x_2) \end{pmatrix} \tag{3.100}$$

$$F^{k}_{135,54,101} = \begin{pmatrix} x_1 \oplus (\bar{x}_2 \cdot \bar{x}_3) \\ x_2 \oplus (x_1 \cdot x_3) \\ x_3 \oplus (\bar{x}_1 \cdot x_2) \end{pmatrix} \qquad F^{d}_{135,54,101} = \begin{pmatrix} x_1 \oplus (\bar{x}_2 \cdot \bar{x}_3) \\ x_2 \oplus (x_1 \cdot x_3) \\ x_3 \oplus (\bar{x}_1 \cdot x_2) \end{pmatrix} \tag{3.101}$$

$$F^{k}_{135,99,86} = \begin{pmatrix} x_1 \oplus (\bar{x}_2 \cdot \bar{x}_3) \\ x_2 \oplus (\bar{x}_1 \cdot x_3) \\ x_3 \oplus (x_1 \cdot x_2) \end{pmatrix} \qquad F^{d}_{135,99,86} = \begin{pmatrix} x_1 \oplus (\bar{x}_2 \cdot \bar{x}_3) \\ x_2 \oplus (\bar{x}_1 \cdot x_3) \\ x_3 \oplus (x_1 \cdot x_2) \end{pmatrix} \tag{3.102}$$

Операції криптографічного перетворення (3.94) – (3.102) забезпечують 8 перестановок. Результати їх виконання наведені в табл. 3.2.

Для спрощення розробки методів синтезу операцій криптографічного перетворення доцільно було б виявити закономірності поєднання елементарних функцій в операцію криптоперетворення та побудувати модель операції. Це дозволить спростити методи синтезу базових операцій за рахунок використання аналітичного перебору.

Таблиця 3.2

Результати виконання базових трирозрядних операцій розширеного матричного криптографічного перетворення

	$F^k_{30,57,149}$	$F^k_{30,147,89}$	$F^k_{45,54,149}$	$F^k_{45,99,89}$	$F^k_{75,57,101}$	$F^k_{75,147,86}$	$F^k_{135,54,101}$	$F^k_{135,99,86}$
000	001	010	001	000	000	010	100	100
001	000	001	000	011	101	101	001	011
010	010	000	110	110	011	000	011	010
011	111	111	011	001	010	011	010	001
100	110	101	100	101	110	100	000	000
101	101	100	111	100	001	001	111	101
110	100	110	010	010	100	111	110	111
111	011	011	101	111	111	110	101	110

На основі аналізу виразів (3.94) – (3.102) нами встановлені наступні закономірності:

– першим доданком по модулю завжди є x_1, x_2, або x_3, другим доданком – добуток двох інших аргументів;

– x_1 у других доданках завжди присутній в прямому та інверсному значенні;

– x_2 у других доданках завжди присутній в прямому та інверсному значенні;

– x_3 у других доданках завжди присутній в прямоту та інверсному значенні.

Формалізуємо наведені правила для побудови операції криптографічного перетворення під час синтезу, починаючи з першої елементарної функції:

$$F^k = \begin{bmatrix} x_1 \oplus (\hat{x}_2 \cdot \hat{x}_3) \\ x_2 \oplus (\hat{x}_1 \cdot \bar{\hat{x}}_3) \\ x_3 \oplus (\bar{\hat{x}}_1 \cdot \bar{\hat{x}}_2) \end{bmatrix} \tag{3.103}$$

де x – пряме значення аргументу; $\bar{x}$ – інверсне значення аргументу; $\hat{x}$ – будь-яке значення аргументу; $\bar{\hat{x}}$ – інверсне щодо будь-якого значення аргументу.

Аналогічно, якщо почати синтез з другої функції отримаємо:

$$F^k = \begin{bmatrix} x_1 \oplus (\hat{x}_2 \cdot \bar{\hat{x}}_3) \\ x_2 \oplus (\hat{x}_1 \cdot \hat{x}_3) \\ x_3 \oplus (\bar{\hat{x}}_1 \cdot \bar{\hat{x}}_2) \end{bmatrix} \tag{3.104}$$

Аналогічно, якщо почати синтез з третьої функції отримаємо:

$$F^k = \begin{bmatrix} x_1 \oplus (\bar{\hat{x}}_2 \cdot \bar{\hat{x}}_3) \\ x_2 \oplus (\bar{\hat{x}}_1 \cdot \hat{x}_3) \\ x_3 \oplus (\hat{x}_1 \cdot \hat{x}_2) \end{bmatrix} \tag{3.105}$$

Вирази (3.103) – (3.105) дозволяють синтезувати операції криптографічного перетворення на основі розширеного матричного представлення.

Оскільки вирази (3.103) – (3.105) приводять до одного і того ж самого результату, при подальших дослідженнях використано лише вираз (3.103).

Сформулюємо метод синтезу трирозрядних базових операцій розширеного матричного криптографічного перетворення за наявності трьох розширень: на основі виразу (3.103) шляхом перебору значень $\hat{x}_1$, $\hat{x}_2$, $\hat{x}_3$ де $\hat{x}_1 \in [x_1, \bar{x}_1]$, $\hat{x}_2 \in [x_2, \bar{x}_2]$, $\hat{x}_3 \in [x_3, \bar{x}_3]$ побудувати 8 трирозрядних базових операцій розширеного матричного криптографічного представлення, в яких присутні усі три розширення.

Синтезувати групу базових трирозрядних операцій розширеного матричного криптографічного перетворення сумісно з групою операцій перестановки можливо на основі узагальненої моделі операції:

$$F^k = \begin{bmatrix} x_i \oplus (\hat{x}_j \cdot \hat{x}_l) \\ x_j \oplus (\hat{x}_i \cdot \bar{\hat{x}}_l) \\ x_l \oplus (\bar{\hat{x}}_i \cdot \bar{\hat{x}}_j) \end{bmatrix}, \quad (3.106)$$

де $i, j, l \in [1, 2, 3]$ за умови $i \neq j \neq l$; $\hat{x}_i \in [x_i,\ \bar{x}_i]$, $\hat{x}_j \in [x_j,\ \bar{x}_j]$, $\hat{x}_l \in [x_l,\ \bar{x}_l]$.

Метод синтезу операцій розширеного матричного криптографічного перетворення на основі моделі операції полягає в наступному: на основі виразу (3.106) шляхом перебору значень i, j, l, де $i, j, l \in [1, 2, 3]$, за виконання умови $i \neq j \neq l$ та перебору значень інверсії $\hat{x}_i$, $\hat{x}_j$, $\hat{x}_l$, де $\hat{x}_i \in [x_i,\ \bar{x}_i]$, $\hat{x}_j \in [x_j,\ \bar{x}_j]$, $\hat{x}_l \in [x_l,\ \bar{x}_l]$ отримати групу операцій розширеного матричного криптографічного перетворення, яка включає у себе групу базових операцій та групу операцій перестановки.

Для синтезу групи базових операцій розширеного матричного криптографічного перетворення на основі виразу (3.106) необхідно обмежитися випадком, коли $i = 1$, $j = 2$, $l = 3$ та проводити перебір лише значень інверсії $\hat{x}_i$, $\hat{x}_j$, $\hat{x}_l$, де $\hat{x}_i \in [x_i,\ \bar{x}_i]$, $\hat{x}_j \in [x_j,\ \bar{x}_j]$, $\hat{x}_l \in [x_l,\ \bar{x}_l]$.

Синтезувати групу базових трирозрядних операцій розширеного матричного криптографічного перетворення сумісно з групою операцій перестановки та сумісно з групою операцій інверсії можливо на основі узагальненої моделі операції:

$$F^k = \begin{bmatrix} x_i \oplus (\hat{x}_j \cdot \hat{x}_l) \\ x_j \oplus (\hat{x}_i \cdot \bar{\hat{x}}_l) \\ x_l \oplus (\bar{\hat{x}}_i \cdot \bar{\hat{x}}_j) \end{bmatrix} \oplus \begin{bmatrix} b_i \\ b_j \\ b_l \end{bmatrix}, \quad (3.107)$$

де $i, j, l \in [1, 2, 3]$ за умови $i \neq j \neq l$; $\hat{x}_i \in [x_i,\ \bar{x}_i]$, $\hat{x}_j \in [x_j,\ \bar{x}_j]$, $\hat{x}_l \in [x_l,\ \bar{x}_l]$, $b \in [0,\ 1]$.

Синтез повної групи трирозрядних операцій розширеного матричного криптографічного перетворення за наявності трьох розширень, яка включає у себе групу базових операцій, групу операцій перестановок та групу операцій інверсії здійснюється аналогічно.

3.3.2 Синтез операцій криптографічного перетворення на основі елементарних функцій розширеного матричного представлення методом заміни

Розглянуті методи синтезу на основі виразів (3.106) та (3.107) синтезують лише операції криптографічного перетворення за наявності трьох заміщень.

За результатами обчислювального експерименту встановлено, що в операціях розширеного матричного криптографічного перетворення може бути три заміщення, два заміщення або одне заміщення.

Використати метод заміщення [30, 52] для синтезу базових операцій розширеного матричного криптографічного перетворення представляється достатньо складним, тому що після виконання кожної операції заміщення необхідно здійснювати перевірку щодо коректності виконання операції криптоперетворення, тобто коректність отриманої перестановки вхідного набору даних.

Вдосконалимо метод синтезу базових операцій криптографічного перетворення на основі заміщення з урахуванням отриманої моделі операції.

1. Виберемо операцію повторення інформації (нульову операцію) (2.20):

$$F^{k}_{15,51,85} = F^{d}_{15,51,85} = (f^{1}_{15},\ f^{2}_{51},\ f^{3}_{85}) = \begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix} .$$

2. Синтезуємо елементарні функції для заміщення:

2.1. Для заміщення першої елементарної функції на основі виразу (3.83):

$$f_{30} = x_1 \oplus (x_2 \cdot x_3); \tag{3.108}$$

$$f_{45} = x_1 \oplus (x_1 \cdot \bar{x}_3); \tag{3.109}$$

$$f_{75} = x_1 \oplus (\bar{x}_2 \cdot x_3); \tag{3.110}$$

$$f_{135} = x_1 \oplus (\bar{x}_2 \cdot \bar{x}_3). \tag{3.111}$$

2.2. Для заміщення другої елементарної функції на основі виразу (3.84):

$$f_{54} = x_2 \oplus (x_1 \cdot x_3); \tag{3.112}$$

$$f_{57} = x_2 \oplus (x_1 \cdot \bar{x}_3); \tag{3.113}$$

$$f_{99} = x_2 \oplus (\bar{x}_1 \cdot x_3); \tag{3.114}$$

$$f_{147} = x_2 \oplus (\bar{x}_1 \cdot \bar{x}_3). \tag{3.115}$$

2.3. Для заміщення третьої елементарної функції на основі виразу (3.85):

$$f_{86} = x_3 \oplus (x_1 \cdot x_2); \tag{3.116}$$

$$f_{89} = x_3 \oplus (x_1 \cdot \bar{x}_2); \tag{3.117}$$

$$f_{101} = x_3 \oplus (\bar{x}_1 \cdot x_2); \tag{3.118}$$

$$f_{149} = x_3 \oplus (\bar{x}_1 \cdot \bar{x}_2). \tag{3.119}$$

3. Проведемо заміну однієї з елементарних функцій:

3.1. Виразами (3.108) – (3.111) проведемо заміну першої елементарної функції:

$$F^{k}_{30,51,85} = \begin{pmatrix} x_1 \oplus (x_2 \cdot x_3) \\ x_2 \\ x_3 \end{pmatrix}; \tag{3.120}$$

$$F^{k}_{45,51,85} = \begin{pmatrix} x_1 \oplus (x_2 \cdot \bar{x}_3) \\ x_2 \\ x_3 \end{pmatrix} ; \quad (3.121)$$

$$F^{k}_{75,51,85} = \begin{pmatrix} x_1 \oplus (\bar{x}_2 \cdot x_3) \\ x_2 \\ x_3 \end{pmatrix} ; \quad (3.122)$$

$$F^{k}_{135,51,85} = \begin{pmatrix} x_1 \oplus (\bar{x}_2 \cdot \bar{x}_3) \\ x_2 \\ x_3 \end{pmatrix} . \quad (3.123)$$

3.2. Виразами (3.112) – (3.115) проведемо заміну другої елементарної функції:

$$F^{k}_{15,54,85} = \begin{pmatrix} x_1 \\ x_2 \oplus (x_1 \cdot x_3) \\ x_3 \end{pmatrix} ; \quad (3.124)$$

$$F^{k}_{15,57,85} = \begin{pmatrix} x_1 \\ x_2 \oplus (x_1 \cdot \bar{x}_3) \\ x_3 \end{pmatrix} ; \quad (3.125)$$

$$F^{k}_{15,99,85} = \begin{pmatrix} x_1 \\ x_2 \oplus (\bar{x}_1 \cdot x_3) \\ x_3 \end{pmatrix} ; \quad (3.126)$$

$$F^{k}_{15,147,85} = \begin{pmatrix} x_1 \\ x_2 \oplus (\bar{x}_1 \cdot \bar{x}_3) \\ x_3 \end{pmatrix} . \quad (3.127)$$

3.3. Виразами (3.116) – (3.119) проведемо заміну третьої елементарної функції:

$$F^{k}_{15,51,86} = \begin{pmatrix} x_1 \\ x_2 \\ x_3 \oplus (x_1 \cdot x_2) \end{pmatrix} ; \quad (3.128)$$

$$F^{k}_{15,51,89} = \begin{pmatrix} x_1 \\ x_2 \\ x_3 \oplus (x_1 \cdot \bar{x}_2) \end{pmatrix} ; \quad (3.129)$$

$$F^{k}_{15,51,101} = \begin{pmatrix} x_1 \\ x_2 \\ x_3 \oplus (\bar{x}_1 \cdot x_2) \end{pmatrix} ; \quad (3.130)$$

$$F^{k}_{15,51,149} = \begin{pmatrix} x_1 \\ x_2 \\ x_3 \oplus (\bar{x}_1 \cdot \bar{x}_2) \end{pmatrix} . \quad (3.131)$$

4. Проведемо заміну двох елементарних функцій [30]:

4.1. На основі виразів (3.120) – (3.123) виразами (3.112) – (3.115) проведемо заміну другої елементарної функції при заміненій першій з урахуванням обмежень моделі (3.106):

$$F^{k}_{30,57,85} = \begin{pmatrix} x_1 \oplus (x_2 \cdot x_3) \\ x_2 \oplus (x_1 \cdot \bar{x}_3) \\ x_3 \end{pmatrix} ; \quad (3.132)$$

$$F^{k}_{30,147,85} = \begin{pmatrix} x_1 \oplus (x_2 \cdot x_3) \\ x_2 \oplus (\bar{x}_1 \cdot \bar{x}_3) \\ x_3 \end{pmatrix} ; \quad (3.133)$$

$$F^{k}_{45,54,85} = \begin{pmatrix} x_1 \oplus (x_2 \cdot \bar{x}_3) \\ x_2 \oplus (x_1 \cdot x_3) \\ x_3 \end{pmatrix} ; \quad (3.134)$$

$$F^{k}_{45,99,85} = \begin{pmatrix} x_1 \oplus (x_2 \cdot \bar{x}_3) \\ x_2 \oplus (\bar{x}_1 \cdot x_3) \\ x_3 \end{pmatrix} ; \quad (3.135)$$

$$F^{k}_{75,57,85} = \begin{pmatrix} x_1 \oplus (\bar{x}_2 \cdot x_3) \\ x_2 \oplus (x_1 \cdot \bar{x}_3) \\ x_3 \end{pmatrix} ; \quad (3.136)$$

$$F^{k}_{75,51,147} = \begin{pmatrix} x_1 \oplus (\bar{x}_2 \cdot x_3) \\ x_2 \oplus (\bar{x}_1 \cdot \bar{x}_3) \\ x_3 \end{pmatrix} ; \quad (3.137)$$

$$F^{k}_{135,54,85} = \begin{pmatrix} x_1 \oplus (\bar{x}_2 \cdot \bar{x}_3) \\ x_2 \oplus (x_1 \cdot x_3) \\ x_3 \end{pmatrix} . \quad (3.138)$$

$$F^{k}_{135,99,85} = \begin{pmatrix} x_1 \oplus (\bar{x}_2 \cdot \bar{x}_3) \\ x_2 \oplus (\bar{x}_1 \cdot x_3) \\ x_3 \end{pmatrix} . \quad (3.139)$$

4.2. На основі виразів (3.120) – (3.123) виразами (3.116) – (3.119) проведемо заміну третьої елементарної функції при заміненій першій з урахуванням обмежень моделі (3.106):

$$F^{k}_{30,51,89} = \begin{pmatrix} x_1 \oplus (x_2 \cdot x_3) \\ x_2 \\ x_3 \oplus (x_1 \cdot \bar{x}_2) \end{pmatrix} ; \quad (3.140)$$

$$F^{k}_{30,51,149} = \begin{pmatrix} x_1 \oplus (x_2 \cdot x_3) \\ x_2 \\ x_3 \oplus (\bar{x}_1 \cdot \bar{x}_2) \end{pmatrix} ; \quad (3.141)$$

$$F^{k}_{45,51,101} = \begin{pmatrix} x_1 \oplus (x_2 \cdot \bar{x}_3) \\ x_2 \\ x_3 \oplus (x_1 \cdot \bar{x}_2) \end{pmatrix} ; \quad (3.142)$$

$$F^{k}_{45,51,149} = \begin{pmatrix} x_1 \oplus (x_2 \cdot \bar{x}_3) \\ x_2 \\ x_3 \oplus (\bar{x}_1 \cdot \bar{x}_2) \end{pmatrix} ; \quad (3.143)$$

$$F^{k}_{75,51,86} = \begin{pmatrix} x_1 \oplus (\bar{x}_2 \cdot x_3) \\ x_2 \\ x_3 \oplus (x_1 \cdot x_2) \end{pmatrix} ; \quad (3.144)$$

$$F^{k}_{75,51,101} = \begin{pmatrix} x_1 \oplus (\bar{x}_2 \cdot x_3) \\ x_2 \\ x_3 \oplus (\bar{x}_1 \cdot x_2) \end{pmatrix} ; \quad (3.145)$$

$$F^{k}_{135,51,86} = \begin{pmatrix} x_1 \oplus (\bar{x}_2 \cdot \bar{x}_3) \\ x_2 \\ x_3 \oplus (x_1 \cdot x_2) \end{pmatrix} . \quad (3.146)$$

$$F^{k}_{135,51,101} = \begin{pmatrix} x_1 \oplus (\bar{x}_2 \cdot \bar{x}_3) \\ x_2 \\ x_3 \oplus (\bar{x}_1 \cdot x_2) \end{pmatrix} . \quad (3.147)$$

4.3. На основі виразів (3.124) – (3.127) виразами (3.116) – (3.119) проведемо заміну третьої елементарної функції при заміненій другій з урахуванням обмежень моделі (3.106):

$$F^{k}_{15,54,101} = \begin{pmatrix} x_1 \\ x_2 \oplus (x_1 \cdot x_3) \\ x_3 \oplus (\bar{x}_1 \cdot x_2) \end{pmatrix} ; \quad (3.148)$$

$$F^{k}_{15,54,149} = \begin{pmatrix} x_1 \\ x_2 \oplus (x_1 \cdot x_3) \\ x_3 \oplus (\bar{x}_1 \cdot \bar{x}_2) \end{pmatrix} ; \quad (3.149)$$

$$F^{k}_{15,57,101} = \begin{pmatrix} x_1 \\ x_2 \oplus (x_1 \cdot \bar{x}_3) \\ x_3 \oplus (\bar{x}_1 \cdot x_2) \end{pmatrix} ; \quad (3.150)$$

$$F^{k}_{15,57,149} = \begin{pmatrix} x_1 \\ x_2 \oplus (x_1 \cdot \bar{x}_3) \\ x_3 \oplus (\bar{x}_1 \cdot \bar{x}_2) \end{pmatrix} ; \quad (3.151)$$

$$F^{k}_{15,99,86} = \begin{pmatrix} x_1 \\ x_2 \oplus (\bar{x}_1 \cdot x_3) \\ x_3 \oplus (x_1 \cdot x_2) \end{pmatrix} ; \quad (3.152)$$

$$F^{k}_{15,99,89} = \begin{pmatrix} x_1 \\ x_2 \oplus (\bar{x}_1 \cdot x_3) \\ x_3 \oplus (x_1 \cdot \bar{x}_2) \end{pmatrix} ; \quad (3.153)$$

$$F^{k}_{15,147,86} = \begin{pmatrix} x_1 \\ x_2 \oplus (\bar{x}_1 \cdot \bar{x}_3) \\ x_3 \oplus (x_1 \cdot x_2) \end{pmatrix} . \quad (3.154)$$

$$F^{k}_{15,147,89} = \begin{pmatrix} x_1 \\ x_2 \oplus (\bar{x}_1 \cdot \bar{x}_3) \\ x_3 \oplus (x_1 \cdot \bar{x}_2) \end{pmatrix} . \quad (3.155)$$

4.4. На основі виразів (3.132) – (3.139) виразами (3.116) – (3.119) проведемо заміну третьої елементарної функції при замінених першій і другій елементарних функціях з урахуванням обмежень моделі (3.106):

$$F^{k}_{30,57,149} = \begin{pmatrix} x_1 \oplus (x_2 \cdot x_3) \\ x_2 \oplus (x_1 \cdot \bar{x}_3) \\ x_3 \oplus (\bar{x}_1 \cdot \bar{x}_2) \end{pmatrix} ; \quad (3.156)$$

$$F^{k}_{30,147,89} = \begin{pmatrix} x_1 \oplus (x_2 \cdot x_3) \\ x_2 \oplus (\bar{x}_1 \cdot \bar{x}_3) \\ x_3 \oplus (x_1 \cdot \bar{x}_2) \end{pmatrix} ; \quad (3.157)$$

$$F^{k}_{45,54,149} = \begin{pmatrix} x_1 \oplus (x_2 \cdot \bar{x}_3) \\ x_2 \oplus (x_1 \cdot x_3) \\ x_3 \oplus (\bar{x}_1 \cdot \bar{x}_2) \end{pmatrix} ; \quad (3.158)$$

$$F^{k}_{45,99,89} = \begin{pmatrix} x_1 \oplus (x_2 \cdot \bar{x}_3) \\ x_2 \oplus (\bar{x}_1 \cdot x_3) \\ x_3 \oplus (x_1 \cdot \bar{x}_2) \end{pmatrix} ; \quad (3.159)$$

$$F^{k}_{75,57,101} = \begin{pmatrix} x_1 \oplus (\bar{x}_2 \cdot x_3) \\ x_2 \oplus (x_1 \cdot \bar{x}_3) \\ x_3 \oplus (\bar{x}_1 \cdot x_2) \end{pmatrix} ; \quad (3.160)$$

$$F^{k}_{75,51,86} = \begin{pmatrix} x_1 \oplus (\bar{x}_2 \cdot x_3) \\ x_2 \oplus (\bar{x}_1 \cdot \bar{x}_3) \\ x_3 \oplus (x_1 \cdot x_2) \end{pmatrix} ; \quad (3.161)$$

$$F^{k}_{135,54,101} = \begin{pmatrix} x_1 \oplus (\bar{x}_2 \cdot \bar{x}_3) \\ x_2 \oplus (x_1 \cdot x_3) \\ x_3 \oplus (\bar{x}_1 \cdot x_2) \end{pmatrix} . \quad (3.162)$$

$$F^{k}_{135,99,86} = \begin{pmatrix} x_1 \oplus (\bar{x}_2 \cdot \bar{x}_3) \\ x_2 \oplus (\bar{x}_1 \cdot x_3) \\ x_3 \oplus (x_1 \cdot x_2) \end{pmatrix} . \quad (3.163)$$

Вирази (2.20), (3.120 – 3.160) представляють базову групу операцій розширеного матричного криптографічного перетворення, що співпадає з результатами обчислювального експерименту [30].

3.3.3 Синтез операцій криптографічного перетворення на основі моделі операції методом виключення (обернений метод синтезу)

Дослідження методу синтезу базових операцій криптографічного перетворення на основі заміщення з урахуванням отриманої моделі операції показало, що його можливо модифікувати, створивши для нього обернений метод синтезу.

Синтез операцій криптографічного перетворення на основі моделі операції методом виключення (обернений метод синтезу) полягає у наступному:

1. На основі виразу (3.106) шляхом обмеження перебору значень i, j, l, де $i, j, l \in [1, 2, 3]$, умовою $i = 1$, $j = 2$, $l = 3$ і, провівши перебір значень інверсії $\hat{x}_i$, $\hat{x}_j$, $\hat{x}_l$, де $\hat{x}_i \in [x_i, \bar{x}_i]$, $\hat{x}_j \in [x_j, \bar{x}_j]$, $\hat{x}_l \in [x_l, \bar{x}_l]$, отримати 8 базових операцій розширеного матричного криптографічного перетворення з трьома заміщеннями (замінами) (3.156) – (3.163);

2. Із операцій розширеного матричного криптографічного перетворення із трьома заміщеннями (замінами) (3.156) – (3.163) шляхом видалення одного з розширень отримати операції розширеного матричного криптографічного перетворення з двома розширеннями (заміщеннями):

   2.1. На основі виразів (3.156) – (3.163), виключивши перше розширення, отримано вирази (3.148) – (3.155);

   2.2. На основі виразів (3.156) – (3.163), виключивши друге розширення, отримано вирази (3.140) – (3.147);

   2.3. На основі виразів (3.156) – (3.163), виключивши третє розширення, отримано вирази (3.132) – (3.139);

3. Із операцій розширеного матричного криптографічного перетворення з трьома заміщеннями (замінами) (3.156) – (3.163) шляхом видалення двох розширень отримати операції розширеного матричного криптографічного перетворення з одним розширенням:

3.1. На основі виразів (3.156) – (3.163), виключивши перше і друге розширення, отримано вирази 4 операцій (3.128) – (3.131), оскільки кожна в процесі видалення отримана двічі;

3.2. На основі виразів (3.156) – (3.163), виключивши перше і третє розширення, отримано вирази 4 операцій (3.124) – (3.127), оскільки кожна в процесі видалення отримана двічі;

3.3. На основі виразів (3.156) – (3.163), виключивши друге і третє розширення, отримано вирази 4 операцій (3.120) – (3.123), оскільки кожна в процесі видалення отримана двічі;

4. З любої операції розширеного матричного криптографічного перетворення з трьома заміщеннями (замінами) (3.156) – (3.163) шляхом видалення трьох розширень отримати операцію повторення інформації (нульову операцію) (2.20).

Сформульований метод синтезу операцій криптографічного перетворення на основі моделі операції виключення, на відміну від методу синтезу на основі операції видалення [53], відрізняється такими перевагами:

– відбувається зменшення складності алгоритму за рахунок зменшеної, фіксованої кількості початкових операцій криптоперетворення на кожному етапі видалення;

– відсутня необхідність проводити порівняльний аналіз кожної нової синтезованої операції щодо її повторення (співпадіння) з усіма раніше синтезованими операціями.

Слід відзначити, що синтез операцій криптографічного перетворення на основі моделі операції методом виключення спрощує процес синтезу, шляхом використання формалізованої моделі операції перетворення.

У результаті синтезу отримано 45 базових операції криптографічного перетворення на основі розширеного матричного представлення.

Кількість базових операцій співпадає з кількістю операцій, отриманих на основі обчислювального експерименту, та складає 42 операції. Ця розбіжність зумовлена некоректним поділом елементарних функцій розширеного матричного

криптографічного перетворення на прямі та обернені. Під час проведення експерименту елементарні функції $f_{106}(3.59)$, $f_{108}(3.60)$, $f_{120}(3.61)$, вважалися прямими, оскільки їх порядковий номер менший за порядковий номер елементарних функцій $f_{149}(3.56)$, $f_{147}(3.57)$, $f_{135}(3.58)$, які вважалися оберненими. В ході внесення змін результати експерименту співпали з теоретичним розрахунком кількості базових операцій розширеного матричного криптографічного перетворення.

Таким чином, загальна кількість операцій, що утворюються поєднанням базової, перестановки та інверсії визначається як загальна кількість комбінацій таких операцій:

$$N = N_{б} \cdot N_{n} \cdot N_{i} = N_{б} \cdot 3! \cdot 2^{3} = 45 \cdot 6 \cdot 8 = 2160 .$$

Подальші дослідження будуть направлені на розробку методів синтезу обернених операцій криптографічного перетворення.

3.4. Математична модель операцій розширеного матричного криптографічного перетворення

У загальному вигляді операції прямого і оберненого розширеного матричного криптографічного перетворення відповідно до виразу (3.106) можна представити:

$$F = \begin{bmatrix} x_i \oplus a_1 \cdot (\hat{x}_j \cdot \hat{x}_l) \oplus b_1 \\ x_j \oplus a_2 \cdot (\hat{x}_i \cdot \bar{\hat{x}}_l) \oplus b_2 \\ x_l \oplus a_3 \cdot (\bar{\hat{x}}_i \cdot \bar{\hat{x}}_j) \oplus b_3 \end{bmatrix} = \begin{bmatrix} x_i \\ x_j \\ x_l \end{bmatrix} \oplus \begin{bmatrix} a_1 \cdot (\hat{x}_j \cdot \hat{x}_l) \\ a_2 \cdot (\hat{x}_i \cdot \bar{\hat{x}}_l) \\ a_3 \cdot (\bar{\hat{x}}_i \cdot \bar{\hat{x}}_j) \end{bmatrix} \oplus \begin{bmatrix} b_1 \\ b_2 \\ b_3 \end{bmatrix} \qquad (3.164)$$

де $a \in [0,1]$; $b \in [0,1]$; $i, j, l \in [1, 2, 3]$ за умови $i \neq j \neq l$; $\hat{x}_i \in [x_i, \bar{x}_i]$, $\hat{x}_j \in [x_j, \bar{x}_j]$, $\hat{x}_l \in [x_l, \bar{x}_l]$.

Згідно виразу (3.164) операцію розширеного матричного криптографічного перетворення можна представити як суму по модулю 2 трьох перетворень: матричного перетворення (F_m), перетворення розширення матричного перетворення (F_r) та перетворення на основі інверсії (F_i):

$$F = \begin{bmatrix} x_i \oplus a_1 \cdot (\hat{x}_j \cdot \hat{x}_l) \oplus b_1 \\ x_j \oplus a_2 \cdot (\hat{x}_i \cdot \bar{\hat{x}}_l) \oplus b_2 \\ x_l \oplus a_3 \cdot (\bar{\hat{x}}_i \cdot \bar{\hat{x}}_j) \oplus b_3 \end{bmatrix} = F_m \oplus F_r \oplus F_i . \qquad (3.165)$$

Слід відмітити, що перетворення F_m та F_i є лінійними перетвореннями, а перетворення F_r – нелінійним перетворенням, оскільки елементарні функції є не афінними, тобто функції перетворення не можуть бути описані поліномом $f = a_0 \oplus a_1 x_1 \oplus a_2 x_2 \oplus ... \oplus a_n x_n$, де $n = 1,2,...$ [176].

Дане представлення дає змогу спростити знаходження оберненого матричного перетворення, тому що виокремлює нелінійне матричне перетворення F_r.

Подамо операцію розширеного матричного криптографічного перетворення без урахування інверсії як суму по модулю 2 лінійної та нелінійної матриць:

$$\vec{F} = \begin{pmatrix} a_{11}x_1 \oplus a_{12}x_2 \oplus a_{13}x_3 \\ a_{21}x_1 \oplus a_{22}x_2 \oplus a_{23}x_3 \\ a_{31}x_1 \oplus a_{32}x_2 \oplus a_{3\,3}x_3 \end{pmatrix} \oplus \begin{pmatrix} a_{11}\hat{x}_2\hat{x}_3 \oplus a_{12}\hat{x}_1\hat{x}_3 \oplus a_{13}\hat{x}_1\hat{x}_2 \\ a_{21}\hat{x}_2\bar{\hat{x}}_3 \oplus a_{22}\hat{x}_1\bar{\hat{x}}_3 \oplus a_{23}\hat{x}_1\bar{\hat{x}}_2 \\ a_{31}\bar{\hat{x}}_2\bar{\hat{x}}_3 \oplus a_{32}\bar{\hat{x}}_1\bar{\hat{x}}_3 \oplus a_{3\,3}\bar{\hat{x}}_1\bar{\hat{x}}_2 \end{pmatrix}, \qquad (3.167)$$

де $\begin{pmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{3\,3} \end{pmatrix}$ –матриця перестановки.

Як видно з виразу (3.167), правила побудови матриці розширення не залежать від операції перестановки елементарних функцій базової операції.

Подання (2.1) дає змогу розглядати групу операцій криптоперетворення як поєднання групи базових операцій, групи операцій перестановки та групи операцій інверсії. Отже, і операцію розширеного матричного криптографічного перетворення можна представити як поєднання цих трьох операцій базової F_b, операції перестановки F_p та операції інверсії F_i:

$$F = F_b \times F_p \oplus F_i \tag{3.166}$$

Відповідно до виразів (3.165) і (3.166) можна виділити операцію інверсії, оскільки вона самостійна і реалізується аналогічно операції інверсії в операціях матричного криптографічного перетворення.

Аналіз узагальненої моделі операції розширеного матричного криптографічного перетворення (3.106) за наявності трьох розширень, вирази (3.156) – (3.163), дозволив сформулювати наступні правила:

Правило 3.1.1. Якщо в операції криптоперетворення елементарна функція має в розширенні логічний добуток двох аргументів без інверсії, тоді в даній операції будуть присутні елементарна функція, яка матиме у розширенні логічний добуток двох аргументів з інверсіями та елементарна функція, яка матиме у розширенні логічний добуток двох аргументів, один із яких із інверсією, а інший без інверсії;

Правило 3.1.2. Якщо в операції криптоперетворення елементарна функція має в розширенні логічний добуток двох аргументів з інверсіями, тоді в даній операції будуть присутні елементарна функція, яка матиме у розширенні логічний добуток двох аргументів без інверсій та елементарна функція, яка матиме у розширенні логічний добуток двох аргументів, один із яких із інверсією, а інший без інверсії;

Правило 3.1.3. Якщо в операції криптоперетворення елементарна функція має в розширенні логічний добуток двох аргументів, один із яких із інверсією, а інший без інверсії, тоді в даній операції будуть присутні елементарні функції, які

матимуть у розширенні логічний добуток двох аргументів із інверсіями та без інверсій, або елементарну функцію, яка матиме в розширенні логічний добуток двох аргументів, один із яких із інверсією, а інший без інверсії.

Формалізуємо дані правила.

Для $F\begin{pmatrix} a_i \\ a_j \\ a_l \end{pmatrix}$ заданої множиною f другої степені $f = a_i \oplus (a_j \cdot a_l)$ змінних

$a_i,\ a_j,\ a_l,\ i=1,2,3;\quad j=1,2,3;\quad l=1,2,3;\quad i \neq j \neq l;\quad a_i, b_i, c_i, d_i \in \{x_i, \bar{x}_i\}$

$F\begin{pmatrix} a_i \\ a_j \\ a_l \end{pmatrix} = \begin{pmatrix} b_i \oplus b_j \cdot b_l \\ c_j \oplus c_i \cdot c_l \\ d_l \oplus d_i \cdot d_j \end{pmatrix}$ існує $F^{-1}\begin{pmatrix} a_i \\ a_j \\ a_l \end{pmatrix}$ лише тоді:

Для правила 3.1.1: якщо $b_j = x_j,\ b_l = x_l,$ то або $\begin{cases} c_i = \bar{x}_i,\ c_l = \bar{x}_l, \\ \left[\begin{array}{l} d_i = \bar{x}_i,\ d_l = x_l, \\ d_i = x_i,\ d_j = \bar{x}_j. \end{array}\right. \end{cases}$,

або $\begin{cases} \left[\begin{array}{l} c_i = \bar{x}_i,\ c_l = x_l, \\ c_i = x_i,\ c_l = \bar{x}_l, \end{array}\right. \\ d_i = \bar{x}_i,\ d_j = \bar{x}_j. \end{cases}$.

Для правила 3.1.2: якщо $b_j = \bar{x}_j,\ b_l = \bar{x}_l,$ то або $\begin{cases} c_i = x_i,\ c_l = x_l, \\ \left[\begin{array}{l} d_i = \bar{x}_i,\ d_l = x_l, \\ d_i = x_i,\ d_j = \bar{x}_j. \end{array}\right. \end{cases}$,

або $\begin{cases} \left[\begin{array}{l} c_i = \bar{x}_i,\ c_l = x_l, \\ c_i = x_i,\ c_l = \bar{x}_l, \end{array}\right. \\ d_i = x_i,\ d_j = x_j. \end{cases}$.

Для правила 3.1.3: якщо $\left[\begin{array}{l} b_i = \bar{x}_j, b_l = x_l, \\ b_i = x_j, b_l = \bar{x}_l, \end{array}\right.$ то або $\begin{cases} c_i = \bar{x}_i,\ c_l = \bar{x}_l, \\ d_i = x_i,\ d_j = x_j. \end{cases}$,

або $\begin{cases} c_i = x_i,\ c_l = x_l, \\ d_i = \bar{x}_i,\ \ d_j = \bar{x}_j. \end{cases}$, або $\begin{cases} \left[\begin{array}{l} c_i = \bar{x}_i,\ c_l = x_l, \\ c_i = x_i,\ c_l = \bar{x}_l, \end{array}\right. \\ \left[\begin{array}{l} d_i = \bar{x}_i,\ d_l = x_l, \\ d_i = x_i,\ d_j = \bar{x}_j. \end{array}\right. \end{cases}$.

На основі правил 3.1.1 – 3.1.3 можна сформулювати наступне правило.

Правило 3.1.4. Для $F\begin{pmatrix} a_i \\ a_j \\ a_l \end{pmatrix} = \begin{pmatrix} b_i \oplus b_j \cdot b_l \\ c_j \oplus c_i \cdot c_l \\ d_l \oplus d_i \cdot d_j \end{pmatrix}$ існує $F^{-1}\begin{pmatrix} a_i \\ a_j \\ a_l \end{pmatrix}$ лише тоді, якщо

$$\left[\begin{array}{l} \begin{cases} b_i \oplus c_i \oplus d_i = 1 \\ b_i \vee c_i \vee d_i = 1 \end{cases} \\ \begin{cases} b_j \oplus c_j \oplus d_j = 1 \\ b_j \vee c_j \vee d_j = 1 \end{cases} \\ \begin{cases} b_l \oplus c_l \oplus d_l = 1 \\ b_l \vee c_l \vee d_l = 1 \end{cases} \end{array}\right. .$$

Дані правила дозволяють синтезувати операцію розширеного матричного криптографічного перетворення на основі випадкового вибору трьох значень булевих змінних b_j, b_l, c_i. Крім цього, дані правила необхідні для побудови оберненої операції криптоперетворення.

3.5 Розробка методів синтезу обернених операцій розширеного матричного криптографічного перетворення

3.5.1 Формалізація правил побудови операцій розширеного матричного криптографічного перетворення

Розглянемо можливість синтезу обернених операцій для базових операцій розширеного матричного криптографічного перетворення.

Відповідно до виразів (3.94) – (3.102), що отримані на основі обчислювального експерименту, прямі та обернені операції за наявності трьох

розширень співпадають. Звідси, можна зробити наступні правила:

Правило 3.2.1. Якщо у прямій операції криптоперетворення елементарна функція має в розширенні логічний добуток двох аргументів без інверсії, тоді у відповідній їй оберненій операції криптоперетворення елементарна функція матиме в розширенні логічний добуток двох аргументів без інверсії.

Правило 3.2.2. Якщо у прямій операції криптоперетворення елементарна функція має в розширенні логічний добуток двох аргументів з інверсіями, тоді у відповідній їй оберненій операції криптоперетворення елементарна функція матиме у розширенні логічний добуток двох аргументів із інверсіями.

Правило 3.2.3. Якщо у прямій операції криптоперетворення елементарна функція має в розширенні логічний добуток двох аргументів, один із яких з інверсією, а інший без інверсії, тоді у відповідній їй оберненій операції криптоперетворення елементарна функція матиме у розширенні логічний добуток двох аргументів, один із яких із інверсією, а інший без інверсії.

Формалізуємо дані правила.

Нехай заданій множині f другої степені $f = a_1 \oplus (a_2 \cdot a_3)$ змінних $a_1,\ a_2,\ a_3$ існує обернена і, при чому, єдина f^{-1} того ж класу, а саме:

$$f^{-1} = A_1 \oplus (A_2 \cdot A_3),$$

при цьому, якщо:

Для правила 3.2.1 змінна $a_i \in \{a_1;\ a_2;\ a_3\}$, то $A_i \in \{a_1;\ a_2;\ a_3\}$ для $i = 1, 2, 3;$

Для правила 3.2.2 змінна $a_i \in \{\bar{a}_1;\ \bar{a}_2;\ \bar{a}_3\}$, то $A_i \in \{\bar{a}_1;\ \bar{a}_2;\ \bar{a}_3\}$ для $i = 1, 2, 3;$

Для правила 3.2.3 для $\begin{cases} a_2 \in \{\bar{a}_1;\ \bar{a}_2;\ \bar{a}_3\} \\ a_3 \in \{a_1;\ a_2;\ a_3\} \end{cases}$ і $\begin{cases} a_2 \in \{a_1;\ a_2;\ a_3\} \\ a_3 \in \{\bar{a}_1;\ \bar{a}_2;\ \bar{a}_3\} \end{cases}$,

то або $\begin{cases} A_2 \in \{\bar{a}_1;\ \bar{a}_2;\ \bar{a}_3\} \\ A_3 \in \{a_1;\ a_2;\ a_3\} \end{cases}$, або $\begin{cases} A_2 \in \{a_1;\ a_2;\ a_3\} \\ A_3 \in \{\bar{a}_1;\ \bar{a}_2;\ \bar{a}_3\} \end{cases}$.

Вирази (3.94) – (3.102) доводять коректність правил 3.2.1 – 3.2.2.

На основі аналізу прямих і обернених базових операцій розширеного матричного криптоперетворення нами сформульовано додаткове правило:

Правило 3.2.4. Якщо у прямій операції криптоперетворення елементарна функція не має розширення, тоді і у відповідній їй оберненій операції криптоперетворення відповідна елементарна функція не буде мати розширення.

Формалізуємо дане правило.

Нехай заданій множині f першої степені $f = a_1$ змінних a_1, a_2, a_3 існує обернена і, при чому, єдина f^{-1} того ж класу, а саме: $f^{-1} = A_1$, при цьому, якщо:

Для правила 3.2.4 змінна $a_i \in \{a_1;\ a_2;\ a_3\}$, то $A_i \in \{a_1;\ a_2;\ a_3\}$ для $i = 1, 2, 3$.

Доведемо коректність використання правил 3.2.1 – 3.2.4 на основі повної множини прямих і відповідних їм обернених базових операцій за наявності двох та одного розширень.

Прямі та обернені трирозрядні базові операції з двома розширеннями:

$$F^k_{30,57,85} = \begin{pmatrix} x_1 \oplus (x_2 \cdot x_3) \\ x_2 \oplus (x_1 \cdot \bar{x}_3) \\ x_3 \end{pmatrix} \qquad F^d_{30,57,85} = \begin{pmatrix} x_1 \oplus (x_2 \cdot x_3) \\ x_2 \oplus (x_1 \cdot \bar{x}_3) \\ x_3 \end{pmatrix} \qquad (3.167)$$

$$F^k_{30,147,85} = \begin{pmatrix} x_1 \oplus (x_2 \cdot x_3) \\ x_2 \oplus (\bar{x}_1 \cdot \bar{x}_3) \\ x_3 \end{pmatrix} \qquad F^d_{30,147,85} = \begin{pmatrix} x_1 \oplus (x_2 \cdot x_3) \\ x_2 \oplus (\bar{x}_1 \cdot \bar{x}_3) \\ x_3 \end{pmatrix} \qquad (3.168)$$

$$F^k_{45,54,85} = \begin{pmatrix} x_1 \oplus (x_2 \cdot \bar{x}_3) \\ x_2 \oplus (x_1 \cdot x_3) \\ x_3 \end{pmatrix} \qquad F^d_{45,54,85} = \begin{pmatrix} x_1 \oplus (x_2 \cdot \bar{x}_3) \\ x_2 \oplus (x_1 \cdot x_3) \\ x_3 \end{pmatrix} \qquad (3.169)$$

$$F^{k}_{45,99,85}=\begin{pmatrix} x_1 \oplus (x_2 \cdot \bar{x}_3) \\ x_2 \oplus (\bar{x}_1 \cdot x_3) \\ x_3 \end{pmatrix} \qquad F^{d}_{45,99,85}=\begin{pmatrix} x_1 \oplus (x_2 \cdot \bar{x}_3) \\ x_2 \oplus (\bar{x}_1 \cdot x_3) \\ x_3 \end{pmatrix} \tag{3.170}$$

$$F^{k}_{75,57,85}=\begin{pmatrix} x_1 \oplus (\bar{x}_2 \cdot x_3) \\ x_2 \oplus (x_1 \cdot \bar{x}_3) \\ x_3 \end{pmatrix} \qquad F^{d}_{75,57,85}=\begin{pmatrix} x_1 \oplus (\bar{x}_2 \cdot x_3) \\ x_2 \oplus (x_1 \cdot \bar{x}_3) \\ x_3 \end{pmatrix} \tag{3.171}$$

$$F^{k}_{75,51,147}=\begin{pmatrix} x_1 \oplus (\bar{x}_2 \cdot x_3) \\ x_2 \oplus (\bar{x}_1 \cdot \bar{x}_3) \\ x_3 \end{pmatrix} \qquad F^{d}_{75,51,147}=\begin{pmatrix} x_1 \oplus (\bar{x}_2 \cdot x_3) \\ x_2 \oplus (\bar{x}_1 \cdot \bar{x}_3) \\ x_3 \end{pmatrix} \tag{3.172}$$

$$F^{k}_{135,54,85}=\begin{pmatrix} x_1 \oplus (\bar{x}_2 \cdot \bar{x}_3) \\ x_2 \oplus (x_1 \cdot x_3) \\ x_3 \end{pmatrix} \qquad F^{d}_{135,54,85}=\begin{pmatrix} x_1 \oplus (\bar{x}_2 \cdot \bar{x}_3) \\ x_2 \oplus (x_1 \cdot x_3) \\ x_3 \end{pmatrix} \tag{3.173}$$

$$F^{k}_{135,99,85}=\begin{pmatrix} x_1 \oplus (\bar{x}_2 \cdot \bar{x}_3) \\ x_2 \oplus (\bar{x}_1 \cdot x_3) \\ x_3 \end{pmatrix} \qquad F^{d}_{135,99,85}=\begin{pmatrix} x_1 \oplus (\bar{x}_2 \cdot \bar{x}_3) \\ x_2 \oplus (\bar{x}_1 \cdot x_3) \\ x_3 \end{pmatrix} \tag{3.174}$$

$$F^{k}_{30,51,89}=\begin{pmatrix} x_1 \oplus (x_2 \cdot x_3) \\ x_2 \\ x_3 \oplus (x_1 \cdot \bar{x}_2) \end{pmatrix} \qquad F^{d}_{30,51,89}=\begin{pmatrix} x_1 \oplus (x_2 \cdot x_3) \\ x_2 \\ x_3 \oplus (x_1 \cdot \bar{x}_2) \end{pmatrix} \tag{3.175}$$

$$F^{k}_{30,51,149}=\begin{pmatrix} x_1 \oplus (x_2 \cdot x_3) \\ x_2 \\ x_3 \oplus (\bar{x}_1 \cdot \bar{x}_2) \end{pmatrix} \qquad F^{d}_{30,51,149}=\begin{pmatrix} x_1 \oplus (x_2 \cdot x_3) \\ x_2 \\ x_3 \oplus (\bar{x}_1 \cdot \bar{x}_2) \end{pmatrix} \tag{3.176}$$

$$F^{k}_{45,51,101}=\begin{pmatrix} x_1 \oplus (x_2 \cdot \bar{x}_3) \\ x_2 \\ x_3 \oplus (x_1 \cdot \bar{x}_2) \end{pmatrix} \qquad F^{d}_{45,51,101}=\begin{pmatrix} x_1 \oplus (x_2 \cdot \bar{x}_3) \\ x_2 \\ x_3 \oplus (x_1 \cdot \bar{x}_2) \end{pmatrix} \tag{3.177}$$

$$F^{k}_{45,51,149}=\begin{pmatrix} x_1 \oplus (x_2 \cdot \bar{x}_3) \\ x_2 \\ x_3 \oplus (\bar{x}_1 \cdot \bar{x}_2) \end{pmatrix} \qquad F^{d}_{45,51,149}=\begin{pmatrix} x_1 \oplus (x_2 \cdot \bar{x}_3) \\ x_2 \\ x_3 \oplus (\bar{x}_1 \cdot \bar{x}_2) \end{pmatrix} \tag{3.178}$$

$$F^{k}_{75,51,86} = \begin{pmatrix} x_1 \oplus (\bar{x}_2 \cdot x_3) \\ x_2 \\ x_3 \oplus (x_1 \cdot x_2) \end{pmatrix} \qquad F^{d}_{75,51,86} = \begin{pmatrix} x_1 \oplus (\bar{x}_2 \cdot x_3) \\ x_2 \\ x_3 \oplus (x_1 \cdot x_2) \end{pmatrix} \tag{3.179}$$

$$F^{k}_{75,51,101} = \begin{pmatrix} x_1 \oplus (\bar{x}_2 \cdot x_3) \\ x_2 \\ x_3 \oplus (\bar{x}_1 \cdot x_2) \end{pmatrix} \qquad F^{d}_{75,51,101} = \begin{pmatrix} x_1 \oplus (\bar{x}_2 \cdot x_3) \\ x_2 \\ x_3 \oplus (\bar{x}_1 \cdot x_2) \end{pmatrix} \tag{3.180}$$

$$F^{k}_{135,51,86} = \begin{pmatrix} x_1 \oplus (\bar{x}_2 \cdot \bar{x}_3) \\ x_2 \\ x_3 \oplus (x_1 \cdot x_2) \end{pmatrix} \qquad F^{d}_{135,51,86} = \begin{pmatrix} x_1 \oplus (\bar{x}_2 \cdot \bar{x}_3) \\ x_2 \\ x_3 \oplus (x_1 \cdot x_2) \end{pmatrix} \tag{3.181}$$

$$F^{k}_{135,51,101} = \begin{pmatrix} x_1 \oplus (\bar{x}_2 \cdot \bar{x}_3) \\ x_2 \\ x_3 \oplus (\bar{x}_1 \cdot x_2) \end{pmatrix} \qquad F^{d}_{135,51,101} = \begin{pmatrix} x_1 \oplus (\bar{x}_2 \cdot \bar{x}_3) \\ x_2 \\ x_3 \oplus (\bar{x}_1 \cdot x_2) \end{pmatrix} \tag{3.182}$$

$$F^{k}_{15,54,101} = \begin{pmatrix} x_1 \\ x_2 \oplus (x_1 \cdot x_3) \\ x_3 \oplus (\bar{x}_1 \cdot x_2) \end{pmatrix} \qquad F^{d}_{15,54,101} = \begin{pmatrix} x_1 \\ x_2 \oplus (x_1 \cdot x_3) \\ x_3 \oplus (\bar{x}_1 \cdot x_2) \end{pmatrix} \tag{3.183}$$

$$F^{k}_{15,54,149} = \begin{pmatrix} x_1 \\ x_2 \oplus (x_1 \cdot x_3) \\ x_3 \oplus (\bar{x}_1 \cdot \bar{x}_2) \end{pmatrix} \qquad F^{d}_{15,54,149} = \begin{pmatrix} x_1 \\ x_2 \oplus (x_1 \cdot x_3) \\ x_3 \oplus (\bar{x}_1 \cdot \bar{x}_2) \end{pmatrix} \tag{3.184}$$

$$F^{k}_{15,57,101} = \begin{pmatrix} x_1 \\ x_2 \oplus (x_1 \cdot \bar{x}_3) \\ x_3 \oplus (\bar{x}_1 \cdot x_2) \end{pmatrix} \qquad F^{d}_{15,57,101} = \begin{pmatrix} x_1 \\ x_2 \oplus (x_1 \cdot \bar{x}_3) \\ x_3 \oplus (\bar{x}_1 \cdot x_2) \end{pmatrix} \tag{3.185}$$

$$F^{k}_{15,57,149} = \begin{pmatrix} x_1 \\ x_2 \oplus (x_1 \cdot \bar{x}_3) \\ x_3 \oplus (\bar{x}_1 \cdot \bar{x}_2) \end{pmatrix} \qquad F^{d}_{15,57,149} = \begin{pmatrix} x_1 \\ x_2 \oplus (x_1 \cdot \bar{x}_3) \\ x_3 \oplus (\bar{x}_1 \cdot \bar{x}_2) \end{pmatrix} \tag{3.186}$$

$$F^{k}_{15,99,86} = \begin{pmatrix} x_1 \\ x_2 \oplus (\bar{x}_1 \cdot x_3) \\ x_3 \oplus (x_1 \cdot x_2) \end{pmatrix} \qquad F^{d}_{15,99,86} = \begin{pmatrix} x_1 \\ x_2 \oplus (\bar{x}_1 \cdot x_3) \\ x_3 \oplus (x_1 \cdot x_2) \end{pmatrix} \tag{3.187}$$

$$F^{k}_{15,99,89}=\begin{pmatrix} x_1 \\ x_2 \oplus (\bar{x}_1 \cdot x_3) \\ x_3 \oplus (x_1 \cdot \bar{x}_2) \end{pmatrix} \qquad F^{d}_{15,99,89}=\begin{pmatrix} x_1 \\ x_2 \oplus (\bar{x}_1 \cdot x_3) \\ x_3 \oplus (x_1 \cdot \bar{x}_2) \end{pmatrix} \tag{3.188}$$

$$F^{k}_{15,147,86}=\begin{pmatrix} x_1 \\ x_2 \oplus (\bar{x}_1 \cdot \bar{x}_3) \\ x_3 \oplus (x_1 \cdot x_2) \end{pmatrix} \qquad F^{d}_{15,147,86}=\begin{pmatrix} x_1 \\ x_2 \oplus (\bar{x}_1 \cdot \bar{x}_3) \\ x_3 \oplus (x_1 \cdot x_2) \end{pmatrix} \tag{3.189}$$

$$F^{k}_{15,147,89}=\begin{pmatrix} x_1 \\ x_2 \oplus (\bar{x}_1 \cdot \bar{x}_3) \\ x_3 \oplus (x_1 \cdot \bar{x}_2) \end{pmatrix} \qquad F^{d}_{15,147,89}=\begin{pmatrix} x_1 \\ x_2 \oplus (\bar{x}_1 \cdot \bar{x}_3) \\ x_3 \oplus (x_1 \cdot \bar{x}_2) \end{pmatrix} \tag{3.190}$$

Прямі та обернені трирозрядні базові операції з одним розширенням:

$$F^{k}_{30,51,85}=\begin{pmatrix} x_1 \oplus (x_2 \cdot x_3) \\ x_2 \\ x_3 \end{pmatrix} \qquad F^{d}_{30,51,85}=\begin{pmatrix} x_1 \oplus (x_2 \cdot x_3) \\ x_2 \\ x_3 \end{pmatrix} \tag{3.191}$$

$$F^{k}_{45,51,85}=\begin{pmatrix} x_1 \oplus (x_2 \cdot \bar{x}_3) \\ x_2 \\ x_3 \end{pmatrix} \qquad F^{d}_{45,51,85}=\begin{pmatrix} x_1 \oplus (x_2 \cdot \bar{x}_3) \\ x_2 \\ x_3 \end{pmatrix} \tag{3.192}$$

$$F^{k}_{75,51,85}=\begin{pmatrix} x_1 \oplus (\bar{x}_2 \cdot x_3) \\ x_2 \\ x_3 \end{pmatrix} \qquad F^{d}_{75,51,85}=\begin{pmatrix} x_1 \oplus (\bar{x}_2 \cdot x_3) \\ x_2 \\ x_3 \end{pmatrix} \tag{3.193}$$

$$F^{k}_{135,51,85}=\begin{pmatrix} x_1 \oplus (\bar{x}_2 \cdot \bar{x}_3) \\ x_2 \\ x_3 \end{pmatrix} \qquad F^{d}_{135,51,85}=\begin{pmatrix} x_1 \oplus (\bar{x}_2 \cdot \bar{x}_3) \\ x_2 \\ x_3 \end{pmatrix} \tag{3.194}$$

$$F^{k}_{15,54,85}=\begin{pmatrix} x_1 \\ x_2 \oplus (x_1 \cdot x_3) \\ x_3 \end{pmatrix} \qquad F^{d}_{15,54,85}=\begin{pmatrix} x_1 \\ x_2 \oplus (x_1 \cdot x_3) \\ x_3 \end{pmatrix} \tag{3.195}$$

$$F^{k}_{15,57,85}=\begin{pmatrix} x_1 \\ x_2 \oplus (x_1 \cdot \bar{x}_3) \\ x_3 \end{pmatrix} \qquad F^{d}_{15,57,85}=\begin{pmatrix} x_1 \\ x_2 \oplus (x_1 \cdot \bar{x}_3) \\ x_3 \end{pmatrix} \tag{3.196}$$

$$F^{k}_{15,99,85}=\begin{pmatrix} x_1 \\ x_2 \oplus (\bar{x}_1 \cdot x_3) \\ x_3 \end{pmatrix} \qquad F^{d}_{15,99,85}=\begin{pmatrix} x_1 \\ x_2 \oplus (\bar{x}_1 \cdot x_3) \\ x_3 \end{pmatrix} \tag{3.197}$$

$$F^{k}_{15,147,85}=\begin{pmatrix} x_1 \\ x_2 \oplus (\bar{x}_1 \cdot \bar{x}_3) \\ x_3 \end{pmatrix} \qquad F^{d}_{15,147,85}=\begin{pmatrix} x_1 \\ x_2 \oplus (\bar{x}_1 \cdot \bar{x}_3) \\ x_3 \end{pmatrix} \tag{3.198}$$

$$F^{k}_{15,51,86}=\begin{pmatrix} x_1 \\ x_2 \\ x_3 \oplus (x_1 \cdot x_2) \end{pmatrix} \qquad F^{d}_{15,51,86}=\begin{pmatrix} x_1 \\ x_2 \\ x_3 \oplus (x_1 \cdot x_2) \end{pmatrix} \tag{3.199}$$

$$F^{k}_{15,51,89}=\begin{pmatrix} x_1 \\ x_2 \\ x_3 \oplus (x_1 \cdot \bar{x}_2) \end{pmatrix} \qquad F^{d}_{15,51,89}=\begin{pmatrix} x_1 \\ x_2 \\ x_3 \oplus (x_1 \cdot \bar{x}_2) \end{pmatrix} \tag{3.200}$$

$$F^{k}_{15,51,101}=\begin{pmatrix} x_1 \\ x_2 \\ x_3 \oplus (\bar{x}_1 \cdot x_2) \end{pmatrix} \qquad F^{d}_{15,51,101}=\begin{pmatrix} x_1 \\ x_2 \\ x_3 \oplus (\bar{x}_1 \cdot x_2) \end{pmatrix} \tag{3.201}$$

$$F^{k}_{15,51,149}=\begin{pmatrix} x_1 \\ x_2 \\ x_3 \oplus (\bar{x}_1 \cdot \bar{x}_2) \end{pmatrix} \qquad F^{d}_{15,51,149}=\begin{pmatrix} x_1 \\ x_2 \\ x_3 \oplus (\bar{x}_1 \cdot \bar{x}_2) \end{pmatrix} \tag{3.202}$$

При розробці методу синтезу операцій оберненого криптографічного перетворення слід поєднати базові операції та операції перестановки за аналогією з методом синтезу обернених матричних операцій. Сумісне використання даних операцій дозволяє зменшити час криптоперетворення.

У результаті дослідження прямих то обернених операцій розширеного матричного криптоперетворення були отримані наступні правила:

Правило 3.3.1. Якщо у прямій операції криптоперетворення елементарна функція має в розширенні логічний добуток двох аргументів без інверсії, то і в оберненій операції криптоперетворення елементарна функція матиме в розширенні логічний добуток двох аргументів без інверсії;

Правило 3.3.2. Якщо у прямій операції криптоперетворення елементарна функція має в розширенні логічний добуток двох аргументів із інверсіями, то і в оберненій операції криптоперетворення елементарна функція матиме в розширенні логічний добуток двох аргументів з інверсіями;

Правило 3.3.3. Якщо у прямій операції криптоперетворення елементарна функція має в розширенні логічний добуток двох аргументів, один із яких із інверсією, а інший без інверсії, то і в оберненій операції криптоперетворення елементарна функція матиме в розширенні логічний добуток двох аргументів, один із яких із інверсією, а інший без інверсії.

Формалізуємо дані правила.

Нехай заданій множині f другої степені $f = a_1 \oplus (a_2 \cdot a_3)$ змінних $a_1,\ a_2,\ a_3$ існує обернена і, при чому, єдина f^{-1} того ж класу, а саме:

$$f^{-1} = A_1 \oplus (A_2 \cdot A_3),$$

при цьому, якщо:

Для правила 3.3.1 змінна $a_i \in \{a_1;\ a_2;\ a_3\}$, то $A_j \in \{a_1;\ a_2;\ a_3\}$ для $i = 1, 2, 3; \quad j = 1, 2, 3.$

Для правила 3.3.2 змінна $a_i \in \{\bar{a}_1;\ \bar{a}_2;\ \bar{a}_3\}$, то $A_j \in \{\bar{a}_1;\ \bar{a}_2;\ \bar{a}_3\}$ для $i = 1, 2, 3; \quad j = 1, 2, 3.$

Для правила 3.3.3 для $\begin{cases} a_2 \in \{\bar{a}_1;\ \bar{a}_2;\ \bar{a}_3\} \\ a_3 \in \{a_1;\ a_2;\ a_3\} \end{cases}$ і $\begin{cases} a_2 \in \{a_1;\ a_2;\ a_3\} \\ a_3 \in \{\bar{a}_1;\ \bar{a}_2;\ \bar{a}_3\}, \end{cases}$

то або $\begin{cases} A_2 \in \{\bar{a}_1;\ \bar{a}_2;\ \bar{a}_3\} \\ A_3 \in \{a_1;\ a_2;\ a_3\}, \end{cases}$ або $\begin{cases} A_2 \in \{a_1;\ a_2;\ a_3\} \\ A_3 \in \{\bar{a}_1;\ \bar{a}_2;\ \bar{a}_3\}. \end{cases}$

Правило 3.3.4. Якщо у прямій операції криптоперетворення елементарна функція не має розширення, тоді і в оберненій операції криптоперетворення відповідна елементарна функція не матиме розширення.

Формалізуємо дане правило.

Нехай заданій множині f першої степені $f = a_1$ змінних $a_1,\ a_2,\ a_3$ існує обернена і, при чому, єдина f^{-1} того ж класу, а саме: $f^{-1} = A_1$, при цьому, якщо для правила 3.3.4 змінна $a_i \in \{a_1;\ a_2;\ a_3\}$, тоді $A_i \in \{a_1;\ a_2;\ a_3\}$ для $i = 1, 2, 3$.

Перевіримо коректність використання правил 3.3.1 – 3.3.4:

$$F^{k}_{30,57,149} = \begin{bmatrix} x_1 \oplus (x_2 \cdot x_3) \\ x_2 \oplus (x_1 \cdot \bar{x}_3) \\ x_3 \oplus (\bar{x}_1 \cdot \bar{x}_2) \end{bmatrix} \quad F^{\mathrm{d}}_{30,57,149} = \begin{bmatrix} x_1 \oplus (x_2 \cdot x_3) \\ x_2 \oplus (x_1 \cdot \bar{x}_3) \\ x_3 \oplus (\bar{x}_1 \cdot \bar{x}_2) \end{bmatrix} \tag{3.203}$$

$$F^{k}_{30,149,57} = \begin{bmatrix} x_1 \oplus (x_2 \cdot x_3) \\ x_3 \oplus (\bar{x}_1 \cdot \bar{x}_2) \\ x_2 \oplus (x_1 \cdot \bar{x}_3) \end{bmatrix} \quad F^{\mathrm{d}}_{30,89,147} = \begin{bmatrix} x_1 \oplus (x_2 \cdot x_3) \\ x_3 \oplus (x_1 \cdot \bar{x}_2) \\ x_2 \oplus (\bar{x}_1 \cdot \bar{x}_3) \end{bmatrix} \tag{3.204}$$

$$F^{k}_{57,30,149} = \begin{bmatrix} x_2 \oplus (x_1 \cdot \bar{x}_3) \\ x_1 \oplus (x_2 \cdot x_3) \\ x_3 \oplus (\bar{x}_1 \cdot \bar{x}_2) \end{bmatrix} \quad F^{d}_{54,45,149} = \begin{bmatrix} x_2 \oplus (x_1 \cdot x_3) \\ x_1 \oplus (x_2 \cdot \bar{x}_3) \\ x_3 \oplus (\bar{x}_1 \cdot \bar{x}_2) \end{bmatrix} \tag{3.205}$$

$$F^{k}_{57,149,30} = \begin{bmatrix} x_2 \oplus (x_1 \cdot \bar{x}_3) \\ x_3 \oplus (\bar{x}_1 \cdot \bar{x}_2) \\ x_1 \oplus (x_2 \cdot x_3) \end{bmatrix} \quad F^{d}_{86,75,147} = \begin{bmatrix} x_3 \oplus (x_1 \cdot x_2) \\ x_1 \oplus (\bar{x}_2 \cdot x_3) \\ x_2 \oplus (\bar{x}_1 \cdot \bar{x}_3) \end{bmatrix} \tag{3.206}$$

$$F^{k}_{149,30,57} = \begin{bmatrix} x_3 \oplus (\bar{x}_1 \cdot \bar{x}_2) \\ x_1 \oplus (x_2 \cdot x_3) \\ x_2 \oplus (x_1 \cdot \bar{x}_3) \end{bmatrix} \quad F^{d}_{54,101,135} = \begin{bmatrix} x_2 \oplus (x_1 \cdot x_3) \\ x_3 \oplus (\bar{x}_1 \cdot x_2) \\ x_1 \oplus (\bar{x}_2 \cdot \bar{x}_3) \end{bmatrix} \tag{3.207}$$

$$F^{k}_{149,57,30} = \begin{bmatrix} x_3 \oplus (\bar{x}_1 \cdot \bar{x}_2) \\ x_2 \oplus (x_1 \cdot \bar{x}_3) \\ x_1 \oplus (x_2 \cdot x_3) \end{bmatrix} \quad F^{d}_{86,99,135} = \begin{bmatrix} x_3 \oplus (x_1 \cdot x_2) \\ x_2 \oplus (\bar{x}_1 \cdot x_3) \\ x_1 \oplus (\bar{x}_2 \cdot \bar{x}_3) \end{bmatrix} \tag{3.208}$$

$$F^{k}_{45,54,149}=\begin{bmatrix}x_1\oplus(x_2\cdot\bar{x}_3)\\ x_2\oplus(x_1\cdot x_3)\\ x_3\oplus(\bar{x}_1\cdot\bar{x}_2)\end{bmatrix}\quad F^{d}_{45,54,149}=\begin{bmatrix}x_1\oplus(x_2\cdot\bar{x}_3)\\ x_2\oplus(x_1\cdot x_3)\\ x_3\oplus(\bar{x}_1\cdot\bar{x}_2)\end{bmatrix}$$

$$F^{k}_{45,149,54}=\begin{bmatrix}x_1\oplus(x_2\cdot\bar{x}_3)\\ x_3\oplus(\bar{x}_1\cdot\bar{x}_2)\\ x_2\oplus(x_1\cdot x_3)\end{bmatrix}\quad F^{\mathrm{d}}_{75,86,147}=\begin{bmatrix}x_1\oplus(\bar{x}_2\cdot x_3)\\ x_3\oplus(x_1\cdot x_2)\\ x_2\oplus(\bar{x}_1\cdot\bar{x}_3)\end{bmatrix}$$

$$F^{k}_{54,45,149}=\begin{bmatrix}x_2\oplus(x_1\cdot x_3)\\ x_1\oplus(x_2\cdot\bar{x}_3)\\ x_3\oplus(\bar{x}_1\cdot\bar{x}_2)\end{bmatrix}\quad F^{d}_{57,30,149}=\begin{bmatrix}x_2\oplus(x_1\cdot\bar{x}_3)\\ x_1\oplus(x_2\cdot x_3)\\ x_3\oplus(\bar{x}_1\cdot\bar{x}_2)\end{bmatrix}$$

$$F^{k}_{54,149,45}=\begin{bmatrix}x_2\oplus(x_1\cdot x_3)\\ x_3\oplus(\bar{x}_1\cdot\bar{x}_2)\\ x_1\oplus(x_2\cdot\bar{x}_3)\end{bmatrix}\quad F^{d}_{89,30,147}=\begin{bmatrix}x_3\oplus(x_1\cdot\bar{x}_2)\\ x_1\oplus(x_2\cdot x_3)\\ x_2\oplus(\bar{x}_1\cdot\bar{x}_3)\end{bmatrix}$$

$$F^{k}_{149,45,54}=\begin{bmatrix}x_3\oplus(\bar{x}_1\cdot\bar{x}_2)\\ x_1\oplus(x_2\cdot\bar{x}_3)\\ x_2\oplus(x_1\cdot x_3)\end{bmatrix}\quad F^{d}_{99,86,135}=\begin{bmatrix}x_2\oplus(\bar{x}_1\cdot x_3)\\ x_3\oplus(x_1\cdot x_2)\\ x_1\oplus(\bar{x}_2\cdot\bar{x}_3)\end{bmatrix}$$

$$F^{k}_{149,54,45}=\begin{bmatrix}x_3\oplus(\bar{x}_1\cdot\bar{x}_2)\\ x_2\oplus(x_1\cdot x_3)\\ x_1\oplus(x_2\cdot\bar{x}_3)\end{bmatrix}\quad F^{d}_{101,54,135}=\begin{bmatrix}x_3\oplus(\bar{x}_1\cdot x_2)\\ x_2\oplus(x_1\cdot x_3)\\ x_1\oplus(\bar{x}_2\cdot\bar{x}_3)\end{bmatrix}$$

$$F^{k}_{30,57,85}=\begin{bmatrix}x_1\oplus(x_2\cdot x_3)\\ x_2\oplus(x_1\cdot\bar{x}_3)\\ x_3\end{bmatrix}\quad F^{d}_{30,57,85}=\begin{bmatrix}x_1\oplus(x_2\cdot x_3)\\ x_2\oplus(x_1\cdot\bar{x}_3)\\ x_3\end{bmatrix}\tag{3.209}$$

$$F^{k}_{30,85,57}=\begin{bmatrix}x_1\oplus(x_2\cdot x_3)\\ x_3\\ x_2\oplus(x_1\cdot\bar{x}_3)\end{bmatrix}\quad F^{k}_{30,89,51}=\begin{bmatrix}x_1\oplus(x_2\cdot x_3)\\ x_3\oplus(x_1\cdot\bar{x}_2)\\ x_2\end{bmatrix}\tag{3.210}$$

$$F^{k}_{57,30,85}=\begin{bmatrix}x_2\oplus(x_1\cdot\bar{x}_3)\\ x_1\oplus(x_2\cdot x_3)\\ x_3\end{bmatrix}\quad F^{k}_{54,45,85}=\begin{bmatrix}x_2\oplus(x_1\cdot x_3)\\ x_1\oplus(x_2\cdot\bar{x}_3)\\ x_3\end{bmatrix}\tag{3.211}$$

$$F^{k}_{57,85,30}=\begin{bmatrix} x_2 \oplus (x_1 \cdot \bar{x}_3) \\ x_3 \\ x_1 \oplus (x_2 \cdot x_3) \end{bmatrix} \quad F^{k}_{86,75,51}=\begin{bmatrix} x_3 \oplus (x_1 \cdot x_2) \\ x_1 \oplus (\bar{x}_2 \cdot x_3) \\ x_2 \end{bmatrix} \tag{3.212}$$

$$F^{k}_{85,30,57}=\begin{bmatrix} x_3 \\ x_1 \oplus (x_2 \cdot x_3) \\ x_2 \oplus (x_1 \cdot \bar{x}_3) \end{bmatrix} \quad F^{k}_{54,101,15}=\begin{bmatrix} x_2 \oplus (x_1 \cdot x_3) \\ x_3 \oplus (\bar{x}_1 \cdot x_2) \\ x_1 \end{bmatrix} \tag{3.212}$$

$$F^{k}_{85,57,30}=\begin{bmatrix} x_3 \\ x_2 \oplus (x_1 \cdot \bar{x}_3) \\ x_1 \oplus (x_2 \cdot x_3) \end{bmatrix} \quad F^{k}_{86,99,15}=\begin{bmatrix} x_3 \oplus (x_1 \cdot x_2) \\ x_2 \oplus (\bar{x}_1 \cdot x_3) \\ x_1 \end{bmatrix} \tag{3.212}$$

$$F^{k}_{30,147,85}=\begin{bmatrix} x_1 \oplus (x_2 \cdot x_3) \\ x_2 \oplus (\bar{x}_1 \cdot \bar{x}_3) \\ x_3 \end{bmatrix} \quad F^{d}_{30,147,85}=\begin{bmatrix} x_1 \oplus (x_2 \cdot x_3) \\ x_2 \oplus (\bar{x}_1 \cdot \bar{x}_3) \\ x_3 \end{bmatrix}$$

$$F^{k}_{30,85,147}=\begin{bmatrix} x_1 \oplus (x_2 \cdot x_3) \\ x_3 \\ x_2 \oplus (\bar{x}_1 \cdot \bar{x}_3) \end{bmatrix} \quad F^{k}_{30,149,51}=\begin{bmatrix} x_1 \oplus (x_2 \cdot x_3) \\ x_3 \oplus (\bar{x}_1 \cdot \bar{x}_2) \\ x_2 \end{bmatrix}$$

$$F^{k}_{147,30,85}=\begin{bmatrix} x_2 \oplus (\bar{x}_1 \cdot \bar{x}_3) \\ x_1 \oplus (x_2 \cdot x_3) \\ x_3 \end{bmatrix} \quad F^{k}_{54,135,85}=\begin{bmatrix} x_2 \oplus (x_1 \cdot x_3) \\ x_1 \oplus (\bar{x}_2 \cdot \bar{x}_3) \\ x_3 \end{bmatrix}$$

$$F^{k}_{147,85,30}=\begin{bmatrix} x_2 \oplus (\bar{x}_1 \cdot \bar{x}_3) \\ x_3 \\ x_1 \oplus (x_2 \cdot x_3) \end{bmatrix} \quad F^{k}_{86,135,51}=\begin{bmatrix} x_3 \oplus (x_1 \cdot x_2) \\ x_1 \oplus (\bar{x}_2 \cdot \bar{x}_3) \\ x_2 \end{bmatrix}$$

$$F^{k}_{85,30,147}=\begin{bmatrix} x_3 \\ x_1 \oplus (x_2 \cdot x_3) \\ x_2 \oplus (\bar{x}_1 \cdot \bar{x}_3) \end{bmatrix} \quad F^{k}_{54,149,15}=\begin{bmatrix} x_2 \oplus (x_1 \cdot x_3) \\ x_3 \oplus (\bar{x}_1 \cdot \bar{x}_2) \\ x_1 \end{bmatrix}$$

$$F^{k}_{85,147,30}=\begin{bmatrix} x_3 \\ x_2 \oplus (\bar{x}_1 \cdot \bar{x}_3) \\ x_1 \oplus (x_2 \cdot x_3) \end{bmatrix} \quad F^{k}_{86,147,15}=\begin{bmatrix} x_3 \oplus (x_1 \cdot x_2) \\ x_2 \oplus (\bar{x}_1 \cdot \bar{x}_3) \\ x_1 \end{bmatrix}$$

$$F^{k}_{30,51,85}=\begin{bmatrix} x_1 \oplus (x_2 \cdot x_3) \\ x_2 \\ x_3 \end{bmatrix} \qquad F^{d}_{30,51,85}=\begin{bmatrix} x_1 \oplus (x_2 \cdot x_3) \\ x_2 \\ x_3 \end{bmatrix} \tag{3.213}$$

$$F^{k}_{30,85,51}=\begin{bmatrix} x_1 \oplus (x_2 \cdot x_3) \\ x_3 \\ x_2 \end{bmatrix} \quad F^{d}_{30,85,51}=\begin{bmatrix} x_1 \oplus (x_2 \cdot x_3) \\ x_3 \\ x_2 \end{bmatrix} \tag{3.214}$$

$$F^{k}_{51,30,85}=\begin{bmatrix} x_2 \\ x_1 \oplus (x_2 \cdot x_3) \\ x_3 \end{bmatrix} \quad F^{d}_{54,15,85}=\begin{bmatrix} x_2 \oplus (x_1 \cdot x_3) \\ x_1 \\ x_3 \end{bmatrix} \tag{3.214}$$

$$F^{k}_{51,85,30}=\begin{bmatrix} x_2 \\ x_3 \\ x_1 \oplus (x_2 \cdot x_3) \end{bmatrix} \quad F^{d}_{86,15,51}=\begin{bmatrix} x_3 \oplus (x_1 \cdot x_2) \\ x_1 \\ x_2 \end{bmatrix} \tag{3.215}$$

$$F^{k}_{85,30,51}=\begin{bmatrix} x_3 \\ x_1 \oplus (x_2 \cdot x_3) \\ x_2 \end{bmatrix} \quad F^{d}_{54,85,15}=\begin{bmatrix} x_2 \oplus (x_1 \cdot x_3) \\ x_3 \\ x_1 \end{bmatrix} \tag{3.216}$$

$$F^{k}_{85,51,30}=\begin{bmatrix} x_3 \\ x_2 \\ x_1 \oplus (x_2 \cdot x_3) \end{bmatrix} \quad F^{d}_{86,51,15}=\begin{bmatrix} x_3 \oplus (x_1 \cdot x_2) \\ x_2 \\ x_1 \end{bmatrix} \tag{3.217}$$

$$F^{k}_{135,51,85}=\begin{bmatrix} x_1 \oplus (\bar{x}_2 \cdot \bar{x}_3) \\ x_2 \\ x_3 \end{bmatrix} \qquad F^{d}_{135,51,85}=\begin{bmatrix} x_1 \oplus (\bar{x}_2 \cdot \bar{x}_3) \\ x_2 \\ x_3 \end{bmatrix}$$

$$F^{\mathrm{k}}_{135,85,51}=\begin{bmatrix} x_1 \oplus (\bar{x}_2 \cdot \bar{x}_3) \\ x_3 \\ x_2 \end{bmatrix} \qquad F^{d}_{135,85,51}=\begin{bmatrix} x_1 \oplus (\bar{x}_2 \cdot \bar{x}_3) \\ x_3 \\ x_2 \end{bmatrix}$$

$$F^{k}_{51,135,85}=\begin{bmatrix} x_2 \\ x_1 \oplus (\bar{x}_2 \cdot \bar{x}_3) \\ x_3 \end{bmatrix} \qquad F^{d}_{147,15,85}=\begin{bmatrix} x_2 \oplus (\bar{x}_1 \cdot \bar{x}_3) \\ x_1 \\ x_3 \end{bmatrix}$$

$$F^{k}_{51,85,135}=\begin{bmatrix} x_2 \\ x_3 \\ x_1 \oplus (\bar{x}_2 \cdot \bar{x}_3) \end{bmatrix} \qquad F^{d}_{149,15,51}=\begin{bmatrix} x_3 \oplus (\bar{x}_1 \cdot \bar{x}_2) \\ x_1 \\ x_2 \end{bmatrix}$$

$$F^{k}_{85,135,51}=\begin{bmatrix} x_3 \\ x_1 \oplus (\bar{x}_2 \cdot \bar{x}_3) \\ x_2 \end{bmatrix} \qquad F^{d}_{147,85,15}=\begin{bmatrix} x_2 \oplus (\bar{x}_1 \cdot \bar{x}_3) \\ x_3 \\ x_1 \end{bmatrix}$$

$$F^{k}_{85,51,135}=\begin{bmatrix} x_3 \\ x_2 \\ x_1 \oplus (\bar{x}_2 \cdot \bar{x}_3) \end{bmatrix} \qquad F^{d}_{149,51,15}=\begin{bmatrix} x_3 \oplus (\bar{x}_1 \cdot \bar{x}_2) \\ x_2 \\ x_1 \end{bmatrix}.$$

Правила 3.3.1 – 3.3.4 виконуються на повній множині прямих і обернених трирозрядних операцій розширеного матричного криптоперетворення, що отримана на основі обчислювального експерименту.

З урахуванням правил 3.3.1 – 3.3.4 розглянемо можливість побудови операції оберненого перетворення, що проводиться шляхом побудови оберненої операції матричного перетворення та добудови матриці розширеного перетворення.

3.5.2 Алгоритмічний метод синтезу операції оберненого розширеного матричного криптографічного перетворення

Розглянемо більш детально операцію розширеного матричного криптоперетворення (3.167).

Знайти обернену матрицю для першої лінійної матриці можна, використавши метод синтезу операцій оберненого матричного криптографічного перетворення інформації (підрозділ 2.1.5).

Враховуючи, що перша лінійна матриця є матрицею перестановки, в ході дослідження встановлено, що процес пошуку оберненої матриці можливо спростити.

Якщо A_{ij} – матриця перестановки, то A_{ji}^{-1} [31, 52, 53].

$$F_{15,51,85}^{k}=\begin{pmatrix} a_{11}\cdot x_1 \\ a_{22}\cdot x_2 \\ a_{33}\cdot x_3 \end{pmatrix} \qquad F_{15,51,85}^{d}=\begin{pmatrix} a_{11}\cdot x_1 \\ a_{22}\cdot x_2 \\ a_{33}\cdot x_3 \end{pmatrix}$$

$$F_{15,85,51}^{k}=\begin{pmatrix} a_{11}\cdot x_1 \\ a_{23}\cdot x_3 \\ a_{32}\cdot x_2 \end{pmatrix} \qquad F_{15,85,51}^{d}=\begin{pmatrix} a_{11}\cdot x_1 \\ a_{23}\cdot x_3 \\ a_{32}\cdot x_2 \end{pmatrix}$$

$$F_{51,15,85}^{k}=\begin{pmatrix} a_{12}\cdot x_2 \\ a_{21}\cdot x_1 \\ a_{33}\cdot x_3 \end{pmatrix} \qquad F_{51,15,85}^{d}=\begin{pmatrix} a_{12}\cdot x_2 \\ a_{21}\cdot x_1 \\ a_{33}\cdot x_3 \end{pmatrix}$$

$$F_{51,85,15}^{k}=\begin{pmatrix} a_{12}\cdot x_2 \\ a_{23}\cdot x_3 \\ a_{31}\cdot x_1 \end{pmatrix} \qquad F_{85,15,51}^{d}=\begin{pmatrix} a_{13}\cdot x_3 \\ a_{21}\cdot x_1 \\ a_{32}\cdot x_2 \end{pmatrix}$$

$$F_{85,15,51}^{k}=\begin{pmatrix} a_{13}\cdot x_3 \\ a_{21}\cdot x_1 \\ a_{32}\cdot x_2 \end{pmatrix} \qquad F_{51,85,15}^{d}=\begin{pmatrix} a_{12}\cdot x_2 \\ a_{23}\cdot x_3 \\ a_{31}\cdot x_1 \end{pmatrix}$$

$$F_{85,51,15}^{k}=\begin{pmatrix} a_{13}\cdot x_3 \\ a_{22}\cdot x_2 \\ a_{31}\cdot x_1 \end{pmatrix} \qquad F_{85,51,15}^{d}=\begin{pmatrix} a_{13}\cdot x_3 \\ a_{22}\cdot x_2 \\ a_{31}\cdot x_1 \end{pmatrix}$$

Доведено, що для матриці перестановок компланарна матриця буде оберненою. Виходячи з цього, справедлива рівність:

$$A_{ji}^{-1}=A_{ij} \tag{3.218}$$

Формалізуємо правила 3.2.1 – 3.2.4 з урахуванням виразів (3.164) та (3.218).

Нехай заданій множині f другої степені $f = a_{ij} \oplus (a_{ii} \cdot a_{il})$ змінних $a_1,\ a_2,\ a_3$ існує обернена і, при чому, єдина f^{-1} того ж класу, а саме: $f^{-1} = A_{ji} \oplus (A_{jj} \cdot A_{jl})$, при цьому якщо:

Правило 3.4.1. Якщо змінні $a_{ij} \in \{a_1;\ a_2;\ a_3\}$, $a_{ii} \in \{a_1;\ a_2;\ a_3\}$, $a_{il} \in \{a_1;\ a_2;\ a_3\}$, то $A_{ji} \in \{a_1;\ a_2;\ a_3\}$, $A_{jj} \in \{a_1;\ a_2;\ a_3\}$, $A_{jl} \in \{a_1;\ a_2;\ a_3\}$ для $i = 1, 2, 3;\quad j = 1, 2, 3;\quad l = 1, 2, 3$.

Правило 3.4.2. Якщо змінні $a_{ij} \in \{a_1;\ a_2;\ a_3\}$, $a_{ii} \in \{\bar{a}_1;\ \bar{a}_2;\ \bar{a}_3\}$, $a_{il} \in \{\bar{a}_1;\ \bar{a}_2;\ \bar{a}_3\}$, то $A_{ji} \in \{a_1;\ a_2;\ a_3\}$, $A_{jj} \in \{a_1;\ a_2;\ a_3\}$, $A_{jl} \in \{\bar{a}_1;\ \bar{a}_2;\ \bar{a}_3\}$ для $i = 1, 2, 3;\quad j = 1, 2, 3;\quad l = 1, 2, 3$.

Правило 3.4.3. Для $\begin{cases} a_{ii} \in \{\bar{a}_1;\ \bar{a}_2;\ \bar{a}_3\} \\ a_{il} \in \{a_1;\ a_2;\ a_3\} \end{cases}$ і $\begin{cases} a_{ii} \in \{a_1;\ a_2;\ a_3\} \\ a_{il} \in \{\bar{a}_1;\ \bar{a}_2;\ \bar{a}_3\} \end{cases}$, то або

$\begin{cases} A_{jj} \in \{\bar{a}_1;\ \bar{a}_2;\ \bar{a}_3\} \\ A_{jl} \in \{a_1;\ a_2;\ a_3\} \end{cases}$, або $\begin{cases} A_{jj} \in \{a_1;\ a_2;\ a_3\} \\ A_{jl} \in \{\bar{a}_1;\ \bar{a}_2;\ \bar{a}_3\} \end{cases}$.

Нехай заданій множині f першої степені $f = a_{ij}$ змінних $a_1,\ a_2,\ a_3$ існує обернена і, при чому, єдина f^{-1} того ж класу, а саме: $f^{-1} = A_{ji}$, при цьому, якщо:

Правило 3.4.4. Якщо змінна $a_{ij} \in \{a_1;\ a_2;\ a_3\}$, то $A_{ji} \in \{a_1;\ a_2;\ a_3\}$ для $i = 1, 2, 3,\ j = 1, 2, 3$.

Коректність правил 3.4.1 – 3.4.4 перевірена на повній множині розширених матричних операцій криптоперетворення, які поєднують у собі базові операції та операції перестановки, що отримані за результатами обчислювального експерименту.

Розглянемо синтез обернених операцій розширеного матричного криптографічного перетворення за наявності у прямій операції трьох розширень.

Відповідно до правила 3.1.3 можливі два узагальнених варіанти операції прямого криптоперетворення

$$F^k\begin{pmatrix} a_i \\ a_j \\ a_l \end{pmatrix} = \begin{pmatrix} a_{pi} \oplus a_{pj} \cdot a_{pl} \\ a_{rj} \oplus a_{ri} \cdot a_{rl} \\ a_{tl} \oplus a_{ti} \cdot a_{tj} \end{pmatrix}, \qquad (3.219)$$

де $i = 1, 2, 3;$ $j = 1, 2, 3;$ $l = 1, 2, 3;$ $i \neq j \neq l;$ $p = 1, 2, 3;$ $r = 1, 2, 3;$ $t = 1, 2, 3;$ $p \neq r \neq t;$ $a_{ji} \in \{x_i, \bar{x}_i\}$:

Варіант 1. Вираз (3.219) умова 1: якщо $\begin{bmatrix} a_{pj} = \bar{x}_j, a_{pl} = x_l, \\ a_{pj} = x_j, a_{pl} = \bar{x}_l, \end{bmatrix}$ то

або $\begin{cases} a_{ri} = \bar{x}_i, \ a_{rl} = \bar{x}_l, \\ a_{ti} = x_i, a_{tl} = x_l, \end{cases}$ або $\begin{cases} a_{ri} = x_i, a_{rl} = x_l, \\ a_{ti} = \bar{x}_i, \ a_{tl} = \bar{x}_l. \end{cases}$

Варіант 2. Вираз (3.219) умова 2: якщо $\begin{bmatrix} a_{jp} = \bar{x}_j, a_{lp} = x_l, \\ a_{jp} = x_j, a_{lp} = \bar{x}_l, \end{bmatrix}$ то

$$\begin{cases} \begin{bmatrix} a_{ir} = \bar{x}_i, a_{lr} = x_l, \\ a_{ir} = x_i, a_{lr} = \bar{x}_l, \end{bmatrix} \\ \begin{bmatrix} a_{it} = \bar{x}_i, a_{lt} = x_l, \\ a_{it} = x_i, a_{jt} = \bar{x}_j. \end{bmatrix} \end{cases}$$

Побудову операції оберненого перетворення будемо проводити за умови $i < j < l; \ t < p < r$.

Розглянемо перший варіант операції криптоперетворення (умова 1).

Згідно виразу (3.218) та правил 3.4.1-3.4.4 отримаємо:

$$F^d\begin{pmatrix} A_i \\ A_j \\ A_l \end{pmatrix} = \begin{pmatrix} A_{ir} \oplus A_{it} \cdot A_{ip} \\ A_{jt} \oplus A_{jp} \cdot A_{jr} \\ A_{lp} \oplus A_{lt} \cdot A_{lr} \end{pmatrix}, \qquad (3.220)$$

де $i=1,2,3;\quad j=1,2,3;\quad l=1,2,3;\quad i\neq j\neq l;\qquad p=1,2,3;\quad r=1,2,3;$

$t=1,2,3;\quad p\neq r\neq t;\quad A_{ji}\in\{y_i,\bar{y}_i\}.$

Оскільки $\begin{cases}a_{ir}=\bar{x}_i,\ a_{lr}=\bar{x}_l,\\ a_{it}=x_i,\ a_{jt}=x_j\end{cases}$ або $\begin{cases}a_{ri}=x_i,\ a_{rl}=x_l,\\ a_{ti}=\bar{x}_i,\ a_{tl}=\bar{x}_l,\end{cases}$

то відповідно до правил 3.4.1 – 3.4.2

$$\begin{cases}A_{lt}=\bar{y}_t,\ A_{lr}=\bar{y}_r,\\ A_{lt}=y_t,\ A_{lr}=y_r\end{cases}\ \text{або}\ \begin{cases}A_{lt}=y_t,\ A_{lr}=y_r,\\ A_{lt}=\bar{y}_t,\ A_{lr}=\bar{y}_r.\end{cases}$$

Оскільки $\begin{bmatrix}a_{pj}=\bar{x}_j,\ a_{pl}=x_l,\\ a_{pj}=x_j,\ a_{pl}=\bar{x}_l,\end{bmatrix}$ то відповідно до правил 3.4.3 та 3.1.4 отримаємо:

$$\begin{cases}\begin{bmatrix}A_{jp}=y_p\\ A_{jr}=\bar{y}_r\end{bmatrix}\ якщо\ A_{ip}=\bar{y}_p;\\ \begin{bmatrix}A_{jp}=\bar{y}_p\\ A_{jr}=y_r\end{bmatrix}\ якщо\ A_{ip}=y_p;\end{cases}\ \text{або}\ \begin{cases}\begin{bmatrix}A_{jp}=y_p\\ A_{jr}=\bar{y}_r\end{bmatrix}\ якщо\ A_{ir}=y_r;\\ \begin{bmatrix}A_{jp}=\bar{y}_p\\ A_{jr}=y_r\end{bmatrix}\ якщо\ A_{ir}=\bar{y}_r.\end{cases}$$

Операцію оберненого криптоперетворення при трьох розширеннях за умови 1 побудовано.

Розглянемо другий варіант операції криптоперетворення (умова 2).

Згідно виразу (3.218) та правила 3.4.3 отримаємо (3.220).

$$\text{Оскільки } \begin{cases} \begin{bmatrix} a_{jp} = \bar{x}_j,\ a_{lp} = x_l, \\ a_{jp} = x_j,\ a_{lp} = \bar{x}_l, \end{bmatrix} \\ \begin{bmatrix} a_{ir} = \bar{x}_i,\ a_{lr} = x_l, \\ a_{ir} = x_i,\ a_{lr} = \bar{x}_l, \end{bmatrix} \\ \begin{bmatrix} a_{it} = \bar{x}_i,\ a_{lt} = x_l, \\ a_{it} = x_i,\ a_{jt} = \bar{x}_j, \end{bmatrix} \end{cases} \text{ то } \begin{cases} \begin{bmatrix} A_{it} = \bar{y}_t,\ A_{ip} = y_p, \\ A_{it} = y_t,\ A_{ip} = \bar{y}_p, \end{bmatrix} \\ \begin{bmatrix} A_{jp} = \bar{y}_p,\ A_{jr} = y_r, \\ A_{jp} = y_p,\ A_{jr} = \bar{y}_r, \end{bmatrix} \\ \begin{bmatrix} A_{lt} = \bar{y}_t,\ A_{lr} = y_r, \\ A_{lt} = y_t,\ A_{jr} = \bar{y}_r, \end{bmatrix} \end{cases} \qquad (3.221)$$

Згідно правила 3.1.4 система (3.221) має декілька рішень, що призведе до неоднозначності операції оберненого перетворення.

За відомого одного розширення може бути побудовано лише дві операції, причому одна з них відповідає умові 1, інша – умові 2.

Якщо $a_{pj} = \bar{x}_j,\ a_{pl} = x_l$, то

$$\text{або } \begin{cases} a_{ri} = \bar{x}_i,\ a_{rl} = \bar{x}_l, \\ a_{ti} = x_i,\ a_{tl} = x_l, \end{cases} \quad \text{або } \begin{cases} a_{ri} = x_i,\ a_{rl} = \bar{x}_l, \\ a_{ti} = \bar{x}_i,\ a_{tl} = x_l. \end{cases}$$

Якщо $a_{pj} = x_j,\ a_{pl} = \bar{x}_l,$ то

$$\text{або } \begin{cases} a_{ri} = x_i,\ a_{rl} = x_l, \\ a_{ti} = \bar{x}_i,\ a_{tl} = \bar{x}_l, \end{cases} \quad \text{або } \begin{cases} a_{ri} = \bar{x}_i,\ a_{rl} = x_l, \\ a_{ti} = x_i,\ a_{tl} = \bar{x}_l. \end{cases}$$

Виходячи з цього, можна, змінивши два розширення, перейти від операції перетворення за умовою 2 до операції перетворення за умовою 1.

Тоді вираз (3.219) буде представлено:

$$F^k\begin{pmatrix} a_i \\ a_j \\ a_l \end{pmatrix} = \begin{pmatrix} a_{pi} \oplus a_{pj} \cdot a_{pl} \\ a^*_{rj} \oplus a_{ri} \cdot a_{rl} \\ a^*_{tl} \oplus a_{ti} \cdot a_{tj} \end{pmatrix},$$

де a^* – елементарна функція операції прямого перетворення, яка була модифікована.

Побудувавши операцію оберненого криптоперетворення при трьох розширеннях при умові 1, отримаємо:

$$F^d\begin{pmatrix} A_i \\ A_j \\ A_l \end{pmatrix} = \begin{pmatrix} A^*_{ir} \oplus A_{it} \cdot A_{ip} \\ A_{jt} \oplus A_{jp} \cdot A_{jr} \\ A^*_{lp} \oplus A_{lt} \cdot A_{lr} \end{pmatrix}, \qquad (3.222)$$

де A^* – елементарна функція операції оберненого перетворення, яку необхідно модифікувати.

Змінимо обернену операцію з умови 1 на умову 2, модифікувавши позначені елементарні функції:

Оскільки $\begin{bmatrix} A_{jp} = \bar{y}_p, A_{jr} = y_r, \\ A_{jp} = y_p, A_{jr} = \bar{y}_r, \end{bmatrix}$ то відповідно до правила 3.1.4 отримаємо:

$$\begin{cases} \begin{bmatrix} A_{ip} = y_p;\ A_{it} = \bar{y}_t;\ якщо\ A_{jp} = \bar{y}_p \\ A_{ip} = \bar{y}_p;\ A_{it} = y_t;\ якщо\ A_{jp} = y_p \end{bmatrix} \\ \begin{bmatrix} A_{lt} = y_t;\ A_{lr} = \bar{y}_r;\ якщо\ A_{jr} = y_p \\ A_{lt} = \bar{y}_t;\ A_{lr} = y_r;\ якщо\ A_{jr} = \bar{y}_r \end{bmatrix} \end{cases}.$$

Операцію оберненого криптоперетворення при трьох розширеннях за умови 2 побудовано.

При відомих двох розширеннях у прямій операції криптоперетворення може бути добудовано третє розширення відповідно до правила 3.1.4, що призводить до пошуку оберненої операції з трьома розширеннями з наступним видаленням відповідного добудованого розширення.

Нехай операція криптоперетворення не має другого розширення та відповідає умові 2.

Виходячи з цього, можна, змінивши два розширення, перейти від операції перетворення за умовою 2 до операції за умовою 1:

$$F^k\begin{pmatrix} a_i \\ a_j \\ a_l \end{pmatrix} = \begin{pmatrix} a_{pi} \oplus a_{pj} \cdot a_{pl} \\ a_{rj} \\ a_{tl} \oplus a_{ti} \cdot a_{tj} \end{pmatrix}.$$

Відповідно до правила 3.1.4 отримаємо:

$$F^k\begin{pmatrix} a_i \\ a_j \\ a_l \end{pmatrix} = \begin{pmatrix} a_{pi} \oplus a_{pj} \cdot a_{pl} \\ a_{rj}^{\#} \oplus a_{ri} \cdot a_{rl} \\ a_{tl} \oplus a_{ti} \cdot a_{tj} \end{pmatrix},$$

де $a^{\#}$ – елементарна функція операції прямого перетворення, яка була доповнена розширенням.

Перейдемо від операції перетворення за умовою 2 до операції перетворення за умовою 1.

Тоді вираз (3.219) буде представлено:

$$F^k\begin{pmatrix} a_i \\ a_j \\ a_l \end{pmatrix} = \begin{pmatrix} a_{pi} \oplus a_{pj} \cdot a_{pl} \\ a_{rj}^{\#*} \oplus a_{ri} \cdot a_{rl} \\ a_{tl}^{*} \oplus a_{ti} \cdot a_{tj} \end{pmatrix},$$

де $a^{\#*}$ – елементарна функція операції прямого перетворення, яка була доповнена розширенням та модифікована.

Побудувавши операцію оберненого криптоперетворення при трьох розширеннях при умові 1, отримаємо:

$$F^d\begin{pmatrix} A_i \\ A_j \\ A_l \end{pmatrix} = \begin{pmatrix} A_{ir}^{*} \oplus A_{it} \cdot A_{ip} \\ A_{jt} \oplus A_{jp} \cdot A_{jr} \\ A_{lp}^{\#*} \oplus A_{lt} \cdot A_{lr} \end{pmatrix}, \qquad (3.222)$$

де A^* – елементарна функція операції оберненого перетворення, в якій необхідно після модифікації видалити розширення.

Аналогічно будується обернена операція криптоперетворення за умови відсутності двох розширень.

Слід відмітити, що процес побудови оберненої операції за відсутності одного чи двох розширень може бути спрощений за наявності лише розширень, що відповідають правилам побудови 3.4.1 та 3.4.2.

Отримані результати сформували теоретичну базу, а наведені правила забезпечили практичну основу реалізації алгоритмічного методу синтезу операції оберненого розширеного матричного криптографічного перетворення.

Основною перевагою алгоритмічного методу синтезу операції оберненого розширеного матричного криптографічного перетворення є проста реалізація на програмно-апаратному рівні. Недоліком є обмеженість розрядності криптоперетворення.

3.5.3 Розробка методу синтезу операції оберненого розширеного матричного криптографічного перетворення на основі індексації рядків

Подолати даний недолік можливо на основі введення індексів рядків. Розглянемо даний підхід для розробки методу синтезу операції оберненого розширеного матричного криптографічного перетворення на основі індексації рядків.

Індекс рядка – це індекс доданка лінійної матриці перетворення. Доведено, що послідовність індексів розширення утворює зростаючу послідовність.

Правило синтезу розширення наступне: для того, щоб утворити розширення одного з рядків матриці, яка позначає операцію розширеного матричного перетворення, за допомогою двох інших, потрібно виконати логічне множення цих рядків, інвертуючи при цьому ті рядки, індекси яких збігаються з індексами інвертованих змінних.

Метод синтезу операції оберненого розширеного матричного криптографічного перетворення на основі індексації рядків полягає в наступному.

Для того, щоб побудувати для операції розширеного матричного криптографічного перетворення з двома доповненнями (розширеннями) операцію оберненого перетворення, потрібно:

1. Побудувати лінійну операцію оберненого перетворення у матричному представленні;

2. Побудувати відповідні два доповнення, враховуючи, що прямі доповнення переходять у прямі, інверсні у інверсні, а у змішаних доповненнях порядок інвертування зберігається, якщо послідовність індексів доповнення співпадає з послідовністю індексів відповідних рядків матричної моделі для операції перетворення, і змінюється в протилежному випадку.

Доведення коректності застосування методу. Розглянемо одну з можливих операцій перетворення. Для інших доведення аналогічне.

Нехай дана матриця, яка описує операцію розширеного перетворення $\overline{F}_k = \begin{pmatrix} x_i \oplus x_j \overline{x}_l \\ x_j \\ x_l \end{pmatrix}$. Кожний рядок матриці $\overline{F}_k$ є операндом-розрядом інформації, який одержаний в результаті застосування основної елементарної функції перетворення, тобто $y_i = F_k(x_i)$.

Позначимо рядки матриці $\overline{F}_k$ змінними $y_1, y_{2,} y_3$ відповідно:

$$\overline{F}_k = \begin{pmatrix} x_i \oplus x_j \overline{x}_l \\ x_j \\ x_l \end{pmatrix} \begin{matrix} \to y_1 \\ \to y_2 \\ \to y_3 \end{matrix}.$$

Насамперед будується матриця для лінійної операції оберненого перетворення. Вона визначає порядок розміщення змінних y_i, $i \in [1,2,3]$ у шуканій операції оберненого перетворення. Потім будуються відповідні розширення таким чином, щоб у результаті перетворення рядків матриці $\overline{F}_k$ відповідно вказаним перетворенням у матриці $\overline{F}_d$, утворилась діагональна матриця, складена із змінних x_i, x_j, x_l.

Для того, щоб одержати змінну x_i, потрібно за допомогою рядків з j-м та l-м індексами утворити вираз розширення $x_j \overline{x}_l$ та виконати додавання за модулем 2 з рядком i-го індексу. Тоді одержимо: $x_i \oplus x_j \overline{x}_l \oplus x_j \overline{x}_l = x_i$.

Використовуючи змінні $y_1, y_{2,} y_3$, утворення змінної x_i матиме вигляд: $y_1 + y_2 \overline{y}_3$.

Якщо ж у матриці, яка описує операцію перетворення, послідовність індексів розширення не буде збігатися з послідовністю індексів відповідних рядків, тобто послідовність індексів відповідних рядків утворює спадну

послідовність, то порядок інвертування зміниться, що обумовлено встановленим порядком розташування змінних в розширенні.

Для випадку з одним розширенням коректність застосування даного методу доведена.

Доведення коректності методу для двох розширень наведена в роботі [14], а для трьох розширень – в роботі [53].

Основною перевагою розробленого методу є можливість синтезу обернених операцій розширеного матричного криптографічного перетворення будь-якої розрядності [53, 54].

У загальному вигляді операції криптографічного прямого перетворення, побудовані на основі елементарних функцій розширеного матричного криптографічного перетворення будуть описані наступною моделлю [31]:

$$\overline{F}_k = \begin{pmatrix} x_i \oplus a_i \hat{x}_j \hat{x}_k \ldots \hat{x}_l \hat{x}_m \oplus c_i \\ x_j \oplus a_j \hat{x}_i \hat{x}_k \ldots \hat{x}_l \hat{x}_m \oplus c_j \\ x_k \oplus a_k \hat{x}_i \hat{x}_j \ldots \hat{x}_l \hat{x}_m \oplus c_k \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ x_l \oplus a_l \hat{x}_i \hat{x}_j \hat{x}_k \ldots \hat{x}_m \oplus c_l \\ x_m \oplus a_m \hat{x}_i \hat{x}_j \hat{x}_k \ldots \hat{x}_l \oplus c_m \end{pmatrix} \quad (3.223)$$

де $i, j, k, l, m \in [1,\ldots,n]$ $n \in N$, $i \neq j \neq k \neq l \neq m$, $a_t, x_t, c_t \in [0,1]$, $t \in \{i, j, k, l, m\}$;

x_t – операнди-розряди інформації;

$\hat{x}_t$ – операнди-розряди інформації, які можуть входити у доповнення у прямому та інверсному вигляді;

a_t – коефіцієнти доповнень елементарних функцій, які визначають кількість замін елементарних функцій на функції розширеного матричного криптографічного перетворення;

c_t – ознака наявності групи операцій інверсії.

Якщо операція розширеного матричного криптографічного прямого перетворення без урахування групи операцій інверсії задана виразом:

$$\overline{F}_k = \begin{pmatrix} x_i \oplus a_i \hat{x}_j \hat{x}_k \ldots \hat{x}_l \hat{x}_m \\ x_j \oplus a_j \hat{x}_i \hat{x}_k \ldots \hat{x}_l \hat{x}_m \\ x_k \oplus a_k \hat{x}_i \hat{x}_j \ldots \hat{x}_l \hat{x}_m \\ \ldots\ldots\ldots\ldots\ldots\ldots \\ x_l \oplus a_l \hat{x}_i \hat{x}_j \hat{x}_k \ldots \hat{x}_m \\ x_m \oplus a_m \hat{x}_i \hat{x}_j \hat{x}_k \ldots \hat{x}_l \end{pmatrix}, \qquad (3.224)$$

тоді операція розширеного матричного криптографічного оберненого перетворення буде задана виразом:

$$\overline{F}_d = \begin{pmatrix} y_p \oplus b_p \hat{y}_q y_r \ldots \hat{y}_s \hat{y}_t \\ y_q \oplus b_q \hat{y}_p \hat{y}_r \ldots \hat{y}_s \hat{y}_t \\ y_r \oplus b_r \hat{y}_p \hat{y}_q \ldots \hat{y}_s \hat{y}_t \\ \ldots\ldots\ldots\ldots\ldots\ldots \\ y_s \oplus b_s \hat{y}_p \hat{y}_q \hat{y}_r \ldots \hat{y}_t \\ y_t \oplus b_t \hat{y}_p \hat{y}_q \hat{y}_r \ldots \hat{y}_s \end{pmatrix}, \qquad (3.225)$$

де $p,q,r,s,t \in [1,\ldots,n]$, $n \in N$, $p \neq q \neq r \neq s \neq t$, $b_j, y_j \in [0,1]$, $j \in \{p,q,r,s,t\}$;

y_j – операнди-розряди інформації, які отримані в результаті застосування операції прямого перетворення відповідно.

b_j – коефіцієнти доповнень елементарних функцій операції оберненого перетворення.

Алгоритм реалізації методу синтезу обернених операцій на основі методу індексації рядків розглянемо на прикладі [31].

Нехай операція розширеного матричного криптографічного прямого перетворення задана матрицею:

$$\overline{F}_k = \begin{pmatrix} x_2 \oplus x_1\overline{x}_3x_4\overline{x}_5 \\ x_5 \\ x_1 \oplus \overline{x}_2\overline{x}_3\overline{x}_4x_5 \\ x_3 \\ x_4 \oplus \overline{x}_1\overline{x}_2x_3x_5 \end{pmatrix} \tag{3.226}$$

Побудуємо для неї операцію розширеного матричного криптографічного оберненого перетворення.

Позначимо рядки матриці (3.226) змінними y_1, y_2, y_3, y_4, y_5 відповідно:

$$\overline{F}_k = \begin{pmatrix} x_2 \oplus x_1\overline{x}_3x_4\overline{x}_5 \to y_1 \\ x_5 \to y_2 \\ x_1 \oplus \overline{x}_2\overline{x}_3\overline{x}_4x_5 \to y_3 \\ x_3 \to y_4 \\ x_4 \oplus \overline{x}_1\overline{x}_2x_3x_5 \to y_5 \end{pmatrix} \tag{3.227}$$

1. Побудуємо лінійну матрицю оберненого перетворення для матриці

$$\overline{F}_k^{lin} = \begin{pmatrix} x_2 \\ x_5 \\ x_1 \\ x_3 \\ x_4 \end{pmatrix}.$$

Вона матиме вигляд:

$$\overline{F}_d^{lin} = \begin{pmatrix} y_3 \\ y_1 \\ y_4 \\ y_5 \\ y_2 \end{pmatrix}.$$

2. При побудові нелінійної матриці доповнень, потрібно врахувати, що елементарні функції y_2 та y_4 не матимуть доповнень, оскільки відповідні їм елементарні функції x_5 та x_3 не є функціями розширеного матричного криптографічного перетворення. Побудувавши відповідні доповнення, операція оберненого перетворення без врахування знаків інверсії матиме вигляд:

$$\overline{F}_d = \begin{pmatrix} y_3 \\ y_1 \\ y_4 \\ y_5 \\ y_2 \end{pmatrix} \oplus \begin{pmatrix} \widehat{y}_1\widehat{y}_2\widehat{y}_4\widehat{y}_5 \\ \widehat{y}_2\widehat{y}_3\widehat{y}_4\widehat{y}_5 \\ \\ \widehat{y}_1\widehat{y}_2\widehat{y}_3\widehat{y}_4 \\ \\ \end{pmatrix}.$$

3. Розстановку знаків інверсії у нелінійній матриці доповнень операції оберненого перетворення проводимо наступним чином:

- Розстановка знаків інверсії доповнення 1-го рядка: вибираємо елементарну функцію операції прямого перетворення, синтезовану на основі x_1. Її доповнення $\overline{x}_2\overline{x}_3\overline{x}_4x_5$ містить три інвертовані змінні, яким відповідають перший, четвертий і п’ятий рядки операції прямого перетворення, тому змінні y_1, y_4, y_5 будуть інвертованими у доповненні елементарної функції першого рядка нелінійної матриці доповнень операції оберненого перетворення.
- Розстановка знаків інверсії доповнення 2-го рядка: вибираємо елементарну функцію операції прямого перетворення, синтезовану на основі x_2. Її доповнення $x_1\overline{x}_3x_4\overline{x}_5$ містить дві інвертовані змінні – x_3 та x_5, яким відповідають четвертий та другий рядки операції прямого перетворення, тому змінні y_2 та y_4 будуть інвертованими у доповненні елементарної функції другого рядка нелінійної матриці доповнень операції оберненого перетворення.

– Розстановка знаків інверсії доповнення 4-го рядка: вибираємо елементарну функцію операції прямого перетворення, синтезовану на основі x_4. Її доповнення $\bar{x}_1\bar{x}_2x_3x_5$ містить дві інвертовані змінні, яким відповідають третій та перший рядки операції прямого перетворення, тому змінні y_1 та y_3 будуть інвертованими у доповненні елементарної функції четвертого рядка нелінійної матриці доповнень операції оберненого перетворення.

Таким чином, отримана операція розширеного матричного криптографічного оберненого перетворення матиме вигляд:

$$\overline{F}_d = \begin{pmatrix} y_3 \\ y_1 \\ y_4 \\ y_5 \\ y_2 \end{pmatrix} \oplus \begin{pmatrix} \bar{y}_1y_2\bar{y}_4\bar{y}_5 \\ \bar{y}_2y_3\bar{y}_4y_5 \\ \\ \bar{y}_1y_2\bar{y}_3y_4 \\ \\ \end{pmatrix} = \begin{pmatrix} y_3 \oplus \bar{y}_1y_2\bar{y}_4\bar{y}_5 \\ y_1 \oplus \bar{y}_2y_3\bar{y}_4y_5 \\ y_4 \\ y_5 \oplus \bar{y}_1y_2\bar{y}_3y_4 \\ y_2 \end{pmatrix}.$$

Наведені приклади знаходження математичної моделі оберненої операції криптографічного перетворення підтверджують можливість застосування розробленого методу синтезу нелінійних операцій розширеного матричного криптографічного перетворення для будь-якої кількості змінних [31, 53].

Даний метод забезпечує синтез обернених операцій розширеного матричного криптографічного перетворення і може знайти своє практичне застосування при розробці програмно-апаратних засобів.

Одержані в розділі результати підтверджують коректність методології дослідження та синтезу логічних функцій та операцій для криптографічного перетворення інформації, а також доцільність її застосування при розробці нових методів синтезу операцій, що можуть бути використані для побудови алгоритмів комп'ютерної криптографії.

3.6 Висновки до третього розділу

Вперше, на прикладі вибраної із класифікації групи елементарних функцій розширеного матричного криптоперетворення, у рамках розробленої методології побудовано комплекс математичних моделей та методів синтезу елементарних функцій та операцій криптоперетварення, які в сукупності забезпечили можливість вдосконалення систем комп'ютерної криптографії та підтвердили коректність основних положень методології.

1. Вперше розроблено класифікацію трирозрядних елементарних функцій на основі складності дискретних моделей та функціональних особливостей елементарних функцій, що дало змогу визначити напрями дослідження для практичної реалізації методології синтезу операцій криптографічного перетворення інформації.

2. Удосконалено та формалізовано методи синтезу елементарних функцій розширеного матричного перетворення, на основі поліноміального та дискретно-алгебраїчного подання, що дало змогу будувати елементарні функції з розширеною кількість аргументів, виходячи з практичних задач. Отримано залежності розрахунку потужності множин елементарних функцій розширеного матричного перетворення в залежності від кількості розрядів інформації, яка перетворюється.

3. Удосконалено існуючі та розроблено нові методи синтезу операцій розширеного матричного криптоперетворення на основі запропонованої моделі базової операції, що забезпечило можливість розробки нових та вдосконалення існуючих алгоритмів криптографічного шифрування інформації.

4. Вперше побудовано математичну модель операцій розширеного матричного криптографічного перетворення, що забезпечило формалізацію правил синтезу операцій прямого та оберненого криптоперетворення.

5. Удосконалено існуючі та розроблено нові методи синтезу обернених операцій розширеного матричного криптографічного перетворення на основі формалізованих правил побудови операцій розширеного матричного

криптографічного перетворення, що забезпечило можливість використання даних операцій для комп'ютерної криптографії.

Матеріали розділу опубліковані [13, 16, 17, 22, 23, 30, 31, 50, 53].

РОЗДІЛ 4
РЕАЛІЗАЦІЯ КРИПТОПРИМІТИВІВ МАТРИЧНИМИ ОПЕРАЦІЯМИ КРИПТОГРАФІЧНОГО ПЕРЕТВОРЕННЯ

4.1 Дослідження матричних операцій криптографічного перетворення на основі арифметичних операцій за модулем

Оскільки комп’ютерна злочинність стала невід’ємною частиною сучасного суспільства, значно підвищились вимоги до захисту інформації як підприємств та установ, так і персональної інформації користувачів глобальної мережі. Одним із ефективних засобів боротьби з несанкціонованим доступом до інформації, її модифікацією, є використання криптографічних засобів захисту.

У зв’язку із значним ростом обсягів інформації та кількості користувачів гостро постають питання не лише підвищення швидкодії комп’ютерних систем та мереж, а й підвищення швидкості та стійкості криптоалгоритмів, зокрема алгоритмів комп'ютерної криптографії.

Останні роки характеризуються вдосконаленням існуючих та розробкою нових криптоалгоритмів, примітиви яких базуються на використанні арифметичних операцій за різними модулями [177, 178].

Проте дослідженням щодо ефективного вибору основи модуля або поєднанню операцій з різними модулями не приділялась достатня увага.

Головною задачею є провести дослідження матричних операцій криптографічного перетворення на основі арифметичних операцій за модулем та розробити рекомендації щодо вибору основи модуля при розробці криптоалгоритмів.

Арифметичні операції за модулем широко застосовуються в сучасних симетричних блокових шифрах. Головним недоліком таких криптоалгоритмів є використання фіксованого відомого значення модуля, що зумовлює зниження криптографічної стійкості алгоритму. Одним із варіантів рішення даної задачі в

[179] запропоновано використання набору значень модулів, які формуються на основі секретного ключа. При чому значення модуля може змінюватися залежно від значення блоку даних та обиратися з визначеного діапазону.

На рис. 4.1 наведена процедура зашифрування блоку тексту P, яка описується виразом [179]:

$$C_j = \begin{cases} \left[\left(\left[C_{j-1} \oplus A_j^{(1)}\right] \cdot A'_j\right) \bmod m'_j + A_j^{(2)}\right] \bmod 2^n, \ якщо\ C_{j-1} < m'_j; \\ \left[\left(\left(\left[C_{j-1} \oplus A_j^{(1)}\right] - m'_j\right) \cdot A''_j\right) \bmod m''_j + m'_j + A_j^{(2)}\right] \bmod 2^n, \ якщо\ C_{j-1} \geq m'_j, \end{cases} \quad (4.1)$$

де C_j - значення блоку зашифрованого тексту після j-го раунду перетворення,

$j = \overline{1;L}$, $C_0 = P$, $C = C_L$;

$A_j^{(1)}$, $A_j^{(2)}$, A'_j, A''_j – цілі додатні числа, які використовуються на j-му раунді;

m'_j, m''_j – модулі, які використовуються на j-му раунді перетворення.

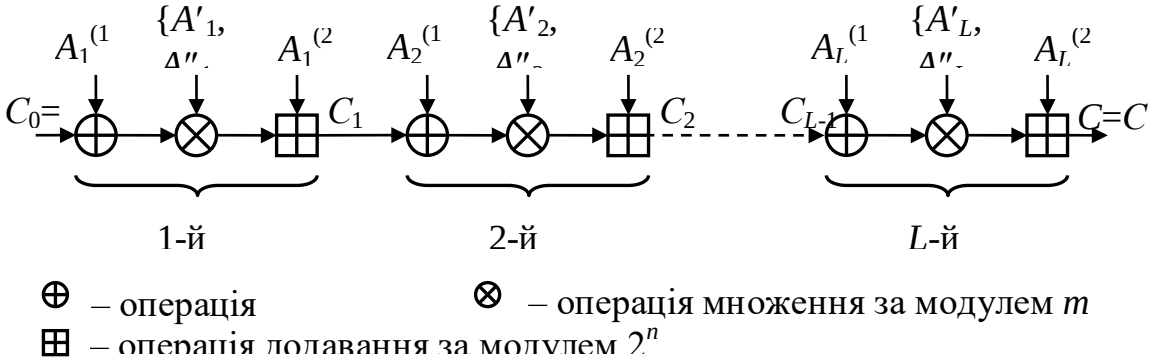


Рис. 4.1 .Схема зашифрування блоку відкритого тексту

Блок відкритого тексту P зашифровується на блоковому ключі BK, який розгортається в L раундових ключів зашифрування [179]:

$$RK_j = A_j^{(1)} \,||\, A_j^{(2)} \,||\, A'_j \,||\, A''_j \,||\, m'_j \,||\, m''_j . \quad (4.2)$$

Крім цього арифметичні та логічні операції за модулем складають основу примітивів ковзного кодування [178].

Вказані примітиви будуються на основі арифметичних, логічних або змішаних операцій перетворення елементів тексту, що шифрується. При чому елемент – це сукупність n-бітних комбінацій.

Структурна схема чотирьохелементного прямого лівостороннього арифметичного ковзного кодування (АКК) наведена на рис. 4.2, $\boxed{+}$ – оператор арифметичного додавання за $\bmod 2^{32}$; R' – 32-бітний вхідний раундовий ключ; R'' – 32-бітний вихідний раундовий ключ, що використовується в якості вхідного для наступного блока, що перетворюється [178].

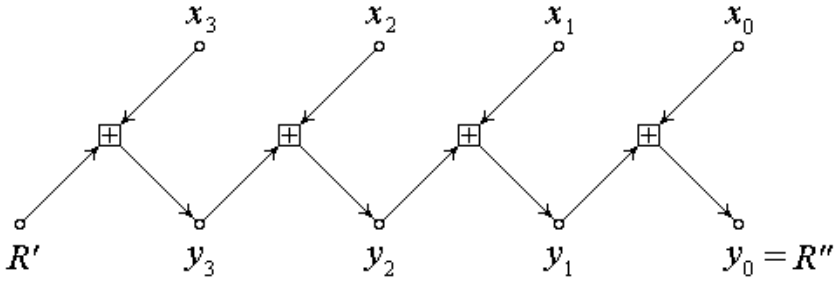


Рис. 4.2. Структурна схема алгоритму
формування прямого лівостороннього АКК

Алгоритму прямого лівостороннього АКК відповідає система лінійних модульних алгебраїчних рівнянь [178]:

$$\begin{aligned} y_3 &= (x_3 + R') \bmod m; \\ y_2 &= (x_2 + y_3) \bmod m; \\ y_1 &= (x_1 + y_2) \bmod m; \\ y_0 &= (x_0 + y_1) \bmod m, \end{aligned} \tag{4.3}$$

де $m = \bmod 2^{32}$.

Якщо замінити оператор арифметичного додавання за модулем $m = \bmod 2^{32}$ на оператор порозрядного додавання за $\bmod 2$, то отримаємо структурну схему прямого логічного ковзного кодування (ЛКК) (рис. 4.3), яка описується такою системою:

$$
\begin{aligned}
y_3 &= x_3 \oplus R';\\
y_2 &= x_2 \oplus y_3;\\
y_1 &= x_1 \oplus y_2;\\
y_0 &= x_0 \oplus y_1,
\end{aligned}
\qquad (4.4)
$$

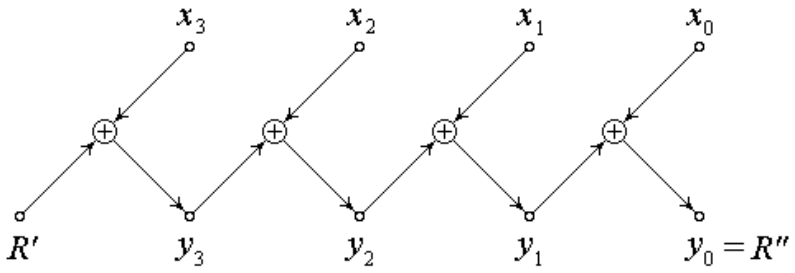


Рис. 4.3. Структурна схема алгоритму
формування прямого лівостороннього ЛКК

Для зашифрування даних примітивами ковзного шифрування використовують схему змішаного ковзного кодування (ЗКК), де спочатку виконується ЛКК, а потім АКК (рис.4.4) [178].

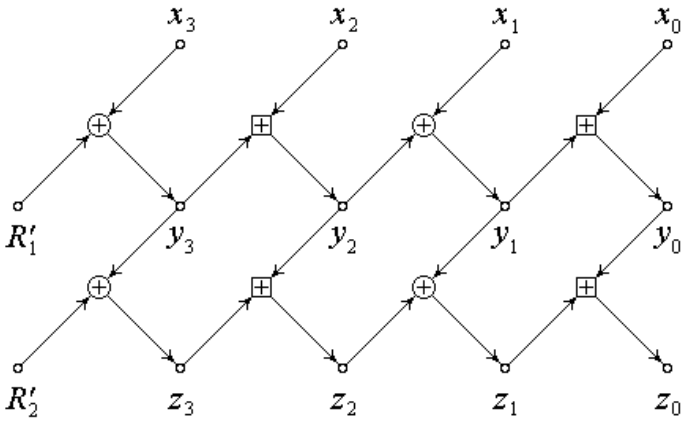


Рис. 4.4. Структурна схема алгоритму
ЗКК на першому раунді зашифрування

Як бачимо для ефективного шифрування даних використовується комбінація операцій за модулем.

Як видно із проаналізованих схем шифрування доцільніше використовувати комбінацію операцій на основі різного модуля.

4.2 Паралельна реалізація криптопримітива ковзного шифрування

У сучасних умовах розвитку інформаційних технологій велика значущість і недостатнє як теоретичне, так і практичне вирішення завдання підвищення швидкодії криптографічного перетворення даних в системах обробки і передачі інформації визначає безперечну важливість проведення досліджень, які можуть бути основою для створення швидкісних криптографічних методів.

Таким чином, розробка та реалізація швидкодіючих програмно-апаратних засобів захисту інформації на основі криптографічних алгоритмів безпосередньо пов'язана зі швидкістю виконання арифметичних і логічних операцій , що лежать в основі алгоритмів. Одним з перспективних напрямків вирішення завдання збільшення швидкості реалізації таких операцій є паралельне виконання криптографічних перетворень над великою кількістю інформації.

Останнім часом багато публікацій присвячено матричним операціям криптографічного перетворення, які дозволяють виконувати шифрування даних паралельно [14, 16, 20, 52].

В алгоритмах "Симетричний блоковий алгоритм криптографічного перетворення інформації з динамічно-керованими параметрами шифрування" і "Блочний симетричний алгоритм криптографічного перетворення інформації з динамічно керованим процесом стохастичною заміни криптографічних примітивів" представлених на відкритий конкурс симетричних блокових криптографічних алгоритмів [180], вперше були використані примітиви ковзного шифрування [178, 181]. Основним недоліком даних примітивів є їх послідовна реалізація. Тому подальші дослідження будуть направлені на розробку моделей паралельної реалізації примітивів ковного шифрування [2].

Процес реалізації примітиву логічного ковного шифрування (ЛСК) може бути представлений структурною схемою алгоритму формування рис. 4.3 [178, 181]. Схемі перетворення, наведеній на рис. 4.3, відповідає система лінійних модульних рівнянь (4.4).

Проведемо дослідження можливості паралельної реалізації примітиву ЛСК (рис. 4.3) без урахування раундового ключа R'. Паралельна реалізація можлива на основі використання матричних операцій криптографічного перетворення [14, 16, 20, 52].

Розглянемо матричну модель операції спрощеного ковзного шифрування.

Спрощене ковзне шифрування перетворює послідовність x_k у y_k, тоді

$$\begin{aligned}
&y_1 = x_1;\\
&y_2 = x_1 \oplus x_2;\\
&y_3 = x_1 \oplus x_2 \oplus x_3;\\
&y_4 = x_1 \oplus x_2 \oplus x_3 \oplus x_4;\\
&y_5 = x_1 \oplus x_2 \oplus x_3 \oplus x_4 \oplus x_5;\\
&\quad . \ . \ . \ . \ . \ . \ . \ . \ . \ .\\
&y_n = x_1 \oplus x_2 \oplus x_3 \oplus \ldots\ldots \oplus x_n.
\end{aligned} \tag{4.7}$$

Функція перетворення одного елемента ковзного шифрування може бути описана моделлю, яка представляється рекуррентною послідовністю

$$y_n = y_{n-1}. \oplus x_n\,. \tag{4.8}$$

Дана модель дозволяє отримати матричну операцію криптографічного перетворення для паралельної реалізації примітиву [2].

Повторне спрощене ковзне шифрування перетворює послідовність y_k у z_k:

$$\begin{aligned}
&z_1 = y_1;\\
&z_2 = y_1 \oplus y_2;\\
&z_3 = y_1 \oplus y_2 \oplus y_3;\\
&z_4 = y_1 \oplus y_2 \oplus y_3 \oplus y_4;\\
&z_5 = y_1 \oplus y_2 \oplus y_3 \oplus y_4 \oplus y_5;\\
&\quad . \ . \ . \ . \ . \ . \ . \ . \ . \ .\\
&z_n = y_1 \oplus y_2 \oplus y_3 \oplus \ldots\ldots \oplus y_n.
\end{aligned} \tag{4.9}$$

Підставивши у вираз (4.9) вираз (4.7), отримаємо [2]:

$$
\begin{aligned}
&z_1 = x_1;\\
&z_2 = x_1 \oplus (x_1 \oplus x_2);\\
&z_3 = x_1 \oplus (x_1 \oplus x_2) \oplus (x_1 \oplus x_2 \oplus x_3);\\
&z_4 = x_1 \oplus (x_1 \oplus x_2) \oplus (x_1 \oplus x_2 \oplus x_3) \oplus (x_1 \oplus x_2 \oplus x_3 \oplus x_4);\\
&\quad . \ . \ . \ . \ . \ . \ . \ . \ . \ .\\
&z_n = x_1 \oplus (x_1 \oplus x_2) \oplus (x_1 \oplus x_2 \oplus x_3) \oplus \ldots\ldots \oplus (x_1 \oplus x_2 \oplus \ldots\ldots \oplus x_n).
\end{aligned}
$$

Перетворивши, отримаємо:

$$
\begin{aligned}
&z_1 = x_1;\\
&z_2 = x_2;\\
&z_3 = x_1 \oplus x_3;\\
&z_4 = x_2 \oplus x_4;\\
&z_5 = x_1 \oplus x_3 \oplus x_5;\\
&z_6 = x_2 \oplus x_4 \oplus x_6;\\
&\quad . \ . \ . \ . \ . \ . \ . \ . \ . \ .\\
&z_{2k-1} = x_1 \oplus x_3 \oplus x_5 \oplus \ldots\ldots \oplus x_{2k-1};\\
&z_{2k} = x_2 \oplus x_4 \oplus x_6 \oplus x_8 \oplus \ldots\ldots \oplus x_{2k}.
\end{aligned}
\qquad (4.10)
$$

Функція перетворення одного елемента повторного ковзного шифрування може бути описана рекурентною послідовністю:

$$z_n = z_{n-2} \oplus x_n, \qquad (4.11)$$

за початкових умов: $z_1 = x_1$ і $z_2 = x_2$.

Триразове спрощене ковзне шифрування перетворює послідовність z_k у l_k:

$$\begin{aligned}
&l_1 = z_1;\\
&l_2 = z_1 \oplus z_2;\\
&l_3 = z_1 \oplus z_2 \oplus z_3;\\
&l_4 = z_1 \oplus z_2 \oplus z_3 \oplus z_4;\\
&l_5 = z_1 \oplus z_2 \oplus z_3 \oplus z_4 \oplus z_5;\\
&\quad . \ . \ . \ . \ . \ . \ . \ . \ . \ .\\
&l_n = z_1 \oplus z_2 \oplus z_3 \oplus \ldots\ldots \oplus z_n.
\end{aligned} \tag{4.12}$$

Підставимо у вираз (4.12) вираз (4.10), отримаємо:

$$\begin{aligned}
&l_1 = x_1;\\
&l_2 = x_1 \oplus x_2;\\
&l_3 = x_2 \oplus x_3;\\
&l_4 = x_3 \oplus x_4;\\
&l_5 = x_1 \oplus x_4 \oplus x_5;\\
&l_6 = x_1 \oplus x_2 \oplus x_5 \oplus x_6;\\
&l_7 = x_2 \oplus x_3 \oplus x_6 \oplus x_7;\\
&l_8 = x_3 \oplus x_4 \oplus x_7 \oplus x_8;\\
&l_9 = x_1 \oplus x_4 \oplus x_5 \oplus x_8 \oplus x_9;\\
&l_{10} = x_1 \oplus x_2 \oplus x_5 \oplus x_6 \oplus x_9 \oplus x_{10};\\
&l_{11} = x_2 \oplus x_3 \oplus x_6 \oplus x_7 \oplus x_{10} \oplus x_{11};\\
&\quad . \ . \ . \ . \ . \ . \ . \ . \ . \ .
\end{aligned} \tag{4.13}$$

Функція перетворення одного елемента триразового ковзного шифрування може бути описана рекурентною послідовністю:

$$l_n = l_{n-4} \oplus x_{n-1} \oplus x_n, \tag{4.14}$$

за початкових умов: $l_1 = x_1$, $l_2 = x_1 \oplus x_2$, $l_3 = x_2 \oplus x_3$, $l_4 = x_3 \oplus x_4$.

Чотириразове спрощене ковзне шифрування перетворює послідовність l_k у j_k [2]:

$$\begin{aligned}
&j_1 = l_1;\\
&j_2 = l_1 \oplus l_2;\\
&j_3 = l_1 \oplus l_2 \oplus l_3;\\
&j_4 = l_1 \oplus l_2 \oplus l_3 \oplus l_4;\\
&j_5 = l_1 \oplus l_2 \oplus l_3 \oplus l_4 \oplus l_5;\\
&\quad . \quad . \quad . \quad . \quad . \quad . \quad . \quad . \quad . \quad .\\
&j_n = l_1 \oplus l_2 \oplus l_3 \oplus \ldots\ldots \oplus l_n.
\end{aligned} \tag{4.15}$$

Підставимо у вираз (4.15) вираз (4.13), отримаємо:

$$\begin{aligned}
&j_1 = x_1;\\
&j_2 = x_2;\\
&j_3 = x_3;\\
&j_4 = x_4;\\
&j_5 = x_1 \oplus x_5;\\
&j_6 = x_2 \oplus x_6;\\
&j_7 = x_3 \oplus x_7;\\
&j_8 = x_4 \oplus x_8;\\
&j_9 = x_1 \oplus x_5 \oplus x_9;\\
&j_{10} = x_2 \oplus x_6 \oplus x_{10};\\
&j_{11} = x_3 \oplus x_7 \oplus x_{11};\\
&\quad . \quad . \quad . \quad . \quad . \quad . \quad .
\end{aligned} \tag{4.16}$$

Функція перетворення одного елемента чотириразового спрощеного ковзного шифрування може бути описана рекурентною послідовністю:

$$j_n = j_{n-4} \oplus x_n, \tag{4.17}$$

за початкових умов: $j_1 = x_1,\ j_2 = x_2,\ j_3 = x_3,\ j_4 = x_4$.

П'ятикратне спрощене ковзне шифрування перетворює послідовність j_k у p_k [2]:

$$\begin{aligned}
&p_1 = j_1;\\
&p_2 = j_1 \oplus j_2;\\
&p_3 = j_1 \oplus j_2 \oplus j_3;\\
&p_4 = j_1 \oplus j_2 \oplus j_3 \oplus j_4;\\
&p_5 = j_1 \oplus j_2 \oplus j_3 \oplus j_4 \oplus j_5;\\
&\quad . \ . \ . \ . \ . \ . \ . \ . \ . \ .\\
&p_n = j_1 \oplus j_2 \oplus j_3 \oplus \ldots\ldots \oplus j_n.
\end{aligned} \tag{4.18}$$

Підставивши у вираз (4.18) вираз (4.16), отримаємо:

$$\begin{aligned}
&p_1 = x_1;\\
&p_2 = x_1 \oplus x_2;\\
&p_3 = x_1 \oplus x_2 \oplus x_3;\\
&p_4 = x_1 \oplus x_2 \oplus x_3 \oplus x_4;\\
&p_5 = x_2 \oplus x_3 \oplus x_4 \oplus x_5;\\
&p_6 = x_3 \oplus x_4 \oplus x_5 \oplus x_6;\\
&p_7 = x_4 \oplus x_5 \oplus x_6 \oplus x_7;\\
&p_8 = x_5 \oplus x_6 \oplus x_7 \oplus x_8;\\
&p_9 = x_1 \oplus x_6 \oplus x_7 \oplus x_8 \oplus x_9;\\
&p_{10} = x_1 \oplus x_2 \oplus x_7 \oplus x_8 \oplus x_9 \oplus x_{10};\\
&p_{11} = x_1 \oplus x_2 \oplus x_3 \oplus x_8 \oplus x_9 \oplus x_{10} \oplus x_{11};\\
&p_{11} = x_1 \oplus x_2 \oplus x_3 \oplus x_4 \oplus x_9 \oplus x_{10} \oplus x_{11} \oplus x_{12};\\
&. \ . \ . \ . \ . \ . \ .
\end{aligned} \tag{4.19}$$

Функція перетворення одного елемента п'ятикратного спрощеного ковзного шифрування може бути описана рекурентною послідовністю

$$p_n = p_{n-8} \oplus x_{n-3} \oplus x_{n-2} \oplus x_{n-1} \oplus x_n. \qquad (4.20)$$

Шестиразове спрощене ковзне шифрування перетворює послідовність p_k у q_k [2]:

$$\begin{aligned}
q_1 &= p_1;\\
q_2 &= p_1 \oplus p_2;\\
q_3 &= p_1 \oplus p_2 \oplus p_3;\\
q_4 &= p_1 \oplus p_2 \oplus p_3 \oplus p_4;\\
q_5 &= p_1 \oplus p_2 \oplus p_3 \oplus p_4 \oplus p_5;\\
&\ldots\ldots\ldots\\
q_n &= p_1 \oplus p_2 \oplus p_3 \oplus \ldots\ldots \oplus p_n.
\end{aligned} \qquad (4.21)$$

Підставимо у вираз (4.21) вираз (4.19), отримаємо:

$$\begin{aligned}
q_1 &= x_1;\\
q_2 &= x_2;\\
q_3 &= x_1 \oplus x_3;\\
q_4 &= x_2 \oplus x_4;\\
q_5 &= x_3 \oplus x_5;\\
q_6 &= x_4 \oplus x_6;\\
q_7 &= x_5 \oplus x_7;\\
q_8 &= x_6 \oplus x_8;\\
q_9 &= x_1 \oplus x_7 \oplus x_9;\\
q_{10} &= x_2 \oplus x_8 \oplus x_{10};\\
q_{11} &= x_1 \oplus x_3 \oplus x_9 \oplus x_{11};\\
q_{12} &= x_2 \oplus x_4 \oplus x_{10} \oplus x_{12};\\
q_{13} &= x_3 \oplus x_5 \oplus x_{11} \oplus x_{13};\\
q_{14} &= x_4 \oplus x_6 \oplus x_{12} \oplus x_{14};\\
&\ldots\ldots\ldots
\end{aligned} \qquad (4.22)$$

Функція перетворення одного елемента шестиразового спрощеного ковзного шифрування може бути описана рекурентною послідовністю:

$$q_n = q_{n-8} \oplus x_{n-2} \oplus x_n. \qquad (4.23)$$

На основі вище викладеного, можна стверджувати, що функції перетворення елементів ковзного шифрування представляються рекурентними послідовностями (4.8, 4.11, 4.17, 4.20, 4.23) і є окремими випадками з усього розмаїття рекурентних послідовностей, які можуть бути застосовані для синтезу матричних операцій криптографічного перетворення.

Використання матричних операцій криптографічного перетворення дає можливість розпаралелити процес реалізації примітиву ковзного шифрування [2].

Застосування матричних операцій для багаторазового спрощеного ковзного шифрування дозволяє скоротити кількість операцій у порівнянні з одноразовим спрощеним ковзним шифруванням, що дає виграш, як у часі, так і в складності реалізації примітивів.

4.3 Оптимізація матричних операцій ковзного шифрування

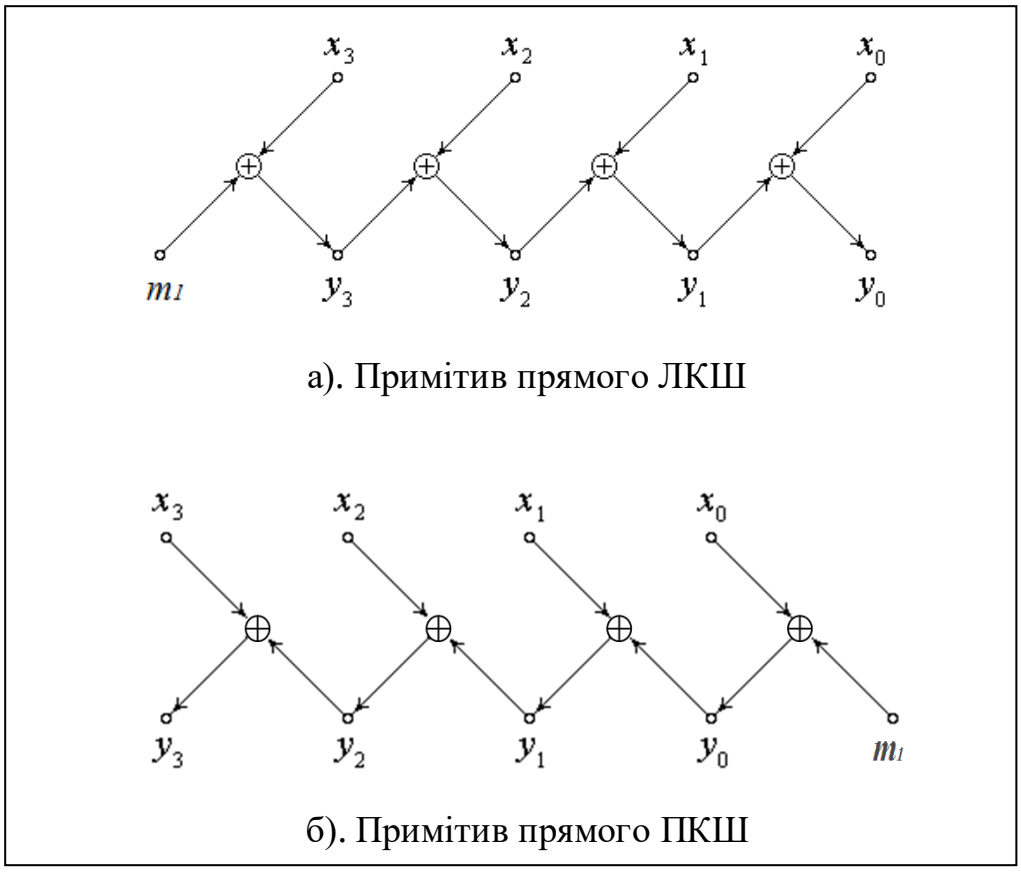
Операції криптографічного перетворення, такі як додавання за модулем і перестановки, можуть бути представлені як матричні операції криптографічного перетворення [14, 15].

Однією з переваг операцій матричного криптографічного перетворення є можливість їх паралельної реалізації [20] .

Реалізація примітивів ковзного шифрування на основі матричних операцій має ряд особливостей, що не досліджувалися [178].

Проведемо моделювання матричних операцій криптографічного перетворення для оптимізації примітивів ковзного шифрування з метою скорочення часу їх реалізації.

Структурні схеми процесу реалізації примітиву прямого лівостороннього ковзного шифрування (ЛКШ) і примітиву прямого правостороннього ковзного шифрування (ПКШ) мають вигляд відповідно рис. 4.8 а) та рис. 4.8 б), де m_1 – елемент раундового ключа [178].



а). Примітив прямого ЛКШ

б). Примітив прямого ПКШ

Рис. 4.8. Структурна схема алгоритму реалізації примітивів прямого ЛКШ та ПКШ

Схемі перетворення, наведеній на рис. 4.8 а), відповідає система лінійних модульних рівнянь

$$\begin{aligned} y_3 &= x_3 \oplus m_1; \\ y_2 &= x_2 \oplus y_3; \\ y_1 &= x_1 \oplus y_2; \\ y_0 &= x_0 \oplus y_1. \end{aligned} \qquad (4.24)$$

Причому в даному випадку операції в (4.24) виконуються порозрядно над кожною парою суміжних операндів.

Аналогічним чином можуть бути побудовані і системи лінійних модульних алгебраїчних рівнянь для прямого ПКШ.

Для подальшого дослідження обмежимося ЛКШ, так як правостороннє виконується аналогічно [2, 181].

Ковзне шифрування перетворює послідовність x_k у y_k, де n – кількість елементів інформації, а $x_1^* = x_1 \oplus m_1$:

$$
\begin{aligned}
&y_1 = x_1^*;\\
&y_2 = x_1^* \oplus x_2;\\
&y_3 = x_1^* \oplus x_2 \oplus x_3;\\
&y_4 = x_1^* \oplus x_2 \oplus x_3 \oplus x_4;\\
&y_5 = x_1^* \oplus x_2 \oplus x_3 \oplus x_4 \oplus x_5;\\
&\quad . \ . \ . \ . \ . \ . \ . \ . \ . \ .\\
&y_n = x_1^* \oplus x_2 \oplus x_3 \oplus \ldots\ldots \oplus x_n;
\end{aligned}
\qquad (4.25)
$$

або

$$
\begin{aligned}
&y_1 = x_1 \oplus m_1;\\
&y_2 = x_1 \oplus x_2 \oplus m_1;\\
&y_3 = x_1 \oplus x_2 \oplus x_3 \oplus m_1;\\
&y_4 = x_1 \oplus x_2 \oplus x_3 \oplus x_4 \oplus m_1;\\
&y_5 = x_1 \oplus x_2 \oplus x_3 \oplus x_4 \oplus x_5 \oplus m_1;\\
&\quad . \ . \ . \ . \ . \ . \ . \ . \ . \ .\\
&y_n = x_1 \oplus x_2 \oplus x_3 \oplus \ldots\ldots \oplus x_n \oplus m_1.
\end{aligned}
$$

Функція перетворення ковзного шифрування може бути описана рекурентною послідовністю:

$$y_n = y_{n-1}. \oplus x_n .$$

Примітив ковзного шифрування побудований на основі отриманої рекурентної послідовності і може бути представлений у вигляді матричної моделі:

$$F(x) = \begin{bmatrix} x_1 \oplus m_1 \\ x_1 \oplus x_2 \oplus m_1 \\ x_1 \oplus x_2 \oplus x_3 \oplus m_1 \\ x_1 \oplus x_2 \oplus x_3 \oplus x_4 \oplus m_1 \\ x_1 \oplus x_2 \oplus x_3 \oplus x_4 \oplus x_5 \oplus m_1 \\ \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \\ x_1 \oplus x_2 \oplus x_3 \oplus \ldots\ldots \oplus x_n \oplus m_1 \end{bmatrix} = \begin{bmatrix} x_1 \\ x_1 \oplus x_{21} \\ x_1 \oplus x_2 \oplus x_3 \\ x_1 \oplus x_2 \oplus x_3 \oplus x_4 \\ x_1 \oplus x_2 \oplus x_3 \oplus x_4 \oplus x_5 \\ \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \\ x_1 \oplus x_2 \oplus x_3 \oplus \ldots\ldots \oplus x_n \end{bmatrix} \oplus \begin{bmatrix} m_1 \\ m_1 \\ m_1 \\ m_1 \\ m_1 \\ \ldots \\ m_1 \end{bmatrix}.$$

При чому, блок обробки ключа може бути описаний рекурентною послідовністю:

$$m_n = m_{n-1}.$$

Результат шифрування складається з порозрядного додавання за модулем 2 результатів виконання блоку обробки інформації і блоку обробки раундового ключа.

Розглянемо повторне ковзне шифрування, яке перетворює послідовність y_k у z_k [3]:

$$\begin{aligned} z_1 &= y_1 \oplus m_2; \\ z_2 &= y_1 \oplus y_2 \oplus m_2; \\ z_3 &= y_1 \oplus y_2 \oplus y_3 \oplus m_2; \\ z_4 &= y_1 \oplus y_2 \oplus y_3 \oplus y_4 \oplus m_2; \\ z_5 &= y_1 \oplus y_2 \oplus y_3 \oplus y_4 \oplus y_5 \oplus m_2; \\ &\cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \\ z_n &= y_1 \oplus y_2 \oplus y_3 \oplus \ldots\ldots \oplus y_n \oplus m_2; \end{aligned} \qquad (4.26)$$

Підставимо у вираз (4.26) вираз (4.25), отримаємо:

$$
\begin{aligned}
&z_1 = x_1 \oplus m_1 \oplus m_2;\\
&z_2 = x_2;\oplus m_2\\
&z_3 = x_1 \oplus x_3 \oplus m_1 \oplus m_2;\\
&z_4 = x_2 \oplus x_4 \oplus m_2;\\
&z_5 = x_1 \oplus x_3 \oplus x_5 \oplus m_1 \oplus m_2;\\
&z_6 = x_2 \oplus x_4 \oplus x_6 \oplus m_2;\\
&\quad . \ . \ . \ . \ . \ . \ . \ . \ . \ .\\
&z_{2k-1} = x_1 \oplus x_3 \oplus x_5 \oplus \ldots\ldots \oplus x_{2k-1} \oplus m_1 \oplus m_2;\\
&z_{2k} = x_2 \oplus x_4 \oplus x_6 \oplus x_8 \oplus \ldots\ldots \oplus x_{2k} \oplus m_2;
\end{aligned}
$$

Функція перетворення повторного ковзного шифрування може бути описана рекурентною моделлю:

$$z_n = z_{n-2} \oplus x_n.$$

Примітив ковзного шифрування побудований на основі рекурентної моделі й може бути представлений у вигляді матричної моделі:

$$
F(x) = \begin{bmatrix}
x_1 \oplus m_1 \oplus m_2\\
x_2 \oplus m_2\\
x_1 \oplus x_3 \oplus m_1 \oplus m_2\\
x_2 \oplus x_4 \oplus m_2\\
x_1 \oplus x_3 \oplus x_5 \oplus m_1 \oplus m_2\\
x_2 \oplus x_4 \oplus x_6 \oplus m_2\\
\quad . \ . \ . \ . \ . \ . \ . \ . \ . \ .\\
x_1 \oplus x_3 \oplus x_5 \oplus \ldots\ldots \oplus x_{2k-1} \oplus m_1 \oplus m_2\\
x_2 \oplus x_4 \oplus x_6 \oplus x_8 \oplus \ldots\ldots \oplus x_{2k} \oplus m_2
\end{bmatrix} =
$$

$$= \begin{bmatrix} x_1 \\ x_2 \\ x_1 \oplus x_3 \\ x_2 \oplus x_4 \\ x_1 \oplus x_3 \oplus x_5 \\ x_2 \oplus x_4 \oplus x_6 \\ \quad . \ . \ . \ . \ . \ . \ . \ . \ . \ . \\ x_1 \oplus x_3 \oplus x_5 \oplus \ldots\ldots \oplus x_{2k-1} \\ x_2 \oplus x_4 \oplus x_6 \oplus x_8 \oplus \ldots\ldots \oplus x_{2k} \end{bmatrix} \oplus \begin{bmatrix} m_1 \oplus m_2; \\ m_2 \\ m_1 \oplus m_2; \\ m_2; \\ m_1 \oplus m_2; \\ m_2; \\ \ldots\ldots\ldots \\ m_1 \oplus m_2; \\ m_2; \end{bmatrix}.$$

А блок обробки раундового ключа може бути описаний рекурентною послідовністю:

$$m_n = m_{n-2}.$$

Функція перетворення триразового ковзного шифрування може бути описана рекурентною моделлю:

$$l_n = l_{n-4} \oplus x_{n-1} \oplus x_n.$$

Примітив триразового ковзного шифрування, побудований на її основі, буде мати вигляд:

$$F(x) = \begin{bmatrix} x_1 \\ x_1 \oplus x_2 \\ x_2 \oplus x_3 \\ lx_3 \oplus x_4 \\ x_1 \oplus x_4 \oplus x_5 \\ x_1 \oplus x_2 \oplus x_5 \oplus x_6 \\ x_2 \oplus x_3 \oplus x_6 \oplus x_7 \\ x_3 \oplus x_4 \oplus x_7 \oplus x_8 \\ x_1 \oplus x_4 \oplus x_5 \oplus x_8 \oplus x_9 \\ x_1 \oplus x_2 \oplus x_5 \oplus x_6 \oplus x_9 \oplus x_{10} \\ x_2 \oplus x_3 \oplus x_6 \oplus x_7 \oplus x_{10} \oplus x_{11} \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots \end{bmatrix} \oplus \begin{bmatrix} m_1 \oplus m_2 \oplus m_3; \\ m_1 \\ m_2 \oplus m_3; \\ 0; \\ m_1 \oplus m_2 \oplus m_3; \\ m_1 \\ m_2 \oplus m_3 \\ 0 \\ m_1 \oplus m_2 \oplus m_3; \\ m_1 \\ m_2 \oplus m_3 \\ \ldots\ldots\ldots\ldots \end{bmatrix}.$$

Рекурентна послідовність, яка описує блок обробки раундового ключа триразового ковзного шифрування, представляється як:

$$m_n = m_{n-4}.$$

Аналогічно отримали рекурентні моделі функції перетворення чотириразового ковзного шифрування і блоку обробки раундового ключа відповідно:

$$j_n = j_{n-4} \oplus x_n; \quad m_n = m_{n-4}.$$

П'ятикратне ковзне шифрування перетворює послідовність j_k у p_k [3].

Рекурентні послідовності функції перетворення п'ятикратного ковзного шифрування і блоку обробки раундового ключа можуть бути описані в такому вигляді:

$$p_n = p_{n-8} \oplus x_{n-3} \oplus x_{n-2} \oplus x_{n-1} \oplus x_n;$$

$$m_n = m_{n-8}.$$

Шестиразове ковзне шифрування перетворює послідовність p_k у q_k [3].

Функція перетворення шестиразового ковзного шифрування може бути описана рекурентною моделлю:

$$q_n = q_{n-8} \oplus x_{n-2} \oplus x_n.$$

Примітив шестиразового ковзаючого шифрування представлений

матричною моделлю:

$$F(x)=\begin{bmatrix} x_1 \\ x_2 \\ x_1 \oplus x_3 \\ x_2 \oplus x_4 \\ x_3 \oplus x_5 \\ x_4 \oplus x_6 \\ x_5 \oplus x_7 \\ x_6 \oplus x_8 \\ x_1 \oplus x_7 \oplus x_9 \\ x_2 \oplus x_8 \oplus x_{10} \\ x_1 \oplus x_3 \oplus x_9 \oplus x_{11} \\ x_2 \oplus x_4 \oplus x_{10} \oplus x_{12} \\ x_3 \oplus x_5 \oplus x_{11} \oplus x_{13} \\ x_4 \oplus x_6 \oplus x_{12} \oplus x_{14} \\ \cdots\cdots\cdots \end{bmatrix} \oplus \begin{bmatrix} m_1 \oplus m_2 \oplus m_3 \oplus m_4 \oplus m_5 \oplus m_6 \\ m_2 \oplus m_3 \oplus m_5 \\ m_1 \oplus m_2 \oplus m_3 \oplus m_6 \\ m_2 \oplus m_3 \\ m_4 \oplus m_5 \oplus m_6 \\ m_5 \\ m_6 \\ 0 \\ m_1 \oplus m_2 \oplus m_3 \oplus m_4 \oplus m_5 \oplus m_6 \\ m_2 \oplus m_3 \oplus m_5 \\ m_1 \oplus m_2 \oplus m_3 \oplus m_6 \\ m_2 \oplus m_3 \\ m_4 \oplus m_5 \oplus m_6 \\ m_5 \\ \cdots\cdots\cdots \end{bmatrix} \quad (4.27)$$

Рекурентна послідовність, яка описує блок обробки раундового ключа, представляється як:

$$m_n = m_{n-8}.$$

Розглянемо варіант оптимізації примітиву ковзного шифрування, реалізований матричної операцією. Оскільки $m_1 \oplus m_2 \oplus \ldots\ldots \oplus m_n = m_k$ і випадкові елементи раундового ключа формуються на основі одного і того ж алгоритму, отже, враховуючи теорему Шеннона [171], можна стверджувати, що повторне застосування елементів раундового ключа не підвищує криптостійкість.

Виходячи з цього, з'явилася можливість оптимізувати операцію криптографічного перетворення блоку обробки раундового ключа без зменшення криптостійкості наступною системою [3]:

$$F(x)=\begin{bmatrix} x_1 \\ x_1 \oplus x_{21} \\ x_1 \oplus x_2 \oplus x_3 \\ x_1 \oplus x_2 \oplus x_3 \oplus x_4 \\ x_1 \oplus x_2 \oplus x_3 \oplus x_4 \oplus x_5 \\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot \\ x_1 \oplus x_2 \oplus x_3 \oplus \ldots\ldots \oplus x_n \end{bmatrix} \oplus \begin{bmatrix} m_1 \\ m_2 \\ m_3 \\ m_4 \\ m_5 \\ m_6 \\ m_6 \\ \ldots\ldots\ldots \\ m_L \end{bmatrix}, \qquad (4.28)$$

де L - кількість раундів.

Таким чином, оптимізована операція (4.28) дозволяє збільшити швидкість обробки раундового ключа для моделі (4.27) до 5 разів, а швидкість виконання операцій криптографічного перетворення – до 2 разів відносно реалізації матричної операції [3].

Отримані матричні операції, що реалізують примітиви ковзного шифрування, можуть бути оптимізовані без втрати криптостійкості шляхом паралельного використання елементів раундового ключа [3].

Дана оптимізація дозволяє зменшити апаратну складність реалізації примітиву ковзного шифрування за рахунок скорочення кількості операцій додавання за модулем 2 [3].

4.4 Моделювання примітивів багаторазового ковзного шифрування на основі рекурентних послідовностей

Отримати рекурентну залежність для багаторазового ковзного перетворення виявилося достатньо складним, особливо при її визначенні для невеликої розрядності перетворення.

Спробуємо отримати рекурентні послідовності для опису матричних операцій багаторазового перетворення на основі ковзного примітиву [36].

Нехай y_i^k – умовне позначення одного елемента примітиву багаторазового ковзного шифрування, де i – порядковий номер елемента, а k – кількість етапів (разів, раундів) зашифрування.

Тоді система рівнянь для виконання примітива ковзного шифрування запишеться [36]

$$
\begin{aligned}
y_1^1 &= y_0^1 \oplus x_1 \\
y_2^1 &= y_1^1 \oplus x_2 \\
y_3^1 &= y_2^1 \oplus x_3 \\
y_4^1 &= y_3^1 \oplus x_4 \\
y_5^1 &= y_4^1 \oplus x_5 \\
&\ldots\ldots
\end{aligned}
$$

Звідси отримаємо рекурентну послідовність, яка описує процес виконання примітива ковзного шифрування: [36]

$$y_i^1 = y_{i-1}^1 \oplus x_i \text{, де } y_0^1 = m_1 . \tag{4.29}$$

Система рівнянь для здійснення перетворення інформації на основі двохразового виконання примітива ковзного шифрування має вигляд:

$$y_1^2 = y_0^2 \oplus y_1^1$$
$$y_2^2 = y_1^2 \oplus y_2^1$$
$$y_3^2 = y_2^2 \oplus y_3^1$$
$$y_4^2 = y_3^2 \oplus y_4^1$$
$$y_5^2 = y_4^2 \oplus y_5^1$$
$$\ldots\ldots$$

Звідси отримано рекурентну залежність між елементами примітива ковзного шифрування [36]:

$$y_i^2 = y_{i-1}^2 \oplus y_i^1, \text{ де } y_0^2 = m_2. \tag{4.30}$$

Система рівнянь для триразового виконання примітива ковзного шифрування запишеться [36]:

$$y_1^3 = y_0^3 \oplus y_1^2$$
$$y_2^3 = y_1^3 \oplus y_2^2$$
$$y_3^3 = y_2^3 \oplus y_3^2$$
$$y_4^3 = y_3^3 \oplus y_4^2$$
$$y_5^3 = y_4^3 \oplus y_5^2$$
$$\ldots\ldots$$

Звідси отримаємо рекурентну послідовність, яка описує процес виконання триразового примітива ковзного шифрування:

$$y_i^3 = y_{i-1}^3 \oplus y_i^2, \text{ де } y_0^3 = m_3. \tag{4.31}$$

Чотирьохразове виконання примітива ковзного шифрування описується системою рівнянь:

$$y_1^4 = y_0^4 \oplus y_1^3$$
$$y_2^4 = y_1^4 \oplus y_2^3$$
$$y_3^4 = y_2^4 \oplus y_3^3$$
$$y_4^4 = y_3^4 \oplus y_4^3$$
$$y_5^4 = y_4^4 \oplus y_5^3$$
$$\ldots\ldots$$

Рекурентна послідовність, яка описує процес чотирьохразового виконання примітива ковзного шифрування описується:

$$y_i^4 = y_{i-1}^4 \oplus y_i^3, \text{ де } y_0^4 = m_4. \quad (4.32)$$

Таким чином, на основі описаних моделей багаторазового виконання примітива ковзного шифрування, що описуються рекурентними залежностями (4.29)-(4.32), отримали узагальнену рекурентну модель процесу виконання багаторазового примітиву ковзного шифрування для перетворення n-елементів [36]:

$$y_i^k = y_{i-1}^k \oplus y_i^{k-1}, \text{ де } y_0^k = m_k. \quad (4.33)$$

Використаємо запропонований підхід до математичного опису на основі рекурентних послідовностей для моделювання операцій багаторазового перетворення на основі ковзного примітиву при обмеженій кількості елементів.

Особливістю реалізації даного ковзного шифрування є те, що в якості вхідного раундового ключа використовується вихідний раундовий ключ попереднього етапу перетворення.

Відповідно рис. 4.8 б) система лінійних модульних алгебраїчних рівнянь, що описує реалізацію примітиву чотирьохелементного прямого правостороннього ковзного шифрування, описується як:

$$\begin{aligned} y_1 &= x_1 \oplus m_1; \\ y_2 &= x_2 \oplus y_1; \\ y_3 &= x_3 \oplus y_2; \\ y_4 &= x_4 \oplus y_3. \end{aligned} \qquad (4.34)$$

де m_1 – вхідний раундовий ключ, а $y_4 = m_2$ – вихідний раундовий ключ, що використовується в якості вхідного для наступного блока даних, що перетворюється.

Розглянемо матричну модель операції ковзного шифрування (4.34) у розвернутому вигляді. Операція чотирьохелементного прямого правостороннього ковзного шифрування перетворює послідовність x_k у y_k, $k = 1..4$, тоді

$$\begin{aligned} y_1 &= x_1 \oplus m_1; \\ y_2 &= x_1 \oplus x_2 \oplus m_1; \\ y_3 &= x_1 \oplus x_2 \oplus x_3 \oplus m_1; \\ y_4 &= x_1 \oplus x_2 \oplus x_3 \oplus x_4 \oplus m_1. \end{aligned} \qquad (4.35)$$

Рекурентна послідовність, яка описує операцію чотирьохелементного прямого правостороннього ковзного шифрування має вигляд:

$$y_i^1 = y_{i-1}^1 \oplus x_i \text{, де } y_0^1 = m_1 \text{ та } i \in \{1, \ldots, 4\}. \qquad (4.36)$$

Повторне чотирьохелементне ковзне шифрування перетворює послідовність y_k у z_k:

$$\begin{aligned} z_1 &= y_1 \oplus m_2; \\ z_2 &= y_2 \oplus z_1; \\ z_3 &= y_3 \oplus z_2; \\ z_4 &= y_4 \oplus z_3. \end{aligned} \quad \text{або} \quad \begin{aligned} z_1 &= y_1 \oplus m_2; \\ z_2 &= y_1 \oplus y_2 \oplus m_2; \\ z_3 &= y_1 \oplus y_2 \oplus y_3 \oplus m_2; \\ z_4 &= y_1 \oplus y_2 \oplus y_3 \oplus y_4 \oplus m_2, \end{aligned} \qquad (4.37)$$

де m_2 – вхідний раундовий ключ, і $m_2 = y_4$.

Підставивши у вираз (4.37) вираз (4.35), отримаємо:

$$
\begin{aligned}
&z_1 = (x_1 \oplus m_1) \oplus m_2;\\
&z_2 = (x_1 \oplus m_1) \oplus (x_1 \oplus x_2 \oplus m_1) \oplus m_2;\\
&z_3 = (x_1 \oplus m_1) \oplus (x_1 \oplus x_2 \oplus m_1) \oplus (x_1 \oplus x_2 \oplus x_3 \oplus m_1) \oplus m_2;\\
&z_4 = (x_1 \oplus m_1) \oplus (x_1 \oplus x_2 \oplus m_1) \oplus (x_1 \oplus x_2 \oplus x_3 \oplus m_1) \oplus\\
&\oplus (x_1 \oplus x_2 \oplus x_3 \oplus x_4 \oplus m_1) \oplus m_2.
\end{aligned}
$$

Провівши перетворення при $m_2 = y_4$, отримаємо:

$$
\begin{aligned}
&z_1 = x_4 \oplus x_3 \oplus x_2;\\
&z_2 = x_4 \oplus x_3 \oplus x_1 \oplus m_1;\\
&z_3 = x_4 \oplus x_2;\\
&z_4 = x_3 \oplus x_1 \oplus m_1.
\end{aligned}
\qquad (4.38)
$$

Рекурентна послідовність, яка описує операцію повторного (двохразового) чотирьохелементного прямого правостороннього ковзного шифрування має вигляд:

$$
y_i^2 = y_{i-1}^2 \oplus y_i^1, \text{ де } y_0^2 = y_4^1, \text{ а } i \in \{1, \ldots, 4\}. \qquad (4.39)
$$

Триразове чотирьохелементне ковзне шифрування перетворює послідовність z_k у l_k:

$$
\begin{aligned}
&l_1 = z_1 \oplus m_3;\\
&l_2 = z_1 \oplus z_2 \oplus m_3;\\
&l_3 = z_1 \oplus z_2 \oplus z_3 \oplus m_3;\\
&l_4 = z_1 \oplus z_2 \oplus z_3 \oplus z_4 \oplus m_3.
\end{aligned}
\quad , \qquad (4.40)
$$

де $m_3 = z_4$ – вхідний раундовий ключ даного етапу шифрування.

Підставимо у вираз (4.40) вираз (4.38), та провівши скорочення змінних, отримаємо:

$$\begin{aligned} l_1 &= x_1 \oplus x_2 \oplus x_4 \oplus m_1; \\ l_2 &= x_2 \oplus x_3; \\ l_3 &= x_3 \oplus x_4; \\ l_4 &= x_1 \oplus x_4 \oplus m_1. \end{aligned} \qquad (4.41)$$

Рекурентна послідовність, яка описує операцію триразового чотирьохелементного прямого правостороннього ковзного шифрування має вигляд:

$$y_i^3 = y_{i-1}^3 \oplus y_i^2 \text{, де } y_0^3 = y_4^2 \text{, а } i \in \{1, \ldots, 4\}. \qquad (4.42)$$

Чотириразове чотирьохелементне ковзне шифрування перетворює послідовність l_k у j_k:

$$\begin{aligned} j_1 &= l_1 \oplus m_4; \\ j_2 &= l_1 \oplus l_2 \oplus m_4; \\ j_3 &= l_1 \oplus l_2 \oplus l_3 \oplus m_4; \\ j_4 &= l_1 \oplus l_2 \oplus l_3 \oplus l_4 \oplus m_4. \end{aligned} \quad , \qquad (4.43)$$

де $m_4 = l_4$ – вхідний раундовий ключ даного етапу шифрування.

Підставимо у вираз (4.43) вираз (4.41), отримаємо [36]:

$$\begin{aligned} j_1 &= x_2; \\ j_2 &= x_3; \\ j_3 &= x_4; \\ j_4 &= x_1 \oplus m_1. \end{aligned}$$

Рекурентна послідовність, яка описує операцію чотириразового чотирьохелементного прямого правостороннього ковзного шифрування має вигляд:

$$y_i^4 = y_{i-1}^4 \oplus y_i^3, \text{ де } y_0^4 = y_4^3, \text{ а } i \in \{1, \ldots, 4\} \quad . \tag{4.44}$$

Операція п’ятиелементного прямого правостороннього ковзного шифрування перетворює послідовність x_k у y_k, $k = 1..5$.

Рекурентна послідовність, яка описує операцію п’ятиелементного прямого правостороннього ковзного шифрування має вигляд:

$$y_i^1 = y_{i-1}^1 \oplus x_i, \text{ де } y_0^1 = m_1, \text{ а } i \in \{1, \ldots, 5\}. \tag{4.45}$$

Повторне п’ятиелементне ковзне шифрування перетворює послідовність y_k у z_k за виконання умов: m_2 – вхідний раундовий ключ, і $m_2 = y_5$. Підставивши відповідні вирази, отримаємо [36]:

$$\begin{aligned}
z_1 &= x_2 \oplus x_3 \oplus x_4 \oplus x_5; \\
z_2 &= x_1 \oplus x_3 \oplus x_4 \oplus x_5 \oplus m_1; \\
z_3 &= x_2 \oplus x_4 \oplus x_5; \\
z_4 &= x_1 \oplus x_3 \oplus x_5 \oplus m_1; \\
z_5 &= x_2 \oplus x_4.
\end{aligned}$$

Рекурентна послідовність, яка описує операцію двохразового п’ятиелементного прямого правостороннього ковзного шифрування має вигляд:

$$y_i^2 = y_{i-1}^2 \oplus y_i^1, \text{ де } y_0^2 = y_5^1, \text{ а } i \in \{1, \ldots, 5\}. \tag{4.46}$$

Триразове п’ятиелементне ковзне шифрування перетворює послідовність z_k у l_k за умови, що $m_3 = z_5$ – вхідний раундовий ключ даного етапу шифрування, та описується моделлю [36]:

$$l_1 = x_1 \oplus x_3;$$
$$l_2 = x_1 \oplus x_4 \oplus m_1;$$
$$l_3 = x_1 \oplus x_2 \oplus x_5 \oplus m_1;$$
$$l_4 = x_1 \oplus x_2 \oplus x_3 \oplus x_5;$$
$$l_5 = x_3 \oplus x_4.$$

Рекурентна послідовність, яка описує операцію триразового п’ятиелементного прямого правостороннього ковзного шифрування має вигляд:

$$y_i^3 = y_{i-1}^3 \oplus y_i^2 \text{, де } y_0^3 = y_5^2 \text{, а } i \in \{1, \ldots, 5\}. \qquad (4.47)$$

Чотириразове п’ятиелементне ковзне шифрування перетворює послідовність l_k у j_k ,.де $m_4 = l_5$ – вхідний раундовий ключ даного етапу шифрування. Підставимо відповідні вирази, отримаємо:

$$j_1 = x_2 \oplus x_4;$$
$$j_2 = m_1;$$
$$j_3 = x_1 \oplus x_2 \oplus x_5;$$
$$j_4 = x_3;$$
$$j_5 = x_4.$$

Рекурентна послідовність, яка описує операцію чотириразового п’ятиелементного прямого правостороннього ковзного шифрування має вигляд:

$$y_i^4 = y_{i-1}^4 \oplus y_i^3 \text{, де } y_0^4 = y_5^3 \text{, а } i \in \{1, \ldots, 5\}. \qquad (4.48)$$

Операція шестиелементного прямого правостороннього ковзного шифрування перетворює послідовність x_k у y_k, $k = 1..6$.

Рекурентна послідовність, яка описує операцію шестиелементного прямого правостороннього ковзного шифрування має вигляд [36]:

$$y_i^1 = y_{i-1}^1 \oplus x_i, \text{ де } y_0^1 = m_1, \text{ а } i \in \{1, \ldots, 6\}. \quad (4.49)$$

Повторне шестиелементне ковзне шифрування перетворює послідовність y_k у z_k за виконання умови: m_2 – вхідний раундовий ключ, і $m_2 = y_6$. Підставивши відповідні вирази отримаємо:

$$\begin{aligned}
z_1 &= x_2 \oplus x_3 \oplus x_4 \oplus x_5 \oplus x_6;\\
z_2 &= x_1 \oplus x_3 \oplus x_4 \oplus x_5 \oplus x_6 \oplus m_1;\\
z_3 &= x_2 \oplus x_4 \oplus x_5 \oplus x_6;\\
z_4 &= x_1 \oplus x_3 \oplus x_5 \oplus x_6 \oplus m_1;\\
z_5 &= x_2 \oplus x_4 \oplus x_6;\\
z_6 &= x_1 \oplus x_3 \oplus x_5 \oplus m_1.
\end{aligned}$$

Рекурентна послідовність, яка описує операцію двохразового шестиелементного прямого правостороннього ковзного шифрування має вигляд:

$$y_i^2 = y_{i-1}^2 \oplus y_i^1, \text{ де } y_0^2 = y_6^1 \text{ та } i \in \{1, \ldots, 6\} \quad (4.50)$$

Триразове шестиелементне ковзне шифрування перетворює послідовність z_k у l_k за умови, що $m_3 = z_6$ – вхідний раундовий ключ даного етапу шифрування та описується моделлю:

$$
\begin{aligned}
l_1 &= x_1 \oplus x_2 \oplus x_4 \oplus x_6 \oplus m_1;\\
l_2 &= x_2 \oplus x_3 \oplus x_5;\\
l_3 &= x_3 \oplus x_4 \oplus x_6;\\
l_4 &= x_1 \oplus x_4 \oplus x_5 \oplus m_1;\\
l_5 &= x_1 \oplus x_2 \oplus x_5 \oplus x_6 \oplus m_1;\\
l_6 &= x_2 \oplus x_3 \oplus x_6.
\end{aligned}
$$

Рекурентна послідовність, яка описує операцію триразового шестиелементного прямого правостороннього ковзного шифрування має вигляд:

$$y_i^3 = y_{i-1}^3 \oplus y_i^2 \text{, де } y_0^3 = y_6^2 \text{ та } i \in \{1, \ldots, 6\}. \qquad (4.51)$$

Чотириразове шестиелементне ковзне шифрування перетворює послідовність l_k у j_k, де $m_4 = l_6$ – вхідний раундовий ключ даного етапу шифрування. Підставимо відповідні вирази, отримаємо:

$$
\begin{aligned}
j_1 &= x_1 \oplus x_3 \oplus x_4 \oplus m_1;\\
j_2 &= x_1 \oplus x_2 \oplus x_4 \oplus x_5 \oplus m_1;\\
j_3 &= x_1 \oplus x_2 \oplus x_3 \oplus x_5 \oplus x_6 \oplus m_1;\\
j_4 &= x_2 \oplus x_3 \oplus x_4 \oplus x_6;\\
j_5 &= x_1 \oplus x_3 \oplus x_4 \oplus x_5 \oplus m_1;\\
j_6 &= x_1 \oplus x_2 \oplus x_4 \oplus x_5 \oplus x_6 \oplus m_1.
\end{aligned}
$$

Рекурентна послідовність, яка описує операцію чотириразового шестиелементного прямого правостороннього ковзного шифрування має вигляд:

$$y_i^4 = y_{i-1}^4 \oplus y_i^3 \text{, де } y_0^4 = y_6^3 \text{ та } i \in \{1, \ldots, 6\}. \qquad (4.52)$$

Операція семиелементного прямого правостороннього ковзного шифрування перетворює послідовність x_k у y_k, $k = 1..7$.

Рекурентна послідовність, яка описує операцію семиелементного прямого правостороннього ковзного шифрування має вигляд:

$$y_i^1 = y_{i-1}^1 \oplus x_i, \text{ де } y_0^1 = m_1 \text{ та } i \in \{1, \ldots, 7\}. \quad (4.53)$$

Повторне семиелементне ковзне шифрування перетворює послідовність y_k у z_k за виконання умови: m_2 – вхідний раундовий ключ, і $m_2 = y_7$. Підставивши відповідні вирази, отримаємо:

$$\begin{aligned}
z_1 &= x_2 \oplus x_3 \oplus x_4 \oplus x_5 \oplus x_6 \oplus x_7;\\
z_2 &= x_1 \oplus x_3 \oplus x_4 \oplus x_5 \oplus x_6 \oplus x_7 \oplus m_1;\\
z_3 &= x_2 \oplus x_4 \oplus x_5 \oplus x_6 \oplus x_7;\\
z_4 &= x_1 \oplus x_3 \oplus x_5 \oplus x_6 \oplus x_7 \oplus m_1;\\
z_5 &= x_2 \oplus x_4 \oplus x_6 \oplus x_7;\\
z_6 &= x_1 \oplus x_3 \oplus x_5 \oplus x_7 \oplus m_1;\\
z_7 &= x_2 \oplus x_4 \oplus x_6.
\end{aligned}$$

Рекурентна послідовність, яка описує операцію двохразового семиелементного прямого правостороннього ковзного шифрування має вигляд:

$$y_i^2 = y_{i-1}^2 \oplus y_i^1, \text{ де } y_0^2 = y_7^1, \; i \in \{1, \ldots, 7\}. \quad (4.54)$$

Триразове семиелементне ковзне шифрування перетворює послідовність z_k у l_k за умови, що $m_3 = z_7$ – вхідний раундовий ключ даного етапу шифрування

та описується моделлю [36]:

$$
\begin{aligned}
l_1 &= x_3 \oplus x_5 \oplus x_7;\\
l_2 &= x_1 \oplus x_4 \oplus x_6 \oplus m_1;\\
l_3 &= x_1 \oplus x_2 \oplus x_5 \oplus x_7 \oplus m_1;\\
l_4 &= x_2 \oplus x_3 \oplus x_6;\\
l_5 &= x_3 \oplus x_4 \oplus x_7;\\
l_6 &= x_1 \oplus x_4 \oplus x_5 \oplus m_1;\\
l_7 &= x_1 \oplus x_2 \oplus x_5 \oplus x_6 \oplus m_1.
\end{aligned}
$$

Рекурентна послідовність, яка описує операцію триразового семиелементного прямого правостороннього ковзного шифрування має вигляд:

$$y_i^3 = y_{i-1}^3 \oplus y_i^2 \text{, де } y_0^3 = y_7^2 \text{ та } i \in \{1, \ldots, 7\}. \qquad (4.55)$$

Чотириразове семиелементне ковзне шифрування перетворює послідовність l_k у j_k, де $m_4 = l_7$ – вхідний раундовий ключ даного етапу шифрування. Підставимо відповідні вирази, отримаємо:

$$
\begin{aligned}
j_1 &= x_1 \oplus x_2 \oplus x_3 \oplus x_6 \oplus x_7 \oplus m_1;\\
j_2 &= x_2 \oplus x_3 \oplus x_4 \oplus x_7;\\
j_3 &= x_1 \oplus x_3 \oplus x_4 \oplus x_5 \oplus m_1;\\
j_4 &= x_1 \oplus x_2 \oplus x_4 \oplus x_5 \oplus x_6 \oplus m_1;\\
j_5 &= x_1 \oplus x_2 \oplus x_3 \oplus x_5 \oplus x_6 \oplus x_7 \oplus m_1;\\
j_6 &= x_2 \oplus x_3 \oplus x_4 \oplus x_6 \oplus x_7;\\
j_7 &= x_1 \oplus x_3 \oplus x_4 \oplus x_5 \oplus x_7 \oplus m_1.
\end{aligned}
$$

Рекурентна послідовність, яка описує операцію чотириразового семиелементного прямого правостороннього ковзного шифрування має вигляд:

$$y_i^4 = y_{i-1}^4 \oplus y_i^3, \text{ де } y_0^4 = y_7^3 \text{ та } i \in \{1, \ldots, 7\}. \quad (4.56)$$

Операція восьмиелементного прямого правостороннього ковзного шифрування перетворює послідовність x_k у y_k, $k = 1..8$.

Рекурентна послідовність, яка описує операцію восьмиелементного прямого правостороннього ковзного шифрування має вигляд:

$$y_i^1 = y_{i-1}^1 \oplus x_i, \text{ де } y_0^1 = m_1 \text{ та } i \in \{1, \ldots, 8\}. \quad (4.57)$$

Повторне восьмиелементне ковзне шифрування перетворює послідовність y_k у z_k за виконання умови: m_2 – вхідний раундовий ключ, і $m_2 = y_8$. Підставивши відповідні вирази, отримаємо:

$$\begin{aligned}
z_1 &= x_2 \oplus x_3 \oplus x_4 \oplus x_5 \oplus x_6 \oplus x_7 \oplus x_8;\\
z_2 &= x_1 \oplus x_3 \oplus x_4 \oplus x_5 \oplus x_6 \oplus x_7 \oplus x_8 \oplus m_1;\\
z_3 &= x_2 \oplus x_4 \oplus x_5 \oplus x_6 \oplus x_7 \oplus x_8;\\
z_4 &= x_1 \oplus x_3 \oplus x_5 \oplus x_6 \oplus x_7 \oplus x_8 \oplus m_1;\\
z_5 &= x_2 \oplus x_4 \oplus x_6 \oplus x_7 \oplus x_8;\\
z_6 &= x_1 \oplus x_3 \oplus x_5 \oplus x_7 \oplus x_8 \oplus m_1;\\
z_7 &= x_2 \oplus x_4 \oplus x_6 \oplus x_8;\\
z_8 &= x_1 \oplus x_3 \oplus x_5 \oplus x_7 \oplus m_1.
\end{aligned}$$

Рекурентна послідовність, яка описує операцію двохразового восьмиелементного прямого правостороннього ковзного шифрування має вигляд:

$$y_i^2 = y_{i-1}^2 \oplus y_i^1, \text{ де } y_0^2 = y_8^1 \text{ та } i \in \{1, \ldots, 8\}. \quad (4.58)$$

Триразове восьмиелементне ковзне шифрування перетворює послідовність z_k у l_k за умови, що $m_3 = z_8$ – вхідний раундовий ключ даного етапу шифрування та описується моделлю [36]:

$$
\begin{aligned}
l_1 &= x_1 \oplus x_2 \oplus x_4 \oplus x_6 \oplus x_8 \oplus m_1;\\
l_2 &= x_2 \oplus x_3 \oplus x_5 \oplus x_7;\\
l_3 &= x_3 \oplus x_4 \oplus x_6 \oplus x_8;\\
l_4 &= x_1 \oplus x_4 \oplus x_5 \oplus x_7 \oplus m_1;\\
l_5 &= x_1 \oplus x_2 \oplus x_5 \oplus x_6 \oplus x_8;\\
l_6 &= x_2 \oplus x_3 \oplus x_6 \oplus \oplus x_7;\\
l_7 &= x_3 \oplus x_4 \oplus x_7 \oplus \oplus x_8;\\
l_8 &= x_1 \oplus x_4 \oplus x_5 \oplus x_8 \oplus m_1.
\end{aligned}
$$

Рекурентна послідовність, яка описує операцію триразового восьмиелементного прямого правостороннього ковзного шифрування має вигляд:

$$y_i^3 = y_{i-1}^3 \oplus y_i^2 \text{, де } y_0^3 = y_8^2 \text{ та } i \in \{1, \ldots, 8\}. \qquad (4.59)$$

Чотириразове восьмиелементне ковзне шифрування перетворює послідовність l_k у j_k, де $m_4 = l_8$ – вхідний раундовий ключ даного етапу шифрування. Підставимо відповідні вирази, отримаємо:

$$
\begin{aligned}
j_1 &= x_2 \oplus x_5 \oplus x_6;\\
j_2 &= x_3 \oplus x_6 \oplus x_7;\\
j_3 &= x_4 \oplus x_7 \oplus x_8;\\
j_4 &= x_1 \oplus x_5 \oplus x_8 \oplus m_1;\\
j_5 &= x_2 \oplus x_6;\\
j_6 &= x_3 \oplus x_7;\\
j_7 &= x_4 \oplus x_8;\\
j_8 &= x_1 \oplus x_5 \oplus x_7 \oplus m_1.
\end{aligned}
$$

Рекурентна послідовність, яка описує операцію чотириразового восьмиелементного прямого правостороннього ковзного шифрування має вигляд [36]:

$$y_i^4 = y_{i-1}^4 \oplus y_i^3, \text{ де } y_0^4 = y_8^3 \text{ та } i \in \{1, \ldots, 8\}. \quad (4.60)$$

На основі виразів (4.36), (4.39), (4.42), (4.44)-(4.60) отримано узагальнений вираз рекурентної послідовності для опису виконання багаторазового прямого правостороннього ковзного шифрування [36]:

$$y_i^k = y_{i-1}^k \oplus y_i^{k-1}, \quad (4.61)$$

де $y_0^k = y_d^{k-1}$ та $i \in \{1, \ldots, d\}$, де, в свою чергу, k – кількість раундів ковзного перетворення, а d – розрядність перетворення.

4.5 Вдосконалений спосіб багатократного застосування примітива ковзного шифрування

Оскільки із збільшенням кількості разів застосування примітиву ковзного шифрування вироджується псевдовипадковість, то потрібно запропонувати інші способи застосування даного примітиву. Одним із шляхів рішення поставленої задачі є застосування матриць перетворень, які є матрицями перестановок.

Розглянемо основні випадки застосування таких матриць для реалізації примітивів ковзного шифрування.

Враховуючи те, що коли в алгоритмі криптоперетворення застосовується примітив ковзного шифрування, можливо виокремити основні 4 випадки:

Перший випадок. Багатократне застосування примітиву ковзного шифрування є першою процедурою перетворення інформації, потім здійснюється

процедуру перестановки, а останньою процедурою здійснюється додавання раундового ключа.

Тоді формальна модель даного процесу перетворення може бути описати як:

$$F(x) = [M^*] \times [M_{перестановок}] \oplus \begin{bmatrix} R_1 \\ R_2 \\ . \\ . \\ . \\ R_L \end{bmatrix}, \qquad (4.65)$$

де $[M^*]$ – операція багатократного застосування криптографічного примітиву, $[M_{перестановок}]$ – матриця перестановок, матриця-стовпець R_i – це раундовий ключ.

Реалізація процесу перетворення інформації за формальною моделлю (4.65) зображено на рис. 4.9.

Рис. 4.9. Структурна схема послідовності застосування операцій.

Другий випадок. Багатократне застосування примітиву ковзного шифрування є першою процедурою перетворення інформації, потім здійснюється додавання раундового ключа, а останньою процедурою здіснюється перестановка.

Формальна модель даного процесу перетворення може бути описати як:

$$F(x) = ([M^*] \oplus \begin{bmatrix} R_1 \\ R_2 \\ \cdot \\ \cdot \\ \cdot \\ R_L \end{bmatrix}) \times [M_{перестановок}] \qquad (4.66)$$

Реалізація процесу перетворення інформації за формальною моделлю (4.66) зображено на рис. 4.10.

Рис. 4.10. Структурна схема послідовності застосування операцій

Третій випадок. Багатократне застосування примітиву ковзного шифрування є першою процедурою перетворення інформації, потім здійснюється перестановка, потім відбувається додавання раундового ключа, а останньою процедурою знову здійснюється перестановка.

Формальна модель даного процесу перетворення може бути описати як:

$$F(x) = ([M^*] \times [M_{перестановок}] \oplus \begin{bmatrix} R_1 \\ R_2 \\ \cdot \\ \cdot \\ \cdot \\ R_L \end{bmatrix}) \times [M_{перестановок}] \; . \qquad (4.67)$$

Реалізація процесу перетворення інформації за формальною моделлю (4.67) зображено на рис. 4.11.

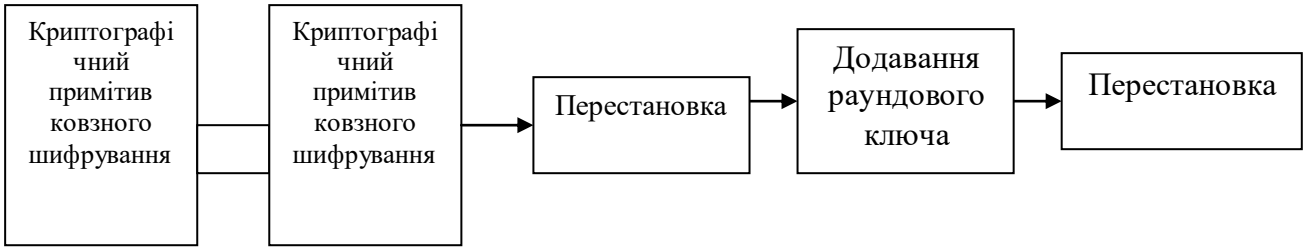


Рис. 4.11. Структурна схема послідовності застосування операцій

Четвертий випадок. Першою процедурою криптографічного перетворення є перестановка блоків інформації, потім виконується операція на основі багатократного застосування примітиву ковзного шифрування, а останньою процедурою відбувається додавання раундового ключа.

Формальна модель даного процесу перетворення може бути описати як:

$$F(x) = [M_{перестановок}] \Rightarrow [M^*] \oplus \begin{bmatrix} R_1 \\ R_2 \\ \cdot \\ \cdot \\ \cdot \\ R_L \end{bmatrix}. \qquad (4.68)$$

Реалізація процесу перетворення інформації за формальною моделлю (4.68) зображено на рис. 4.12.

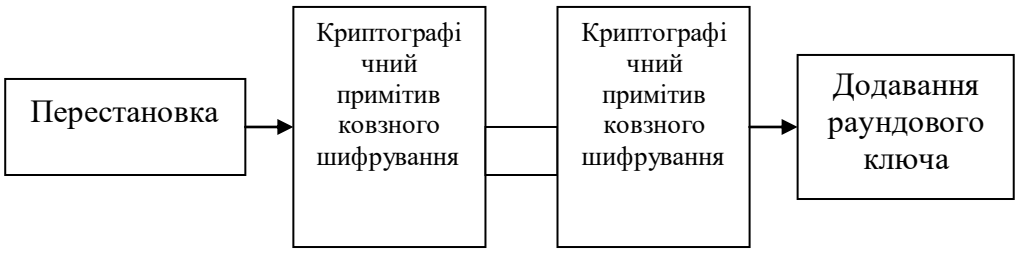


Рис. 4.12. Структурна схема послідовності застосування операцій

Використавши результати досліджень даного розділу підрозділу 4.2, а саме матричні моделі операції спрощеного ковзного шифрування, одержані при розробці моделей паралельної реалізації примітивів ковзного шифрування, можемо стверджувати, що криптопримітиви багаторазового спрощеного ковзного шифрування (4.7), (4.10), (4.13), (4.16), (4.19), (4.22) теж реалізуються матричними моделями.

Так, зокрема, триразове спрощене ковзне шифрування, що описане моделлю (4.13) записується у вигляді матричної моделі як:

$$M^3 = \begin{pmatrix} x_1; \\ x_1 \oplus x_2; \\ x_2 \oplus x_3; \\ x_3 \oplus x_4; \\ x_1 \oplus x_4 \oplus x_5; \\ x_1 \oplus x_2 \oplus x_5 \oplus x_6; \\ x_2 \oplus x_3 \oplus x_6 \oplus x_7; \\ x_3 \oplus x_4 \oplus x_7 \oplus x_8; \\ x_1 \oplus x_4 \oplus x_5 \oplus x_8 \oplus x_9; \\ x_1 \oplus x_2 \oplus x_5 \oplus x_6 \oplus x_9 \oplus x_{10}; \\ x_2 \oplus x_3 \oplus x_6 \oplus x_7 \oplus x_{10} \oplus x_{11}; \\ \ldots\ldots\ldots\ldots \end{pmatrix}. \qquad (4.69)$$

Чотириразове спрощене ковзне шифрування (4.16) записується у вигляді матричної моделі як:

$$M^4 = \begin{pmatrix} x_1; \\ x_2; \\ x_3; \\ x_4; \\ x_1 \oplus x_5; \\ x_2 \oplus x_6; \\ x_3 \oplus x_7; \\ x_4 \oplus x_8; \\ x_1 \oplus x_5 \oplus x_9; \\ x_2 \oplus x_6 \oplus x_{10}; \\ x_3 \oplus x_7 \oplus x_{11}; \\ . \ . \ . \ . \ . \ . \ . \end{pmatrix}. \qquad (4.70)$$

Тоді п'ятикратне спрощене ковзне шифрування (4.19) запишеться як:

$$M^5 = \begin{pmatrix} x_1; \\ x_1 \oplus x_2; \\ x_1 \oplus x_2 \oplus x_3; \\ x_1 \oplus x_2 \oplus x_3 \oplus x_4; \\ x_2 \oplus x_3 \oplus x_4 \oplus x_5; \\ x_3 \oplus x_4 \oplus x_5 \oplus x_6; \\ x_4 \oplus x_5 \oplus x_6 \oplus x_7; \\ x_5 \oplus x_6 \oplus x_7 \oplus x_8; \\ x_1 \oplus x_6 \oplus x_7 \oplus x_8 \oplus x_9; \\ x_1 \oplus x_2 \oplus x_7 \oplus x_8 \oplus x_9 \oplus x_{10}; \\ x_1 \oplus x_2 \oplus x_3 \oplus x_8 \oplus x_9 \oplus x_{10} \oplus x_{11}; \\ x_1 \oplus x_2 \oplus x_3 \oplus x_4 \oplus x_9 \oplus x_{10} \oplus x_{11} \oplus x_{12}; \\ . \ . \ . \ . \ . \ . \ . \end{pmatrix}. \qquad (4.71)$$

Шестиразове спрощене ковзне шифрування (4.22) описується наступною матричною моделлю:

$$M^{6}=\begin{pmatrix} x_1; \\ x_2; \\ x_1 \oplus x_3; \\ x_2 \oplus x_4; \\ x_3 \oplus x_5; \\ x_4 \oplus x_6; \\ x_5 \oplus x_7; \\ x_6 \oplus x_8; \\ x_1 \oplus x_7 \oplus x_9; \\ x_2 \oplus x_8 \oplus x_{10}; \\ x_1 \oplus x_3 \oplus x_9 \oplus x_{11}; \\ x_2 \oplus x_4 \oplus x_{10} \oplus x_{12}; \\ x_3 \oplus x_5 \oplus x_{11} \oplus x_{13}; \\ x_4 \oplus x_6 \oplus x_{12} \oplus x_{14}; \\ . \ . \ . \ . \ . \ . \ . \ . \end{pmatrix}. \quad (4.72)$$

Зважаючи на вище зазначене, доведено що операцію багаторазового застосування криптопримітиву ковзного щифрування можливо записувати операцією матричного криптографічного перетворення (4.69-4.72).

4.6 Метод заміни операцій комп'ютерного криптографічного перетворення матричною операцією

Враховуючи попередні дослідження, справедливо записати, що багатократне застосування примітиву ковзного шифрування та процедуру перестановки можливо записати однією матричною операцією криптографічного перетворення, тому що обидві процедури описуються матричними моделями, тобто:

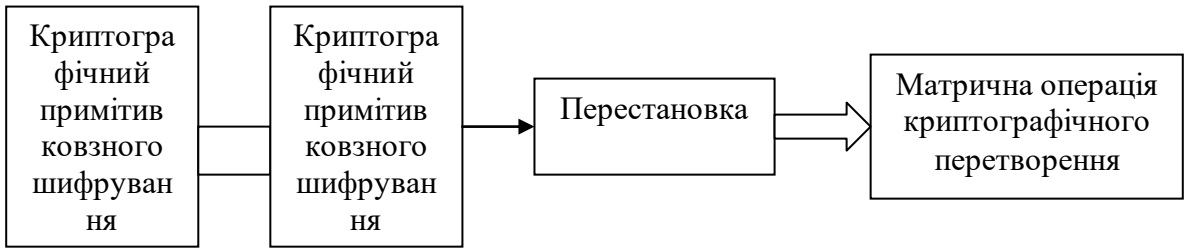
$$[M^{*}]\times[M_{перестановок}]=[O_{crypto}], \quad (4.73)$$

де $[O_{crypto}]$ - операція матричного криптографічного перетворення.

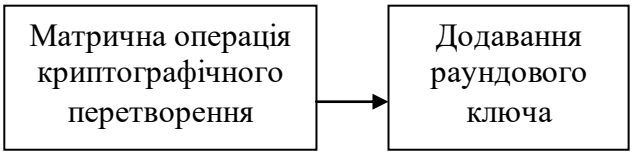
Звідси формальна модель процесу перетворення інформації для першого випадку може бути спрощена шляхом скорочення кількості операцій та описана як:

$$F(x) = [O_{crypto}] \oplus \begin{bmatrix} R_1 \\ R_2 \\ . \\ . \\ . \\ R_L \end{bmatrix}, \qquad (4.74)$$

де $[O_{crypto}]$ - операція матричного криптографічного перетворення, R_i – це раундовий ключ.



а) Структурна схема заміни послідовності застосування операцій матричною операцією



б) Спрощена структурна схема послідовності застосування операцій

Рис. 4.13. Структурні схеми застосування операцій

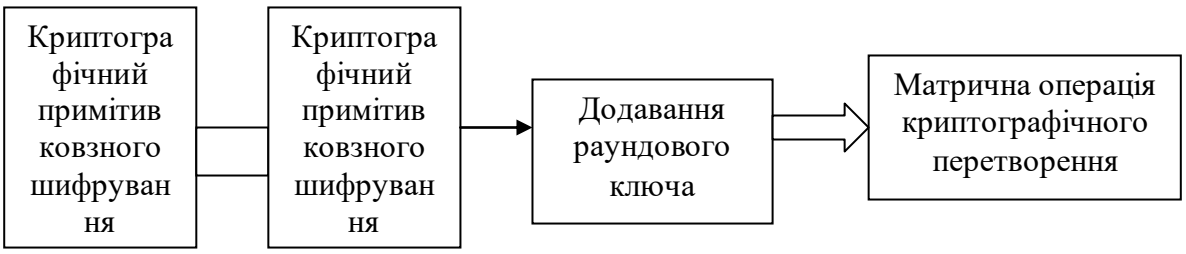
Крім цього, раніше в розділі доведено, що операція матричного криптографічного перетворення може реалізувати криптопримітив ковзного

шифрування багаторазового застосування з доданим до нього раундовим ключем, тобто:

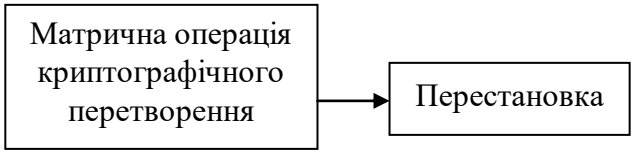
$$[M^*] \oplus \begin{bmatrix} R_1 \\ R_2 \\ . \\ . \\ . \\ R_L \end{bmatrix} = [O_{crypto}]. \qquad (4.75)$$

Звідси формальна модель процедури перетворення для другого випадку описується у скороченому виді:

$$F(x) = [O_{crypto}] \times [M_{перестановок}]. \qquad (4.76)$$



а) Структурна схема заміни послідовності застосування операцій матричною операцією



б) Спрощена структурна схема послідовності застосування операцій

Рисунок 4.14. Структурні схеми застосування операцій

Так як діють (4.73) та (4.75), тоді справедливо:

$$[M^{*}]\times[M_{перестановок}]\oplus\begin{bmatrix}R_1\\R_2\\\cdot\\\cdot\\\cdot\\R_L\end{bmatrix}=[O_{crypto}]. \qquad (4.77)$$

Звідси формальну модель для третього випадку можливо спростити до виду:

$$F(x)=[O_{crypto}]\times[M_{перестановок}]. \qquad (4.78)$$

Так як реалізація процедури перестановки для матричної операції $[O_{crypto}]$ теж описується матричною моделлю, тоді формальну модель для третього випадку можливо записати лише операцією матричного криптографічного перетворення:

$$F(x)=[O_{crypto}].$$

Оскільки доведено, що синтезовані нами операції криптографічного перетворення можуть реалізовувати багатократне застосування криптографічного примітиву ковзного шифрування із врахуванням перестановки та додаванням раундового ключа, то всі запропоновані основні випадки застосування примітиву ковзного шифрування можливо реалізувати за допомогою операції матричного криптографічного перетворення [14], тобто:

$$F(x) = [O_{crypto}] = \vec{F} = \begin{pmatrix} a_{11}x_1 \oplus a_{12}x_2 \oplus ... \oplus a_{1n}x_n \oplus b_1 \\ a_{21}x_1 \oplus a_{22}x_2 \oplus ... \oplus a_{2n}x_n \oplus b_2 \\ . \quad . \quad . \quad . \quad . \quad . \quad . \quad . \quad . \quad . \quad . \\ a_{n1}x_1 \oplus a_{n2}x_2 \oplus ... \oplus a_{n\,n}x_n \oplus b_n \end{pmatrix}.$$

А це дає змогу скоротити час реалізації перетворення інформації шляхом зменшення кількості процедур, що потрібно виконати згідного заданого алгоритму.

4.7 Висновки до четвертого розділу

Удосконалено методи побудови криптографічних примітивів на прикладі примітивів ковзного шифрування на основі матричних операцій криптографічного перетворення та отриманих узагальнених рекурентних послідовностей для побудови моделей шляхом їх паралельної реалізації, що забезпечило підвищення швидкості шифрування до 2 разів та стійкості до лінійного крипто аналізу.

1. Здійснено розробку моделей матричних операцій криптографічного перетворення для реалізації багаторазового застосування примітиву ковзного шифрування на основі отриманих рекурентних послідовностей з метою підвищення швидкості виконання шифрування за рахунок паралельної реалізації даного криптопримітиву та скорочення кількості елементарних операцій, що виконуються послідовно при його реалізації.

2. Розроблено оптимізовану модель процесу багаторазового застосування примітиву ковзного шифрування на основі операції матричного криптографічного перетворення, застосування якої при синтезі алгоритмів дозволяє отримати виграш у часі реалізації перетворення елементів примітива ковзного шифрування за рахунок використання операції матричного криптографічного перетворення замість багаторазового використання примітиву ковзного шифрування. Використання матричних операцій криптографічного перетворення для реалізації

оптимізованої моделі примітиву ковзного шифрування дозволяє збільшити його швидкодію до 2 разів.

3. Запропоновано вдосконалений спосіб багаторазового застосування примітива ковзного шифрування, суть якого полягає у доведенні адекватності реалізації багатократного застосування криптографічного примітиву ковзного шифрування із врахуванням перестановки та додаванням раундового ключа операцією матричного криптографічного перетворення.

Результати розділу опубліковані в [1-3, 29, 32, 36].

РОЗДІЛ 5
МОДЕЛЮВАННЯ ДВОХОПЕРАНДНИХ МАТРИЧНИХ ОПЕРАЦІЙ ДЛЯ МАТРИЧНИХ МОДЕЛЕЙ КРИПТОГРАФІЧНОГО ПЕРЕТВОРЕННЯ

5.1 Синтез і аналіз операцій криптографічного додавання на основі операцій матричного криптографічного перетворення

5.1.1 Синтез і аналіз операцій криптографічного додавання за модулем два на основі операцій матричного криптографічного перетворення

Основною задачею, що підлягає рішенню, є збільшення об’ємів інформації, що обробляється функціями криптографічного перетворення. Саме тому особливу увагу приділено технології виконання матричної операції криптографічного перетворення великої розмірності за допомогою формування на її основі декількох матричних операцій меншої розмірності з подальшою можливістю застосування даної технології для розробки криптоалгоритмів.

Основою функції криптографічного перетворення є базова операція. Тому для вирішення сформульованої проблеми необхідно провести синтез та дослідження множини операцій двохрозрядного криптографічного додавання за модулем два з точністю до перестановки, обґрунтувати можливість застосування виявленої групи операцій в якості операції криптографічного додавання за модулем два.

Отримані результати наукових досліджень в [9] підтверджують, що складність виконання матричних операцій криптографічного перетворення напряму залежить від кількості операндів. Тому одним із варіантів рішення даної проблеми є можливість подання матричної операції великої розмірності у вигляді декількох операцій меншої розмірності, які виконуватимуться набагато швидше, тому що їх складність в рази менша.

Проведемо синтез групи операцій двохрозрядного криптографічного додавання за модулем два та провести аналіз щодо придатності її використання в алгоритмах криптографічного перетворення.

Операцію двохрозрядного криптографічного додавання за модулем два можна представити як $F_{\mathrm{mod}2} = \begin{vmatrix} x_1 \oplus y_1 \\ x_2 \oplus y_2 \end{vmatrix}$, де x_i, $y_i \in \{0,1\}$ – розряди інформації відповідно, $i \in \{1,2\}$, $\oplus$ – операція додавання за модулем два.

Виходячи з наведеної моделі операції, можна побудувати групу аналогічних операцій з точністю до перестановки. Результати синтезу даних операцій наведені в табл. 5.1, де F_i – i-та операція криптографічного додавання, $i \in \{1..24\}$. Оскільки дана операція має 4 операнди, то $i = 4! = 1 \cdot 2 \cdot 3 \cdot 4 = 24$.

Для проведення подальшого аналізу синтезованих операцій доцільно ввести нумерацію операцій, яка необхідна для спрощення дослідження результатів синтезу [29].

Таблиця 5.1

Множина операцій

Модель операції	Модель операції	Модель операції	Модель операції
$F_1 = \begin{vmatrix} x_1 \oplus y_1 \\ x_2 \oplus y_2 \end{vmatrix}$	$F_2 = \begin{vmatrix} x_1 \oplus y_2 \\ x_2 \oplus y_1 \end{vmatrix}$	$F_3 = \begin{vmatrix} x_2 \oplus y_1 \\ x_1 \oplus y_2 \end{vmatrix}$	$F_4 = \begin{vmatrix} x_2 \oplus y_2 \\ x_1 \oplus y_1 \end{vmatrix}$
$F_5 = \begin{vmatrix} x_1 \oplus x_2 \\ y_1 \oplus y_2 \end{vmatrix}$	$F_6 = \begin{vmatrix} x_1 \oplus y_2 \\ y_1 \oplus x_2 \end{vmatrix}$	$F_7 = \begin{vmatrix} y_1 \oplus x_2 \\ x_1 \oplus y_2 \end{vmatrix}$	$F_8 = \begin{vmatrix} y_1 \oplus y_2 \\ x_1 \oplus x_2 \end{vmatrix}$
$F_9 = \begin{vmatrix} x_1 \oplus x_2 \\ y_2 \oplus y_1 \end{vmatrix}$	$F_{10} = \begin{vmatrix} x_1 \oplus y_1 \\ y_2 \oplus x_2 \end{vmatrix}$	$F_{11} = \begin{vmatrix} y_2 \oplus x_2 \\ x_1 \oplus y_1 \end{vmatrix}$	$F_{12} = \begin{vmatrix} y_2 \oplus y_1 \\ x_1 \oplus x_2 \end{vmatrix}$
$F_{13} = \begin{vmatrix} y_1 \oplus x_1 \\ x_2 \oplus y_2 \end{vmatrix}$	$F_{14} = \begin{vmatrix} y_1 \oplus y_2 \\ x_2 \oplus x_1 \end{vmatrix}$	$F_{15} = \begin{vmatrix} x_2 \oplus x_1 \\ y_1 \oplus y_2 \end{vmatrix}$	$F_{16} = \begin{vmatrix} x_2 \oplus y_2 \\ y_1 \oplus x_1 \end{vmatrix}$
$F_{17} = \begin{vmatrix} x_2 \oplus x_1 \\ y_2 \oplus y_1 \end{vmatrix}$	$F_{18} = \begin{vmatrix} x_2 \oplus y_1 \\ y_2 \oplus x_1 \end{vmatrix}$	$F_{19} = \begin{vmatrix} y_2 \oplus y_1 \\ x_2 \oplus x_1 \end{vmatrix}$	$F_{20} = \begin{vmatrix} y_2 \oplus x_1 \\ x_2 \oplus y_1 \end{vmatrix}$
$F_{21} = \begin{vmatrix} y_1 \oplus x_1 \\ y_2 \oplus x_2 \end{vmatrix}$	$F_{22} = \begin{vmatrix} y_1 \oplus x_2 \\ y_2 \oplus x_1 \end{vmatrix}$	$F_{23} = \begin{vmatrix} y_2 \oplus x_1 \\ y_1 \oplus x_2 \end{vmatrix}$	$F_{24} = \begin{vmatrix} y_2 \oplus x_2 \\ y_1 \oplus x_1 \end{vmatrix}$

Оскільки представлені в табл. 5.1 операції можуть розглядатися як одна операція з точністю до перестановки, то вони зберігають усі властивості операції двохрозрядного криптографічного додавання за модулем два та відрізняються лише результатами їх виконання.

Оскільки операція двохрозрядного криптографічного додавання за модулем два є базовою для багатьох функцій перетворення, що застосовуються в криптографічних алгоритмах, то можемо запропонувати замінити її на будь-яку іншу операцію із тих, що отримані в результаті синтезу (табл. 5.1).

У той же час, можемо констатувати, що синтезована множина операцій характеризується надлишковістю, адже в ній присутні операції, які володіють властивістю комутативності. Тому виникає потреба у скороченні кількості операцій, що утворюють множину операцій двохрозрядного криптографічного додавання за модулем два.

Це можливо за рахунок виявлення та викреслення таких операцій, що мають властивість комутативності [182], тобто $x \oplus y = c$, $y \oplus x = c$, звідси $x \oplus y = y \oplus x$. А це означає, що результат застосування двох різних операцій однаковий.

Провівши аналіз отриманої множини операцій, виявлено такі комутативні пари операцій табл. 5.2 [29].

Таблиця 5.2

Комутативні моделі операцій

Відповідні пари моделей операцій		
$F_6 \cong F_2$	$F_{13} \cong F_1$	$F_{19} \cong F_8$
$F_7 \cong F_3$	$F_{14} \cong F_8$	$F_{20} \cong F_2$
$F_9 \cong F_5$	$F_{15} \cong F_5$	$F_{21} \cong F_1$
$F_{10} \cong F_1$	$F_{16} \cong F_4$	$F_{22} \cong F_3$
$F_{11} \cong F_4$	$F_{17} \cong F_5$	$F_{23} \cong F_2$
$F_{12} \cong F_8$	$F_{18} \cong F_3$	$F_{24} \cong F_4$

Скоротивши кількість синтезованих операцій, отримаємо основні операції групи, які наведені в табл. 5.3 [29].

Таблиця 5.3

Основні операції

Модель операції
$F_1 = \begin{vmatrix} x_1 \oplus y_1 \\ x_2 \oplus y_2 \end{vmatrix}$
$F_2 = \begin{vmatrix} x_1 \oplus y_1 \\ x_2 \oplus y_2 \end{vmatrix}$
$F_3 = \begin{vmatrix} x_2 \oplus y_1 \\ x_1 \oplus y_2 \end{vmatrix}$
$F_4 = \begin{vmatrix} x_2 \oplus y_2 \\ x_1 \oplus y_1 \end{vmatrix}$
$F_5 = \begin{vmatrix} x_1 \oplus x_2 \\ y_1 \oplus y_2 \end{vmatrix}$

Дві системи лінійних рівнянь називаються еквівалентними, якщо довільний розв'язок однієї з них є розв'язком іншої та навпаки. Тобто, якщо вони мають одну і ту ж саму множину розв'язків. Очевидно, що поняття еквівалентності володіє властивістю симетричності, тобто якщо A~B, то B~A [182].

У ході дослідження основних операцій групи (табл. 5.3), встановлено, що використання еквівалентних систем (операцій) призводить до перестановки результатів шифрування в криптографії, тому вони можуть використовуватися при розробці криптографічних алгоритмів.

Крім цього, операція F_5 не придатна для застосування у матричних операціях криптографічного перетворення, тому що її застосування призведе до втрати інформації.

Аналіз властивостей операцій в табл. 5.1 показав, що з 24 синтезованих операцій лише перші 5 відрізняються результатами свого виконання, всі інші повторюють їх результати.

У результаті дослідження встановлено, що множину операцій двохрозрядного криптографічного додавання за модулем два, що придатна для практичного використання, розширено на три операції.

Здійснивши аналіз синтезованих на основі перестановок операцій і за допомогою знаходження комутативних операцій, виділили в якості основних 4 операції двохрозрядного криптографічного додавання за модулем два. Оскільки отримана множина операцій є групою перестановок G_4, то дана група має точно такі властивості, як і додавання за модулем два. Тому отримана в дослідженні група операцій двохрозрядного криптографічного додавання за модулем два може розширити кількість операцій, що застосовуються у блокових та потокових шифрах.

5.1.2 Синтез і аналіз операцій криптографічного додавання за модулем чотири на основі операцій матричного криптографічного перетворення

Особливістю побудови матричних операцій є застосування функцій криптографічного перетворення, синтезованих на основі додавання за модулем два. Перспективним напрямком досліджень з даної тематики можна вважати синтез і дослідження множини операцій за модулем, які можуть бути застосовані в якості операцій криптографічного перетворення.

Арифметичні операції за модулем широко застосовуються у сучасних симетричних блокових шифрах [14, 16]. Головним недоліком таких криптоалгоритмів є використання фіксованого відомого значення модуля, що призводить до зниження криптографічної стійкості алгоритму. Одним з варіантів вирішення даної задачі в [15] запропоновано використання набору значень модулів, які формуються на основі секретного ключа. Причому значення модуля може змінюватися в залежності від значення блоку даних і обиратися з певного діапазону [14, 15].

Сучасний етап розвитку систем захисту інформації характеризується вдосконаленням існуючих та розробкою нових криптоалгоритмів, примітиви яких базуються на використанні арифметичних операцій з різними модулями [14-16]. Однак дослідженням з ефективного вибору основи модуля або поєднанню операцій з різними модуля не приділялася достатня увага.

У [20, 29, 51, 52] запропоновано застосовувати матричні операції криптографічного перетворення та криптопримітиви, побудовані на основі їх, для алгоритмів захисту інформаційних ресурсів.

У [51, 52] доведено, що застосування матричних операцій криптографічного перетворення підвищує швидкодію обробки даних в криптосистемах за рахунок паралельного процесу виконання операції криптоперетворення.

У [29] наведені результати обчислювальних експериментів, які підтверджують, що операції за модулем можна використовувати для здійснення криптографічного перетворення в матричних операціях. Проведено дослідження матричних операцій криптографічного перетворення, синтезованих на основі операції додавання за модулем. Показано зміну властивостей результатів криптографічного перетворення залежно від вибору різної основи модуля. Згідно з отриманими результатами запропоновано способи та рекомендації щодо застосування матричних операцій криптографічного перетворення на основі додавання за модулем для підвищення криптостійкості алгоритму шифрування інформації [29].

Отже, потрібно виявити і дослідити групи операцій, що придатні для використання в алгоритмах криптографічного перетворення.

Для цього необхідно провести синтез і дослідження множини двохоперандних операцій криптографічного перетворення з точністю до перестановки, обґрунтувати можливість застосування виявлених груп операцій в системах захисту інформації.

У криптографічних системах використовуються арифметичні операції за модулем. Найпоширенішими операціями вважаються операція множення та додавання за модулем два, чотири, шістдесят чотири і двісті п’ятдесят шість [14-16, 20].

Дослідимо більш детально операцію двохоперандного додавання за модулем два.

У табл. 5.4 представлені результати моделювання даної операції, при чому k, x – інформаційні входи, тобто два двохрозрядні операнди , а y – інформаційний вихід, тобто результат виконання операції.

У табл. 5.4 також наведені матричні операції перетворення, що є перетвореннями другого операнда x залежно від значення першого операнда k. Моделі матричної операції в залежності від значення операнда позначено як F_k. Оскільки операнд k – двохрозрядний ($n = 2$), то він має (2^n) 4 набори різних значень, відповідно і $F_k = \{F_{00}, F_{01}, F_{10}, F_{11}\}$, де k – значення операнда у двійковій системі числення. В останньому рядку табл. 5.4 подана узагальнена модель операції двохоперандного додавання за модулем два, що позначена як $F_{mod\,2}$.

Таблиця 5.4

Матричне додавання за модулем два

k		**x**		**y**		**Модель матричної операції**
1	**2**	**1**	**2**	**1**	**2**	
0	0	0	0	0	0	$F_{00} = \begin{bmatrix} x_1 \\ x_2 \end{bmatrix} \oplus \begin{bmatrix} 0 \\ 0 \end{bmatrix}$
0	0	0	1	0	1	
0	0	1	0	1	0	
0	0	1	1	1	1	
0	1	0	0	0	1	$F_{01} = \begin{bmatrix} x_1 \\ x_2 \end{bmatrix} \oplus \begin{bmatrix} 0 \\ 1 \end{bmatrix}$
0	1	0	1	0	0	
0	1	1	0	1	1	
0	1	1	1	1	0	
1	0	0	0	1	0	$F_{10} = \begin{bmatrix} x_1 \\ x_2 \end{bmatrix} \oplus \begin{bmatrix} 1 \\ 0 \end{bmatrix}$
1	0	0	1	1	1	
1	0	1	0	0	0	
1	0	1	1	0	1	
1	1	0	0	1	1	$F_{11} = \begin{bmatrix} x_1 \\ x_2 \end{bmatrix} \oplus \begin{bmatrix} 1 \\ 1 \end{bmatrix}$
1	1	0	1	1	0	
1	1	1	0	0	1	
1	1	1	1	0	0	
Узагальнена модель						$F_{mod\,2} = \begin{bmatrix} x_1 \\ x_2 \end{bmatrix} \oplus \begin{bmatrix} k_1 \\ k_2 \end{bmatrix}$

Узагальнена модель матричної операції двохоперандного криптографічного додавання за модулем два може бути представлена як

$$F_{\text{mod}2} = \begin{cases} \begin{bmatrix} x_1 \\ x_2 \end{bmatrix}, \ якщо\, k_1 = 0;\ k_2 =;0 \\ \begin{bmatrix} x_1 \\ x_2 \oplus 1 \end{bmatrix}, якщо\, k_1 = 0;\ k_2 = 1; \\ \begin{bmatrix} x_1 \oplus 1 \\ x_2 \end{bmatrix}, якщо\, k_1 = 1;\ k_2 = 0; \\ \begin{bmatrix} x_1 \oplus 1 \\ x_2 \oplus 1 \end{bmatrix}, якщо\, k_1 = 1;\ k_2 = 1. \end{cases},$$

де $x_i, k_i \in \{0,1\},\ i \in \{1,2\}$ – перший та другий двохрозрядні операнди відповідно, $\oplus$ – операція додавання за модулем два.

Дослідимо більш детально операцію двохоперандного додавання за модулем чотири [45, 52].

У табл. 5.5 представлені результати моделювання даної операції, при чому, k, x – інформаційні входи, тобто два двохрозрядних операнди, а y – інформаційний вихід, тобто результат виконання операції.

У табл. 5.5 також наведені матричні операції, суть яких становить перетворення другого операнда x залежно від значення першого операнда k. В останньому рядку табл. 5.5 наведена узагальнена модель операції двохоперандного додавання за модулем чотири позначена як $F_{mod\,4}$.

Таблиця 5.5

Матричне додавання за модулем чотири

k		**x**		**y**		**Модель матричної операції**
1	**2**	**1**	**2**	**1**	**2**	
0	0	0	0	0	0	$F_{00} = \begin{bmatrix} x_1 \\ x_2 \end{bmatrix} \oplus \begin{bmatrix} 0 \\ 0 \end{bmatrix}$
0	0	0	1	0	1	
0	0	1	0	1	0	
0	0	1	1	1	1	
0	1	0	0	0	1	$F_{01} = \begin{bmatrix} x_1 \oplus x_2 \\ x_2 \end{bmatrix} \oplus \begin{bmatrix} 0 \\ 1 \end{bmatrix}$
0	1	0	1	1	0	
0	1	1	0	1	1	
0	1	1	1	0	0	
1	0	0	0	1	0	$F_{10} = \begin{bmatrix} x_1 \\ x_2 \end{bmatrix} \oplus \begin{bmatrix} 1 \\ 0 \end{bmatrix}$
1	0	0	1	1	1	
1	0	1	0	0	0	
1	0	1	1	0	1	
1	1	0	0	1	1	$F_{11} = \begin{bmatrix} x_1 \oplus x_2 \\ x_2 \end{bmatrix} \oplus \begin{bmatrix} 1 \\ 1 \end{bmatrix}$
1	1	0	1	0	0	
1	1	1	0	0	1	
1	1	1	1	1	0	
Узагальнена модель						$F_{\text{mod}4} = \begin{bmatrix} x_1 \oplus k_2 \cdot x_2 \\ x_2 \end{bmatrix} \oplus \begin{bmatrix} k_1 \\ k_2 \end{bmatrix}$

Узагальнену модель матричної операції двохоперандного криптографічного додавання за модулем чотири можна представити як:

$$F_{\text{mod}\,4} = \begin{cases} \begin{bmatrix} x_1 \\ x_2 \end{bmatrix}, \ якщо\, k_1 = 0;\ k_2 = 0 \\ \begin{bmatrix} x_1 \oplus x_2 \\ x_2 \oplus 1 \end{bmatrix}, якщо\, k_1 = 0;\ k_2 = 1 \\ \begin{bmatrix} x_1 \oplus 1 \\ x_2 \end{bmatrix}, якщо\, k_1 = 1;\ k_2 = 0 \\ \begin{bmatrix} x_1 \oplus x_2 \oplus 1 \\ x_2 \oplus 1 \end{bmatrix}, якщо\, k_1 = 1;\ k_2 = 1 \end{cases},$$

де $x_i, k_i \in \{0,1\}$, $i \in \{1,2\}$ – перший та другий двохрозрядні операнди відповідно, $\oplus$ – операція додаваня за модулем два.

5.2 Моделювання двохоперандних операцій криптографічного перетворення інформації

З'ясуємо, чи можливо побудувати ще якісь операції аналогічні додаванню за модулем, крім досліджених операцій криптографічного додавання.

Відомо, що, якщо такі операції існують, то вони повинні мати такі властивості [78]:

$$\begin{aligned} &A@B=C \\ &B@A=C \\ &A@C=B \\ &C@A=B \\ &B@C=A \\ &C@B=A, \end{aligned} \qquad (5.1)$$

де @ – позначення операції.

Проведемо моделювання двохоперандних операцій, які відповідають властивостям (5.1) та можуть використовуватися для розробки криптоалгоритмів.

При проведенні дослідження обмежимося двохрозрядними операціями.

Оскільки шукані операції можуть бути представлені таблично, то на основі аналізу таблиці подання (представлення) операцій (табл. 5.6) може бути розроблений алгоритм побудови операцій криптографічного перетворення, суть якого полягає в наступному.

Для того, щоб операція відповідала виразу (5.1), необхідно виконання наступних умов:

1. У кожному стовпці матриці перетворення не повинно бути повтору команди (значення операнда);

2. У кожному рядку матриці перетворення не повинно бути повтору значення операнда (команди);

3. Матриця повинна бути симетрична відносно головної діагоналі, тобто має виконуватися рівність $A[i, j] = A[j, i]$.

Слід зазначити, що в табл. 5.6 значення операндів представлені в десятковій системі числення.

Таблиця 5.6

Варіанти табличного представления операцій

Значення операнда 1	**Значення операнда 2**				**Значення операнда 2**				**Значення операнда 2**			
	0	**1**	**2**	**3**	**0**	**1**	**2**	**3**	**0**	**1**	**2**	**3**
0	0	1	2	3	0	1	2	3	0	1	2	3
1	1	0	3	2	1	3	0	2	1	0	3	2
2	2	3	1	0	2	0	3	1	2	3	0	1
3	3	2	0	1	3	2	1	0	3	2	1	0

Проведемо обчислювальний експеримент для отримання двохоперандних операцій.

Вихідними (початковими) даними для експерименту повинні бути двохрозрядні операції матричного криптографічного перетворення. Повна множина даних операцій містить 24 операції і наведена в табл. 5.7, де X – вхід, Y – вихід прямого перетворення, значення яких відповідають значенням рядків табл. 5.6 і представлені в десятковій системі числення. Операції в табл. 5.6 пронумеровані для забезпечення відповідності вихідних(початкових) даних, які використовуватимуться в обчислювальному експерименті, з результатами моделювання.

У процесі експерименту необхідно на основі перебору можливих варіантів поєднання матричних операцій отримати таблиці операцій криптографічного перетворення, які відповідають вимогам згідно виразу (5.1) [52].

Таблиця 5.7

Двохрозрядні операції матричного перетворення

Номер операції	Модель операції		X	Y
	Пряме перетворення	Обернене перетворення		
1	$F=\begin{bmatrix}x_1\\x_2\end{bmatrix}\oplus\begin{bmatrix}0\\0\end{bmatrix}$	$F=\begin{bmatrix}x_1\\x_2\end{bmatrix}\oplus\begin{bmatrix}0\\0\end{bmatrix}$	**0**	**0**
			1	**1**
			2	**2**
			3	**3**
2	$F=\begin{bmatrix}x_1\oplus x_2\\x_2\end{bmatrix}\oplus\begin{bmatrix}0\\0\end{bmatrix}$	$F=\begin{bmatrix}x_1\oplus x_2\\x_2\end{bmatrix}\oplus\begin{bmatrix}0\\0\end{bmatrix}$	**0**	**0**
			1	**3**
			2	**2**
			3	**1**
3	$F=\begin{bmatrix}x_1\\x_1\oplus x_2\end{bmatrix}\oplus\begin{bmatrix}0\\0\end{bmatrix}$	$F=\begin{bmatrix}x_1\\x_1\oplus x_2\end{bmatrix}\oplus\begin{bmatrix}0\\0\end{bmatrix}$	**0**	**0**
			1	**1**
			2	**3**
			3	**2**
4	$F=\begin{bmatrix}x_2\\x_1\end{bmatrix}\oplus\begin{bmatrix}0\\0\end{bmatrix}$	$F=\begin{bmatrix}x_2\\x_1\end{bmatrix}\oplus\begin{bmatrix}0\\0\end{bmatrix}$	**0**	**0**
			1	**2**
			2	**1**
			3	**3**
5	$F=\begin{bmatrix}x_2\\x_1\oplus x_2\end{bmatrix}\oplus\begin{bmatrix}0\\0\end{bmatrix}$	$F=\begin{bmatrix}x_1\oplus x_2\\x_1\end{bmatrix}\oplus\begin{bmatrix}0\\0\end{bmatrix}$	**0**	**0**
			1	**3**
			2	**1**
			3	**2**
6	$F=\begin{bmatrix}x_1\oplus x_2\\x_1\end{bmatrix}\oplus\begin{bmatrix}0\\0\end{bmatrix}$	$F=\begin{bmatrix}x_2\\x_1\oplus x_2\end{bmatrix}\oplus\begin{bmatrix}0\\0\end{bmatrix}$	**0**	**0**
			1	**2**
			2	**3**
			3	**1**
7	$F=\begin{bmatrix}x_1\\x_2\end{bmatrix}\oplus\begin{bmatrix}0\\1\end{bmatrix}$	$F=\begin{bmatrix}x_1\\x_2\end{bmatrix}\oplus\begin{bmatrix}0\\1\end{bmatrix}$	**0**	**1**
			1	**0**
			2	**3**
			3	**2**
8	$F=\begin{bmatrix}x_1\oplus x_2\\x_2\end{bmatrix}\oplus\begin{bmatrix}0\\1\end{bmatrix}$	$F=\begin{bmatrix}x_2\\x_1\oplus x_2\end{bmatrix}\oplus\begin{bmatrix}1\\1\end{bmatrix}$	**0**	**1**
			1	**2**
			2	**3**
			3	**0**
9	$F=\begin{bmatrix}x_1\\x_1\oplus x_2\end{bmatrix}\oplus\begin{bmatrix}0\\1\end{bmatrix}$	$F=\begin{bmatrix}x_1\\x_1\oplus x_2\end{bmatrix}\oplus\begin{bmatrix}0\\1\end{bmatrix}$	**0**	**1**
			1	**0**
			2	**2**
			3	**3**

Продовження табл. 5.7

Номер операції	Модель операції		X	Y
	Пряме перетворення	Обернене перетворення		
10	$F=\begin{bmatrix}x_2\\x_1\end{bmatrix}\oplus\begin{bmatrix}0\\1\end{bmatrix}$	$F=\begin{bmatrix}x_2\\x_1\end{bmatrix}\oplus\begin{bmatrix}1\\0\end{bmatrix}$	**0**	**1**
			1	**3**
			2	**0**
			3	**2**
11	$F=\begin{bmatrix}x_2\\x_1\oplus x_2\end{bmatrix}\oplus\begin{bmatrix}0\\1\end{bmatrix}$	$F=\begin{bmatrix}x_1\oplus x_2\\x_1\end{bmatrix}\oplus\begin{bmatrix}1\\0\end{bmatrix}$	**0**	**1**
			1	**2**
			2	**0**
			3	**3**
12	$F=\begin{bmatrix}x_1\oplus x_2\\x_1\end{bmatrix}\oplus\begin{bmatrix}0\\1\end{bmatrix}$	$F=\begin{bmatrix}x_1\oplus x_2\\x_2\end{bmatrix}\oplus\begin{bmatrix}1\\1\end{bmatrix}$	**0**	**1**
			1	**3**
			2	**2**
			3	**0**
13	$F=\begin{bmatrix}x_1\\x_2\end{bmatrix}\oplus\begin{bmatrix}1\\0\end{bmatrix}$	$F=\begin{bmatrix}x_1\\x_2\end{bmatrix}\oplus\begin{bmatrix}1\\0\end{bmatrix}$	**0**	**2**
			1	**3**
			2	**0**
			3	**1**
14	$F=\begin{bmatrix}x_1\oplus x_2\\x_2\end{bmatrix}\oplus\begin{bmatrix}1\\0\end{bmatrix}$	$F=\begin{bmatrix}x_1\oplus x_2\\x_2\end{bmatrix}\oplus\begin{bmatrix}1\\0\end{bmatrix}$	**0**	**2**
			1	**1**
			2	**0**
			3	**3**
15	$F=\begin{bmatrix}x_1\\x_1\oplus x_2\end{bmatrix}\oplus\begin{bmatrix}1\\0\end{bmatrix}$	$F=\begin{bmatrix}x_1\\x_1\oplus x_2\end{bmatrix}\oplus\begin{bmatrix}1\\1\end{bmatrix}$	**0**	**2**
			1	**3**
			2	**1**
			3	**0**
16	$F=\begin{bmatrix}x_2\\x_1\end{bmatrix}\oplus\begin{bmatrix}1\\0\end{bmatrix}$	$F=\begin{bmatrix}x_2\\x_1\end{bmatrix}\oplus\begin{bmatrix}0\\1\end{bmatrix}$	**0**	**2**
			1	**0**
			2	**3**
			3	**1**
17	$F=\begin{bmatrix}x_2\\x_1\oplus x_2\end{bmatrix}\oplus\begin{bmatrix}1\\0\end{bmatrix}$	$F=\begin{bmatrix}x_1\oplus x_2\\x_1\end{bmatrix}\oplus\begin{bmatrix}1\\1\end{bmatrix}$	**0**	**2**
			1	**1**
			2	**3**
			3	**0**
18	$F=\begin{bmatrix}x_1\oplus x_2\\x_1\end{bmatrix}\oplus\begin{bmatrix}1\\0\end{bmatrix}$	$F=\begin{bmatrix}x_2\\x_1\oplus x_2\end{bmatrix}\oplus\begin{bmatrix}0\\1\end{bmatrix}$	**0**	**2**
			1	**0**
			2	**1**
			3	**3**
19	$F=\begin{bmatrix}x_1\\x_2\end{bmatrix}\oplus\begin{bmatrix}1\\1\end{bmatrix}$	$F=\begin{bmatrix}x_1\\x_2\end{bmatrix}\oplus\begin{bmatrix}1\\1\end{bmatrix}$	**0**	**3**
			1	**2**
			2	**1**
			3	**0**

Продовження табл. 5.7

Номер операції	Модель операції		X	Y
	Пряме перетворення	Обернене перетворення		
20	$F=\begin{bmatrix} x_1 \oplus x_2 \\ x_2 \end{bmatrix} \oplus \begin{bmatrix} 1 \\ 1 \end{bmatrix}$	$F=\begin{bmatrix} x_1 \oplus x_2 \\ x_2 \end{bmatrix} \oplus \begin{bmatrix} 0 \\ 1 \end{bmatrix}$	**0**	**3**
			1	**0**
			2	**1**
			3	**2**
21	$F=\begin{bmatrix} x_1 \\ x_1 \oplus x_2 \end{bmatrix} \oplus \begin{bmatrix} 1 \\ 1 \end{bmatrix}$	$F=\begin{bmatrix} x_1 \\ x_1 \oplus x_2 \end{bmatrix} \oplus \begin{bmatrix} 1 \\ 0 \end{bmatrix}$	**0**	**3**
			1	**2**
			2	**0**
			3	**1**
22	$F=\begin{bmatrix} x_2 \\ x_1 \end{bmatrix} \oplus \begin{bmatrix} 1 \\ 1 \end{bmatrix}$	$F=\begin{bmatrix} x_2 \\ x_1 \end{bmatrix} \oplus \begin{bmatrix} 1 \\ 1 \end{bmatrix}$	**0**	**3**
			1	**1**
			2	**2**
			3	**0**
23	$F=\begin{bmatrix} x_2 \\ x_1 \oplus x_2 \end{bmatrix} \oplus \begin{bmatrix} 1 \\ 1 \end{bmatrix}$	$F=\begin{bmatrix} x_1 \oplus x_2 \\ x_1 \end{bmatrix} \oplus \begin{bmatrix} 0 \\ 1 \end{bmatrix}$	**0**	**3**
			1	**0**
			2	**2**
			3	**1**
24	$F=\begin{bmatrix} x_1 \oplus x_2 \\ x_1 \end{bmatrix} \oplus \begin{bmatrix} 1 \\ 1 \end{bmatrix}$	$F=\begin{bmatrix} x_2 \\ x_1 \oplus x_2 \end{bmatrix} \oplus \begin{bmatrix} 1 \\ 0 \end{bmatrix}$	**0**	**3**
			1	**1**
			2	**0**
			3	**2**

При проведенні дослідження обмежимося лише симетричними операціями криптографічного перетворення, тобто таким операціями, для яких пряме і обернене перетворення збігаються (табл. 5.7).

У результаті проведеного експерименту нами отримані операції криптографічного перетворення, які наведені в табл. 5.8.

Розглянемо більш детально результати моделювання, представивши їх математичними моделями [52].

Операція <1, 7, 13, 19> матиме вигляд:

$$O_{1,7,13,19} = \begin{cases} \begin{bmatrix} x_1 \\ x_2 \end{bmatrix}, \ якщо\ k_1 = 0;\ k_2 = 0 \\ \begin{bmatrix} x_1 \\ x_2 \oplus 1 \end{bmatrix}, якщо\ k_1 = 0;\ k_2 = 1 \\ \begin{bmatrix} x_1 \oplus 1 \\ x_2 \end{bmatrix}, \ якщо\ k_1 = 1;\ k_2 = 0 \\ \begin{bmatrix} x_1 \oplus 1 \\ x_2 \oplus 1 \end{bmatrix}, якщо\ k_1 = 1;\ k_2 = 1 \end{cases}$$

Таблиця 5.8

Результати моделювання операцій над двома операндами

Набори матричних операцій			
<1, 7, 13, 19> **<7, 1, 19, 13>** **<13, 19, 1, 7>** **<19, 13, 7, 1>**	**<1, 7, 15, 21>** **<7, 1, 21, 15>** **<15, 21, 7, 1>** **<21, 15, 1, 7>**	**<1, 8, 13, 20>** **<8, 13, 20, 1>** **<13, 20, 1, 8>** **<20, 1, 8, 13>**	**<1, 10, 16, 19>** **<10, 19, 1, 16>** **<16, 1, 19, 10>** **<19, 16, 10, 1>**
<2, 19, 14, 7> **<7, 2, 19, 14>** **<14, 7, 2, 19>** **<19, 14, 7, 2>**	**<2, 20, 14, 8>** **<8, 14, 20, 2>** **<14, 8, 2, 20>** **<20, 2, 8, 14>**	**<2, 20, 17, 11>** **<11, 17, 2, 20>** **<17, 11, 20, 2>** **<20, 2, 11, 17>**	**<2, 24, 18, 8>** **<8, 18, 24, 2>** **<18, 2, 8, 24>** **<24, 8, 2, 18>**
<3, 9, 19, 13> **<9, 3, 13, 19>** **<13, 19, 3, 9>** **<19, 13, 9, 3>**	**<3, 9, 21, 15>** **<9, 3, 15, 21>** **<15, 21, 9, 3>** **<21, 15, 3, 9>**	**<3, 11, 23, 15>** **<11, 15, 3, 23>** **<15, 23, 11, 3>** **<23, 3, 15, 11>**	**<3, 12, 21, 18>** **<12, 21, 18, 3>** **<18, 3, 12, 21>** **<21, 18, 3, 12>**
<4, 13, 7, 22> **<7, 4, 22, 13>** **<13, 22, 4, 7>** **<22, 7, 13, 4>**	**<4, 16, 10, 22>** **<10, 22, 4, 16>** **<16, 4, 22, 10>** **<22, 10, 16, 4>**	**<4, 16, 12, 24>** **<12, 24, 16, 4>** **<16, 4, 24, 12>** **<24, 12, 4, 16>**	**<4, 17, 10, 23>** **<10, 23, 4, 17>** **<17, 10, 23, 4>** **<23, 4, 17, 10>**
<5, 21, 9, 17> **<9, 5, 17, 21>** **<17, 9, 21, 5>** **<21, 17, 5, 9>**	**<5, 22, 11, 16>** **<11, 16, 5, 22>** **<16, 5, 22, 11>** **<22, 11, 16, 5>**	**<5, 23, 8, 14>** **<8, 14, 23, 5>** **<14, 8, 5, 23>** **<23, 5, 14, 8>**	**<5, 23, 11, 17>** **<11, 17, 5, 23>** **<17, 11, 23, 5>** **<23, 5, 17, 11>**
<6, 14, 20, 12> **<12, 20, 14, 6>** **<14, 12, 6, 20>** **<20, 6, 12, 14>**	**<6, 15, 24, 9>** **<9, 6, 15, 24>** **<15, 24, 9, 6>** **<24, 9, 6, 15>**	**<6, 18, 22, 10>** **<10, 22, 6, 18>** **<18, 6, 10, 22>** **<22, 10, 18, 6>**	**<6, 18, 24, 12>** **<12, 24, 18, 6>** **<18, 6, 12, 24>** **<24, 12, 6, 18>**

Операція <2, 20, 17, 11> матиме вигляд:

$$O_{2,20,17,11} = \begin{cases} \begin{bmatrix} x_1 \oplus x_2 \\ x_2 \end{bmatrix}, \text{ якщо } k_1 = 0;\ k_2 = 0 \\ \begin{bmatrix} x_1 \oplus x_2 \oplus 1 \\ x_2 \oplus 1 \end{bmatrix}, \text{ якщо } k_1 = 0;\ k_2 = 1 \\ \begin{bmatrix} x_2 \oplus 1 \\ x_1 \oplus x_2 \end{bmatrix}, \text{ якщо } k_1 = 1;\ k_2 = 0 \\ \begin{bmatrix} x_2 \\ x_1 \oplus x_2 \oplus 1 \end{bmatrix}, \text{ якщо } k_1 = 1;\ k_2 = 1 \end{cases}$$

Операція <3, 9, 19, 13> запишеться як:

$$O_{3,9,19,13} = \begin{cases} \begin{bmatrix} x_1 \\ x_1 \oplus x_2 \end{bmatrix}, \text{ якщо } k_1 = 0;\ k_2 = 0 \\ \begin{bmatrix} x_1 \\ x_1 \oplus x_2 \oplus 1 \end{bmatrix}, \text{ якщо } k_1 = 0;\ k_2 = 1 \\ \begin{bmatrix} x_1 \oplus 1 \\ x_2 \oplus 1 \end{bmatrix}, \text{ якщо } k_1 = 1;\ k_2 = 0 \\ \begin{bmatrix} x_1 \oplus 1 \\ x_2 \end{bmatrix}, \text{ якщо } k_1 = 1;\ k_2 = 1 \end{cases}$$

Операція <4, 17, 10, 23> матиме вигляд:

$$O_{4,17,10,23} = \begin{cases} \begin{bmatrix} x_2 \\ x_1 \end{bmatrix}, \ якщо\, k_1 = 0;\ k_2 = 0 \\ \begin{bmatrix} x_2 \oplus 1 \\ x_1 \oplus x_2 \end{bmatrix}, якщо\, k_1 = 0;\ k_2 = 1 \\ \begin{bmatrix} x_2 \\ x_1 \oplus 1 \end{bmatrix}, \ якщо\, k_1 = 1;\ k_2 = 0 \\ \begin{bmatrix} x_2 \oplus 1 \\ x_1 \oplus x_2 \oplus 1 \end{bmatrix}, якщо\, k_1 = 1;\ k_2 = 1 \end{cases}$$

Операція <5, 22, 11, 16> запишеться як:

$$O_{5,22,11,16} = \begin{cases} \begin{bmatrix} x_2 \\ x_1 \oplus x_2 \end{bmatrix}, \ якщо\, k_1 = 0;\ k_2 = 0 \\ \begin{bmatrix} x_2 \oplus 1 \\ x_1 \oplus 1 \end{bmatrix}, якщо\, k_1 = 0;\ k_2 = 1 \\ \begin{bmatrix} x_2 \\ x_1 \oplus x_2 \oplus 1 \end{bmatrix}, \ якщо\, k_1 = 1;\ k_2 = 0 \\ \begin{bmatrix} x_2 \oplus 1 \\ x_1 \end{bmatrix}, якщо\, k_1 = 1;\ k_2 = 1 \end{cases}$$

Операція <6, 15, 24, 9> матиме вигляд:

$$O_{6,15,24,9} = \begin{cases} \begin{bmatrix} x_1 \oplus x_2 \\ x_1 \end{bmatrix}, \text{ якщо } k_1 = 0;\ k_2 = 0 \\ \begin{bmatrix} x_1 \oplus 1 \\ x_1 \oplus x_2 \end{bmatrix}, \text{ якщо } k_1 = 0;\ k_2 = 1 \\ \begin{bmatrix} x_1 \oplus x_2 \oplus 1 \\ x_1 \oplus 1 \end{bmatrix}, \text{ якщо } k_1 = 1;\ k_2 = 0 \\ \begin{bmatrix} x_1 \\ x_1 \oplus x_2 \oplus 1 \end{bmatrix}, \text{ якщо } k_1 = 1;\ k_2 = 1 \end{cases}$$

Розглянемо таблично формування операції <1, 7, 13, 19> із точністю до перестановки.

Результати побудови даних операцій наведені в табл. 5.9 [52].

Таблиця 5.9

Група операцій порозрядного додавання за модулем два

Операція	**<1, 7, 13, 19>**				**<7, 1, 19, 13>**				**<13, 19, 1, 7>**			
Значення операндів	**0**	**1**	**2**	**3**	**0**	**1**	**2**	**3**	**0**	**1**	**2**	**3**
0	0	1	2	3	1	0	3	2	2	3	0	1
1	1	0	3	2	0	1	2	3	3	2	1	0
2	2	3	0	1	3	2	1	0	0	1	2	3
3	3	2	1	0	2	3	0	1	1	0	3	2
Перестановка	**0=0, 1=1, 2=2, 3=3**				**0=1, 1=0, 2=3, 3=2**				**0=2, 1=3, 2=0, 3=1**			
Операція	**<19, 13, 7, 1>**				**<2, 20, 14, 8>**				**<8, 14, 20, 2>**			
Значення операндів	**0**	**1**	**2**	**3**	**0**	**1**	**2**	**3**	**0**	**1**	**2**	**3**
0	3	2	1	0	0	3	2	1	1	2	3	0
1	2	3	0	1	3	0	1	2	2	1	0	3
2	1	0	3	2	2	1	0	3	3	0	1	2
3	0	1	2	3	1	2	3	0	0	3	2	1
Перестановка	**0=3, 1=2, 2=1, 3=0**				**0=0, 1=3, 2=2, 3=1**				**0=1, 1=2, 2=3, 3=0**			

Продовження табл. 5.9

Операція	**<14, 8, 2, 20>**				**<20, 2, 8, 14>**				**<3, 9, 21, 15>**			
Значення операндів	**0**	**1**	**2**	**3**	**0**	**1**	**2**	**3**	**0**	**1**	**2**	**3**
0	2	1	0	3	3	0	1	2	0	1	3	2
1	1	2	3	0	0	3	2	1	1	0	2	3
2	0	3	2	1	1	2	3	0	3	2	0	1
3	3	0	1	2	2	1	0	3	2	3	1	0
Перестановка	**0=2, 1=1, 2=0, 3=3**				**0=3, 1=0, 2=1, 3=2**				**0=0, 1=1, 2=3, 3=2**			
Операція	**<9, 3, 15, 21>**				**<15, 21, 9, 3>**				**<21, 15, 3, 9>**			
Значення операндів	**0**	**1**	**2**	**3**	**0**	**1**	**2**	**3**	**0**	**1**	**2**	**3**
0	1	0	2	3	2	3	1	0	3	2	0	1
1	0	1	3	2	3	2	0	1	2	3	1	0
2	2	3	1	0	1	0	2	3	0	1	3	2
3	3	2	0	1	0	1	3	2	1	0	2	3
Перестановка	**0=1, 1=0, 2=2, 3=3**				**0=2, 1=3, 2=1, 3=0**				**0=3, 1=2, 2=0, 3=1**			
Операція	**<4, 16, 10, 22>**				**<10, 22, 4, 16>**				**<16, 4, 22, 10>**			
Значення операндів	**0**	**1**	**2**	**3**	**0**	**1**	**2**	**3**	**0**	**1**	**2**	**3**
0	0	2	1	3	1	3	0	2	2	0	3	1
1	2	0	3	1	3	1	2	0	0	2	1	3
2	1	3	0	2	0	2	1	3	3	1	2	0
3	3	1	2	0	2	0	3	1	1	3	0	2
Перестановка	**0=0, 1=2, 2=1, 3=3**				**0=1, 1=3, 2=0, 3=2**				**0=2, 1=0, 2=3, 3=1**			
Операція	**<22, 10, 16, 4>**				**<5, 23, 11, 17>**				**<11, 17, 5, 23>**			
Значення операндів	**0**	**1**	**2**	**3**	**0**	**1**	**2**	**3**	**0**	**1**	**2**	**3**
0	3	1	2	0	0	3	1	2	1	2	0	3
1	1	3	0	2	3	0	2	1	2	1	3	0
2	2	0	3	1	1	2	0	3	0	3	1	2
3	0	2	1	3	2	1	3	0	3	0	2	1
Перестановка	**0=3, 1=1, 2=2, 3=0**				**0=0, 1=3, 2=1, 3=2**				**0=1, 1=2, 2=0, 3=3**			
Операція	**<17, 11, 23, 5>**				**<23, 5, 17, 11>**				**<6, 18, 24, 12>**			
Значення операндів	**0**	**1**	**2**	**3**	**0**	**1**	**2**	**3**	**0**	**1**	**2**	**3**
0	2	1	3	0	3	0	2	1	0	2	3	1
1	1	2	0	3	0	3	1	2	2	0	1	3
2	3	0	2	1	2	1	3	0	3	1	0	2
3	0	3	1	2	1	2	0	3	1	3	2	0
Перестановка	**0=2, 1=1, 2=3, 3=0**				**0=3, 1=0, 2=2, 3=1**				**0=0, 1=2, 2=3, 3=1**			
Операція	**<12, 24, 18, 6>**				**<18, 6, 12, 24>**				**<24, 12, 6, 18>**			
Значення операндів	**0**	**1**	**2**	**3**	**0**	**1**	**2**	**3**	**0**	**1**	**2**	**3**
0	1	3	2	0	2	0	1	3	3	1	0	2
1	3	1	0	2	0	2	3	1	1	3	2	0
2	2	0	1	3	1	3	2	0	0	2	3	1
3	0	2	3	1	3	1	0	2	2	0	1	3
Перестановка	**0=1, 1=3, 2=2, 3=0**				**0=2, 1=0, 2=1, 3=3**				**0=3, 1=1, 2=0, 3=2**			

Результати моделювання операцій представлені в табл. 5.9 показали, що дана множина операцій є математичною групою.

Перевірка існування групи операцій порозрядного додавання за модулем два наведена в табл. 5.9, де показано, що будь-яка операція із сформованої групи є перестановкою операції <1, 7, 13, 19>.

Узагальнена модель пошуку операцій, які входять в групу, зображена як табл. 5.10.

Кожна операція групи операцій, сформованої на основі узагальненої моделі табл. 5.10, має властивості вихідної (початкової / основної) операції <1, 7, 13, 19> – порозрядного додавання за модулем два.

Таблиця 5.10

Узагальнена модель пошуку операцій <1, 7, 13, 19>

Основна операція	**<1, 7, 13, 19>**			
Значення операнду	**0**	**1**	**2**	**3**
0	a	b	c	d
1	b	a	d	c
2	c	d	a	b
3	d	c	b	a

Подальші дослідження операцій дозволили виділити дві групи операцій з точністю до перестановки на основі узагальнених моделей, які представлені в табл. 5.11.

Таблиця 5.11

Узагальнені моделі пошуку операцій <5, 22, 11, 16> та <1, 10, 16, 19>

Основна операція	**<5, 22, 11, 16>**				**<1, 10, 16, 19>**			
Значення операнду	**0**	**1**	**2**	**3**	**0**	**1**	**2**	**3**
0	a	d	b	c	a	b	c	d
1	d	b	c	a	b	d	a	c
2	b	c	a	d	c	a	d	b
3	c	a	d	b	d	c	b	a

Потрібно відмітити, що у табл. 5.9-5.11 значення операндів представлені в деятковій системі числення.

У табл. 5.12 наведено виявлені три групи операцій. Потрібно відмітити, що група операцій 2 (в табл 5.12) є групою операцій додавання за модулем чотири з точністю до перестановки.

Таблиця 5.12

Об'єднання операцій у групи

Група операцій 1	Група операцій 2	Група операцій 3
<1, 7, 13, 19> <7, 1, 19, 13> <13, 19, 1, 7> <19, 13, 7, 1>	<1, 8, 13, 20> <8, 13, 20, 1> <13, 20, 1, 8> <20, 1, 8, 13>	<1, 10, 16, 19> <10, 19, 1, 16> <16, 1, 19, 10> <19, 16, 10, 1>
<2, 20, 14, 8> <8, 14, 20, 2> <14, 8, 2, 20> <20, 2, 8, 14>	<2, 19, 14, 7> <7, 2, 19, 14> <14, 7, 2, 19> <19, 14, 7, 2>	<2, 24, 18, 8> <8, 18, 24, 2> <18, 2, 8, 24> <24, 8, 2, 18>
<3, 9, 21, 15> <9, 3, 15, 21> <15, 21, 9, 3> <21, 15, 3, 9>	<3, 12, 21, 18> <12, 21, 18, 3> <18, 3, 12, 21> <21, 18, 3, 12>	<3, 11, 23, 15> <11, 15, 3, 23> <15, 23, 11, 3> <23, 3, 15, 11>
<4, 16, 10, 22> <10, 22, 4, 16> <16, 4, 22, 10> <22, 10, 16, 4>	<4, 17, 10, 23> <10, 23, 4, 17> <17, 10, 23, 4> <23, 4, 17, 10>	<4, 13, 7, 22> <7, 4, 22, 13> <13, 22, 4, 7> <22, 7, 13, 4>
<5, 23, 11, 17> <11, 17, 5, 23> <17, 11, 23, 5> <23, 5, 17, 11>	<5, 22, 11, 16> <11, 16, 5, 22> <16, 5, 22, 11> <22, 11, 16, 5>	<5, 21, 9, 17> <9, 5, 17, 21> <17, 9, 21, 5> <21, 17, 5, 9>
<6, 18, 24, 12> <12, 24, 18, 6> <18, 6, 12, 24> <24, 12, 6, 18>	<6, 15, 24, 9> <9, 6, 15, 24> <15, 24, 9, 6> <24, 9, 6, 15>	<6, 14, 20, 12> <12, 20, 14, 6> <14, 12, 6, 20> <20, 6, 12, 14>

Для проведення подальших досліджень була висунута гіпотеза, що будь-яка із синтезованих операцій (табл. 5.8) може бути застосована замість операції додавання за модулем при виконанні матричних криптоперетворень. Для

виконання матричного криптографічного перетворення необхідно існування прямого та оберненого перетворення.

Операції оберненого матричного криптографічного перетворення можуть бути побудовані на основі застосування розробленого в підрозділі 2.1.5. методу синтезу матричних операцій оберненого криптографічного перетворення інформації.

Здійснимо перевірку коректності застосування інших операцій із синтезованих (табл. 5.8) для матричних операцій криптографічного перетворення [78].

Розглянемо приклад заміни операції додавання за модулем два на операцію <7, 2, 19, 14> із множини синтезованих (табл. 5.8) для випадку, коли матричні моделі прямого і оберненого криптографічного перетворення збігаються [78].

Нехай модель прямого перетворення задана матрицею:

$$F_k = \begin{bmatrix} x_1 \\ x_1 \oplus x_2 \oplus x_3 \\ x_3 \end{bmatrix}.$$

Тоді модель оберненого перетворення задана матрицею виду:

$$F_d = \begin{bmatrix} y_1 \\ y_1 \oplus y_2 \oplus y_3 \\ y_3 \end{bmatrix}.$$

Застосуємо для цієї матриці операцію <7, 2, 19, 14>, позначивши її символом «↔». Оскільки пряма і обернена операції збігаються, тоді пряме перетворення запишеться моделлю:

$$F_k = \begin{bmatrix} x_1 \\ x_1 \leftrightarrow x_2 \leftrightarrow x_3 \\ x_3 \end{bmatrix},$$

а модель оберненого перетворення як:

$$F_d = \begin{bmatrix} y_1 \\ y_1 \leftrightarrow y_2 \leftrightarrow y_3 \\ y_3 \end{bmatrix}.$$

Оскільки $x_1 = \begin{bmatrix} x_{1.1} \\ x_{1.2} \end{bmatrix}$, $x_2 = \begin{bmatrix} x_{2.1} \\ x_{2.2} \end{bmatrix}$, $x_3 = \begin{bmatrix} x_{3.1} \\ x_{3.2} \end{bmatrix}$, отже, операція прямого перетворення буде представлена:

$$\mathrm{F_k} = \begin{bmatrix} \begin{bmatrix} \mathrm{x}_{1.1} \\ \mathrm{x}_{1.2} \end{bmatrix} \\ \begin{bmatrix} \mathrm{x}_{1.1} \\ \mathrm{x}_{1.2} \end{bmatrix} \leftrightarrow \begin{bmatrix} \mathrm{x}_{2.1} \\ \mathrm{x}_{2.2} \end{bmatrix} \leftrightarrow \begin{bmatrix} \mathrm{x}_{3.1} \\ \mathrm{x}_{3.2} \end{bmatrix} \\ \begin{bmatrix} \mathrm{x}_{3.1} \\ \mathrm{x}_{3.2} \end{bmatrix} \end{bmatrix}.$$

Необхідно перевірити чи відповідає даній моделі прямого перетворення визначена модель оберненого перетворення:

$$F_d = \begin{bmatrix} \begin{bmatrix} y_{1.1} \\ y_{1.2} \end{bmatrix} \\ \begin{bmatrix} y_{1.1} \\ y_{1.2} \end{bmatrix} \leftrightarrow \begin{bmatrix} y_{2.1} \\ y_{2.2} \end{bmatrix} \leftrightarrow \begin{bmatrix} y_{3.1} \\ y_{3.2} \end{bmatrix} \\ \begin{bmatrix} y_{3.1} \\ y_{3.2} \end{bmatrix} \end{bmatrix}.$$

Приклад 1.

x_1=11	y_1=11	x_1=11
x_2=11	$y_2 = x_1 \leftrightarrow x_2 \leftrightarrow x_3$=01	$x_2 = y_1 \leftrightarrow y_2 \leftrightarrow y_3$=11
x_3=01	y_3=01	x_3=01

При обчисленні y_2 використана операція <7, 2, 19, 14> у вигляді $y_2 = x_1 \leftrightarrow x_2 \leftrightarrow x_3$. Оскільки при описі моделі даної операції використовувалися

позначення інформаційних входів як k, x, а результату операції як y, і, враховуючи те, що ця операція для двох операндів, то знаходження y_2 розбивається на 2 етапи:

1) $y_2^* = x_1 \leftrightarrow x_2$, де $k = x_1,\ x = x_2,\ y = y_2^*$;

2) $y_2 = y_2^* \leftrightarrow x_3$ де $k = y_2^*,\ x = x_3,\ y = y_2$.

Такий же підхід потрібно застосовувати і для інших наведених прикладів.

Приклад 2.

x_1=11	y_1=11	x_1=11
x_2=10	$y_2 = x_1 \leftrightarrow x_2 \leftrightarrow x_3$=01	$x_2 = y_1 \leftrightarrow y_2 \leftrightarrow y_3$=11
x_3=11	y_3=11	x_3=11

Знайдемо результат прямого перетворення:

$$y_1 = \begin{bmatrix} y_{1.1} \\ y_{1.2} \end{bmatrix} = \begin{bmatrix} x_{1.1} \\ x_{1.2} \end{bmatrix} = x_1; \qquad y_3 = \begin{bmatrix} y_{3.1} \\ y_{3.2} \end{bmatrix} = \begin{bmatrix} x_{3.1} \\ x_{3.2} \end{bmatrix} = x_3.$$

Необхідно знайти y_2.

$$\begin{bmatrix} x_{1.1} \\ x_{1.2} \end{bmatrix} \leftrightarrow \begin{bmatrix} x_{2.1} \\ x_{2.2} \end{bmatrix} \leftrightarrow \begin{bmatrix} x_{3.1} \\ x_{3.2} \end{bmatrix} = y_2.$$

$$\begin{bmatrix} x_{1.1} \\ x_{1.2} \end{bmatrix} \leftrightarrow \begin{bmatrix} x_{2.1} \\ x_{2.2} \end{bmatrix} = \begin{bmatrix} y_{2.1}^* \\ y_{2.2}^* \end{bmatrix}.$$

$$\begin{bmatrix} y_{2.1}^* \\ y_{2.2}^* \end{bmatrix} \leftrightarrow \begin{bmatrix} x_{3.1} \\ x_{3.2} \end{bmatrix} = \begin{bmatrix} y_{2.1} \\ y_{2.2} \end{bmatrix} = y_2.$$

Розглянемо другий приклад, випадок, коли матричні моделі прямого і оберненого криптографічного перетворення не збігаються, при заміні операції додавання за модулем два на іншу операцію із множини синтезованих (табл. 5.8).

Нехай модель прямого перетворення задана матрицею $F_k = \begin{bmatrix} x_1 \oplus x_2 \\ x_1 \oplus x_2 \oplus x_3 \\ x_2 \oplus x_3 \end{bmatrix}$,

а модель оберненого перетворення задана матрицею виду $F_d = \begin{bmatrix} y_2 \oplus y_3 \\ y_1 \oplus y_2 \oplus y_3 \\ y_1 \oplus y_2 \end{bmatrix}$.

Застосуємо для цієї матриці операцію <1, 8, 13, 20>, позначивши її символом «$\succ$». Тоді пряме перетворення запишеться моделлю $\mathrm{F_k} = \begin{bmatrix} \mathrm{x_1} \succ \mathrm{x_2} \\ \mathrm{x_1} \succ \mathrm{x_2} \succ \mathrm{x_3} \\ \mathrm{x_2} \succ \mathrm{x_3} \end{bmatrix}$,

а модель оберненого перетворення як $\mathrm{F_d} = \begin{bmatrix} \mathrm{y_2} \succ \mathrm{y_3} \\ \mathrm{y_1} \succ \mathrm{y_2} \succ \mathrm{y_3} \\ \mathrm{y_1} \succ \mathrm{y_2} \end{bmatrix}$.

Оскільки $x_1 = \begin{bmatrix} x_{1.1} \\ x_{1.2} \end{bmatrix}$, $x_2 = \begin{bmatrix} x_{2.1} \\ x_{2.2} \end{bmatrix}$, $x_3 = \begin{bmatrix} x_{3.1} \\ x_{3.2} \end{bmatrix}$, отже, операція прямого перетворення буде представлена моделлю

$$\mathrm{F_k} = \begin{bmatrix} \begin{bmatrix} \mathrm{x_{1.1}} \\ \mathrm{x_{1.2}} \end{bmatrix} \succ \begin{bmatrix} \mathrm{x_{2.1}} \\ \mathrm{x_{2.2}} \end{bmatrix} \\ \begin{bmatrix} \mathrm{x_{1.1}} \\ \mathrm{x_{1.2}} \end{bmatrix} \succ \begin{bmatrix} \mathrm{x_{2.1}} \\ \mathrm{x_{2.2}} \end{bmatrix} \succ \begin{bmatrix} \mathrm{x_{3.1}} \\ \mathrm{x_{3.2}} \end{bmatrix} \\ \begin{bmatrix} \mathrm{x_{2.1}} \\ \mathrm{x_{2.2}} \end{bmatrix} \succ \begin{bmatrix} \mathrm{x_{3.1}} \\ \mathrm{x_{3.2}} \end{bmatrix} \end{bmatrix}.$$

Необхідно перевірити чи відповідає даній моделі прямого перетворення визначена модель оберненого перетворення

$$F_d = \begin{bmatrix} \begin{bmatrix} y_{2.1} \\ y_{2.2} \end{bmatrix} \succ \begin{bmatrix} y_{3.1} \\ y_{3.2} \end{bmatrix} \\ \begin{bmatrix} y_{1.1} \\ y_{1.2} \end{bmatrix} \succ \begin{bmatrix} y_{2.1} \\ y_{2.2} \end{bmatrix} \succ \begin{bmatrix} y_{3.1} \\ y_{3.2} \end{bmatrix} \\ \begin{bmatrix} y_{1.1} \\ y_{1.2} \end{bmatrix} \succ \begin{bmatrix} y_{2.1} \\ y_{2.2} \end{bmatrix} \end{bmatrix}.$$

Приклад 3.

x_1=11	$y_1 = x_1 \succ x_2 = 10$	$x_1 = y_2 \succ y_3 = 11$
x_2=11	$y_2 = x_1 \succ x_2 \succ x_3 = 11$	$x_2 = y_1 \succ y_2 \succ y_3 = 01$
x_3=01	$y_3 = x_2 \succ x_3 = 00$	$x_3 = y_1 \succ y_2 = 01$

Наведені приклади показали, що не всі операції табл. 5.8 можуть бути використані в матричних криптографічних перетвореннях.

5.3 Технологія синтезу операцій для мультиопераційних матричних криптографічних примітивів

Необхідно провести моделювання коректності реалізації криптографічних перетворень із використанням синтезованих операцій (табл. 5.8) [45, 55, 56].

У результаті комп'ютерного моделювання на повній множині варіантів вихідних(початкових) даних було встановлено, що з 96 операцій тільки 16 можуть бути використані для реалізації матричного криптоперетворення.

Наведемо отримані результати комп'ютерного моделювання у вигляді табличного представлення операцій, а також їх узагальнені моделі пошуку даних операцій (табл. 5.13 , табл. 5.14) [45, 52,55].

Оскільки операції представлені в табл. 5.13 відповідають чотирьом моделям пошуку операцій з точністю до перестановки, то, слід зазначити, що вони представляють чотири групи операцій з точністю до перестановки.

Таблиця 5.13

Табличне представлення операцій

	0	**1**	**2**	**3**	**0**	**1**	**2**	**3**	**0**	**1**	**2**	**3**	**0**	**1**	**2**	**3**
	<1,7,13,19>				**<2,19,14,7>**				**<3,9,19,13>**				**<4,13,7,22>**			
0	0	1	2	3	0	3	2	1	0	1	3	2	0	2	1	3
1	1	0	3	2	3	2	1	0	1	0	2	3	2	3	0	1
2	2	3	0	1	2	1	0	3	3	2	1	0	1	0	3	2
3	3	2	1	0	1	0	3	2	2	3	0	1	3	1	2	0
	0=0, 1=1, 2=2, 3=3				**0=0, 3=3, 2=2, 1=1**				**0=0, 1=1, 3=3, 2=2**				**0=0, 2=2, 1=1, 3=3**			
	<7,1,19,13>				**<7,2,19,14>**				**<9,3,13,19>**				**<7,4,22,13>**			
0	1	0	3	2	1	0	3	2	1	0	2	3	1	0	3	2
1	0	1	2	3	0	3	2	1	0	1	3	2	0	2	1	3
2	3	2	1	0	3	2	1	0	2	3	0	1	3	1	2	0
3	2	3	0	1	2	1	0	3	3	2	1	0	2	3	1	0
	0=1, 1=0, 2=3, 3=2				**0=1, 3=0, 2=3, 1=2**				**0=1, 1=0, 3=2, 2=3**				**0=1, 2=0, 1=3, 3=2**			
	0	**1**	**2**	**3**	**0**	**1**	**2**	**3**	**0**	**1**	**2**	**3**	**0**	**1**	**2**	**3**
	<13,19,1,7>				**<14,7,2,19>**				**<13,19,3,9>**				**<13,22,4,7>**			
0	2	3	0	1	2	1	0	3	2	3	0	1	2	3	0	1
1	3	2	1	0	1	0	3	2	3	2	1	0	3	1	2	0
2	0	1	2	3	0	3	2	1	0	1	3	2	0	2	1	3
3	1	0	3	2	3	2	1	0	1	0	2	3	1	0	3	2
	0=2, 1=3, 2=0, 3=1				**0=2, 3=1, 2=0, 1=3**				**0=2, 1=3, 3=0, 2=1**				**0=2, 2=3, 1=0, 3=1**			
	<19,13,7,1>				**<19,14,7,2>**				**<19,13,9,3>**				**<22,7,13,4>**			
0	3	2	1	0	3	2	1	0	3	2	1	0	3	1	2	**0**
1	2	3	0	1	2	1	0	3	2	3	0	1	1	0	3	**2**
2	1	0	3	2	1	0	3	2	1	0	2	3	2	3	0	**1**
3	0	1	2	3	0	3	2	1	0	1	2	3	0	2	1	**3**
	0=3, 1=2, 2=1, 3=0				**0=3, 3=2, 2=1, 1=0**				**0=3, 1=2, 3=1, 2=0**				**0=3, 2=1, 1=2, 3=0**			

Таблиця 5.14

Узагальнені моделі пошуку операцій

	0	**1**	**2**	**3**	**0**	**1**	**2**	**3**	**0**	**1**	**2**	**3**	**0**	**1**	**2**	**3**
	<1,7,13,19>				**<2,19,14,7>**				**<3,9,19,13>**				**<4,13,7,22>**			
0	a	b	d	c	a	c	d	b	a	b	c	d	a	d	b	c
1	b	a	c	d	c	d	b	a	b	a	d	c	d	c	a	b
2	d	c	a	b	d	b	a	c	c	d	b	a	b	a	c	d
3	c	d	b	a	b	a	c	d	d	c	a	b	c	b	d	a

Розглянемо більш детально результати моделювання, представивши табличне подання операцій їх математичними моделями [52].

$$O_{1,7,13,19} = \begin{cases} \begin{bmatrix} x_1 \\ x_2 \end{bmatrix}, \textit{якщо} \;\; k_1 = 0; k_2 = 0 \\ \begin{bmatrix} x_1 \\ x_2 \oplus 1 \end{bmatrix}, \textit{якщо} \;\; k_1 = 0; k_2 = 1 \\ \begin{bmatrix} x_1 \oplus 1 \\ x_2 \end{bmatrix}, \textit{якщо} \;\; k_1 = 1; k_2 = 0 \\ \begin{bmatrix} x_1 \oplus 1 \\ x_2 \oplus 1 \end{bmatrix}, \textit{якщо} \;\; k_1 = 1; k_2 = 1 \end{cases}$$

$$O_{7,1,19,13} = \begin{cases} \begin{bmatrix} x_1 \\ x_2 \oplus 1 \end{bmatrix}, \textit{якщо} \;\; k_1 = 0; k_2 = 0 \\ \begin{bmatrix} x_1 \\ x_2 \end{bmatrix}, \textit{якщо} \;\; k_1 = 0; k_2 = 1 \\ \begin{bmatrix} x_1 \oplus 1 \\ x_2 \oplus 1 \end{bmatrix}, \textit{якщо} \;\; k_1 = 1; k_2 = 0 \\ \begin{bmatrix} x_1 \oplus 1 \\ x_2 \end{bmatrix}, \textit{якщо} \;\; k_1 = 1; k_2 = 1 \end{cases}$$

$$O_{13,19,1,7} = \begin{cases} \begin{bmatrix} x_1 \oplus 1 \\ x_2 \end{bmatrix}, \textit{якщо} \;\; k_1 = 0; k_2 = 0 \\ \begin{bmatrix} x_1 \oplus 1 \\ x_2 \oplus 1 \end{bmatrix}, \textit{якщо} \;\; k_1 = 0; k_2 = 1 \\ \begin{bmatrix} x_1 \\ x_2 \end{bmatrix}, \textit{якщо} \;\; k_1 = 1; k_2 = 0 \\ \begin{bmatrix} x_1 \\ x_2 \oplus 1 \end{bmatrix}, \textit{якщо} \;\; k_1 = 1; k_2 = 1 \end{cases}$$

$$O_{19,13,7,1} = \begin{cases} \begin{bmatrix} x_1 \oplus 1 \\ x_2 \oplus 1 \end{bmatrix}, \textit{якщо} \;\; k_1 = 0; k_2 = 0 \\ \begin{bmatrix} x_1 \oplus 1 \\ x_2 \end{bmatrix}, \textit{якщо} \;\; k_1 = 0; k_2 = 1 \\ \begin{bmatrix} x_1 \\ x_2 \oplus 1 \end{bmatrix}, \textit{якщо} \;\; k_1 = 1; k_2 = 0 \\ \begin{bmatrix} x_1 \\ x_2 \end{bmatrix}, \textit{якщо} \;\; k_1 = 1; k_2 = 1 \end{cases}$$

Досліджуючи отримані математичні моделі операцій, можна зробити висновок, що операції основані на моделі <1, 7, 13, 9> відрізняються наявністю чотирьох варіантів інверсії результату, які можна описати функціональними залежностями від вхідного операнда k_i, $i \in [1,2]$ як:

1. $k_1^* = k_1, \;\; k_2^* = k_2$; – основна модель;
2. $k_1^* = k_1, \;\; k_2^* = \bar{k}_2$;
3. $k_1^* = \bar{k}_1, \;\; k_2^* = k_2$;
4. $k_1^* = \bar{k}_1, \;\; k_2^* = \bar{k}_2$, де k_1, k_2 – значення розрядів першого операнда моделі, на основі якої проводиться синтез, k_1^*, k_2^* – значення розрядів першого операнда нової синтезованої моделі. Порядок розміщення перетворення другого операнда в операції залежить від значення першого операнда.

Математичні моделі операцій синтезовані на основі моделі <2, 19, 14, 7> подаються у вигляді:

$$O_{2,19,14,7} = \begin{cases} \begin{bmatrix} x_1 \oplus x_2 \\ x_2 \end{bmatrix}, якщо \;\; k_1 = 0; k_2 = 0 \\ \begin{bmatrix} x_1 \oplus 1 \\ x_2 \oplus 1 \end{bmatrix}, якщо \;\; k_1 = 0; k_2 = 1 \\ \begin{bmatrix} x_1 \oplus x_2 \oplus 1 \\ x_2 \end{bmatrix}, якщо \;\; k_1 = 1; k_2 = 0 \\ \begin{bmatrix} x_1 \\ x_2 \oplus 1 \end{bmatrix}, якщо \;\; k_1 = 1; k_2 = 1 \end{cases}$$

$$O_{7,2,19,14} = \begin{cases} \begin{bmatrix} x_1 \\ x_2 \oplus 1 \end{bmatrix}, якщо \;\; k_1 = 0; k_2 = 0 \\ \begin{bmatrix} x_1 \oplus x_2 \\ x_2 \end{bmatrix}, якщо \;\; k_1 = 0; k_2 = 1 \\ \begin{bmatrix} x_1 \oplus 1 \\ x_2 \oplus 1 \end{bmatrix}, якщо \;\; k_1 = 1; k_2 = 0 \\ \begin{bmatrix} x_1 \oplus x_2 \oplus 1 \\ x_2 \end{bmatrix}, якщо \;\; k_1 = 1; k_2 = 1 \end{cases}$$

$$O_{14,7,2,19} = \begin{cases} \begin{bmatrix} x_1 \oplus x_2 \oplus 1 \\ x_2 \end{bmatrix}, якщо \;\; k_1 = 0; k_2 = 0 \\ \begin{bmatrix} x_1 \\ x_2 \oplus 1 \end{bmatrix}, якщо \;\; k_1 = 0; k_2 = 1 \\ \begin{bmatrix} x_1 \oplus x_2 \\ x_2 \end{bmatrix}, якщо \;\; k_1 = 1; k_2 = 0 \\ \begin{bmatrix} x_1 \oplus 1 \\ x_2 \oplus 1 \end{bmatrix}, якщо \;\; k_1 = 1; k_2 = 1 \end{cases}$$

$$O_{19,14,7,2}=\begin{cases}\begin{bmatrix}x_1\oplus 1\\ x_2\oplus 1\end{bmatrix}, \textit{якщо}\ \ k_1=0;\ k_2=0\\ \begin{bmatrix}x_1\oplus x_2\oplus 1\\ x_2\end{bmatrix}, \textit{якщо}\ \ k_1=0;\ k_2=1\\ \begin{bmatrix}x_1\\ x_2\oplus 1\end{bmatrix}, \textit{якщо}\ \ k_1=1;\ k_2=0\\ \begin{bmatrix}x_1\oplus x_2\\ x_2\end{bmatrix}, \textit{якщо}\ \ k_1=1;\ k_2=1\end{cases}$$

Дослідження отриманих моделей операцій допомогло отримати правила синтезу даних операцій з урахуванням перестановок, які можна описати функціональними залежностями від вхідного операнда $k_i, i\in[1,2]$. Таким чином, синтез математичних моделей операцій, що побудовані на основі моделі <2, 19, 14, 7> полягає в наступному:

1. $k_1^*=k_1,\quad k_2^*=k_2$; – основна модель;
2. $k_1^*=\bar{k}_1,\quad k_2^*=k_2$;
3. $k_1^*=k_1\oplus k_2,\quad k_2^*=\bar{k}_2$;
4. $k_1^*=\overline{(k_1\oplus k_2)},\quad k_2^*=\bar{k}_2$.

Проведемо дослідження отриманих операцій на основі моделі <3, 9, 19, 13>, математичні моделі яких подані як:

$$O_{3,9,19,13} = \begin{cases} \begin{bmatrix} x_1 \\ x_1 \oplus x_2 \end{bmatrix}, якщо \;\; k_1 = 0; k_2 = 0 \\ \begin{bmatrix} x_1 \\ x_1 \oplus x_2 \oplus 1 \end{bmatrix}, якщо \;\; k_1 = 0; k_2 = 1 \\ \begin{bmatrix} x_1 \oplus 1 \\ x_2 \oplus 1 \end{bmatrix}, якщо \;\; k_1 = 1; k_2 = 0 \\ \begin{bmatrix} x_1 \oplus 1 \\ x_2 \end{bmatrix}, якщо \;\; k_1 = 1; k_2 = 1 \end{cases}$$

$$O_{9,3,13,19} = \begin{cases} \begin{bmatrix} x_1 \\ x_1 \oplus x_2 \oplus 1 \end{bmatrix}, якщо \;\; k_1 = 0; k_2 = 0 \\ \begin{bmatrix} x_1 \\ x_1 \oplus x_2 \end{bmatrix}, якщо \;\; k_1 = 0; k_2 = 1 \\ \begin{bmatrix} x_1 \oplus 1 \\ x_2 \end{bmatrix}, якщо \;\; k_1 = 1; k_2 = 0 \\ \begin{bmatrix} x_1 \oplus 1 \\ x_2 \oplus 1 \end{bmatrix}, якщо \;\; k_1 = 1; k_2 = 1 \end{cases}$$

$$O_{13,19,3,9} = \begin{cases} \begin{bmatrix} x_1 \oplus 1 \\ x_2 \end{bmatrix}, якщо \;\; k_1 = 0; k_2 = 0 \\ \begin{bmatrix} x_1 \oplus 1 \\ x_2 \oplus 1 \end{bmatrix}, якщо \;\; k_1 = 0; k_2 = 1 \\ \begin{bmatrix} x_1 \\ x_1 \oplus x_2 \end{bmatrix}, якщо \;\; k_1 = 1; k_2 = 0 \\ \begin{bmatrix} x_1 \\ x_1 \oplus x_2 \oplus 1 \end{bmatrix}, якщо \;\; k_1 = 1; k_2 = 1 \end{cases}$$

$$O_{19,13,9,3} = \begin{cases} \begin{bmatrix} x_1 \oplus 1 \\ x_2 \oplus 1 \end{bmatrix}, \text{якщо} \quad k_1 = 0; k_2 = 0 \\ \begin{bmatrix} x_1 \oplus 1 \\ x_2 \end{bmatrix}, \text{якщо} \quad k_1 = 0; k_2 = 1 \\ \begin{bmatrix} x_1 \\ x_1 \oplus x_2 \oplus 1 \end{bmatrix}, \text{якщо} \quad k_1 = 1; k_2 = 0 \\ \begin{bmatrix} x_1 \\ x_1 \oplus x_2 \end{bmatrix}, \text{якщо} \quad k_1 = 1; k_2 = 1 \end{cases}$$

Досліджуючи дані математичні моделі, засновані на моделі <3, 9, 19, 13>, можна зробити висновок, що ці операції можна отримати, виконавши синтез операцій на базі основної операції таким чином:

1. $k_1^* = k_1, \quad k_2^* = k_2$; – основна модель;
2. $k_1^* = k_1, \quad k_2^* = \bar{k}_2$;
3. $k_1^* = \overline{k_1}, \quad k_2^* = k_1 \oplus k_2$;
4. $k_1^* = \bar{k}_1, \; k_2^* = \overline{(k_1 \oplus k_2)}$.

Математичні моделі операцій синтезовані на основі моделі <4, 13, 7, 22> подаються у вигляді:

$$O_{4,13,7,22} = \begin{cases} \begin{bmatrix} x_2 \\ x_1 \end{bmatrix}, \text{якщо} \quad k_1 = 0; k_2 = 0 \\ \begin{bmatrix} x_1 \oplus 1 \\ x_2 \end{bmatrix}, \text{якщо} \quad k_1 = 0; k_2 = 1 \\ \begin{bmatrix} x_1 \\ x_2 \oplus 1 \end{bmatrix}, \text{якщо} \quad k_1 = 1; k_2 = 0 \\ \begin{bmatrix} x_2 \oplus 1 \\ x_1 \oplus 1 \end{bmatrix}, \text{якщо} \quad k_1 = 1; k_2 = 1 \end{cases}$$

$$O_{7,4,22,13} = \begin{cases} \begin{bmatrix} x_1 \\ x_2 \oplus 1 \end{bmatrix}, \textit{якщо} \;\; k_1 = 0; k_2 = 0 \\ \begin{bmatrix} x_2 \\ x_1 \end{bmatrix}, \textit{якщо} \;\; k_1 = 0; k_2 = 1 \\ \begin{bmatrix} x_2 \oplus 1 \\ x_1 \oplus 1 \end{bmatrix}, \textit{якщо} \;\; k_1 = 1; k_2 = 0 \\ \begin{bmatrix} x_1 \oplus 1 \\ x_2 \end{bmatrix}, \textit{якщо} \;\; k_1 = 1; k_2 = 1 \end{cases}$$

$$O_{13,22,4,7} = \begin{cases} \begin{bmatrix} x_1 \oplus 1 \\ x_2 \end{bmatrix} \textit{якщо} \;\; k_1 = 0; k_2 = 0 \\ \begin{bmatrix} x_2 \oplus 1 \\ x_1 \oplus 1 \end{bmatrix}, \textit{якщо} \;\; k_1 = 0; k_2 = 1 \\ \begin{bmatrix} x_2 \\ x_1 \end{bmatrix}, \textit{якщо} \;\; k_1 = 1; k_2 = 0 \\ \begin{bmatrix} x_1 \\ x_2 \oplus 1 \end{bmatrix}, \textit{якщо} \;\; k_1 = 1; k_2 = 1 \end{cases}$$

$$O_{22,7,13,4} = \begin{cases} \begin{bmatrix} x_2 \oplus 1 \\ x_1 \oplus 1 \end{bmatrix}, \textit{якщо} \;\; k_1 = 0; k_2 = 0 \\ \begin{bmatrix} x_1 \\ x_2 \oplus 1 \end{bmatrix}, \textit{якщо} \;\; k_1 = 0; k_2 = 1 \\ \begin{bmatrix} x_1 \oplus 1 \\ x_2 \end{bmatrix}, \textit{якщо} \;\; k_1 = 1; k_2 = 0 \\ \begin{bmatrix} x_2 \\ x_1 \end{bmatrix}, \textit{якщо} \;\; k_1 = 1; k_2 = 1 \end{cases}$$

Дослідження отриманих моделей операцій привело до наступних функціональних залежностей, які описують синтез математичних моделей операцій заснованих на моделі <4, 13, 7, 22>:

1. $k_1^* = k_1, \quad k_2^* = k_2$; – основна модель;
2. $k_1^* = k_2, \quad k_2^* = \bar{k}_1$;
3. $k_1^* = \bar{k}_2, \quad k_2^* = k_1,$;
4. $k_1^* = \bar{k}_1, \quad k_2^* = \bar{k}_2$.

Таким чином, синтезовані операції можна розділити на групи.

Множина операцій складається із 16 синтезованих операцій і ділиться на чотири групи по чотири операції в кожній.

Використання при виконанні криптоперетворень операцій, які входять в різні групи, відповідно до теореми Шеннона [171] дозволяє підвищити крипостійкість алгоритму шифрування.

Оскільки вони входять в різні групи операцій з точністю до перестановки, то повторне виконання операцій з іншої групи призводить до підвищення криптостійкості.

Розглянута технологія отримання операцій криптографічного перетворення у матричних криптографічних алгоритмах може бути застосована для побудови операцій з більшою кількістю операндів різної розрядності.

Розроблена технологія синтезу операцій може бути використана, наприклад, при реалізації криптографічних примітивів ковзного шифрування.

Мультиопераційні матричні криптографічні примітиви ковзного шифрування можуть бути отримані на основі застосування синтезованих операцій до виразів (4.63), (4.64). Даний підхід дозволяє вдосконалювати існуючі криптографічні примітиви за рахунок варіативності операцій раунду защифрування. Використання операцій, що належать різним математичним групам забезпечує підвищення криптостійкості існуючих криптографічних примітивів.

5.4 Висновки до п’ятого розділу

1. Уперше розроблено технологію синтезу операцій для мультиопераційних матричних криптографічних примітивів на основі побудови нових груп операцій з точністю до перестановки шляхом використання запропонованої табличної моделі операції криптоперетворення, що дозволило за рахунок варіативності операцій підвищити криптостійкість існуючих криптопримітивів.

2. Моделювання операцій криптографічного додавання за модулем два та чотири на основі використання матричних операцій забезпечило побудову групи операцій криптоперетворення з точністю до перестановки. Дані операції можуть бути застосовані для підвищення теоретичної та практичної стійкості криптографічних алгоритмів за рахунок збільшення довжини ключової послідовності та алгоритмічної складності.

3. Вперше розроблено модель двохоперандної операції криптоперетворення на основі табличного представлення, яка забезпечила можливість проведення обчислювального експерименту для пошуку комутативних та некомутативних криптографічних операцій.

4. Розроблено технологію синтезу двохоперандних матричних операцій для матричних моделей криптографічного перетворення з метою розширення кількості операцій криптографічного перетворення інформації в матричних операціях криптографічного перетворення. Використання даної технології забезпечує синтез мультиопераційних матричних криптографічних примітивів.

Результати розділу опубліковані в [1, 5, 29, 50, 52, 55, 56, 65, 67].

РОЗДІЛ 6
МЕТОДИ РЕАЛІЗАЦІЇ СИНТЕЗОВАНИХ ОПЕРАЦІЙ ДЛЯ КОМП'ЮТЕРНОЇ КРИПТОГРАФІЇ ТА ОЦІНКА ЕФЕКТИВНОСТІ ЇХ ЗАСТОСУВАННЯ

6.1 Синтез криптоалгоритмів на основі операцій криптографічного перетворення інформації

6.1.1 Дослідження криптоалгоритмів на структурному рівні

Криптографічний алгоритм можливо представити як послідовність операцій криптографічного перетворення інформації $Y = f(X)$, де $f = [F_1, F_2, ..., F_n]$, тоді [5]:

$$Y = F_n(...(F_2(F_1(X)))) \quad (6.1)$$

Графічно криптографічний алгоритм зображено у загальному вигляді на рис. 6.1.

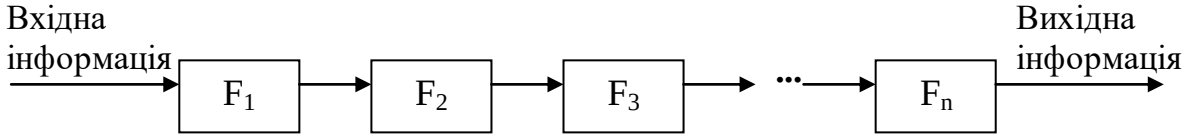


Рис. 6.1. Графічна структура криптографічного алгоритму.

Для забезпечення максимальної криптостійкості повинна виконуватися основна вимога щодо вибору операцій, а саме: будь-які дві вибрані операції, що виконуються послідовно, не належать одній групі. Наприклад: матричні операції, розширені (нелінійні) матричні операції, операції перестановки керовані інформацією та інші.

Кожна операція криптографічного перетворення $F_i(x)$ є складеною функціональною структурою, яка охоплює всю вибрану групу операцій та забезпечує реалізацію однозначно визначеної на основі ключової послідовності операції перетворення.

Структура операції перетворення криптографічного алгоритму наведена на рис. 6.2 [5].

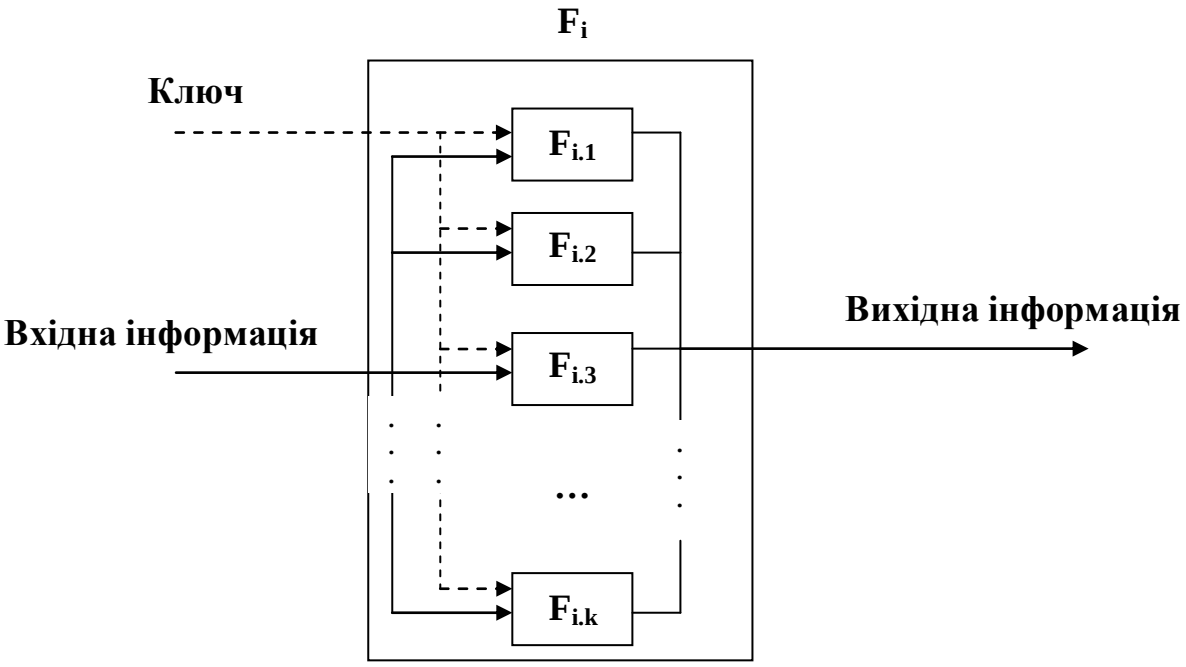


Рис. 6.2. Структура операції перетворення.

Складність реалізації будь-якої операції $F_{i.j}$ однакова, тому складність операції криптографічного перетворення дорівнює складності операції, що виконується [5]:

$$C(F_i) = C(F_{i.j}), \quad j = 1..k \ . \tag{6.2}$$

Звідси, складність криптографічного алгоритму (рис. 6.1) розраховується як сума складностей реалізації кількості операцій криптографічного перетворення, тому що виконання операцій виконується послідовно [5]:

$$C_{ALG} = \sum_{i=1}^{n} C(F_i) = \sum_{i=1}^{n} C(F_{i.j}) = C(F_{1.j}) + C(F_{2.j}) + ... + C(F_{n.j}), \qquad (6.3)$$

де $j = 1..k$, n – кількість операцій перетворення, що реалізують алгоритм криптографічного перетворення ($F_i, i = 1..n$); k – кількість операцій групи, що реалізує операцію перетворення.

Оскільки існує лише єдиний виключний випадок, коли $C(F_{1.j}) = C(F_{2.j}) = ... = C(F_{n.j})$, тоді складність алгоритму розраховуватиметься як $C_{ALG} = n \times C(F_{i.j})$.

Тобто, у загальному випадку всі операції криптографічного перетворення мають різну складність, тому діє залежність, описана в (6.3) [5].

Час виконання будь-якої операції $F_{i.j}$ однаковий, тому час виконання операції криптографічного перетворення дорівнює часу виконання однієї операції:

$$Time(F_i) = Time(F_{i.j}), \quad j = 1..k. \qquad (6.4)$$

Звідси, час виконання криптографічного алгоритму (рис. 6.1) розраховується як сума часу виконання операцій в алгоритмі криптографічного перетворення, тому що операції виконуються послідовно:

$$Time_{ALG} = \sum_{i=1}^{n} Time(F_i) = \sum_{i=1}^{n} Time(F_{i.j}) = Time(F_{1.j}) + Time(F_{2.j}) + ... + Time(F_{n.j}), \qquad (6.5)$$

де $j = 1..k$, n – кількість операцій перетворення, що реалізують алгоритм криптографічного перетворення ($F_i, i = 1..n$); k – кількість операцій групи, що реалізує операцію перетворення.

Швидкість реалізації операції перетворення обернено пропорційна часу виконання та складності.

Виходячи з цього, швидкість реалізації алгоритму визначається як:

$$V_{ALG} = \frac{1}{Time_{ALG}} = \frac{1}{Time(F_{1.j}) + Time(F_{2.j}) + ... + Time(F_{n.j})} = \frac{1}{\sum_{i=1}^{n} Time(F_{i.j})}. \quad (6.6)$$

Час виконання операції прямо пропорційний складності її реалізації, тоді

$$Time(F_i) = k_i \cdot C(F_i).$$

Визначимо час реалізації криптоалгоритму, виходячи із його складності:

$$Time_{ALG} = \sum_{i=1}^{n} k_i \cdot C(F_{i.j}) = k_1 \cdot C(F_{1.j}) + k_2 \cdot C(F_{2.j}) + ... + k_n \cdot C(F_{n.j}). \quad (6.7)$$

Враховуючи вище зазначене, швидкість виконання криптографічного алгоритму визначатиметься як:

$$V_{ALG} = \frac{1}{\sum_{i=1}^{n} k_i \cdot C(F_{i.j})} = \frac{1}{k_1 \cdot C(F_{1.j}) + k_2 \cdot C(F_{2.j}) + ... + k_n \cdot C(F_{n.j})}. \quad (6.8)$$

Криптостійкість операції F_i визначається як криптостійкість $F_{i.j}$, тому що операції, які реалізують F_i, належать одній групі. Повторне використання операції F_i не призводить до збільшення криптостійкості. Оскільки операції алгоритму не створюють єдиної математичної групи та виконуються послідовно, то криптостійкість алгоритму визначається як добуток значень криптостійкості операцій [5]:

$$K_{ALG} = \prod_{i=1}^{n} K(F_i) = \prod_{i=1}^{n} K(F_{i.j}) = K(F_{1.j}) \cdot K(F_{2.j}) \cdot \ldots \cdot K(F_{n.j}) \,. \quad (6.9)$$

Потрібно врахувати і можливість розпаралелення процесу реалізації операції криптографічного перетворення.

Структура паралельного виконання операції перетворення криптографічного алгоритму над блоком інформації наведена на рис. 6.3 [5].

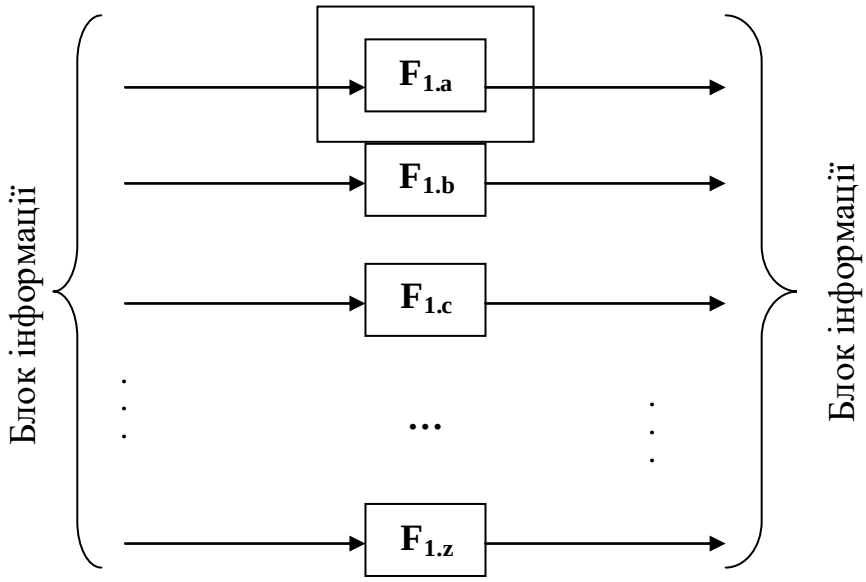


Рис. 6.3. Паралельне виконання операції перетворення блоку інформації.

Криптографічний алгоритм може складатися із операцій різної розрядності, що забезпечує підвищення криптостійкості перетворення, тому що операції, що мають різну кількість змінних належать різним групам операцій.

Крім того, при такому варіанті конструювання криптографічного алгоритму забезпечуються властивості розсіювання та перемішування, так як розряди інформації кожного із підблоків (при перетворенні блоку інформації він розбивається на під блоки згідно розрядності операцій, які будуть над ними виконуватися) будуть мати вплив на значення кінцевого результату. Структурна схема взаємозв’язків для виконання послідовності операцій, в якій кожна

наступна операція має іншу розрядність наведена на рис. 6.4. У даній структурній схемі зображені операції над 8 та 5 операндами (розрядами) [5].

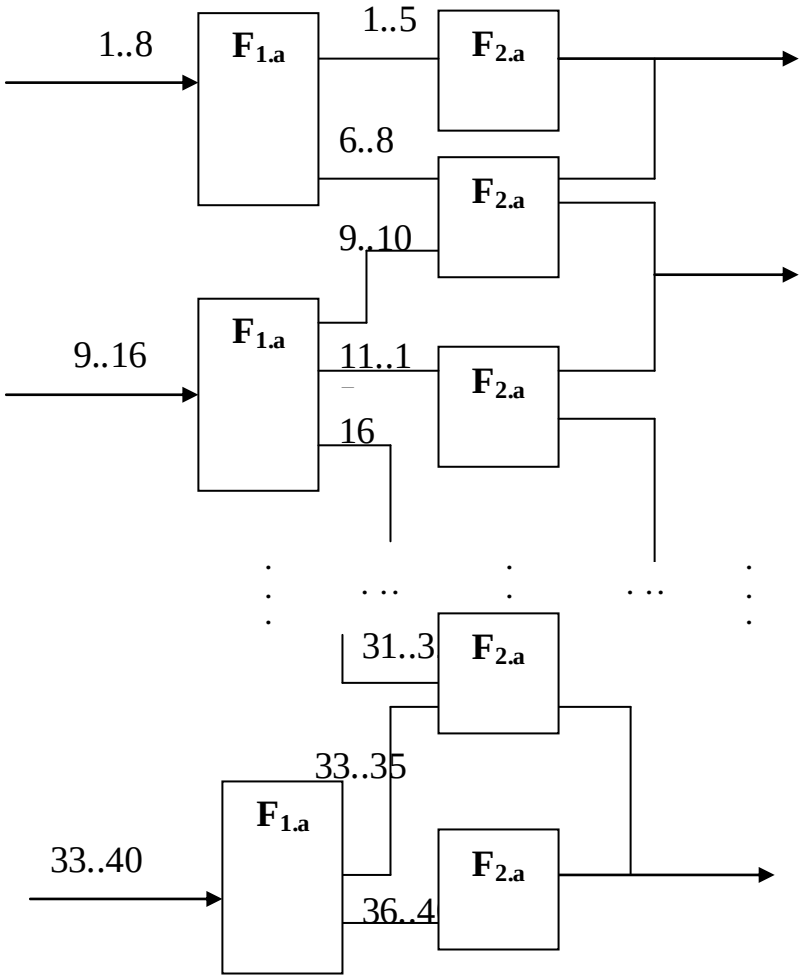


Рис. 6.4. Виконання операції різної розрядності для перетворення блоку інформації.

Вказана схема застосування операцій криптографічного перетворення функціонально може бути використана для заміни однієї операції над 40 операндами (розрядами).

Для порівняння операцій з різною кількістю операндів можна визначати їх складність та час виконання через максимально можливу кількість операндів в операції. Тоді умовна складність реалізації послідовності операцій над 8 та 5 операндами буде не більше ніж 13. А складність операції над 40 операндами

дорівнює 40. Відповідно умовний час виконання операцій будуть 13 та 40 відповідно.

У результаті проведеного дослідження було встановлено, що найефективніше здійснювати вибір кількості змінних для операцій як прості числа, що забезпечує досягнення оптимальної складності алгоритма.

Ще одним із способів застосування операцій для конструювання криптографічного алгоритму можливо вважати послідовність операцій на основі різних модулів, що теж забезпечує покращення криптографічних властивостей перетворення.

Наприклад, якщо операція криптографічного перетворення будується із елементарних функцій матричного криптографічного перетворення, які відповідно до виразу (2.9) мають вигляд:

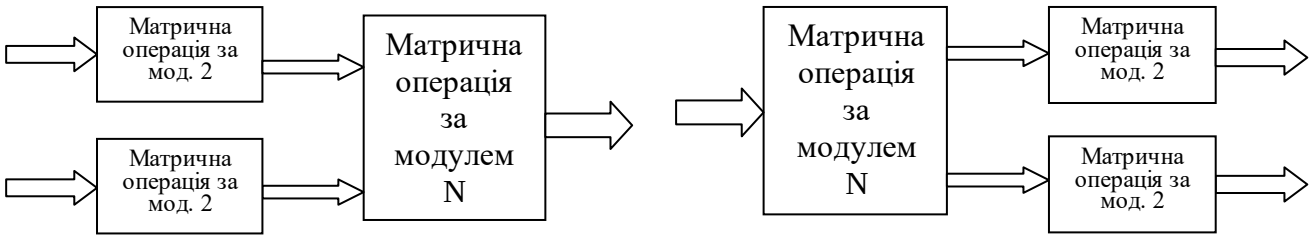
$$f = a_{i1}x_1 \oplus a_{i2}x_2 \oplus \ldots \oplus a_{in}x_n \oplus b_n, \qquad (6.10)$$

тоді реалізувати дану елементарну функцію можливо на основі послідовного поєднання операцій додавання за модулем та логічного множення кожного з доданків на значення елементів рядка матриці перетворення.

Дослідимо матричні операції криптографічного перетворення щодо зміни основи модуля та застосування комбінації таких операцій на прикладі криптопримітивів ковзного шифрування.

Як видно із проаналізованих схем шифрування (4.1)-(4.4) розділу 4 доцільніше використовувати комбінацію операцій на основі різного модуля. Застосуємо дану схему змішаного шифрування за умови використання матричних операцій криптографічного перетворення, синтезованих на основі операції додавання за модулем, де значення модулів різні. Таким чином, існує два способи застосування матричних операцій з різним модулем, коли спочатку криптографічне перетворення відбувається на базі матричної операції, синтезованої на основі суми за модулем 2, а потім застосовується матрична операція, синтезована на основі суми за модулем N та навпаки.

Тоді структурні схеми процесу реалізації криптографічного перетворення із застосуванням матричних операцій відповідно до вище зазначених способів представлені на рис. 6.5 відповідно [1].



а) 1. спосіб б) 2. спосіб

Рис. 6.5. Структурна схема реалізації матричних операцій криптографічного перетворення.

Проведемо дослідження статистичних властивостей результатів шифрування даних за вказаними схемами перетворення та визначимо ефективність застосування кожного способу.

Для цього використаємо пакет NIST STS, який містить 15 статистичних тестів та розроблені для перевірки гіпотези щодо випадковості двійкових послідовностей довільної довжини [184-186].

Для здійснення тестувань були обрані такі параметри: довжина послідовності, що тестується $n=10^6$ біт; кількість послідовностей, що тестується $m=100$; рівень значущості $\alpha=0{,}01$; кількість тестів $q=189$ [184].

Таким чином, обсяг вибірки, що тестується, склав $N=10^6\times100=10^8$ біт, кількість тестів (q) для різних довжин $q=189$. Отже, статистичний портрет ПВП містить 18900 значень імовірності P.

В ідеальному випадку при $m=100$ і $\alpha=0{,}01$ у ході тестування може бути відкинута тільки одна послідовність зі ста, тобто коефіцієнт проходження кожного тесту має складати 99%. Але це занадто жорстке правило. Тому застосовується правило на основі довірчого інтервалу. Нижня межа дорівнює 0,96015 [184].

Статистичні портрети відображають властивості випадковості результатів криптографічного перетворення на основі запропонованих способів використання матричних операцій [52, 53].

Статистичний портрет для 1-го способу зображено на рис. 6.6, а для 2-го способу – на рис. 6.7 відповідно.

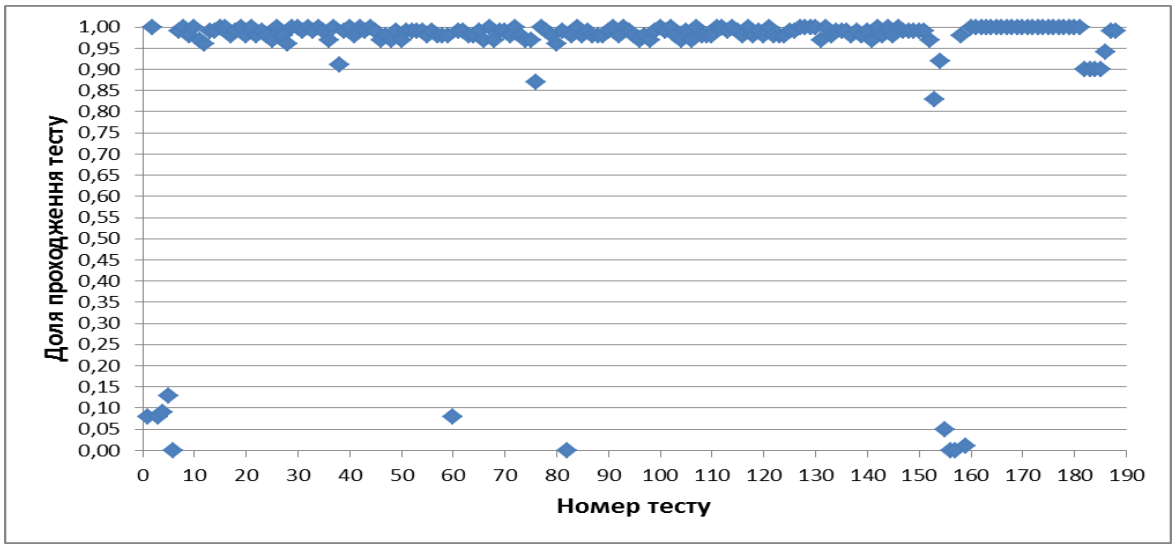


Рис. 6.6. Статистичний портрет результатів криптографічного перетворення на основі першого способу реалізації матричних операцій криптографічного перетворення на основі різних модулів

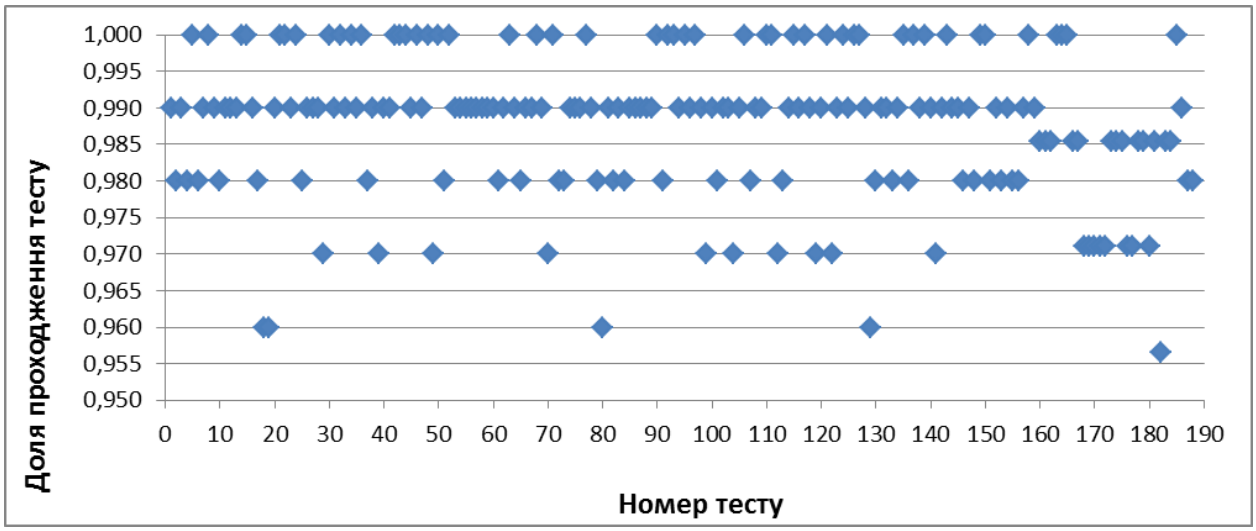


Рис. 6.7. Статистичний портрет результатів криптографічного перетворення на основі другого способу реалізації матричних операцій криптографічного перетворення на основі різних модулів

Зведені результати тестування для 1-го та 2-го способу наведено в табл. 6.1.

Проаналізувавши дані з таблиці зведених результатів (табл. 6.1), можна зробити висновок, що 2-ий спосіб ефективніший за 1-ий спосіб.

Отримані результати показують, що дані матричні операції криптографічного перетворення можливо використовувати в криптоалгоритмах [4.6].

Таблиця 6.1

Зведені результати тестування

Способи реалізації матричних операцій криптографічного перетворення	Кількість тестів, в яких тестування пройшло		Кількість тестів, в яких тестування не
	99% послід.	96% послід.	< 96% послід.
1. спосіб	103(54,5%)	65 (34,4%)	21 (11,1%)
2. спосіб	122 (64,6%)	66 (34,9%)	1 (0,5%)

При комбінованому застосуванні матричних операцій з різними значеннями модулів операції, синтезовані на основі додавання за модулем 2, потрібно використовувати в якості кінцевої операції при здійсненні криптографічного перетворення, а додавання на модулем N можливо використовувати не на завершальних етапах криптографічного перетворення.

Проведені обчислювальні експерименти дозволяють констатувати, що операції за модулем можливо використовувати для здійснення криптографічного перетворення на основі матричних операцій.

Для підвищення криптостійкості алгоритму до статистичного криптоаналізу операцію додавання за модулем 2 доцільно використовувати в якості кінцевої операції для побудови матричних операцій криптографічного перетворення.

Оскільки дані дві операції, операція додавання за модулем 2 та за будь-яким іншим 2^n модулем не утворюють математичної групи, то їх послідовне використання призводить до підвищення криптостійкості [39, 55, 56].

Рекурентні послідовності, що описані у розділі 4, дійсні для багаторазового прямого ПКШ, синтезованого на основі додавання за модулем 2. А при синтезі

прямого ПКШ можуть бути використані і інші операції, наприклад додавання за модулем 2^n. Тоді узагальнену модель рекурентної послідовності можливо записати як:

$$y_i^k = y_{i-1}^k (\nabla) y_i^{k-1},$$

де $y_0^k = y_d^{k-1}$ $i \in \{1,\ldots,d\}$, де , в свою чергу, k – кількість раундів ковзного шифрування, d – розрядність перетворення, а (∇) – двохоперандна криптографічна операція. Такі двохоперандні криптографічні операції (∇) нами розглянуті у п'ятому розділі.

Крім того, операція, яка використовується для реалізації багаторазового криптопримітиву ковзного шифрування, може змінюватися на будь-якому раунді зашифрування. Виходячи з цього, узагальнену модель рекурентної послідовності багаторазового криптопримітиву ковзного шифрування зі змінною раундовою операцією запишемо як:

$$y_i^k = y_{i-1}^k (\nabla k) y_i^{k-1},$$

де $y_0^k = y_d^{k-1}$ $i \in \{1,\ldots,d\}$, де, в свою чергу, k – кількість раундів ковзного шифрування, d – розрядність перетворення, (∇k) – двохоперандна криптографічна операція для k-го раунду.

Крім того, операція, яка використовується для реалізації багаторазового криптопримітиву ковзного шифрування, може змінюватися деяку кількість разів у самому раунді зашифрування. Максимальна кількість змінних операцій раунда визначається кількістю елементів примітиву ковзного шифрування. Тому узагальнена модель рекурентної послідовності багаторазового криптопримітиву ковзного шифрування зі змінними операціями в раунді матиме вигляд:

$$y_i^k = y_{i-1}^k (\nabla k_i) y_i^{k-1},$$

де $y_0^{k_i} = y_d^{k_i-1}$ $i \in \{1,\dots,d\}$, де, в свою чергу, k – кількість раундів ковзного шифрування, d – розрядність перетворення, (∇k_i) – двохоперандна криптографічна операція для перетворення i-того елемента для k-го раунду.

До того ж криптографічний алгоритм може здійснюватися послідовністю перетворень, кожне з яких побудоване на основі різних операцій, при цьому послідовне виконання операцій над однаковою кількістю операндів за умови використання операцій з різних математичних груп забезпечує підвищення криптостійкості.

Даний підхід до використання синтезованих операцій криптографічного перетворення дозволяє визначити макро та мікрорівень використання операцій. Наведені вище алгоритми з використанням операцій можна вважати макрорівнем.

Використання операції для реалізації іншої операції – це мікрорівень.

Графічно криптографічний алгоритм на основі різних операцій на мікрорівні зображено в загальному вигляді на рис. 6.8 [5].

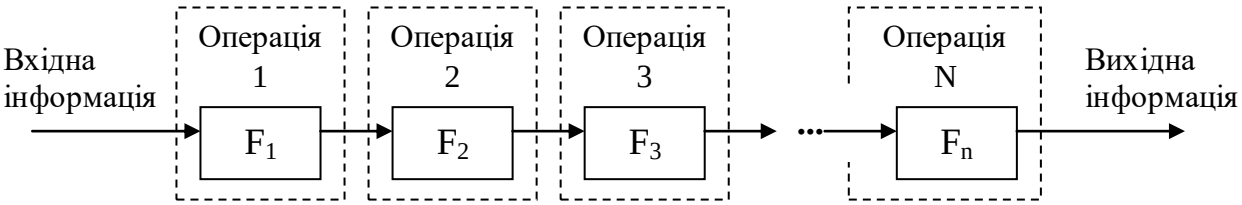


Рис. 6.8 Графічна структура криптографічного алгоритму з додатковим використання операцій на мікрорівні.

У даному алгоритму кожна операція криптографічного перетворення $F_i(x)$, що формує послідовність для виконання перетворення над інформацією, будується на основі вибраної синтезованої операції. При чому для реалізації різних операцій криптографічного перетворення $F_i(x)$ вибираються операції на мікрорівні з різних груп.

6.1.2 Дослідження способів забезпечення нелінійності перетворення матричними операціями криптоперетворення

Особливої уваги заслуговують способи та особливості використання операцій з метою забезпечення нелінійності перетворення. Для їх визначення здійснимо дослідження особливостей використання операцій криптографічного перетворення інформації. У першу чергу необхідно здійснити аналіз способів застосування матричних операцій криптографічного перетворення інформації. Потім виявити закономірності результатів проведеного аналізу та на основі них розробити рекомендації, що складатимуть основу технології використання матричних операцій для побудови криптоалгоритмів.

При перетворенні інформації на основі матричних операцій криптографічного перетворення необхідно забезпечити однозначність перетворення інформації, як під час прямого, так і зворотного перетворення.

Усі операції криптоперетворення, побудовані на основі елементарних операцій, забезпечують роботу з бітами. Проте в залежності від виду операнда матричні операції можуть реалізувати перетворення бітів інформації, байтів інформації, слів і т.д..

Проведемо аналіз властивостей перетворення інформації, що подана у бітовому та байтовому виді на основі матричних операцій. Під час проведення дослідження обмежимося матричними операціями, які в загальному виді представлені операціями криптографічного перетворення побудованими на основі додавання за модулем два та заданими виразом (2.11).

Проведемо перетворення інформації заданої в бітовому форматі, зокрема чисел від 0 до 255, на основі матричного перетворення, що описується виразом [32]:

$$\vec{F} = \begin{pmatrix} x_1 \oplus x_4 \oplus x_8 \\ x_6 \oplus x_8 \\ x_2 \oplus x_7 \\ x_1 \oplus x_7 \oplus x_8 \\ x_1 \oplus x_2 \oplus x_3 \oplus x_6 \\ x_1 \\ x_5 \oplus x_7 \\ x_1 \oplus x_4 \oplus x_6 \oplus x_7 \end{pmatrix} \qquad (6.11)$$

Результати перетворення числової інформації на основі матричної моделі (6.11) представлені в табл. 6.2, де x – початкове значення числа (до здійснення перетворення), y – одержане значення числа (після здійснення перетворення), а «$\rightarrow$» – це матрична операція задана відповідною моделлю.

Аналіз табл. 6.2 показав, що використання матричних операцій криптографічного перетворення при застосуванні інформації в бітовому форматі забезпечує виконання лінійного перетворення [32].

Логічно припустити, що властивості перетворення на основі матричної операції, що здійснюється над інформацією в байтовому представленні, також характеризуються лінійністю, адже байт є вісім бітів. Перевіримо дане припущення на прикладі.

Проведемо перетворення числової інформації заданого діапазону в байтовому форматі на основі матричного перетворення, що описується виразом:

$$\vec{F} = \begin{pmatrix} x_4 \oplus x_7 \\ x_2 \oplus x_6 \oplus x_8 \\ x_1 \oplus x_2 \oplus x_3 \\ x_2 \oplus x_5 \oplus x_6 \\ x_2 \oplus x_3 \oplus x_6 \oplus x_8 \\ x_1 \oplus x_2 \oplus x_5 \oplus x_6 \\ x_2 \oplus x_5 \oplus x_6 \oplus x_8 \\ x_2 \oplus x_5 \oplus x_6 \oplus x_7 \oplus x_8 \end{pmatrix} \qquad (6.12)$$

Таблиця 6.2

Результати перетворення чисел заданого діапазону в бітовому форматі на основі виразу (1)

x → y		x → y		x → y		x → y		x → y		x → y		x → y		x → y	
0	0	32	16	64	20	96	4	128	185	160	169	192	173	224	189
1	11	33	27	65	31	97	15	129	178	161	162	193	166	225	182
2	204	34	220	66	216	98	200	130	117	162	101	194	97	226	113
3	199	35	215	67	211	99	195	131	126	163	110	195	106	227	122
4	146	36	130	68	134	100	150	132	43	164	59	196	63	228	47
5	153	37	137	69	141	101	157	133	32	165	48	197	52	229	36
6	94	38	78	70	74	102	90	134	231	166	247	198	243	230	227
7	85	39	69	71	65	103	81	135	236	167	252	199	248	231	232
8	64	40	80	72	84	104	68	136	249	168	233	200	237	232	253
9	75	41	91	73	95	105	79	137	242	169	226	201	230	233	246
10	140	42	156	74	152	106	136	138	53	170	37	202	33	234	49
11	135	43	151	75	147	107	131	139	62	171	46	203	42	235	58
12	210	44	194	76	198	108	214	140	107	172	123	204	127	236	111
13	217	45	201	77	205	109	221	141	96	173	112	205	116	237	100
14	30	46	14	78	10	110	26	142	167	174	183	206	179	238	163
15	21	47	5	79	1	111	17	143	172	175	188	207	184	239	168
16	129	48	145	80	149	112	133	144	56	176	40	208	44	240	60
17	138	49	154	81	158	113	142	145	51	177	35	209	39	241	55
18	77	50	93	82	89	114	73	146	244	178	228	210	224	242	240
19	70	51	86	83	82	115	66	147	255	179	239	211	235	243	251
20	19	52	3	84	7	116	23	148	170	180	186	212	190	244	174
21	24	53	8	85	12	117	28	149	161	181	177	213	181	245	165
22	223	54	207	86	203	118	219	150	102	182	118	214	114	246	98
23	212	55	196	87	192	119	208	151	109	183	125	215	121	247	105
24	193	56	209	88	213	120	197	152	120	184	104	216	108	248	124
25	202	57	218	89	222	121	206	153	115	185	99	217	103	249	119
26	13	58	29	90	25	122	9	154	180	186	164	218	160	250	176
27	6	59	22	91	18	123	2	155	191	187	175	219	171	251	187
28	83	60	67	92	71	124	87	156	234	188	250	220	254	252	238
29	88	61	72	93	76	125	92	157	225	189	241	221	245	253	229
30	159	62	143	94	139	126	155	158	38	190	54	222	50	254	34
31	148	63	132	95	128	127	144	159	45	191	61	223	57	255	41

Фрагмент результатів перетворення чисел від 0 до 255 на основі моделі (6.12) представлені в табл. 6.3.

Аналіз табл. 6.3 показав, що використання матричних операцій криптографічного перетворення при застосуванні інформації в байтовому форматі забезпечує виконання нелінійного перетворення.

Таким чином, запропоноване припущення не є істинним, адже очікувані результати не співпали.

Як видно із табл. 6.2 і табл. 6.3 властивості результатів перетворення над інформацією в бітовому та байтовому виді різні. Проте результати отримані на основі матричних операцій, що задаються різними виразами, тому вважати закономірністю залежність виявленої властивості результатів перетворення від виду інформації, над якою здійснювалося дане перетворення, хоч інформація вибрана однакова, не коректно. Тому для уточнення та перевірки отриманих результатів проведемо перетворення інформації заданої в байтовому форматі, а саме 256 чисел, на основі матричного перетворення, що описується виразом (6.11).

Таблиця 6.3

Фрагмент результатів перетворення чисел заданого діапазону в байтовому форматі на основі виразу (2)

x → y		x → y		x → y		x → y		x → y		x → y		x → y		x → y	
0	5	32	5	64	5	96	5	128	5	160	5	192	5	224	5
1	4	33	36	65	68	97	100	129	132	161	164	193	196	225	228
2	4	34	36	66	68	98	100	130	132	162	164	194	196	226	228
3	7	35	39	67	71	99	103	131	135	163	167	195	199	227	231
4	1	36	1	68	1	100	1	132	1	164	1	196	1	228	1
5	0	37	0	69	0	101	0	133	0	165	0	197	0	229	0
6	7	38	7	70	7	102	7	134	7	166	7	198	7	230	7
7	6	39	38	71	70	103	102	135	134	167	166	199	198	231	230
8	5	40	5	72	5	104	5	136	5	168	5	200	5	232	5
9	12	41	44	73	76	105	108	137	140	169	172	201	204	233	236
10	12	42	44	74	76	106	108	138	140	170	172	202	204	234	236
11	15	43	47	75	79	107	111	139	143	171	175	203	207	235	239
12	1	44	1	76	1	108	1	140	1	172	1	204	1	236	1
13	0	45	0	77	0	109	0	141	0	173	0	205	0	237	0
14	7	46	7	78	7	110	7	142	7	174	7	206	7	238	7
15	14	47	46	79	78	111	110	143	142	175	174	207	206	239	238

Результати перетворення числової інформації на основі матричної моделі (6.11) представлені в табл. 6.4.

Таблиця 6.4

Результати перетворення чисел заданого діапазону в байтовому форматі на основі виразу (1)

x → y		x → y		x → y		x → y		x → y		x → y		x → y		x → y	
0	3	32	35	64	67	96	99	128	131	160	163	192	195	224	227
1	2	33	2	65	2	97	2	129	2	161	2	193	2	225	2
2	7	34	7	66	7	98	7	130	7	162	7	194	7	226	7
3	6	35	38	67	70	99	102	131	134	163	166	195	198	227	230
4	6	36	6	68	6	100	6	132	6	164	6	196	6	228	6
5	7	37	39	69	71	101	103	133	135	165	167	197	199	229	231
6	2	38	2	70	2	102	2	134	2	166	2	198	2	230	2
7	0	39	0	71	0	103	0	135	0	167	0	199	0	231	0
8	11	40	43	72	75	104	107	136	139	168	171	200	203	232	235
9	2	41	2	73	2	105	2	137	2	169	2	201	2	233	2
10	7	42	7	74	7	106	7	138	7	170	7	202	7	234	7
11	14	43	46	75	78	107	110	139	142	171	174	203	206	235	238
12	6	44	6	76	6	108	6	140	6	172	6	204	6	236	6
13	15	45	47	77	79	109	111	141	143	173	175	205	207	237	239
14	2	46	2	78	2	110	2	142	2	174	2	206	2	238	2
15	0	47	0	79	0	111	0	143	0	175	0	207	0	239	0
16	19	48	51	80	83	112	115	144	147	176	179	208	211	240	243
17	2	49	2	81	2	113	2	145	2	177	2	209	2	241	2
18	7	50	7	82	7	114	7	146	7	178	7	210	7	242	7
19	22	51	54	83	86	115	118	147	150	179	182	211	214	243	246
20	6	52	6	84	6	116	6	148	6	180	6	212	6	244	6
21	23	53	55	85	87	117	119	149	151	181	183	213	215	245	247
22	2	54	2	86	2	118	2	150	2	182	2	214	2	246	2
23	0	55	0	87	0	119	0	151	0	183	0	215	0	247	0
24	27	56	59	88	91	120	123	152	155	184	187	216	219	248	251
25	2	57	2	89	2	121	2	153	2	185	2	217	2	249	2
26	7	58	7	90	7	122	7	154	7	186	7	218	7	250	7
27	30	59	62	91	94	123	126	155	158	187	190	219	222	251	254
28	6	60	6	92	6	124	6	156	6	188	6	220	6	252	6
29	31	61	63	93	95	125	127	157	159	189	191	221	223	253	255
30	2	62	2	94	2	126	2	158	2	190	2	222	2	254	2
31	0	63	0	95	0	127	0	159	0	191	0	223	0	255	0

Аналіз табл. 6.4 показав, що отримані результати перетворення на основі матричної операції криптографічного перетворення при застосуванні інформації в байтовому форматі забезпечує виконання нелінійного перетворення.

У результаті обчислювального експерименту отримані дані (табл. 6.2) показують, що кожне конкретне число перетворюється однозначно в кожне конкретне число, тобто операція є лінійною та реалізує варіант перестановки.

Якщо провести заміну операндів матричної операції – бітів на байти, то матриці прямого та оберненого перетворення будуть одинаковими, тобто повністю співпадуть.

Проте виявилося, що при матричному криптоперетворенні байтів отримано нелінійне перетворення (табл. 6.3, 6.4), отже і матричні моделі прямого та оберненого перетворення повинні відрізнятися.

Аналіз табл. 6.2-6.4 показав, що використання матричних операцій криптографічного перетворення при використанні інформації у байтовому форматі забезпечує виконання нелінійного перетворення, а при використанні бітового формату забезпечується лінійність перетворення.

Отже, виходячи з наведених результатів, можна стверджувати, що одна і та ж сама матрична операція криптографічного перетворення може бути використана для реалізації як лінійного так і нелінійного перетворення, що забезпечує спрощення криптографічного алгоритму за рахунок зменшення кількості операцій, що використовуються для перетворення інформації, а також ускладнює криптоаналіз результатів перетворення.

6.1.3 Дослідження апаратної реалізації криптографічних операцій

Узагальнення результатів проводилося шляхом побудови функціональних схем усіх операцій в кожній групі криптоперетворення (згідно класифікації рис. 3.5) шляхом розширення розрядності операції та обєднання під єдину систему керування.

У результаті дослідження отримані наступні схемотехнічні рішення:

1) функціональна схема реалізації синтезованої групи операцій перестановки та інверсій наведена на рис. 6.9.

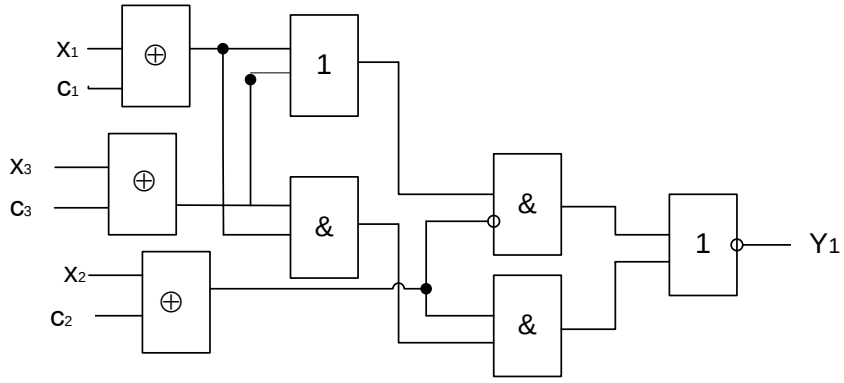


Рис. 6.9. Фунціональна схема реалізації групи операцій перестановки та інверсії

2) функціональна схема реалізації синтезованої групи операцій перестановок, керованих інформацією, наведена на рис. 6.10.

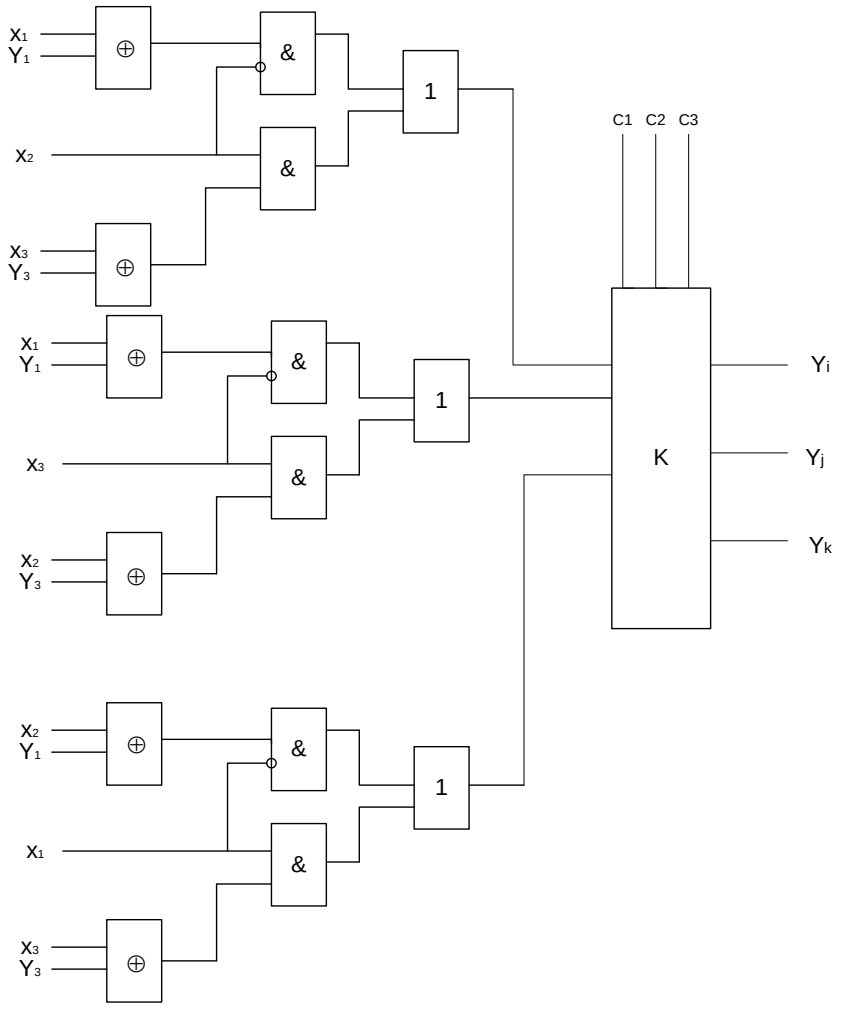


Рис. 6.10. Фунціональна схема реалізації групи операцій перестановок, керованих інформацією

3) функціональна схема реалізації синтезованої групи матричних операцій наведена на рис. 6.11.

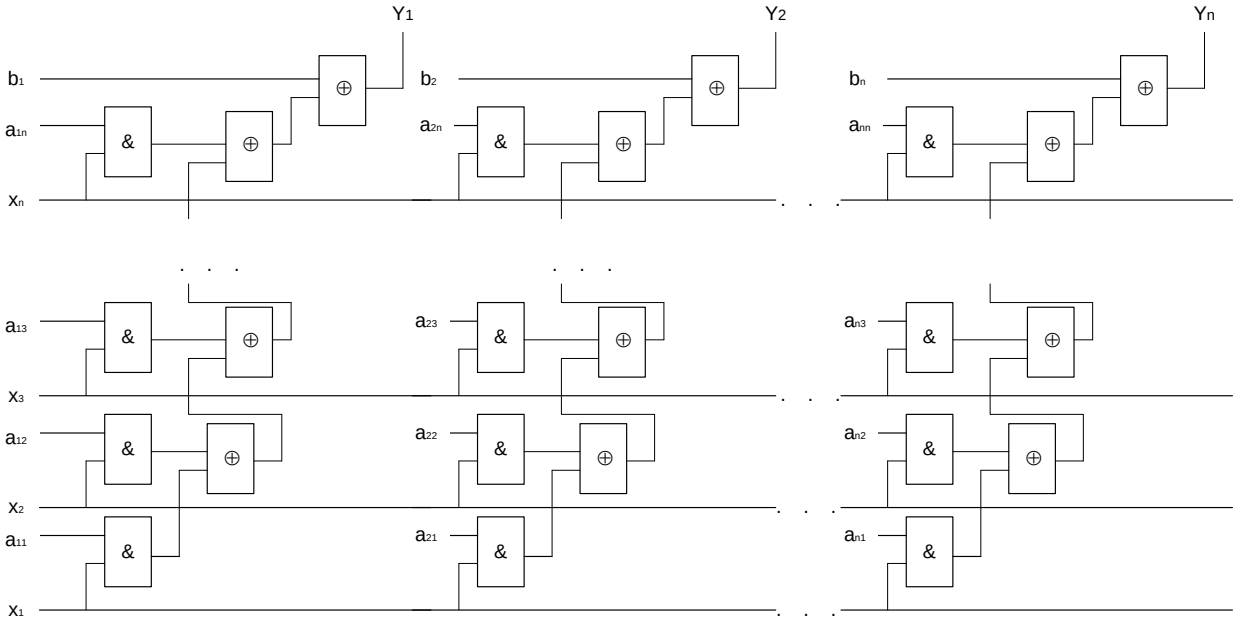


Рис. 6.11. Група матричних операцій

4) функціональна схема реалізації синтезованої групи розширених матричних операцій наведена на рис. 6.12.

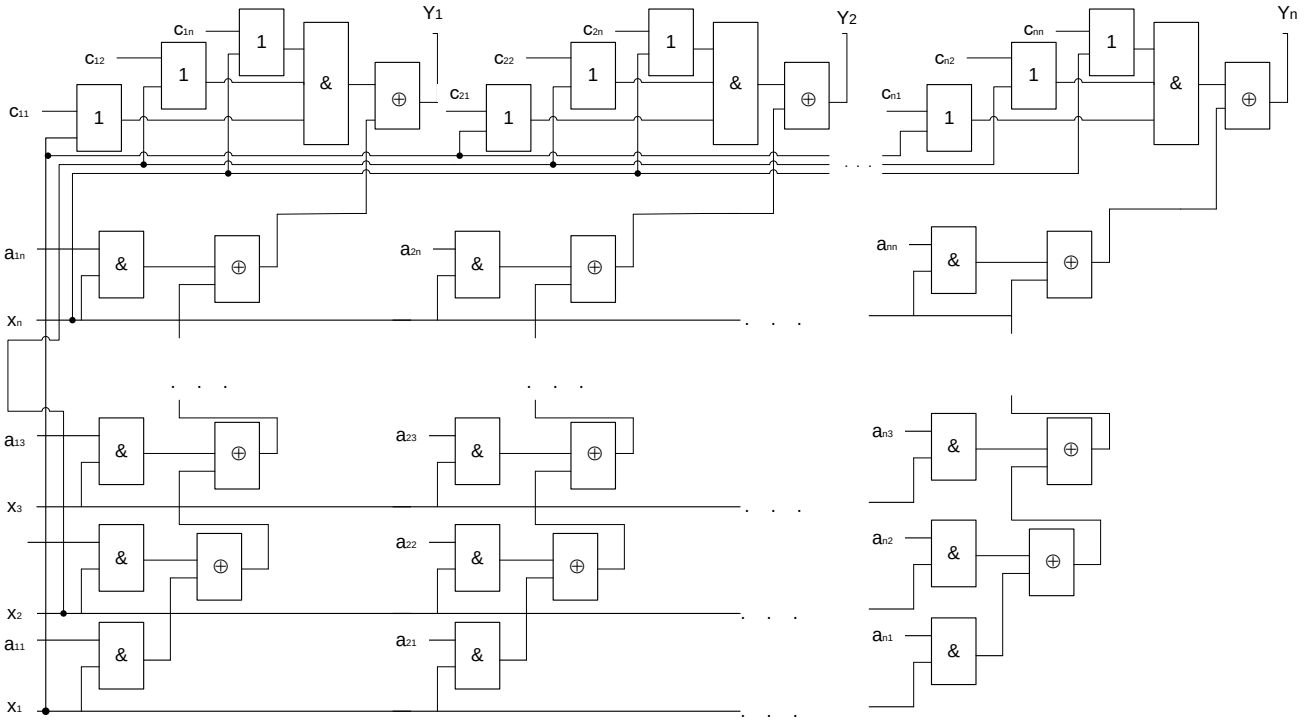


Рис. 6.12. Група розширених матричних операцій

На рис. 6.9-6.12 використані такі позначення:

x_i – вхідні операнди, $x_i \in \{0;1\}$, $i = 1..n$;

a_{ij} – сигнал вибору операнда, $a_{ij} \in \{0;1\}$, $i = 1..n$, $j = 1..n$;

b_i – сигнал наявності інверсії, $b_i \in \{0;1\}$, $i = 1..n$;

Y_i – вихідні змінні, результати перетворення операціями $Y_i \in \{0;1\}$, $i = 1..n$.

Для проведення порівняльного аналізу ефективності реалізації функціональних схем операцій використаємо такі показники якості:

- складність – кількість входів логічних елементів функціональної схеми;
- час виконання операції визначатиметься кількістю переключень логічних елементів;
- час виконання групи операцій функціональною схемою визначається кількістю логічних елементів у найдовшому ланцюгу схемотехнічного рішення.

Оцінка показників ефективності реалізації операцій визначатиметься за наступними параметрами: розрядність операцій; складність операції; час виконання операції; складність перетворення блоку інформації; час виконання перетворення блоку інформації.

Отримані значення показників реалізації функціональних схем операцій наведені в табл. 6.5.

У табл. 6.5 використані наступні позначення:

n – кількість входів логічних елементів;

t – час виконання одного елемента;

k – довжина блоку, $k = n \times m$, де m – розрядність операції.

Наведені розрахунки показників ефективності операцій дозволяють отримати показники ефективності криптоалгоритмів, побудованих на основі комбінації синтезованих груп операцій.

Таблиця 6.5

Оцінка показників ефективності реалізації операцій

Показник/Операції	Матричні операції	Розширені матричні операції	Операції перестановки керованих інформацією	Операції керовані інформацією	Операція додавання
Розрядність операцій	n		3		n
Складність операції	$8n^2$	$8n^2+9n$	66	84	14n
Час виконання операції	2t×n+1	2t×n+1	7t	8t	6t×n
Складність перетворення блоку інформації	$8m\times n^2$	$(8n^2+9)\times m$	66k, k=m×n/3	84k, k=m×n/3	-
Час виконання перетворення блоку інформації	2t×n+1	2t×n+1	7t	8t	-

Основною характеристикою криптоалгоритму є його стійкість.

Сьогодні найбільш поширеною класифікацією блокових шифрів за стійкістю є класифікація на основі наступних умов [72, 73, 75]:

- надвисока стійкість – довжина блока інформації й довжина ключа не менше за 512 бітів;
- висока стійкість – довжина блока інформації й довжина ключа не менші, ніж 256 бітів;
- нормальний рівень стійкості – довжина блока інформації й довжина ключа не менше, ніж 128 бітів;
- задовільний рівень стійкості – довжина блока інформації не менш, ніж 64 бітів, а довжина ключа – не менше, ніж 128 бітів.

Виходячи з даної класифікації, забезпечити підвищення стійкості можна:

a. збільшенням довжини ключової послідовності.
b. збільшенням довжини блока інформації, що шифрується.

Крім того, на якість шифрування впливають лінійність і нелінійність криптоперетворення.

Збільшення довжини ключової послідовності забезпечується збільшенням кількості операцій в алгоритмі шляхом послідовної реалізації, паралельної реалізації, послідовно-паралельної реалізації.

Збільшення довжини блока інформації реалізовується на основі застосування операцій різної розрядності: зміна розрядності при паралельній реалізації; зміна розрядності між етапами послідовної реалізації; зміна розрядності при паралельній і послідовній реалізації в паралельно-послідовній структурі.

Лінійність і нелінійність результатів виконаня операцій криптоперетворення залежать від формату вхідних даних.

Забезпечити протидію засобам статистичного криптографічного аналізу можливо шляхом багатораундавого криптоперетворення. Підвищення ефективності багатораундавого криптоперетворення здійснюється шляхом зміни операцій однієї групи на операції з іншої групи було розглянуто на прикладах побудови криптопримітивів ковзного шифрувння.

Подальші дослідження будуть направлені на дослідження статистичних властивостей запропонованих криптографічних алгоритмів для аналізу ефективності їх застосування при побудові засобів захисту інформації.

6.2. Оцінка статистичних властивостей криптоалгоритмів

6.2.1 Методика оцінки статистичних властивостей криптоалгоритмів

Для дослідження криптографічних алгоритмів і оцінки якості генераторів ПВП використовуються різноманітні програмні комплекси, серед яких на особливу увагу заслуговують: система оцінки статистичних властивостей DIEHARD [183], пакет NIST STS (США) [184-186], система оцінки статистичної безпеки алгоритмів генерації ПВП і криптоалгоритмів [186, 187].

Система оцінки статистичних властивостей DIEHARD має ряд недоліків, а саме: параметри тестування жорстко фіксовані, відсутня довідкова служба і

методика трактування результатів обробки, деякі тести не мають змістовного обґрунтування [183, 189].

На відміну від пакета DIEHARD, пакет NIST STS має більшу гнучкість, розширюваність і ефективність. Крім того, пакет NIST STS має більшу криптографічну спрямованість за рахунок введення в пакет таких тестів, як «лінійна складність» і універсальний статистичний тест Маурера [183-188].

У 1999 р. спеціалістами NIST (Національний інститут стандартів і технологій (НІСТ) США), у рамках проекту AES (Advanced Encryption Standard), було розроблено набір статистичних тестів «NIST STS» (NIST Statistical Test Suite) і запропоновано методику проведення статистичного тестування ГСЧ (ГПСЧ), орієнтованих на використання в задачах криптографічного захисту інформації, яка, на думку фахівців у цій сфері, нині найкраще відповідає вимогам усіх зацікавлених сторін [183, 184].

Пакет NIST STS містить 15 статистичних тестів, які розроблені для перевірки гіпотези щодо випадковості двійкових послідовностей довільної довжини [184]:

- частотний побітовий тест;
- частотний блоковий тест;
- тест на послідовність однакових бітів;
- тест на найдовшу послідовність одиниць у блоці;
- тест рангу бінарних матриць;
- спектральний тест;
- тест на перевірку шаблонів, які перекриваються;
- тест на перевірку шаблонів, які не перекриваються;
- універсальний статистичний тест Маурера;
- тест на лінійну складність;
- тест на періодичність;
- тест приблизної ентропії;
- тест кумулятивних сум;
- тест на випадкові відхилення;

– другий тест на випадкові відхилення.

Ці тести базуються на різних статистичних властивостях, притаманних лише випадковим послідовностям.

В основі статистичного тесту лежить перевірка деякої нульової гіпотези H_0 про те, що досліджувана послідовність – випадкова. Також передбачена альтернативна гіпотеза H_A, що припускає досліджувану послідовність невипадковою. Таким чином, після перевірки згенерованої послідовності для кожного тесту робиться висновок щодо відхилення або прийняття нульової гіпотези H_0 [144-188].

Для кожного тесту обирається адекватна статистика випадковості, на підставі якої далі відхиляється або приймається гіпотеза H_0. Така статистика, відповідно до припущення про випадковість, володіє деяким розподілом випадкових значень. Теоретично розподіл статистики для нульової гіпотези розраховується із застосуванням математичних методів. Далі з такого зразкового розподілу визначається критичне значення. Після проведення тесту розраховується значення тестової статистики, яке порівнюється з критичним значенням. При перевищенні тестового критичного значення над еталонним відхиляється нульова гіпотеза випадковості H_0. В іншому випадку робиться висновок про прийняття нульової гіпотези [188,189].

Для спрощення проведення порівняльного аналізу сатистичних характеристик результатів шифрування будемо перевіряти результати роботи крипто алгоритмів на зростаючих числових послідовностях 64 цифр, 256 цифр, константи 150 та тестового файлу. Так як наведені варіанти є найбільш складними для шифрування, тому що вони циклічні, монотонні. Даний підхід дозволяє порівнюваи криптосистеми побудовані на різних принципах.

Для проведення тестування використаємо пакет NIST STS, який містить 15 статистичних тестів та розроблені для перевірки гіпотези щодо випадковості двійкових послідовностей довільної довжини.

Для здійснення тестувань були обрані такі параметри: довжина послідовності, що тестується $n = 10^6$ біт; кількість послідовностей, що тестується $m = 100$; рівень значущості $\alpha = 0{,}01$; кількість тестів $q = 189$.

Таким чином, обсяг вибірки, що тестується, склав $N = 10^6 \times 100 = 10^8$ біт, кількість тестів (q) для різних довжин $q = 189$. Отже, статистичний портрет ПВП містить 18900 значень імовірності *P*.

В ідеальному випадку при $m = 100$ і $\alpha = 0{,}01$ у ході тестування може бути відкинута тільки одна послідовність зі ста, тобто коефіцієнт проходження кожного тесту має складати 99%. Але це занадто жорстке правило. Тому застосовується правило на основі довірчого інтервалу. Нижня межа дорівнює 0,96015.

6.2.2 Аналіз результатів тестування алгоритмів синтезованих на основі операцій криптографічного перетворення інформації

Проведемо дослідження та аналіз статистичних властивостей деяких варіантів побудови криптоалгоритмів на основі операцій криптографічного перетворення.

Оскільки тести NIST STS спрямовані на виявлення статистичних закономірностей у псевдовипадкових послідовностях, перевіримо можливість виявлення таких закономірностей на невипадковій монотонно зростаючій послідовності з циклом повторення 64 байти, в яку записані коди чисел 64, 65, 66, …, 128 для криптоалгоритму, який складається із матричних операцій.

Результати тестування наведені у додатку Б.

Статистичний портрет програмної реалізації криптографічного алгоритму на основі матричних операцій перетворення інформації зображено на рис. 6.13.

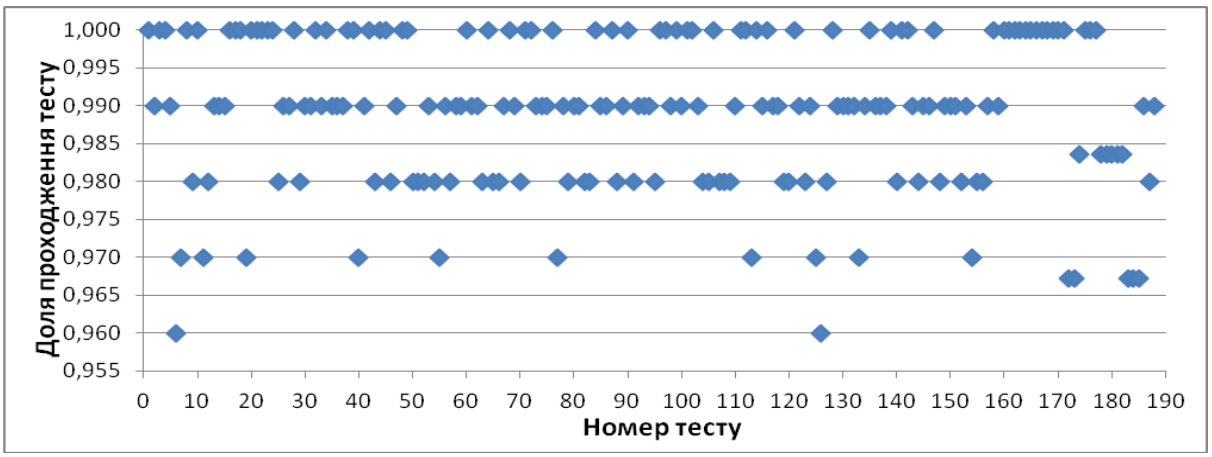


Рис. 6.13. Статистичний портрет програмної реалізації алгоритму на основі матричних операцій

Зведені результати тестування матричного перетворення невипадкової монотонно зростаючої послідовності з циклом повторення 64 байти програмним пакетом NIST STS подані в табл. 6.6.

Таблиця 6.6

Зведені результати тестування матричного перетворення невипадкової монотонно зростаючої послідовності з циклом повторення 64 байти

Генератор	Кількість тестів, в яких тестування пройшло	
	99 % послід.	96 % послід.
Матричне криптографічне перетворення	128 (68,1 %)	188 (100 %)

Як видно з результатів, досліджувана послідовність пройшла комплексний контроль за методикою NIST STS [24].

Перевіримо можливість виявлення статичних властивостей результатів матричного криптографічного перетворення невипадкової монотонно зростаючої послідовності з циклом повторення 256 байтів, в яку записані коди чисел 0, 1, 2, …, 255.

Результати тестування наведені у додатку Б.

Статистичний портрет зображено на рис. 6.14.

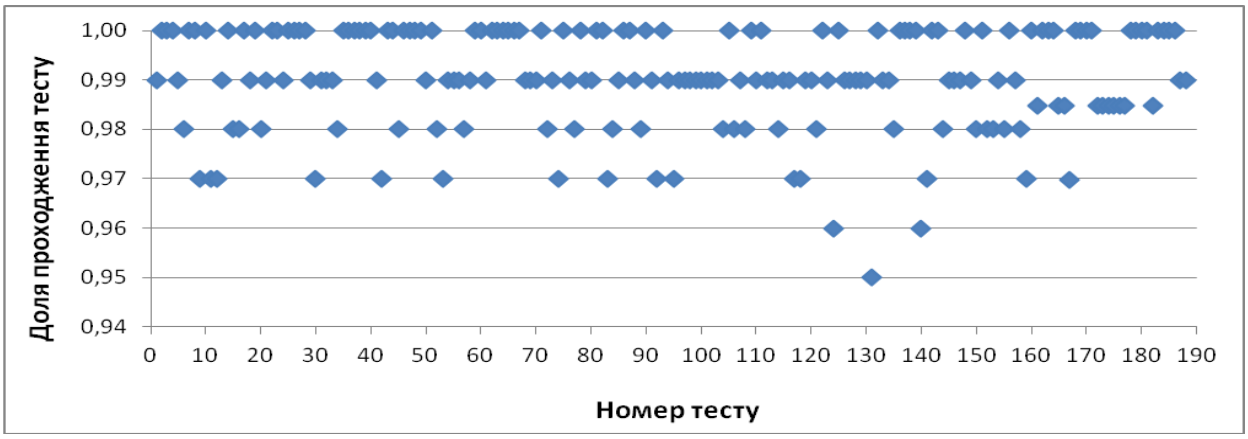


Рис. 6.14. Статистичний портрет програмної реалізації алгоритму на основі матричних операцій

Зведені результати тестування матричного перетворення невипадкової монотонно зростаючої послідовності з циклом повторення 256 байтів програмним пакетом NIST STS подані в табл. 6.7.

Таблиця 6.7

Зведені результати тестування матричного перетворення невипадкової монотонно зростаючої послідовності з циклом повторення 256 байтів

Генератор	Кількість тестів, в яких тестування пройшло	
	99 % послід.	96 % послід.
Матричне криптографічне перетворення	136 (72,3 %)	187 (99,4 %)

Як видно з результатів, досліджувана послідовність не пройшла комплексний контроль за методикою NIST STS, тому що не був пройдений один тест:

```
------------------------------------------------------------------------------
RESULTS FOR THE UNIFORMITY OF P-VALUES AND THE PROPORTION OF PASSING SEQUENCES
------------------------------------------------------------------------------
   generator is <KOD_CHT1.bin>
------------------------------------------------------------------------------
 C1  C2  C3  C4  C5  C6  C7  C8  C9 C10  P-VALUE  PROPORTION  STATISTICAL TEST
------------------------------------------------------------------------------
18   5  10  12  13   7  10   8   8   9  0.213309   0.9500 *  NonOverlappingTemplate
```

Для забезпечення проходження цього тесту проведемо обчислювальний експеримент, додавши в алгоритм криптографічного матричного перетворення додатковий блок криптографічного перетворення групою операцій інверсії результатів матричного перетворення.

Результати тестування наведені у додатку Б.

Статистичний портрет програмної реалізації алгоритму модифікованого матричного перетворення невипадкової монотонно зростаючої послідовності з циклом повторення 256 байтів зображено на рис. 6.15.

Зведені результати тестування матричного перетворення за модифікованим алгоритмом невипадкової монотонно зростаючої послідовності з циклом повторення 256 байтів програмним пакетом NIST STS подані в табл. 6.8.

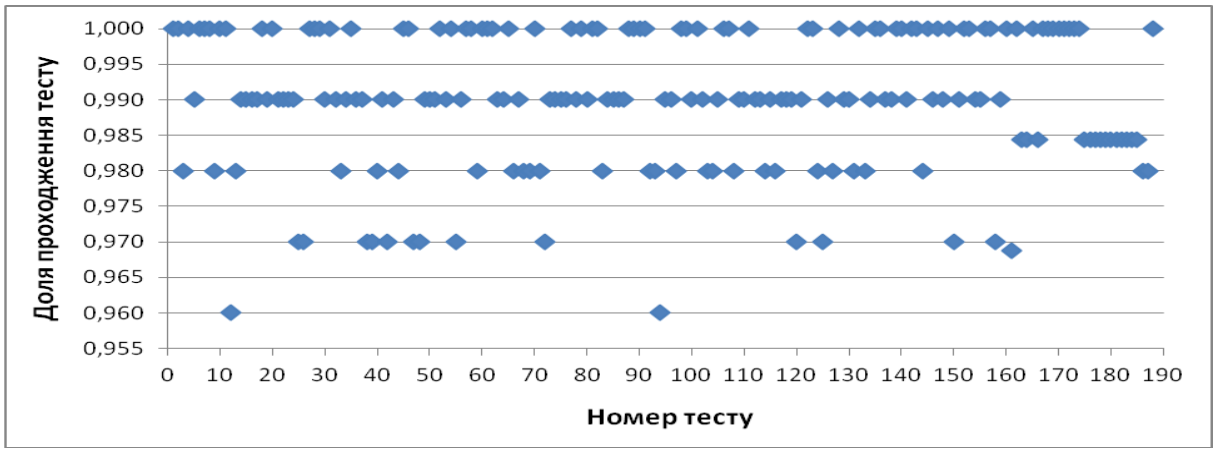


Рис. 6.15. Статистичний портрет програмної реалізації алгоритму модифікованого матричного перетворення невипадкової монотонно зростаючої послідовності з циклом повторення 256 байтів

Таблиця 6.8

Зведені результати тестування даних за модифікованим алгоритмом матричного перетворення

Генератор	Кількість тестів, в яких тестування пройшло	
	99 % послід.	96 % послід.
Модифіковане матричне криптографічне перетворення	131 (69,7 %)	188 (100 %)

Як видно з результатів, досліджувана послідовність пройшла комплексний контроль за методикою NIST STS [24].

Перевіримо статистичні властивості даного крипто алгоритму на основі операцій матричного перетворення на результатах шифрування послідовності, що складається із константи – числа зі значенням 150.

Отримані результати на основі пакету NIST STS наведені у додатку Б.

Статистичний портрет програмної реалізації алгоритму матричного перетворення числової послідовності з константи 150 зображено на рис. 6.16.

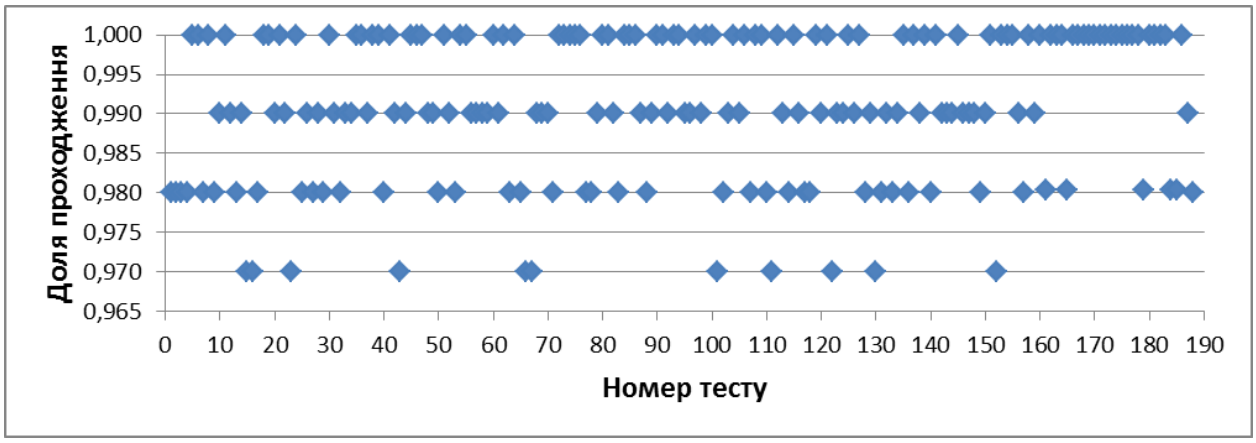


Рис. 6.16. Статистичний портрет програмної реалізації алгоритму матричного перетворення числової послідовні.

Зведені результати тестування матричного перетворення послідовності із числової константи 150 програмним пакетом NIST STS подані в табл. 6.9.

Таблиця 6.9

Зведені результати тестування числа 150 алгоритмом матричного перетворення

Генератор	Кількість тестів, в яких тестування пройшло	
	99 % послід.	96 % послід.
Матричне криптографічне перетворення	136 (72,3 %)	188 (100 %)

Як видно з результатів, досліджувана послідовність пройшла комплексний контроль за методикою NIST STS [24].

Перевіримо статистичні властивості результатів матричного криптографічного перетворення текстової інформації на прикладі електронних інформаційних ресурсів, а саме художньої літератури в текстовому форматі.

Результати тестування наведені у додатку Б.

Статистичний портрет програмної реалізації алгоритму модифікованого матричного криптографічного перетворення текстового файлу зображено на рис. 6.17.

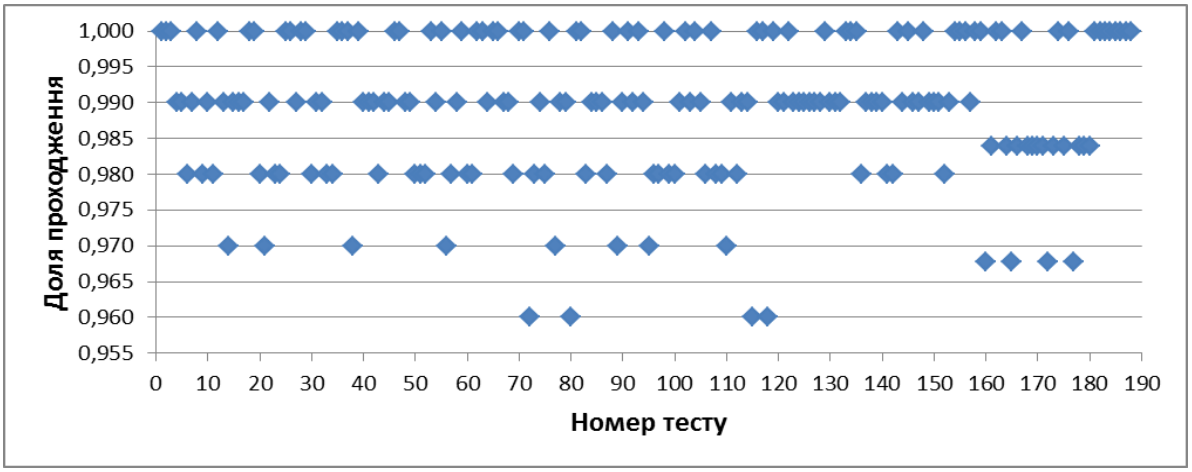


Рис. 6.17. Статистичний портрет програмної реалізації алгоритму на основі матричних операцій текстового файлу

Зведені результати тестування текстового файлу криптоалгоритмом на основі матричних операцій програмним пакетом NIST STS подані в табл. 6.10.

Таблиця 6.10

Зведені результати тестування криптоперетворення текстового файлу на основі матричних операцій

Генератор	Кількість тестів, в яких тестування пройшло	
	99% послід.	96% послід.
Матричне криптографічне перетворення	127 (67,6 %)	188 (100 %)

Як видно з результатів, досліджувана послідовність пройшла комплексний контроль за методикою NIST STS.

Здійснимо тестування статистичних властивостей результатів шифрування алгоритму синтезованого на основі операцій розширеного матричного криптографічного перетворення.

Отримані результати на основі пакету NIST STS наведені в додатку Б.6.

Статистичний портрет програмної реалізації перетворення інформації алгоритмом синтезованим на основі операцій розширеного матричного криптографічного перетворення зображено на рис. 6.18.

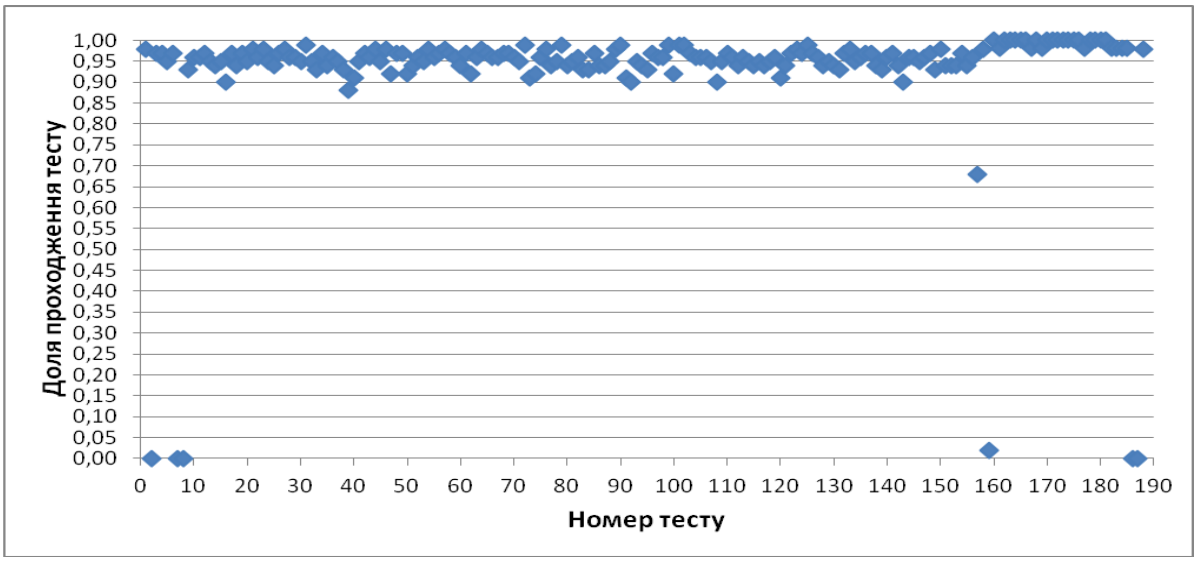


Рис. 6.18. Статистичний портрет програмної реалізації алгоритму на основі розширених матричних операцій криптографічного перетворення.

Зведені результати тестування алгоритму на основі розширених матричних операцій криптографічного перетворення програмним пакетом NIST STS подані в табл. 6.11.

Таблиця 6.11

Зведені результати тестування алгоритму на основі розширених матричних операцій криптографічного перетворення

Генератор	Кількість тестів, в яких	
	99 % послід.	96 % послід.
Алгоритм на основі розширених матричних операцій криптографічного перетворення	26 (13,8 %)	111 (59 %)

Як видно з результатів, досліджувана послідовність не пройшла комплексний контроль за методикою NIST STS [24], тому що не були пройдені 8 тестів:

```
------------------------------------------------------------------------------
RESULTS FOR THE UNIFORMITY OF P-VALUES AND THE PROPORTION OF PASSING SEQUENCES
------------------------------------------------------------------------------
   generator is <V_DI_DR.bin>
------------------------------------------------------------------------------
 C1  C2  C3  C4  C5  C6  C7  C8  C9 C10  P-VALUE  PROPORTION  STATISTICAL TEST
------------------------------------------------------------------------------
100   0   0   0   0   0   0   0   0   0  0.000000 * 0.0000 *  BlockFrequency
 16  12   9   8  13   7  11   8   9   7  0.554420   0.9500 *  Runs
100   0   0   0   0   0   0   0   0   0  0.000000 * 0.0000 *  Rank
100   0   0   0   0   0   0   0   0   0  0.000000 * 0.0000 *  FFT
 28  17  10   8  10   7   5  10   5   0  0.000000 * 0.9300 *  NonOverlappingTemplate
 22  12  10  14  12   5   5  14   1   5  0.000089 * 0.9600    NonOverlappingTemplate
 15  18  11  11   8  12   6   8   8   3  0.045675   0.9500 *  NonOverlappingTemplate
 23  18  17   6   7   9   5   5   7   3  0.000004 * 0.9400 *  NonOverlappingTemplate
 29  10  16   6  12   4   6   5   7   5  0.000000 * 0.9500 *  NonOverlappingTemplate
 34   4  11   9   9   7   7   5   8   6  0.000000 * 0.9000 *  NonOverlappingTemplate
 21  16  10   4  10  10  13   6   6   4  0.001399   0.9400 *  NonOverlappingTemplate
 20  17   8   7   8  13   8  11   5   3  0.002559   0.9500 *  NonOverlappingTemplate
 25  13  12  11   9   6   8   8   6   2  0.000076 * 0.9800    NonOverlappingTemplate
 17  15  19   8   3  13   9   9   6   1  0.000233   0.9500 *  NonOverlappingTemplate
 27  10  11   8   8   9   9  10   4   4  0.000024 * 0.9400 *  NonOverlappingTemplate
 21  16  10   9  12   8  11   4   6   3  0.001509   0.9500 *  NonOverlappingTemplate
 21  12  13   7   7  10  10   9   9   2  0.009535   0.9500 *  NonOverlappingTemplate
 26  15  12  13   8   6   6   4   6   4  0.000004 * 0.9300 *  NonOverlappingTemplate
 26   7  10  11  10  13   6   6   6   5  0.000065 * 0.9400 *  NonOverlappingTemplate
 20  15  17   8  10   7   5   9   6   3  0.001030   0.9500 *  NonOverlappingTemplate
 31  16   9  11   7   6   6   6   3   5  0.000000 * 0.9300 *  NonOverlappingTemplate
 36  12   8   8   6   5   6   7   5   7  0.000000 * 0.8800 *  NonOverlappingTemplate
 25  11  15  10   6   9   7   6   6   5  0.000114   0.9100 *  NonOverlappingTemplate
 16  14  18  10  12   7   7   7   5   4  0.013569   0.9500 *  NonOverlappingTemplate
 26  16  16  12   6   4   5   7   6   2  0.000000 * 0.9700    NonOverlappingTemplate
 30  13   9   6   6   7   8   4   7  10  0.000000 * 0.9600    NonOverlappingTemplate
 28  14  15  11   8   6   8   4   3   3  0.000000 * 0.9800    NonOverlappingTemplate
 23  13  13  11   7   8   6   6   5   8  0.001895   0.9500 *  NonOverlappingTemplate
 27  14   6  12   7   5   8   9   2  10  0.000002 * 0.9800    NonOverlappingTemplate
 29  15   7   5   9   6   8   6   5  10  0.000000 * 0.9200 *  NonOverlappingTemplate
 24  13  13   9  14   7   5   4   5   6  0.000082 * 0.9200 *  NonOverlappingTemplate
 28  13   3   4   8  11  14  12   6   1  0.000000 * 0.9400 *  NonOverlappingTemplate
 25  10   8  10  13  10  12   6   2   4  0.000043 * 0.9600    NonOverlappingTemplate
 26  15   8   9  14  11   7   5   1   4  0.000001 * 0.9500 *  NonOverlappingTemplate
 25   8  12  12  11   9   8   8   6   1  0.000076 * 0.9600    NonOverlappingTemplate
 21  19   4  17  11   9   6   3   5   5  0.000006 * 0.9700    NonOverlappingTemplate
 28  14  11  11   4   6   3  10   7   6  0.000000 * 0.9400 *  NonOverlappingTemplate
 24  18   6  12   9  10   8   6   3   4  0.000014 * 0.9200 *  NonOverlappingTemplate
 22  15  21  11   6   7   3   3   7   5  0.000001 * 0.9600    NonOverlappingTemplate
 17  19  16   8  15   6   5   9   3   2  0.000060 * 0.9600    NonOverlappingTemplate
 23  14  10   9   8   6  11   6   9   4  0.002043   0.9500 *  NonOverlappingTemplate
 26  10  16   7  10   9   5   4   5   8  0.000011 * 0.9100 *  NonOverlappingTemplate
 35  11  12  10  11   5   4   4   5   3  0.000000 * 0.9200 *  NonOverlappingTemplate
 29  11  16   5   8   9  10   3   4   5  0.000000 * 0.9600    NonOverlappingTemplate
 25  16  11   8  11  12   6   6   4   1  0.000003 * 0.9800    NonOverlappingTemplate
 29  10  14   5  11   7   6   8   6   4  0.000000 * 0.9400 *  NonOverlappingTemplate
 22  16  12  12   9   8   9   5   5   2  0.000320   0.9500 *  NonOverlappingTemplate
 25  11  18   7  11   6   8   8   5   1  0.000002 * 0.9900    NonOverlappingTemplate
 21  21  10   5  12   7   4   7   4   9  0.000037 * 0.9400 *  NonOverlappingTemplate
 29  13  11   9   8  11   5   2   8   4  0.000000 * 0.9500 *  NonOverlappingTemplate
 28  17  10   8  10   7   5  10   5   0  0.000000 * 0.9300 *  NonOverlappingTemplate
 19  16  11  12  10   8   8   3  10   3  0.006661   0.9300 *  NonOverlappingTemplate
 25  17   9   5  11   7   8   8   6   4  0.000026 * 0.9700    NonOverlappingTemplate
 25   8  20  13  11   6   6   3   3   5  0.000000 * 0.9400 *  NonOverlappingTemplate
 26  15   8  13   6   5   6   6   7   8  0.000017 * 0.9400 *  NonOverlappingTemplate
 25   9  12  14  12   6   5  10   4   3  0.000021 * 0.9500 *  NonOverlappingTemplate
 27  13   9  16  10   7   6   4   5   3  0.000000 * 0.9100 *  NonOverlappingTemplate
```

```
 27  10  12   9  11   4   9   6   7   5  0.000016 * 0.9000 *  NonOverlappingTemplate
 21  15   7   8  11  11   7   9   2   9  0.004981   0.9500 *  NonOverlappingTemplate
 27  17  10   9   7   5   7   7   6   5  0.000002 * 0.9400 *  NonOverlappingTemplate
 28  15   6   5   5  12   6   5  10   8  0.000001 * 0.9300 *  NonOverlappingTemplate
 24  19   6  10   9   6   9  10   4   3  0.000009 * 0.9600    NonOverlappingTemplate
 27  11  12  13   6   7   6   7   8   3  0.000006 * 0.9900    NonOverlappingTemplate
 25  15  18  11   6   8   7   4   4   2  0.000000 * 0.9200 *  NonOverlappingTemplate
 22  21  12   5   5  10  10   6   4   5  0.000009 * 0.9900    NonOverlappingTemplate
 26  13  11  13   3   7   7  10   6   4  0.000010 * 0.9600    NonOverlappingTemplate
 23  18   8  18   7   8   4   6   3   5  0.000001 * 0.9600    NonOverlappingTemplate
 28  19  10   4  11   8   3  12   3   2  0.000000 * 0.9500 *  NonOverlappingTemplate
 24   8   8  14  12   5   7  12   6   4  0.000253   0.9000 *  NonOverlappingTemplate
 29  15  10  11   5   4   8   8   4   6  0.000000 * 0.9500 *  NonOverlappingTemplate
 25  13  16   7   6   7   7   6   9   4  0.000031 * 0.9700    NonOverlappingTemplate
 18  20  17   9  11   3   5   9   6   2  0.000026 * 0.9600    NonOverlappingTemplate
 26  10  13   5  12  11   5   7   7   4  0.000022 * 0.9400 *  NonOverlappingTemplate
 34  14   8   5  13   9   6   3   5   3  0.000000 * 0.9600    NonOverlappingTemplate
 29  20   8   8   8   5   7   5   7   3  0.000000 * 0.9500 *  NonOverlappingTemplate
 26  16  11  10   8   7   7   5   5   5  0.000012 * 0.9400 *  NonOverlappingTemplate
 22  19   8   9  10   5   7   7   5   8  0.000406   0.9500 *  NonOverlappingTemplate
 26  10  15   9   9   5   9   5   8   4  0.000022 * 0.9400 *  NonOverlappingTemplate
 31  14   8   8   7  10   4   7   6   5  0.000000 * 0.9500 *  NonOverlappingTemplate
 26  13   9  10  12   5   4   8   8   5  0.000034 * 0.9600    NonOverlappingTemplate
 26  13  13   3   8  11   8   2  10   6  0.000005 * 0.9100 *  NonOverlappingTemplate
 21  14   9  19   7   5   2   7   7   9  0.000105   0.9400 *  NonOverlappingTemplate
 26  11   9  13   6   7  11   8   4   5  0.000043 * 0.9700    NonOverlappingTemplate
 24  12  13  15   7   8   3   7   6   5  0.000070 * 0.9700    NonOverlappingTemplate
 16  18  12  10   5   8  10  12   6   3  0.016717   0.9400 *  NonOverlappingTemplate
 25  12   8  14  11   5  11   4   7   3  0.000026 * 0.9500 *  NonOverlappingTemplate
 20  12  14   2   9  10   8  10   9   6  0.014550   0.9400 *  NonOverlappingTemplate
 31  15   8   4  13  10   8   3   5   3  0.000000 * 0.9300 *  NonOverlappingTemplate
 20  17  14   9  10   8   9   5   5   3  0.001399   0.9500 *  NonOverlappingTemplate
 27  12  14   8   8   8   8   5   6   4  0.000007 * 0.9700    NonOverlappingTemplate
 24  15  10  11   7   8   8   7   7   3  0.000347   0.9400 *  NonOverlappingTemplate
 27  16   9   9   9   3   6   5  10   6  0.000002 * 0.9300 *  NonOverlappingTemplate
 27  11   7  10   8  12   7   7   6   5  0.000031 * 0.9600    NonOverlappingTemplate
 27  20   6   2  10  11   4   6  10   4  0.000000 * 0.9700    NonOverlappingTemplate
 24  12  20   5  10   8   6   9   3   3  0.000001 * 0.9400 *  NonOverlappingTemplate
 27  10  16  11   8   8   7   6   6   1  0.000001 * 0.9000 *  NonOverlappingTemplate
 24  15  13   9   8  12   6   4   4   5  0.000055 * 0.9600    NonOverlappingTemplate
 24  18  10   7   6  10   7   5   6   7  0.000076 * 0.9600    NonOverlappingTemplate
 25  15  12  12   7   5  12   4   5   3  0.000006 * 0.9500 *  NonOverlappingTemplate
 27  13   8  14   9   8   9   5   2   5  0.000002 * 0.9600    NonOverlappingTemplate
 30   7  12   8  11   8  12   7   4   1  0.000000 * 0.9700    NonOverlappingTemplate
 25  14   8   9  11   9   9   9   2   4  0.000060 * 0.9300 *  NonOverlappingTemplate
 16  26  15   9  10   7   7   6   3   1  0.000000 * 0.9800    NonOverlappingTemplate
 22  11  11   8  13  12   5   5   6   7  0.004629   0.9400 *  NonOverlappingTemplate
 14   9  11  15  12   9   9   7   9   5  0.494392   0.9400 *  NonOverlappingTemplate
 23  17  11  11   8   9   4   8   3   6  0.000134   0.9400 *  NonOverlappingTemplate
 24  15  12  11   9   5   6  10   4   4  0.000089 * 0.9700    NonOverlappingTemplate
 19  14  10   8  11   7  15   6   7   3  0.012650   0.9400 *  NonOverlappingTemplate
 62  14  10   6   3   2   1   2   0   0  0.000000 * 0.6800 *  OverlappingTemplate
100   0   0   0   0   0   0   0   0   0  0.000000 * 0.0200 *  ApproximateEntropy
100   0   0   0   0   0   0   0   0   0  0.000000 * 0.0000 *  Serial
100   0   0   0   0   0   0   0   0   0  0.000000 * 0.0000 *  Serial
```

Даний портрет статистичних характеристик та зведені результати тестування показують, що існує можливість дешифрації повідомлення криптоаналітиками. Тому дана можливість може бути використана для відволікання криптоаналітичних ресурсів від реалізації їхніх основних задач.

Далі перевіримо можливість виявлення статистичних закономірностей на невипадковій монотонно зростаючій послідовності з циклом повторення 64 байти,

в яку записані коди чисел 64, 65, 66, …, 128 для криптографічного алгоритму, який складається із розширених матричних операцій.

Результати тестування наведені у додатку Б.

Статистичний портрет програмної реалізації криптографічного алгоритму на основі розширених матричних операцій перетворення інформації зображено на рис. 6.19.

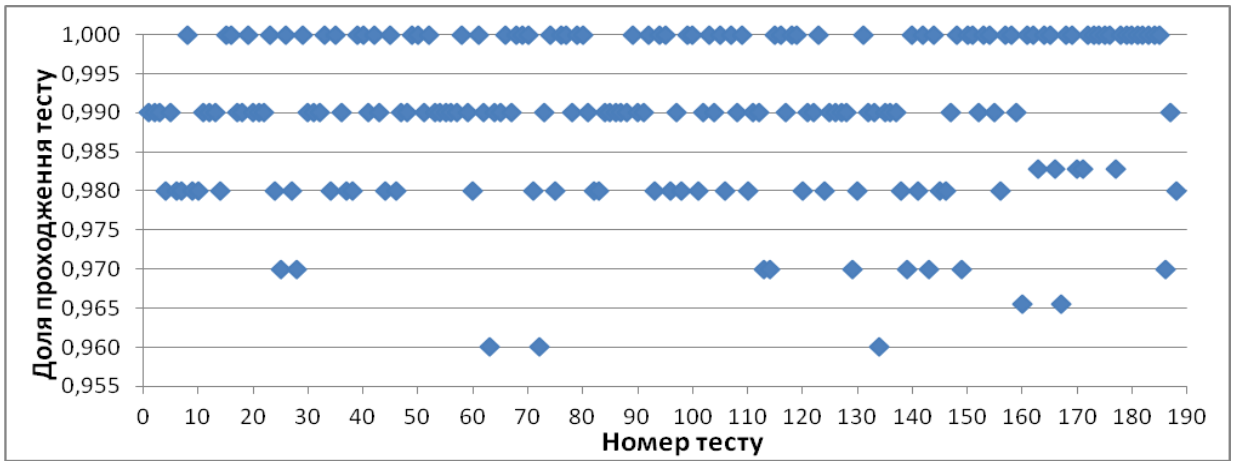


Рис. 6.19. Статистичний портрет програмної реалізації алгоритму на основі розширених матричних операцій

Зведені результати тестування розширеного матричного перетворення невипадкової монотонно зростаючої послідовності з циклом повторення 64 байти програмним пакетом NIST STS подані в табл. 6.12.

Таблиця 6.12

Зведені результати тестування розширеного матричного перетворення невипадкової монотонно зростаючої послідовності з циклом повторення 64 байти

Генератор	Кількість тестів, в яких тестування пройшло	
	99 % послід.	96 % послід.
Розширене матричне криптографічне перетворення	136 (72,3 %)	188 (100 %)

Як видно з результатів, досліджувана послідовність пройшла комплексний контроль за методикою NIST STS [24].

Перевіримо можливість виявлення статичних властивостей результатів розширеного матричного криптографічного перетворення невипадкової монотонно зростаючої послідовності з циклом повторення 256 байтів, в яку записані коди чисел 0, 1, 2, …, 255.

Результати тестування наведені у додатку Б.

Статистичний портрет зображено на рис. 6.20.

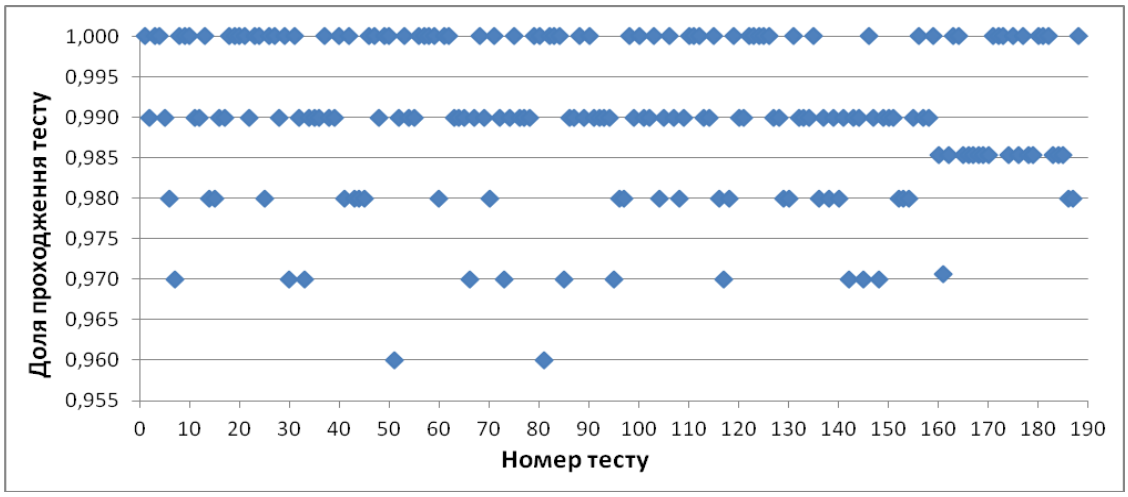


Рис. 6.20. Статистичний портрет програмної реалізації алгоритму на основі розширених матричних операцій

Зведені результати тестування розширеного матричного перетворення невипадкової монотонно зростаючої послідовності з циклом повторення 256 байтів програмним пакетом NIST STS подані в табл. 6.13.

Таблиця 6.13

Зведені результати тестування розширеного матричного перетворення невипадкової монотонно зростаючої послідовності з циклом повторення 256 байтів

Генератор	Кількість тестів, в яких тестування	
	99 % послід.	96 % послід.
Розширене матричне криптографічне перетворення	133 (70,8 %)	188 (100%)

Як видно з результатів, досліджувана послідовність пройшла комплексний контроль за методикою NIST STS.

Перевіримо статистичні властивості даного крипто алгоритму на основі операцій розширеного матричного перетворення на результатах шифрування послідовності, що складається із константи - числа зі значенням 150.

Отримані результати на основі пакету NIST STS наведені у додатку Б.

Статистичний портрет програмної реалізації алгоритму розширеного матричного перетворення числової послідовності з константи 150 зображено на рис. 6.21.

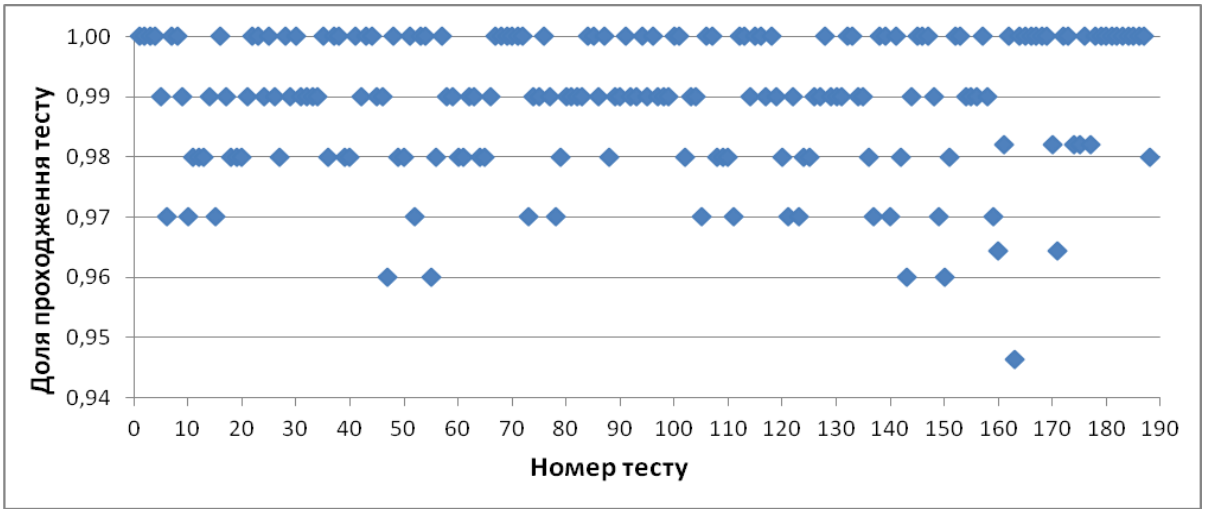


Рис. 6.21. Статистичний портрет програмної реалізації алгоритму розширеного матричного перетворення числової послідовності.

Зведені результати тестування розширеного матричного перетворення послідовності із числової константи 150 програмним пакетом NIST STS подані в табл. 6.14.

Таблиця 6.14

Зведені результати тестування числа 150 алгоритмом матричного перетворення

Генератор	Кількість тестів, в яких тестування	
	99 % послід.	96 % послід.
Розширене матричне криптографічне перетворення	132 (70,2 %)	187 (99,5 %)

Як видно з результатів, досліджувана послідовність не пройшла комплексний контроль за методикою NIST STS [24], тому що не був пройдений один тест:

```
------------------------------------------------------------------------------
RESULTS FOR THE UNIFORMITY OF P-VALUES AND THE PROPORTION OF PASSING SEQUENCES
------------------------------------------------------------------------------
   generator is <KOD_CHT1.bin>
------------------------------------------------------------------------------
 C1  C2  C3  C4  C5  C6  C7  C8  C9 C10  P-VALUE  PROPORTION  STATISTICAL TEST
------------------------------------------------------------------------------
 10   7   6   1   5   5   2   6   7   7  0.171867   0.9464 *  RandomExcursions
```

Перевіримо статистичні властивості результатів розширеного матричного криптографічного перетворення текстової інформації на прикладі електронних інформаційних ресурсів, а саме художньої літератури в текстовому форматі.

Результати тестування наведені у додатку Б.

Статистичний портрет програмної реалізації алгоритму розширеного матричного криптографічного перетворення текстового файлу зображено на рис. 6.22.

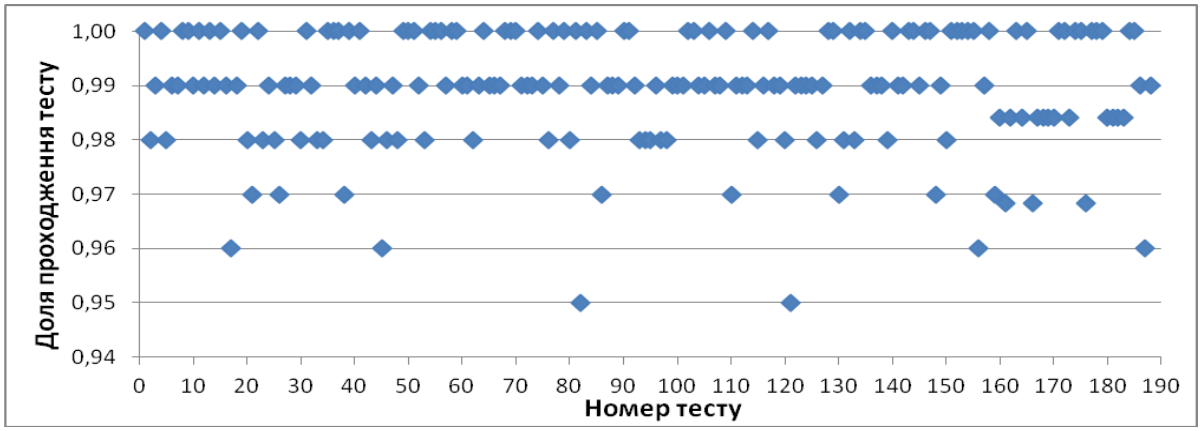


Рис. 6.22. Статистичний портрет програмної реалізації алгоритму на основі розширених матричних операцій текстового файлу

Зведені результати тестування текстового файлу криптоалгоритмом на основі розширених матричних операцій програмним пакетом NIST STS подані в табл. 6.15.

Таблиця 6.15

Зведені результати тестування криптоперетворення текстового файлу на основі розширених матричних операцій

Генератор	Кількість тестів, в яких тестування пройшло	
	99% послід.	96% послід.
Розширене матричне криптографічне перетворення	132 (70,2 %)	186 (98,9 %)

Як видно з результатів, досліджувана послідовність не пройшла комплексний контроль за методикою NIST STS, тому що не був пройдений один тест:

```
---------------------------------------------------------------------------
RESULTS FOR THE UNIFORMITY OF P-VALUES AND THE PROPORTION OF PASSING SEQUENCES
---------------------------------------------------------------------------
   generator is <KOD_CHT1.bin>
---------------------------------------------------------------------------
 C1  C2  C3  C4  C5  C6  C7  C8  C9 C10  P-VALUE  PROPORTION  STATISTICAL TEST
---------------------------------------------------------------------------
11   7  14  15  11   5   8  10  13   6  0.304126   0.9500 *  NonOverlappingTemplate
16  15   6   6   5   9  13  10   8  12  0.137282   0.9500 *  NonOverlappingTemplate
11   7  14  15  11   5   8  10  13   6  0.304126   0.9500 *  NonOverlappingTemplate
```

Для забезпечення проходження цього тесту проведемо обчислювальний експеримент, використавши в алгоритмі криптографічного матричного перетворення додатковий блок криптографічного перетворення розширеного матричного перетворення, тобто використаємо послідовну комбінацію матричного та розширеного матричного перетворення..

Перевіримо можливість виявлення статистичних закономірностей на невипадковій монотонно зростаючій послідовності з циклом повторення 64 байти, в яку записані коди чисел 64, 65, 66, …, 128 для криптографічного алгоритму, який складається із комбінації матричних та розширених матричних операцій.

Результати тестування наведені в додатку Б.

Статистичний портрет програмної реалізації криптографічного алгоритму на основі комбінації матричних та розширених матричних операцій перетворення інформації зображено на рис. 6.23.

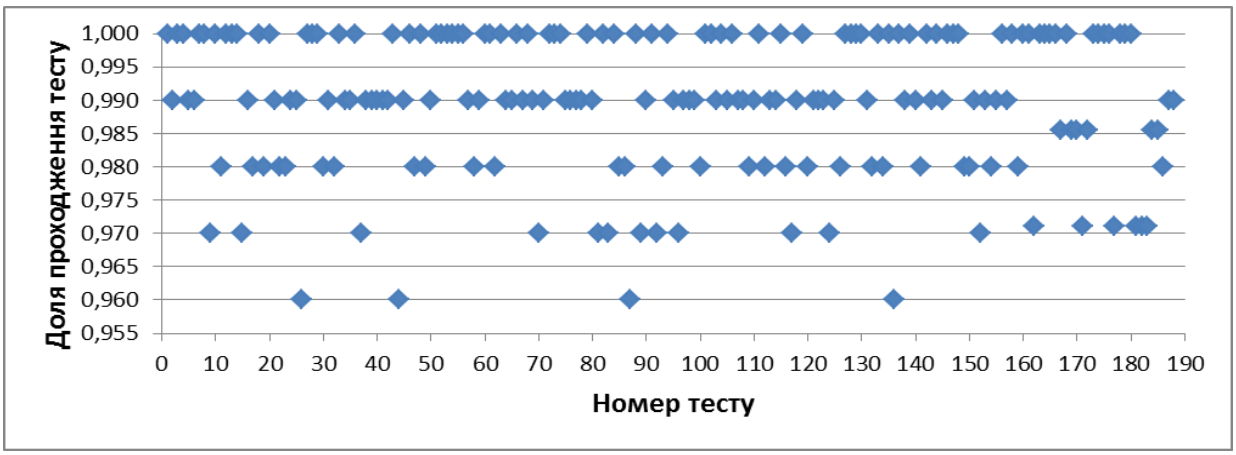


Рис. 6.23. Статистичний портрет програмної реалізації алгоритму на основі комбінації матричних та розширених матричних операцій

Зведені результати тестування комбінаційного матричного-розширеного матричного перетворення невипадкової монотонно зростаючої послідовності з циклом повторення 64 байти програмним пакетом NIST STS подані в табл. 6.16.

Таблиця 6.16

Зведені результати тестування матричного-розширеного матричного перетворення невипадкової монотонно зростаючої послідовності з циклом повторення 64 байти

Генератор	Кількість тестів, в яких тестування пройшло	
	99 % послід.	96 % послід.
Матричне-розширене матричне криптографічне перетворення	132 (70,2 %)	188 (100 %)

Як видно з результатів, досліджувана послідовність пройшла комплексний контроль за методикою NIST STS [24].

Перевіримо можливість виявлення статичних властивостей результатів матричного-розширеного матричного криптографічного перетворення невипадкової монотонно зростаючої послідовності з циклом повторення 256 байтів, в яку записані коди чисел 0, 1, 2, …, 255.

Результати тестування наведені в додатку Б.

Статистичний портрет зображено на рис. 6.24.

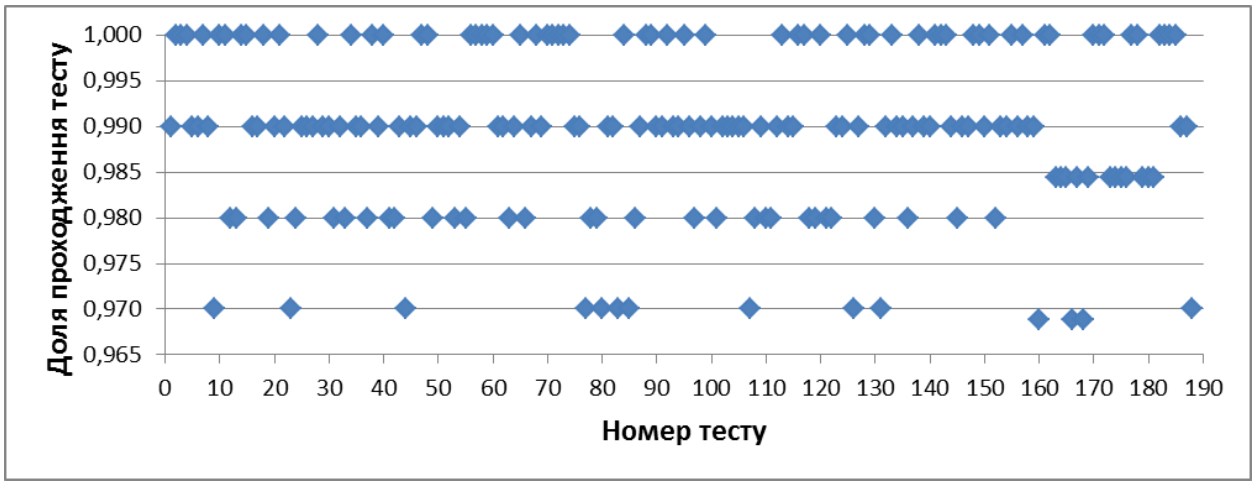


Рис. 6.4. Статистичний портрет програмної реалізації алгоритму на основі комбінації матричних та розширених матричних операцій

Зведені результати тестування комбінації матричного та розширеного матричного перетворення невипадкової монотонно зростаючої послідовності з циклом повторення 256 байтів програмним пакетом NIST STS подані в табл. 6.17.

Таблиця 6.17

Зведені результати тестування комбінації матричного та розширеного матричного перетворення невипадкової монотонно зростаючої послідовності з циклом повторення 256 байтів

Генератор	Кількість тестів, в яких тестування пройшло	
	99 % послід.	96 % послід.
Матричне-розширене матричне криптографічне перетворення	132 (70,2 %)	188 (100%)

Як видно з результатів, досліджувана послідовність пройшла комплексний контроль за методикою NIST STS.

Перевіримо статистичні властивості даного крипто алгоритму на основі комбінації операцій матричного та розширеного матричного перетворення на результатах шифрування послідовності, що складається із константи - числа зі значенням 150.

Отримані результати на основі пакету NIST STS наведені в додатку Б.

Статистичний портрет програмної реалізації комбінаційного алгоритму матричного-розширеного матричного перетворення числової послідовності з константи 150 зображено на рис. 6.26.

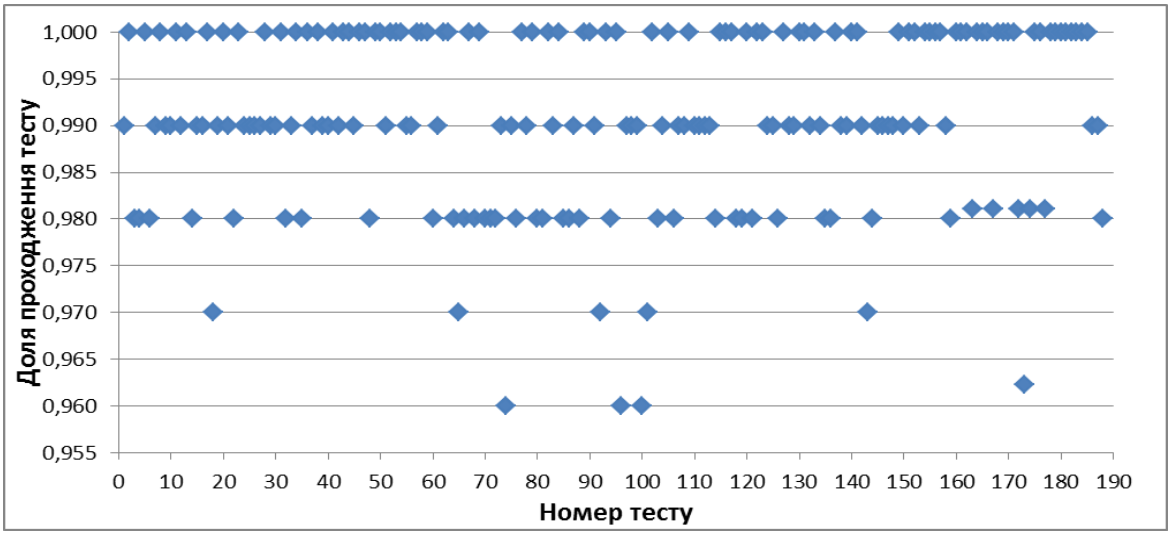


Рис. 6.26. Статистичний портрет програмної реалізації алгоритму комбінації матричного та розширеного матричного перетворення числової послідовності.

Зведені результати тестування комбінації матричного та розширеного матричного перетворення послідовності із числової константи 150 програмним пакетом NIST STS подані в табл. 6.18.

Таблиця 6.18

Зведені результати тестування комбінаційним алгоритмом матричного-розширеного матричного перетворення

Генератор	Кількість тестів, в яких тестування пройшло	
	99 % послід.	96 % послід.
Матричне-розширене матричне криптографічне перетворення	140 (74,5 %)	188 (100 %)

Як видно з результатів, досліджувана послідовність пройшла комплексний контроль за методикою NIST STS [24].

Перевіримо статистичні властивості результатів комбінації операцій матричного та розширеного матричного криптографічного перетворення

текстової інформації на прикладі електронних інформаційних ресурсів, а саме художньої літератури в текстовому форматі.

Результати тестування наведені в додатку Б.

Статистичний портрет програмної реалізації комбінаційного алгоритму матричного-розширеного матричного криптографічного перетворення текстового файлу зображено на рис. 6.28.

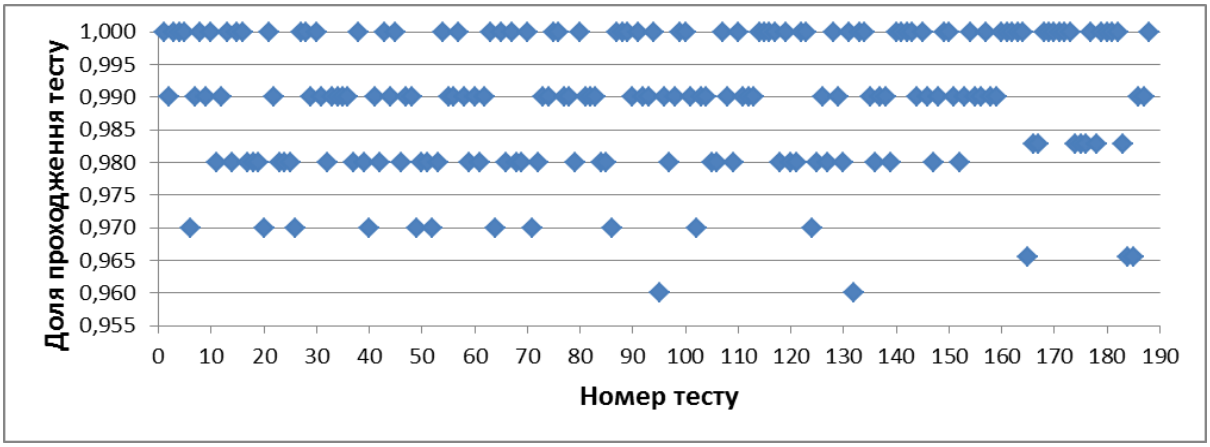


Рис. 6.28. Статистичний портрет програмної реалізації алгоритму на основі комбінації матричних та розширених матричних операцій текстового файлу

Зведені результати тестування текстового файлу криптоалгоритмом на основі комбінації операцій матричного та розширеного матричного перетворення програмним пакетом NIST STS подані в табл. 6.19.

Як видно з результатів, досліджувана послідовність пройшла комплексний контроль за методикою NIST STS.

Проведемо обчислювальний експеримент, використавши в алгоритмі криптографічного розширеного матричного перетворення додатковий блок криптографічного перетворення матричними операціями.

Таблиця 6.19

Зведені результати тестування криптоперетворення текстового файлу на основі комбінації матричних та розширених матричних операцій

Генератор	Кількість тестів, в яких тестування пройшло	
	99% послід.	96% послід.
Матричне-розширене матричне криптографічне перетворення	126 (67 %)	188 (100 %)

Перевіримо можливість виявлення статистичних закономірностей на невипадковій монотонно зростаючій послідовності з циклом повторення 64 байти, в яку записані коди чисел 64, 65, 66, …, 128 для криптоалгоритму, який складається із послідовного виконання комбінації розширених матричних та матричних операцій.

Результати тестування наведені в додатку Б.

Статистичний портрет програмної реалізації крипто алгоритму на основі комбінації розширених матричних та матричних операцій перетворення інформації зображено на рис. 6.29.

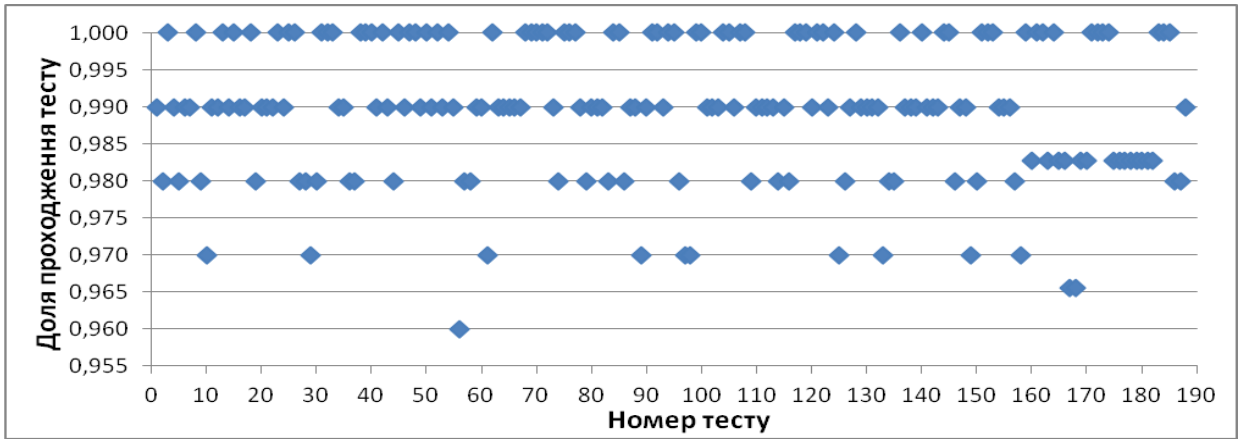


Рис. 6.29. Статистичний портрет програмної реалізації алгоритму на основі комбінації розширених матричних та матричних операцій

Зведені результати тестування комбінаційного розширеного матричного-матричного перетворення невипадкової монотонно зростаючої послідовності з циклом повторення 64 байти програмним пакетом NIST STS подані в табл. 6.20.

Таблиця 6.20

Зведені результати тестування розширеного матричного-матричного перетворення невипадкової монотонно зростаючої послідовності з циклом повторення 64 байти

Генератор	Кількість тестів, в яких тестування пройшло	
	99 % послід.	96 % послід.
Розширене матричне-матричне криптографічне перетворення	133 (70,7 %)	188 (100 %)

Як видно з результатів, досліджувана послідовність пройшла комплексний контроль за методикою NIST STS [24].

Перевіримо можливість виявлення статичних властивостей результатів розширеного матричного-матричного криптографічного перетворення невипадкової монотонно зростаючої послідовності з циклом повторення 256 байтів, в яку записані коди чисел 0, 1, 2, …, 255.

Результати тестування наведені в додатку Б.

Статистичний портрет зображено на рис. 6.30.

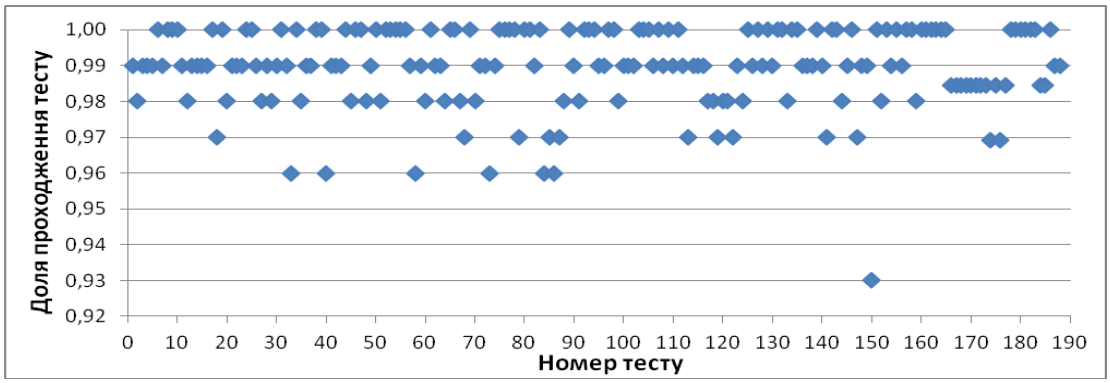


Рис. 6.30. Статистичний портрет програмної реалізації алгоритму на основі комбінації розширених матричних та матричних операцій

Зведені результати тестування комбінації розширеного матричного та матричного перетворення невипадкової монотонно зростаючої послідовності з циклом повторення 256 байтів програмним пакетом NIST STS подані в табл. 6.21.

Таблиця 6.21

Зведені результати тестування комбінації розширеного матричного та матричного перетворення невипадкової монотонно зростаючої послідовності з циклом повторення 256 байтів

Генератор	Кількість тестів, в яких тестування пройшло	
	99 % послід.	96 % послід.
Розширене матричне-матричне криптографічне перетворення	132 (70,2 %)	187 (99,5 %)

Як видно з результатів, досліджувана послідовність не пройшла комплексний контроль за методикою NIST STS, тому що один тест не пройдений:

```
------------------------------------------------------------------------------
RESULTS FOR THE UNIFORMITY OF P-VALUES AND THE PROPORTION OF PASSING SEQUENCES
------------------------------------------------------------------------------
   generator is <KOD_CHT1.bin>
------------------------------------------------------------------------------
 C1  C2  C3  C4  C5  C6  C7  C8  C9 C10  P-VALUE  PROPORTION  STATISTICAL TEST
------------------------------------------------------------------------------
 16  10   5   7   9  11   9   9   8  16  0.249284   0.9300 *  NonOverlappingTemplate
```

Перевіримо статистичні властивості даного крипто алгоритму на основі комбінації операцій розширеного матричного та матричного перетворення на результатах шифрування послідовності, що складається із константи - числа зі значенням 150.

Отримані результати на основі пакету NIST STS наведені в додатку Б.17.

Статистичний портрет програмної реалізації комбінаційного алгоритму розширеного матричного-матричного перетворення числової послідовності з константи 150 зображено на рис. 6.31.

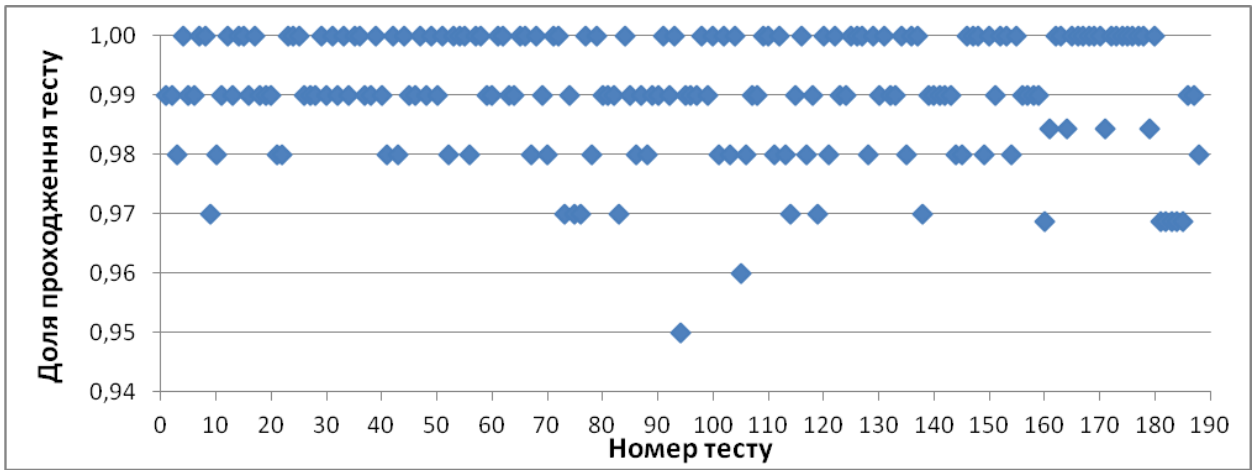


Рис. 6.31. Статистичний портрет програмної реалізації алгоритму комбінації розширеного матричного та матричного перетворення числової послідовності.

Зведені результати тестування комбінації розширеного матричного та матричного перетворення послідовності із числової константи 150 програмним пакетом NIST STS подані в табл. 6.22.

Таблиця 6.22

Зведені результати тестування комбінаційним алгоритмом розширеного матричного-матричного перетворення

Генератор	Кількість тестів, в яких тестування пройшло	
	99 % послід.	96 % послід.
Розширене матричне-матричне криптографічне перетворення	141 (75 %)	187 (99,5 %)

Як видно з результатів, досліджувана послідовність не пройшла комплексний контроль за методикою NIST STS [24]. Один із 15 тестів не пройдений:

```
------------------------------------------------------------------------------
RESULTS FOR THE UNIFORMITY OF P-VALUES AND THE PROPORTION OF PASSING SEQUENCES
------------------------------------------------------------------------------
   generator is <KOD_CHT1.bin>
------------------------------------------------------------------------------
 C1  C2  C3  C4  C5  C6  C7  C8  C9 C10  P-VALUE  PROPORTION  STATISTICAL TEST
------------------------------------------------------------------------------

11  14  13  10  13 7   8  8   8  8  0.739918  0.9500 *
NonOverlappingTemplate
```

Перевіримо статистичні властивості результатів комбінації операцій розширеного матричного та матричного криптографічного перетворення текстової інформації на прикладі електронних інформаційних ресурсів, а саме художньої літератури в текстовому форматі.

Результати тестування наведені в додатку Б.

Статистичний портрет програмної реалізації комбінаційного алгоритму розширеного матричного-матричного криптографічного перетворення текстового файлу зображено на рис. 6.32.

Зведені результати тестування текстового файлу криптоалгоритмом на основі комбінації операцій розширеного матричного та матричного перетворення програмним пакетом NIST STS подані в табл. 6.23.

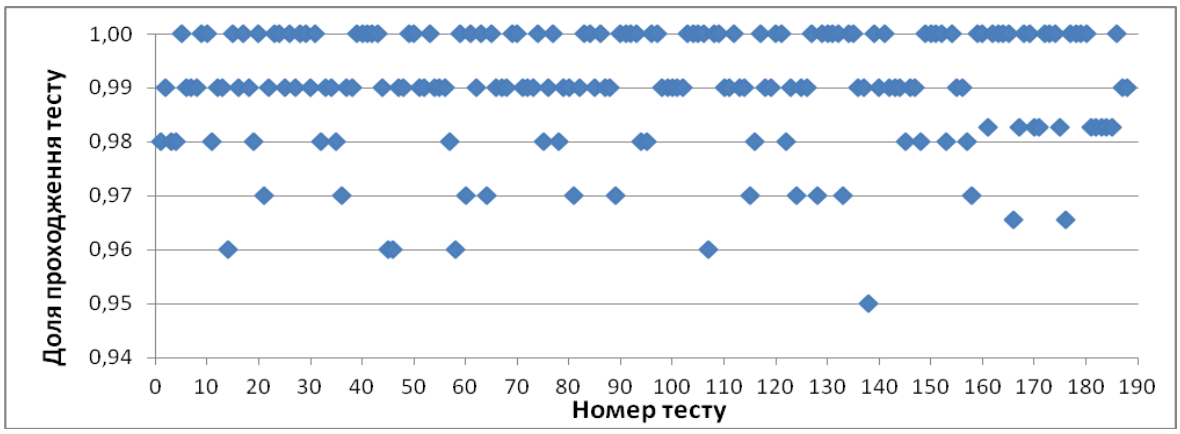


Рис. 6.32. Статистичний портрет програмної реалізації алгоритму на основі комбінації розширених матричних та матричних операцій текстового файлу

Таблиця 6.23

Зведені результати тестування криптоперетворення текстового файлу на основі комбінації розширених матричних та матричних операцій

Генератор	Кількість тестів, в яких тестування пройшло	
	99% послід.	96% послід.
Розширене матричне-матричне криптографічне перетворення	141 (75 %)	187 (99,5 %)

Як видно з результатів, досліджувана послідовність не пройшла комплексний контроль за методикою NIST STS. Один із 15 тестів не пройдений:

```
------------------------------------------------------------------------------
RESULTS FOR THE UNIFORMITY OF P-VALUES AND THE PROPORTION OF PASSING SEQUENCES
------------------------------------------------------------------------------
   generator is <KOD_CHT1.bin>
------------------------------------------------------------------------------
 C1  C2  C3  C4  C5  C6  C7  C8  C9 C10  P-VALUE  PROPORTION  STATISTICAL TEST
------------------------------------------------------------------------------
 2   4   6  13  13  22   6   9   7  18  0.000029 * 0.9900     FFT
9  12   5  17  13   8  11   7 8  10  0.304126  0.9500 * NonOverlappingTemplate
```

Слід відмітити особливість використання операцій розширеного матричного криптографічного перетворення. Використання даних операцій, побудованих на основі лише комбінації груп базових операцій та перестановки без використання групи операцій інверсії, забезпечує погіршення статистичного портрету результатів алгоритму.

Крім того, статистичний аналіз результатів тестування послідовного виконання комбінації матричного та розширеного матричного криптографічного перетворення і навпаки показали, що кращі результати забезпечує використання комбінації операцій, в якій кінцевою операцією є розширене матричне криптографічного перетворення. Це пояснюється тим, що операція розширеного матричного криптографічного перетворення вносить в алгоритм додаткову нелінійність.

Перевіримо статистичні властивості результатів застосування примітиву ковзного шифрування, синтезованого на основі операцій матричного криптографічного перетворення, при шифруванні текстової інформації, а саме художньої літератури в текстовому форматі.

Результати тестування наведені в додатку Б.

Статистичний портрет програмної реалізації шифрування на основі примітиву ковзного шифрування зображено на рис. 6.33.

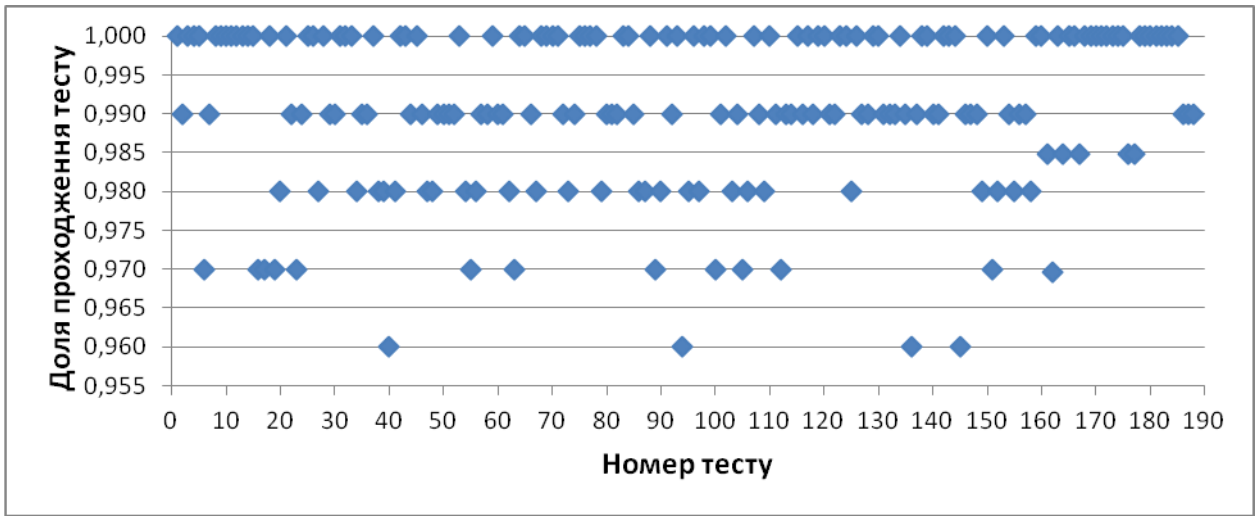


Рис. 6.33. Статистичний портрет програмної реалізації примітиву ковзного шифрування на основі матричних операцій

Зведені результати тестування криптографічного примітиву ковзного шифрування програмним пакетом NIST STS подані в табл. 6.24.

Таблиця 6.24

Зведені результати тестування криптографічного примітиву ковзного шифрування

Генератор	Кількість тестів, в яких тестування пройшло	
	99 % послід.	96 % послід.
Криптографічний примітив ковзного шифрування	139 (74 %)	188 (100 %)

Як видно з результатів, досліджувана послідовність пройшла комплексний контроль за методикою NIST STS [24].

Дослідження статистичних властивостей результатів перетворення інформації за схемами реалізації матричних операцій криптографічного перетворення на основі різних модулів (рис. 6.5 а),б)) та визначення ефективності застосування кожного із запропонованих способів уже здійснено у попередньому підрозділі.

Операції криптографічного перетворення синтезовані на основі розроблених методів можуть бути використані в якості алгоритмів вбудовування інформації в стегоконтейнер на основі ключового елементу [33, 34, 53-55].

6.3 Оцінка ефективності застосування операцій криптографічного перетворення для алгоритмів захисту інформаційних ресурсів

Проведемо оцінку ефективності криптографічних алгоритмів на основі розрахунку показників швидкості та криптостійкості [26].

При проведенні досліджень обмежимося:

– алгоритмами випадкового вибору операцій криптографічного перетворення на основі гамуючої послідовності;

– операціями матричного та розширеного матричного криптографічного перетворення.

З врахуванням вказаних обмежень криптостійкість (K) визначається криптостійкістю гамуючої послідовності ($K_г$) і операцій криптоперетворення ($K_{оп}$), як $K = K_г \cdot K_{оп}$. Слід врахувати, що $K_г$ вже забезпечує вимоги до криптостійкості. Кількісна оцінка зміни криптостійкості відносно криптостійкості гамуючої послідовності визначається як $k_K = \frac{K_г \cdot K_{оп}}{K_г} = K_{оп}$.

Розглянемо більш детально застосування матричних операцій криптографічного перетворення та розрахуємо їх показники криптостікості та швидкості.

Криптостійкість і швидкість шифрування (k_v – коефіцієнт швидкодії) визначаються такими параметрами: $N_{мо}(n)$ – кількість матричних операцій вибраної розмірності (n), n_k – розрядність команди виконання послідовностей операцій криптоперетворення, $N_{оп}$ – кількість операцій у послідовності, яка реалізує команду.

Підмножина випадково вибраних операцій для даного алгоритму визначається як $П_о = 2^{n_k} \cdot N_{оп}$. Кількість випадково вибраних підмножин визначаться як кількість сполучень $N_П = C^{N_{оп}}_{N_{мо}(n)}$.

Практична криптостійкість залежить від розрядності пароля $R_П = (2^{n_k} \cdot N_{оп}) \log_2(N_{мо}(n)) = П_0 \cdot \log_2(N_{мо}(n))$ і буде пропорційною величині $K_{оп} = 2^{R_П}$.

Наприклад, якщо $n = 4$, $n_k = 4$, а $N_{оп} = 4$, тоді $П_о = 64$, $R_П = 64 \cdot \log_2 21840 = 927$ і $K_{оп} = 2^{927}$, що є прийнятним значенням, тому що загальна криптостійкість збільшиться в $1{,}12 \cdot 10^{280}$ разів пропорційно.

Зменшити кількість розрядів додаткового пароля можливо за рахунок визначення $N_{оп}$ при ініціалізації системи, а в додатковий пароль включати лише перестановки вибраних операцій або перестановки послідовностей операцій, які виконуються відповідно до команд перетворення. Для наведеного прикладу в

першому випадку отримаємо: $R_{П1} = 64 \cdot \log_2 64 = 384$ і $K_{оп1} = 2^{386} = 3{,}94 \cdot 10^{115}$, в другому випадку отримаємо $R_{П2} = 16 \cdot \log_2 16 = 64$ і $K_{оп2} = 2^{64} = 1{,}84 \cdot 10^{20}$

Наприклад, якщо $n = 3$, $n_k = 3$, а $N_{оп} = 3$, тоді $R_П = 24 \cdot \log_2 1344 = 251$ і $K_{оп} = 2^{251}$, що є прийнятним значенням.

Наприклад, якщо $n = 4$, $n_k = 5$, а $N_{оп} = 6$, тоді $R_П = 192 \cdot \log_2 21840 = 2780$ і $K_{оп} = 2^{2780}$, що є прийнятним значенням.

Здіснимо оцінку криптостійкості реалізації операцій криптографічного перетвореня інформації на основі операцій розширеного матричного перетворення.

Реалізація операцій розширеного матричного криптографічного перетворення відповідає вимогам програмного пакета статистичного тестування NIST STS.

Практичне використання операцій розширеного матричного криптографічного перетворення, виходячи з проведених досліджень, проводиться на основі гамуючої послідовності.

Застосуємо метод підвищення швидкості шифрування [37-41], сутність якого полягає у використанні гамуючої послідовності як послідовного набору команд виконання випадково вибраної підмножини операцій криптоперетворення. Необхідно відзначити, що криптостійкість (K) використання цього методу визначається як і для матричних операцій $K = K_г \cdot K_{оп}$, де $K_г$ – криптостійкість гамуючої послідовності, $K_{оп}$ – криптостійкість послідовностей операцій криптоперетворення.

Підмножина випадково вибраних операцій для реалізації методу використання розширених операцій визначається як $П_о = 2^{n_k} \cdot N_{оп}$. Практична криптостійкість залежить від розрядності пароля $R_П = (2^{n_k} \cdot N_{оп}) log_2 2160 = П_0 \, log_2 2160$ і буде пропорційною величині $K_{оп} = 2^{R_П}$.

Наприклад, якщо $n_k = 4$, а $N_{оп} = 4$, тоді $П_о = 64$, $R_П = 64 \cdot \log_2 2160 = 709$ і $K_{оп} = 2^{709}$, що є прийнятним значенням, тому що загальна криптостійкість збільшиться в $2{,}7 \times 10^{213}$ разів пропорційно.

Наприклад, якщо $n_k = 4$, а $N_{оп} = 2$, тоді $П_о = 32$, $R_П = 32 \cdot log_2 2160 = 355$ і $K_{оп} = 2^{355}$, що є прийнятним значенням, так як загальна криптостійкість збільшиться в $7{,}3 \times 10^{106}$ разів пропорційно.

Наприклад, якщо $n_k = 3$, а $N_{оп} = 6$, тоді $П_о = 48$, $R_П = 48 \cdot \log_2 2160 = 532$ і $K_{оп} = 2^{532}$, що є прийнятним значенням, так як загальна криптостійкість збільшиться в $1{,}4 \times 10^{160}$ разів пропорційно.

Всі проведені дослідження показали ефективність використання методу розширеного матричного криптографічного перетворення, який забезпечує підвищення криптостійкості перетвореної інформації в 2160^{Nc} разів, де Nc – кількість циклів криптографічного перетворення. Ця криптостійкість розраховувалася теоретично, при цьому не враховувалася її залежність від довжини пароля.

Криптостійкість алгоритму, суть якого полягає у комбінації операцій матричного та розширеного матричного криптографічного перетворення визначається як [4]

$$K = K_M \cdot K_{PM}.$$

Кількісна оцінка зміни криптостійкості алгоритму шифрування на основі гамуючої послідовності визначається як

$$k = \frac{K_M \cdot K_{PM} \cdot K_Г}{K_Г} = K_M \cdot K_{PM}.$$

Так як практична криптостійкість залежить від розрядності пароля, то для комбінації операцій матричного та розширеного матричного криптографічного

перетворення довжина пароля визначається як

$$R_{П} = R_{П}^{M} + R_{П}^{PM} = (2^{n_k} \cdot N_{оп}) \log_2 (N_{мо}(n)) + \\ + (2^{n_k} \cdot N_{оп}) \log_2 (N_{рмо}(n)) = П_0 \log_2 (N_{мо}(n)) + П_0 \log_2 (N_{рмо}(n))$$

і буде пропорційною величині $K_{оп} = 2^{R_{П}} = 2^{(R_{П}^{M} + R_{П}^{PM})}$.

Наприклад, якщо $n = 3$, $n_k = 3$, а $N_{оп} = 3$, тоді $R_{П} = 24 \cdot \log_2 1344 + 24 \cdot \log_2 2160 = 515$ і $K_{оп} = 2^{515} = 10^{155}$, що є прийнятним значенням.

Зведені результати розрахунків довжини пароля для комбінації операцій матричного та розширеного матричного криптографічного перетворення показані в табл. 6.25 та табл. 6.26

Таблиця 6.25

Результати розрахунків довжини пароля

Розрядність матричних та розширених матричних операцій n=3																
n_k	3	4	5	6	3	4	5	6	3	4	5	6	3	4	5	6
Nоп	2	2	2	2	3	3	3	3	4	4	4	4	5	5	5	5
Rп	344	687	1374	2748	515	1031	2061	4122	687	1374	2748	5496	859	1718	3435	6870

Таблиця 6.26

Результати розрахунків довжини пароля

Розрядність матричних операцій n=4 та розширених матричних n=3 операцій																
n_k	3	4	5	6	3	4	5	6	3	4	5	6	3	4	5	6
Nоп	2	2	2	2	3	3	3	3	4	4	4	4	5	5	5	5
Rп	408	816	1632	3263	612	1224	2447	4894	816	1632	3263	6526	1020	2039	4079	8157

Здійснимо розрахунок швидкості виконання матричних операцій криптографічного перетворення. Для цього використаємо показник коефіцієнта швидкодії [53, 54].

Коефіцієнт швидкодії визначається відношеннями кількості розрядів інформації, які зашифровані з використанням матричних операцій і без

використання, як $k_v = \frac{n \cdot N_{on}}{n_k}$.

Наприклад, якщо $n = 3$, $n_k = 3$, а $N_{on} = 3$, тоді, коефіцієнт швидкодії для цього прикладу буде $k_v = \frac{n \cdot N_{on}}{n_k} = \frac{3 \cdot 3}{3} = 3$ за умови паралельної реалізації матричних операцій та елементарних функцій.

Наприклад, якщо $n = 4$, $n_k = 4$, а $N_{on} = 4$, коефіцієнт швидкодії для цього прикладу буде $k_v = \frac{n \cdot N_{on}}{n_k} = \frac{4 \cdot 4}{4} = 4$ за умови паралельної реалізації матричних операцій та елементарних функцій.

Наприклад, якщо $n = 4$, $n_k = 5$, а $N_{on} = 6$, тоді коефіцієнт швидкодії для цього прикладу буде $k_v = \frac{n \cdot N_{on}}{n_k} = \frac{4 \cdot 6}{5} = 4{,}8$ за умови паралельної реалізації матричних операцій та елементарних функцій.

Здійснимо розрахунок швидкості виконання розширених матричних операцій криптографічного перетворення. Для цього використаємо показник коефіцієнта швидкодії.

Оскільки операції криптоперетворення можуть виконуватися паралельно, то час криптоперетворення буде визначатися лише часом формування n_k розрядів гамуючої послідовності. Тоді збільшення швидкості криптографічного перетворення інформації буде визначатися відношенням розрядності інформації, яка шифрується на основі операцій розширеного матричного перетворення під управлінням гамуючої послідовності, до кількості розрядів, над якими виконано гамування. Для нашого прикладу коефіцієнт збільшення швидкості шифрування буде визначатися як $k_v = \frac{3 \cdot N_{on}}{n_k} = 3$.

Наприклад, якщо $n_k = 4$, а $N_{on} = 2$, тоді коефіцієнт збільшення швидкості шифрування буде визначатися як $k_v = \frac{3 \cdot N_{on}}{n_k} = 1{,}5$.

Наприклад, якщо $n_k = 3$, а $N_{on} = 6$, тоді коефіцієнт збільшення швидкості шифрування буде визначатися як $k_v = \frac{3 \cdot N_{on}}{n_k} = 6$.

Наприклад, якщо $n = 5$, $n_k = 3$, а $N_{on} = 5$, тоді коефіцієнт збільшення швидкості шифрування буде визначатися як $k_v = \frac{5 \cdot N_{on}}{n_k} = 8$.

Як видно з прикладів розширене матричне перетворення залежно від параметрів n_k і N_{on} дає змогу збільшити криптостійкість від 10^{32} до 10^{150} разів пропорційно відносно потокового шифрування при зменшенні часу шифрування в 1,5 до 6 разів.

При використанні трирозрядних матричних перетворень результати розрахунку довжини ключової послідовності залежно від розрядності команди виконання послідовностей операцій криптоперетворення та кількості операцій в послідовності, яка реалізує команду, зображені на рис 6.34.

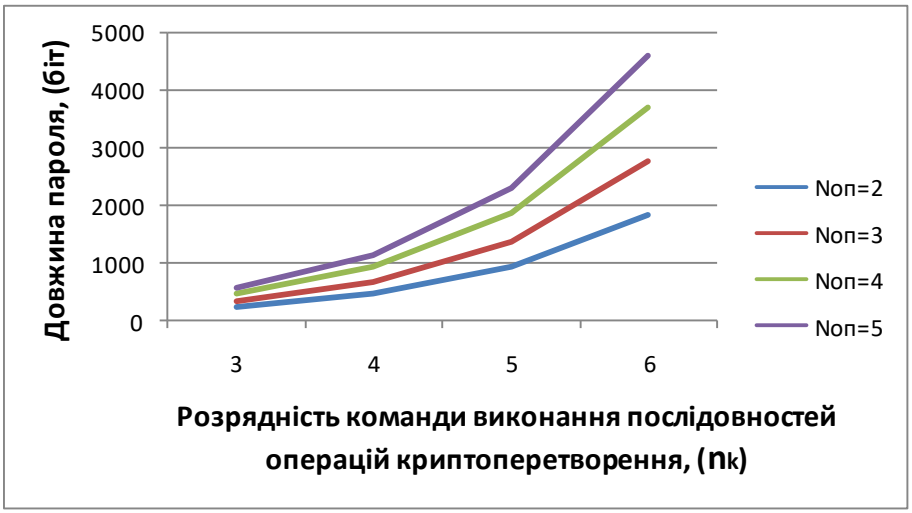
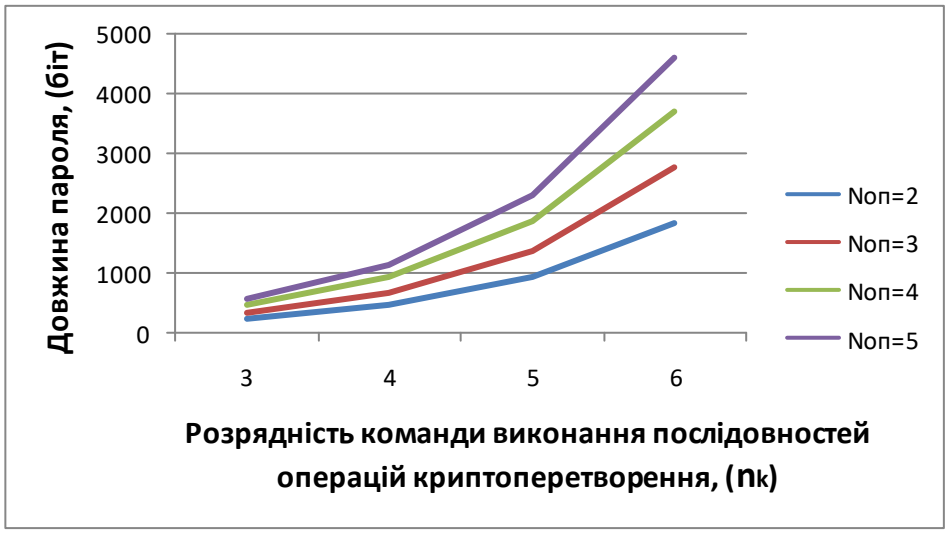


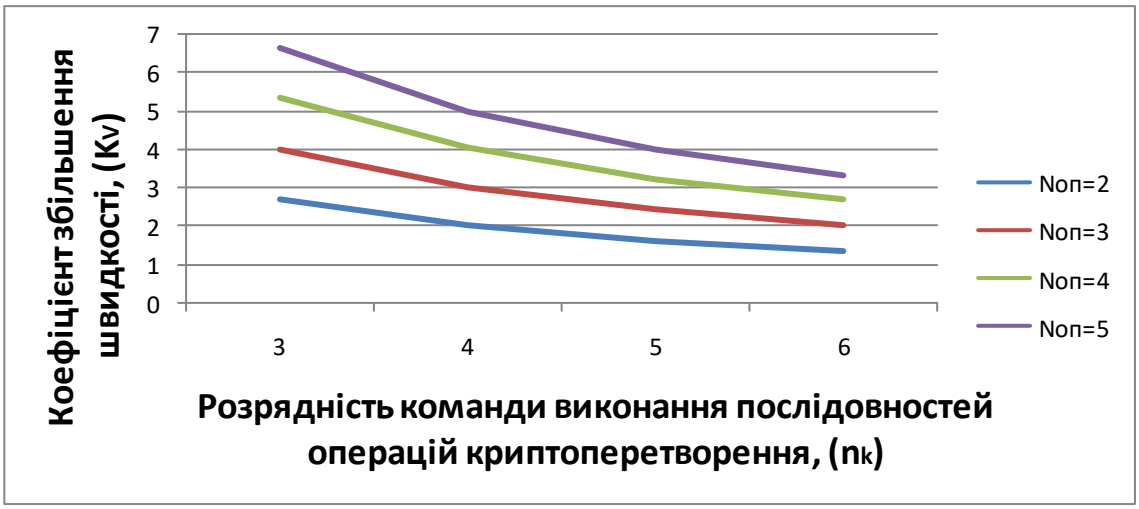
Рис. 6.34. Результати розрахунку довжини ключової послідовності при використанні тририрозрядних матричних перетворень

При використанні чотирирозрядних матричних перетворень результати розрахунку довжини ключової послідовності залежно від розрядності команди

виконання послідовностей операцій криптоперетворення та кількості операцій в послідовності, яка реалізує команду, а також розрахунок коефіцієнта збільшення швидкості зображені на рис 6.35 а) та рис. 6.35 б) відповідно.



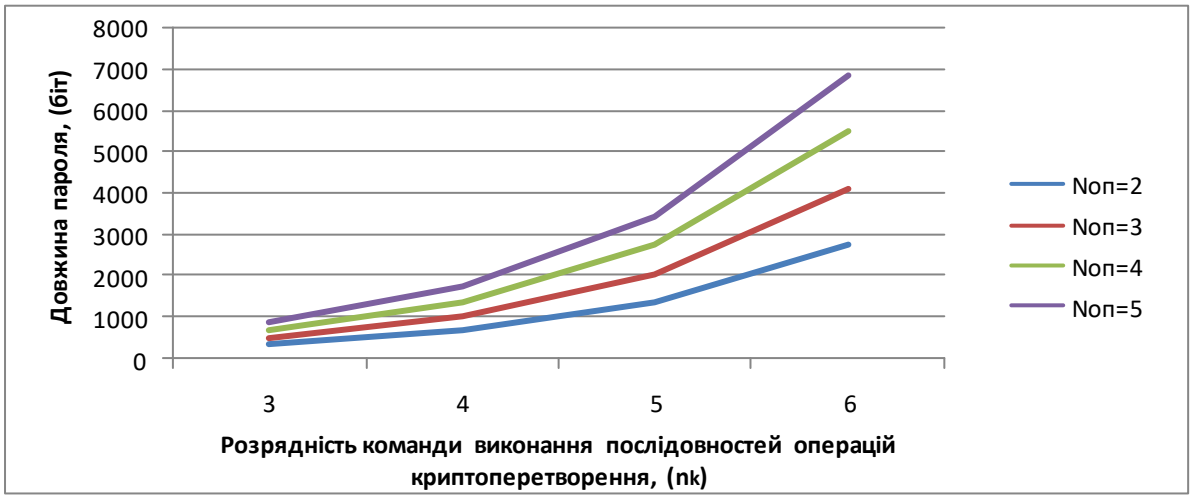
а). Довжина ключової послідовності



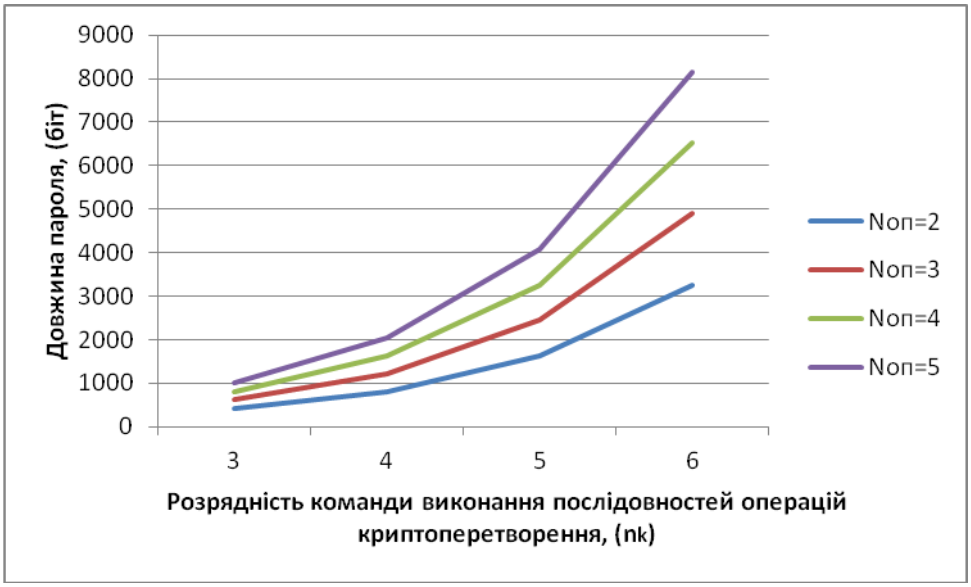
б) Коефіцієнт швидкодії

Рис. 6.35. Результати розрахунку довжини ключової послідовності та коефіцієнта швидкодії при використанні чотирирозрядних матричних перетворень

На рис 6.36 а) та рис. 6.36 б) відображені результати розрахунку довжини ключової послідовності при використанні комбінації матричних та розширених матричних перетворень.



а). Результати розрахунку довжини ключової послідовності



б) Результати розрахунку довжини ключової послідовності

Рис. 6.36. Результати розрахунку довжини ключової послідовності при використанні комбінації матричних та розширених матричних перетворень

Зведені результати розрахунку коефіцієнта швидкодії при використанні матричних перетворень зображені на рис 6.37 [53,54].

Вибір параметрів $N_{мо}(n)$, n_k і $N_{оп}$ дає можливість забезпечити необхідні значення швидкості шифрування та криптостійкості за рахунок збільшення апаратної та програмної складності реалізації системи криптографічного захисту інформації.

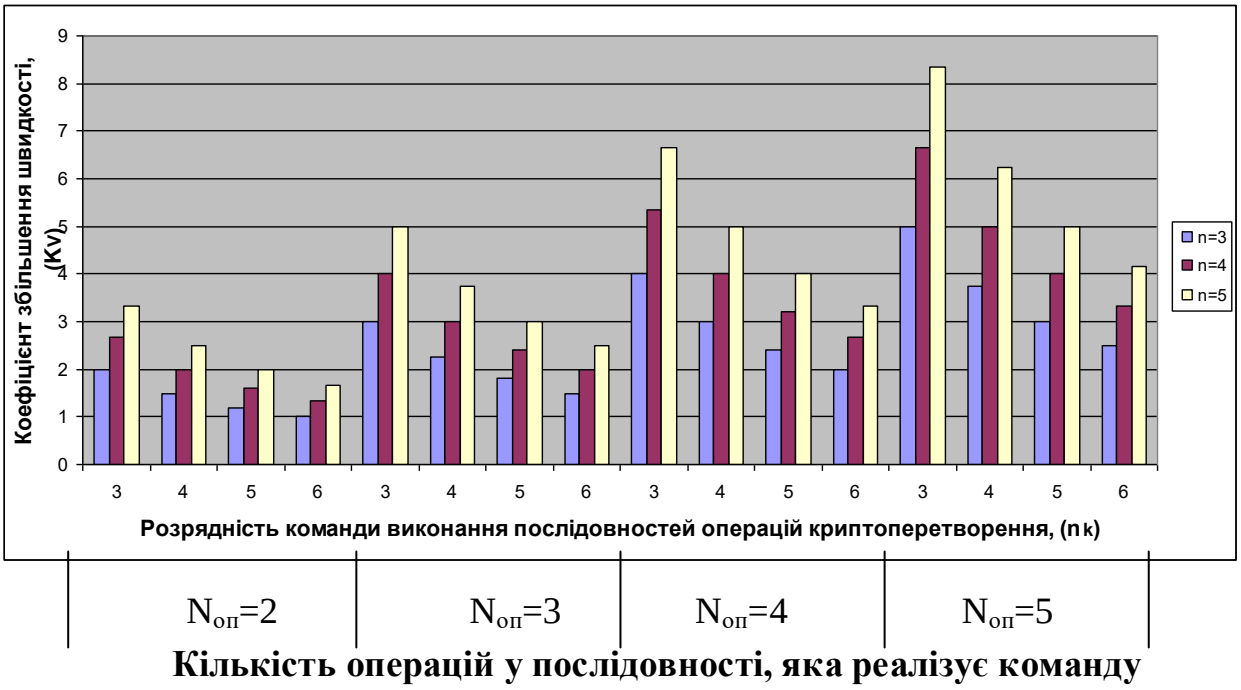


Рис. 6.37. Результати розрахунку коефіцієнта швидкодії при використанні матричних перетворень

Швидкість виконання матричних та розширених матричних операцій алгоритму криптографічного перетворення доцільніше визначати через час [4, 5]:

$$T_{(M+PM)} = T_{(PM+M)} = \frac{1}{T_M} + \frac{1}{T_{PM}} = \frac{T_M + T_{PM}}{T_M \cdot T_{PM}} = \frac{1}{3} + \frac{1}{6} = \frac{6+3}{18} = \frac{9}{18} = \frac{1}{2}.$$

Так як швидкість обернено пропорційна часу, тоді швидкість розраховуватиметься як [4, 5]:

$$V_{(M+PM)} = \frac{T_M \cdot T_{PM}}{T_M + T_{PM}}.$$

Таким чином застосування операцій розширеного матричного перетворення залежно від параметрів n_k і N_{on} дає змогу збільшити криптостійкість від 10^{32} до 10^{150} разів пропорційно відносно потокового шифрування при зменшенні часу шифрування в 1,5 до 6 разів, а застосування синтезованих операції криптографічного перетворення на основі запропонованих варіантів комбінації

використання матричного та розширеного матричного перетворення при конструюванні алгоритмів дає можливість збільшити криптостійкість від 2^{166} до 2^{8157} разів пропорційно відносно потокового шифрування при зменшенні часу шифрування від 1,3 до 8 разів.

Розроблені методи та засоби криптографічного перетворення забезпечують вирішення важливої науково-технічної задачі підвищення якості функціонування систем захисту інформаційних ресурсів на основі матричного криптографічного перетворення.

6.4 Висновки до шостого розділу

Удосконалено методи синтезу та аналізу крипто алгоритмів на основі операцій криптографічного перетворення інформації шляхом послідовно-паралельної реалізації операцій на макро та мікрорівнях, що забезпечило можливість вирішення протирічь між криптостійкістю, складністю та швидкістю для досягнення оптимальної ефективності виходячи з задач проектування.

1. Удосконалено методи синтезу криптографічних алгоритмів на основі операцій криптографічного перетворення інформації, що забезпечило підвищення теоретичної стійкості та швидкодії.

2. На основі дослідження зміни властивостей результатів криптографічного перетворення в залежності від вибору різної основи модуля запропоновані способи та рекомендації щодо застосування матричних операцій криптографічного перетворення на основі суми за модулем для шифрування інформації. За допомогою проведеного тестування статистичних властивостей запропонованих способів реалізації криптографічного перетворення інформації пакетом тестів NIST STS обґрунтовано ефективність використання операції додавання за модулем 2 в якості кінцевої за умови використання комбінації операцій додавання за будь-яким іншим 2^n модулем з метою підвищення стійкості до лінійного криптоаналізу.

3. Проведена оцінка статистичних властивостей криптоалгоритмів на основі пакету тестів NIST STS підтвердила можливість застосування даних крипто алгоритмів в системах захисту інформації. Аналіз результатів тестування підтвердив доцільність використання операцій криптографічного перетворення інформації для синтезу нових та вдосконалення існуючих криптоалгоритмів.

4. Застосування операцій криптографічного перетворення для алгоритмів захисту інформаційних ресурсів за результатами моделювання забезпечила можливість вирішення протирічь між криптостійкістю, складністю та швидкістю для досягнення оптимальної ефективності виходячи з задач проектування.

Результати розділу опубліковані в [1, 5, 26-28, 32, 46-49, 68, 69, 70, 72].

ВИСНОВКИ

У дисертаційній роботі розв’язана актуальна науково-технічна проблема підвищення ефективності функціонування систем комп’ютерної криптографії шляхом створення методології синтезу операцій перетворення інформації та побудови криптографічних примітивів на їх основі.

Основні наукові та практичні результати полягають у наступному:

1. Здійснено побудову та формалізацію методології синтезу і аналізу логічних операцій перетворення інформації для систем комп’ютерної криптографії шляхом розробки й узагальнення методів синтезу елементарних функцій та операцій на основі них. Основні положення методології дозволили розробити технологію побудови методів синтезу операцій прямого, оберненого та взаємного криптографічного перетворення інформації. Одержані результати забезпечують розробників криптографічних алгоритмів новими можливостями вдосконалення як криптопримітивів, так і криптосистем в цілому, зокрема розширенням бази операцій, що використовуються для їх побудови. Удосконалено технологію організації доступу до інформаційних ресурсів шляхом реалізації методу підвищення оперативності доступу до конфіденційних інформаційних ресурсів на основі одержаних математичних моделей синтезу операцій взаємного криптографічного перетворення, застосування яких дозволить створювати програмно-апаратні засоби, які забезпечать підвищення швидкості доступу до конфіденційних інформаційних ресурсів.

2. Отримали подальший розвиток математичні моделі й методи синтезу елементарних функцій і операцій криптоперетворення на основі запропонованої методології та вибраної із класифікації групи нелінійних елементарних функцій розширеного матричного криптоперетворення шляхом вдосконалення математичного апарату для синтезу прямих та обернених матричних моделей не афінних дискретних перетворень, що в сукупності забезпечили можливість синтезу операцій нелінійних криптографічних перетворень. Удосконалено

математичний апарат для синтезу моделей не афінних дискретних перетворень, застосування якого забезпечить можливість побудови нелінійних матричних операцій криптографічного перетворення. Розроблені методи, моделі та вдосконалений математичний апарат в сукупності підтверджують коректність основних положень запропонованої методології синтезу операцій криптографічного перетворення інформації.

3. На прикладі примітивів ковзного шифрування удосконалено методи побудови криптографічних примітивів шляхом застосування матричних операцій криптографічного перетворення, що дало змогу побудувати узагальнені моделі операцій, які реалізують багаторазове ковзне шифрування. Одержано узагальнені рекурентні послідовності, що описують функції перетворення інформації при здійсненні багаторазового ковзного шифрування, що дало змогу побудувати алгоритми паралельної реалізації криптопримітивів багаторазового ковзного шифрування заданої кількості ітерацій. Ці результати забезпечили підвищення швидкості шифрування до двох разів та стійкість до лінійного криптоаналізу при реалізації багаторазового ковзного шифрування.

4. Розроблено технологію синтезу операцій для мультиопераційних матричних криптографічних примітивів на основі побудови нових груп операцій з точністю до перестановки як вхідних операндів, так і результатів виконання операції, шляхом використання запропонованої табличної моделі операції криптоперетворення. Застосування отриманих результатів забезпечило варіативність операцій при вдосконаленні мультиопераційних криптопримітивів та підвищення стійкості криптоалгоритмів, побудованих на їх основі.

5. Удосконалено методи синтезу та аналізу криптографічних алгоритмів на основі узагальненої моделі криптоалгоритму шляхом послідовно-паралельної реалізації операцій криптографічного перетворення інформації на мікро- та макрорівнях. Отримані результати забезпечили можливість вирішення протиріч між криптостійкістю, складністю та швидкістю в процесі проектування криптоалгоритмів. Отримана можливість забезпечення гнучкого керування

даними параметрами в процесі синтезу криптоалгоритмів для досягнення заданої ефективності, виходячи з задач проектування.

6. На підставі проведених досліджень одержано такі практичні результати: розроблено методологію синтезу операцій криптографічного перетворення інформації в рамках запропонованої концепції побудови алгоритмів захисту інформації в комп'ютерних системах та мережах на їх основі з можливістю підбору оптимальних показників криптостійкості та швидкодії, що дає змогу покращити ефективність функціонування системи комп'ютерної криптографії; технологію побудови та використання криптопримітивів на основі синтезованих операцій криптографічного перетворення інформації з можливістю їх паралельного виконання, що дає виграш у швидкості та часі здійснення перетворення безпосередньо інформації, варіанти реалізації на програмному та апаратному рівнях нових груп криптографічних операцій заданої розрядності, що володіють властивостями афінності та нелінійності, зокрема матричного та розширеного матричного перетворення. Застосування синтезованих операцій криптографічного перетворення на основі запропонованих варіантів комбінації використання матричного та розширеного матричного перетворення при конструюванні алгоритмів дає можливість збільшити криптостійкість (від 2^{166} до 2^{8157} разів) пропорційно відносно потокового шифрування при зменшенні часу шифрування (від 1,3 до 8 разів).

Практична цінність роботи підтверджена актами впровадження на підприємствах та організаціях: НВК «Фотоприлад», «Науково-дослідний інститут «Акорд» та ПП «Сенсорна електроніка» (м. Черкаси), ТОВ «Люменс-груп» (м. Кіровоград) та в освітній процес у навчальних закладах: Черкаському державному технологічному університеті, Черкаському національному університеті імені Б. Хмельницького, Національному аерокосмічному університеті імені М. Є. Жуковського «ХАІ», Кіровоградському національному технічному університеті.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Бабенко В. Г. Дослідження матричних операцій криптографічного перетворення на основі арифметичних операцій за модулем. *Системи управління, навігації та зв'язку*. 2012. Вип. 4 (24). С. 85–88.
2. Бабенко В. Г. Параллельная реализация скользящего шифрования. *Системи обробки інформації*. 2013. Вип. 9 (116). С. 131–134.
3. Бабенко В. Г. Оптимизация матричных операций скользящего шифрования. *Системи озброєння і військова техніка*. 2013. № 4 (36). С. 132–135.
4. Бабенко В. Г. Складності та особливості побудови ефективних криптоалгоритмів. *Вісник Черкаського державного технологічного університету*. 2014. № 3. С. 87–91.
5. Бабенко В. Г. Застосування операцій криптографічного перетворення для синтезу криптоалгоритмів. *Сучасна спеціальна техніка*. 2014. № 3 (38). С. 49–55.
6. Рудницький В. М., Миронець І. В., Бабенко В. Г. Обґрунтування можливості розширення набору функцій перекодування інформації для захисту конфіденційних інформаційних ресурсів. *Системи управління, навігації та зв'язку*. 2010. Вип. 2 (14). С. 118–122.
7. Рудницький В. М., Миронець І. В., Бабенко В. Г. Методологія підвищення оперативності доступу до конфіденційних інформаційних ресурсів. *Системи обробки інформації*. 2010. Вип. 5 (86). С. 15–19.
8. Рудницький В. М., Миронець І. В., Бабенко В. Г. Реалізація методу підвищення оперативності доступу до конфіденційних інформаційних ресурсів. *Вісник Черкаського державного технологічного університету.* 2010. № 3. С. 60–65.

9. Рудницький В. М., Бабенко В. Г., Жиляєв Д. А. Алгебраїчна структура множини логічних операцій кодування. *Наука і техніка Повітряних Сил Збройних Сил України*. 2011. Вип. 2 (6). С. 112–114.
10. Рудницький В. М., Миронець І. В., Бабенко В. Г. Систематизація повної множини логічних функцій для криптографічного перетворення інформації. *Системи обробки інформації*. 2011. Вип. 8 (98). С. 184–188.
11. Рудницький В. М., Миронець І. В., Бабенко В. Г. Технологія побудови пристрою реалізації методу підвищення оперативності доступу до конфіденційних інформаційних ресурсів. *Збірник наукових праць Харківського університету Повітряних Сил*. 2011. Вип. 3 (29). С. 145–150.
12. Бабенко В. Г., Миронець І. В., Рудницький С. В. Декодування інформації в групі дворозрядних операцій криптографічного перетворення. *Системи управління, навігації та зв'язку*. 2011. Вип. 4 (20). С. 208–212.
13. Бабенко В. Г., Рудницький С. В., Мельник Р. П. Визначення множини трирозрядних елементарних операцій криптографічного перетворення. *Вісник інженерної академії України*. 2012. Вип. 3 (4). С. 77–79.
14. Рудницький В. М., Бабенко В. Г., Рудницький С. В. Метод синтезу матричних моделей операцій криптографічного кодування та декодування інформації. *Збірник наукових праць Харківського університету Повітряних Сил*. 2012. Вип. 4 (33). С. 198–200.
15. Рудницький В. М., Бабенко В. Г., Рудницький С. В. Метод синтезу матричних моделей операцій криптографічного перекодування інформації. *Захист інформації*. 2012. № 3 (56). С. 50–56.
16. Голуб С. В., Бабенко В. Г., Рудницький С. В. Метод синтезу операцій криптографічного перетворення на основі додавання за модулем два. *Системи обробки інформації*. 2012. Вип. 3 (101). Т. 1. С. 119–122.
17. Бабенко В. Г., Мельник Р. П., Рудницький С. В. Дослідження способів запису трьохрозрядних криптографічних операцій. *Системи управління, навігації та*

зв'язку. 2012. Вип. 1 (21). Т. 2. С. 170–173.

18. Бабенко В. Г., Рудницький С. В. Синтез функцій перекодування для групи трьохрозрядних криптографічних операцій. *Системи озброєння і військова техніка*. 2012. Вип. 1 (29). С. 84–87.
19. Вдосконалення методу синтезу операцій криптографічного перетворення на основі дискретно-алгебраїчного представлення операцій / С. В. Голуб, В. Г. Бабенко, С. В. Рудницький, Р. П. Мельник. *Системи управління, навігації та зв'язку.* 2012. Вип. 2 (22). С. 163–168.
20. Бабенко В. Г., Рудницький С. В. Реалізація методу захисту інформації на основі матричних операцій криптографічного перетворення. *Системи обробки інформації*. 2012. № 9 (107). С. 130–139.
21. Бабенко В. Г., Мельник Р. П., Рудницкий С. В. Синтез операций криптографического декодирования на основе элементарных операций расширенного матричного представления. *Информационные системы и технологии: управление и безопасность:* сб. ст. I междунар. заочной науч.-практ. конф. Тольятти: ПВГУС, 2012. С. 67–77.
22. Бабенко В., Мельник О., Мельник Р. Класифікація трирозрядних елементарних функцій для криптографічного перетворення інформації. *Безпека інформації*. 2013. Т. 19. № 1. С. 56–59.
23. Бабенко В. Г., Стабецька Т. А. Побудова моделі оберненої нелінійної операції матричного криптографічного перетворення. *Системи управління, навігації та зв'язку*. 2013. Вип. 3 (27). С. 117–119.
24. Параллельная реализация нелинейного расширенного матричного криптографического преобразования / В. Г. Бабенко, С. В. Пивнева, О. Г. Мельник, Р. П. Мельник. *Вектор науки Тольяттинского государственного университета*. 2014. № 3 (29). С. 17–19.
25. Синтез модели обратной нелинейной операции расширенного матричного криптографического преобразования / В. Н. Рудницкий, С. В. Пивнева,

В. Г. Бабенко и др. *Вектор науки Тольяттинского государственного университета*. 2014. № 4 (30). С. 18–21.

26. Бабенко В. Г., Мельник Р. П., Гончар С. В. Оцінка ефективності використання операцій криптографічного перетворення. *Вісник Інженерної академії України*. 2014. Вип. 2. С. 39–41.
27. Метод захисту конфіденційної інформації як складова управління інформаційною безпекою ДСНС України / Р. П. Мельник, О. Г. Мельник, С. В. Гончар, В. Г. Бабенко. *Системи обробки інформації*. 2014. Вип. 4 (120). С. 145–148.
28. Рудницкий В. Н., Козлов Е. В., Бабенко В. Г. Способ параллельной реализации операций матричного криптографического преобразования. *Вектор науки Тольяттинского государственного университета*. 2014. № 2 (28). С. 11–15.
29. Бабенко В. Г., Лада Н. В. Синтез і аналіз операцій криптографічного додавання за модулем два. *Системи обробки інформації*. 2014. Вип. 2 (118). С. 116–118.
30. Бабенко В. Г., Мельник О. Г., Стабецька Т. А. Синтез нелінійних операцій криптографічного перетворення. *Безпека інформації*. 2014. Т. 20. № 2. С. 143–147.
31. Рудницький В. М., Бабенко В. Г., Стабецька Т. А. Узагальнений метод синтезу обернених нелінійних операцій розширеного матричного криптографічного перетворення. *Системи обробки інформації*. 2014. Вип. 6 (122). С. 118–121.
32. Бабенко В. Г., Козловська С. Г. Особливості використання матричних операцій криптографічного перетворення інформації. *Системи обробки інформації*. 2015. Вип. 3 (128). С. 84–87.
33. Бабенко В. Г., Ланських Є. В., Зажома В. М. Вбудовування даних в стеганоконтейнер на основі надлишкових позиційних систем числення.

Вісник Черкаського державного технологічного університету. 2015. № 1. С. 111–115.

34. Бабенко В. Г., Мельник Р. П., Гончар С. В. Розробка методів синтезу трирозрядних розширених матричних елементарних функцій. *Наука і техніка Повітряних Сил Збройних Сил України*. 2015. Вип. 1 (18). С. 154–156.
35. Мельник Р. П., Бабенко В. Г., Гончар С. В. Удосконалений метод синтезу розширених матричних елементарних функцій для криптоперетворення даних. *Системи озброєння і військова техніка*. 2015. Вип. 1 (41). С. 132–134.
36. Бабенко В. Г., Мельник О. Г., Нестеренко О. Б. Моделювання примітивів ковзного шифрування на основі рекурентних послідовностей. *Наука і техніка Повітряних Сил Збройних Сил України*. 2015. Вип. 3 (20). С. 129–133.
37. Бабенко В. Г., Мельник О. Г., Мельник Р. П. Мультиопераційне багаторазове ковзне шифрування. *Системи озброєння і військова техніка*. 2015. Вип. 3 (43). С. 70–72.
38. Бабенко В. Г., Зажома В. М., Нестеренко О. Б. Метод вбудовування стегоповідомлення на основі ключового елементу. *Автоматизированные системы управления и приборы автоматики.* Харьков. 2014. Вып. 168. С. 53–58.
39. Бабенко В. Г., Лада Н. В., Лада С. В. Дослідження взаємозв'язків між операціями в матричних моделях криптографічного перетворення. *Вісник Черкаського державного технологічного університету.* 2016. № 1. С. 5–11.
40. Эффективное совмещенное мультиоперандное сложение в избыточной линейной рекуррентной системе счисления третьего порядка / И. Н. Федотова-Пивень, В. Г. Бабенко, О. Б. Пивень, С. Ю. Куницкая. *Wschodnioeuropejskie Czasopismo Naukowe:* East European sci. journ. 2016. No. 11 (15). Part 2. P. 19–24. (Варшава, Польща).
41. Реалізація вершинної мінімізації булевих функцій для моделювання процесів, що не формалізуються / В. М. Рудницький, І. В. Миронець, В. Г. Бабенко та

ін. *Science and Education a New Dimension. Natural and Ttechnical Science:* міжнар. наук. журн. 2017. Vol. 14. Iss. 132. P. 85–88. (BUDAPEST) (Будапешт, Угорщина).

42. Особенности применения операций перестановок, управляемых информацией, для криптографического преобразования / Т. В. Миронюк, И. В. Миронец, В. Г. Бабенко, С. В. Сысоенко. *Wschodnioeuropejskie Czasopismo Naukowe:* East European sci. journ. 2017. No. 11 (27). Part 1. P. 85–93. (Варшава, Польща).
43. Сисоєнко С. В., Миронець І. В., Бабенко В. Г. Побудова узагальненої математичної моделі групового матричного криптографічного перетворення. *Сучасна спеціальна техніка*. 2018. № 4. С. 96–103.
44. Миронець І. В., Бабенко В. Г., Сисоєнко С. В. Метод мінімізації булевих функцій з великою кількістю змінних на основі направленого перебору. *Щомісячний науковий журнал «Smart and Young»*. 2016. № 7. С. 63–71.
45. Бабенко В. Г., Лада Н. В. Технологія дослідження операцій за модулем два. *Щомісячний науковий журнал «Smart and Young»*. 2016. № 11–12. Ч. 1. С. 49–54.
46. Бабенко В. Г., Кучеренко С. Ю., Зажома В. М. Моделирование позиционных избыточных систем счисления. *Системи управління, навігації та зв'язку.* 2010. Вип. 4 (16). С. 51–54.
47. Бабенко В. Г., Кучеренко С. Ю., Зажома В. М. Синтез правил выполнения операций сложения на основе моделей позиционных систем счисления. *Системи обробки інформації*. 2010. Вип. 9 (90). С. 179–182.
48. Бабенко В. Г., Шадхін В. Ю., Шевченко О. О. Дослідження принципів організації передачі даних в TCP/IP-мережах. *Вісник Черкаського державного технологічного університету.* 2010. № 2. С. 3–6.

49. Бабенко В. Г., Шадхін В. Ю., Компанієць В. О. Оперативний розподіл навантаження на мережі передачі даних. *Вісник Хмельницького національного університету*. 2010. Вип. 3. С. 217–220.
50. Эвристические алгоритмы и распределённые вычисления в прикладных задачах (вып. 2): кол. монограф. / под ред. Б. Ф. Мельникова. Ульяновск, 2013. 202 с.
51. Наукоемкие технологии в инфокоммуникациях: обработка и защита информации: кол. монограф. / под ред. В. М. Безрука, В. В. Баранника. Харьков: Компания СМИТ, 2013. 398 с.
52. Криптографическое кодирование: методы и средства реализации: монография / В. Н. Рудницкий, С. В. Пивнева, В. Г. Бабенко и др.; Тольят. гос. ун-т. Тольятти, 2013. 196 с.
53. Криптографическое кодирование: методы и средства реализации (часть 2): монография / В. Н. Рудницкий, В. Я. Мильчевич, В. Г. Бабенко и др. Харьков: Щедрая усадьба плюс, 2014. 224 с.
54. Криптографическое кодирование: кол. монограф. / под ред. В. Н. Рудницкого, В. Я. Мильчевича. Харьков: Щедрая усадьба плюс, 2014. 240 с.
55. Рудницький В. М., Лада Н. В., Бабенко В. Г. Криптографічне кодування: синтез операцій потокового шифрування з точністю до перестановки: монографія. Харків: ДІСА ПЛЮС, 2018. 184 с.
56. Криптографічне кодування: обробка та захист інформації: кол. монографія / Бабенко В. Г., Лада Н. В. та ін.; під. ред. В. М. Рудницького. Харків: ДІСА ПЛЮС, 2018. 139 с.
57. Бабенко В. Г. Етапи реалізації технології підвищення швидкодії систем захисту інформації. *Методи та засоби кодування, захисту й ущільнення інформації:* тези доп. Третьої міжнар. наук.-практ. конф., (20–22 квіт. 2011 р.). Вінниця: ВНТУ, 2011. С. 80–81.
58. Бабенко В. Г. Використання матричних операцій криптографічного

перетворення для ковзного шифрування. *Проблеми інформатизації:* тези доп. Першої міжнар. наук.-техн. конф., (19–20 груд. 2013 р.). Черкаси: ЧДТУ; Київ: ДУТ; Тольятті: ТДУ; Полтава: ПНТУ, 2013. С. 22.

59. Миронець І. В., Бабенко В. Г. Методика синтезу функцій декодування на основі спеціалізованих логічних функцій. *Проблеми інформатизації:* зб. тез доп. наук.-техн. семінару, (15–16 квіт. 2009 р.). Черкаси: ЧДТУ, 2009. Вип. 1 (3). С. 18–19.
60. Миронець І. В., Бабенко В. Г. Вдосконалена методика синтезу функцій декодування на основі спеціалізованих логічних функцій. *Інтегровані інтелектуальні робототехнічні комплекси:* зб. тез Другої міжнар. наук.-практ. конф., (25–28 трав. 2009 р.). Київ: НАУ, 2009. С. 228–229.
61. Бабенко В. Г., Рудницький С. В. Дослідження двохрозрядних операцій криптографічного перетворення. *Інтегровані комп'ютерні технології в машинобудуванні ІКТМ-2011:* тези доп. Всеукр. наук.-техн. конф. Харків: НАУ «ХАІ», 2011. Т. 3. С. 218.
62. Бабенко В. Г., Рудницький С. В. Синтез функцій декодування інформації в групі трьохрозрядних криптографічних операцій перетворення. *Моделювання, ідентифікація, синтез систем керування:* зб. тез П'ятнадцятої міжнар. наук.-техн. конф., (9–16 верес. 2012 р.). Донецьк: Вид-во Ін-ту прикл. математики і механіки НАН України, 2012. С. 190–191.
63. Бабенко В. Г., Рудницький С. В. Моделювання логічних функцій для систем захисту інформації. *Методи та засоби кодування, захисту й ущільнення інформації:* тези доп. Третьої міжнар. наук.-практ. конф. Вінниця: ВНТУ, 2011. С. 82–83.
64. Бабенко В. Г., Рудницький С. В. Дослідження групи трьохрозрядних криптографічних операцій. *Новітні технології – для захисту повітряного простору:* тези доп. Восьмої наук. конф. Харків. ун-ту Повітр. Сил ім. І. Кожедуба, (18–19 квіт. 2012 р.). Харків: ХУПС ім. І. Кожедуба, 2012.

С. 218.

65. Бабенко В. Г., Лада Н. В. Дослідження множини операцій криптографічного додавання. *Інформаційні технології в освіті, науці і техніці (ІТОНТ-2014):* тези доп. ІІ Міжнар. наук.-практ. конф., (м. Черкаси, Україна, 24–26 квіт. 2014 р.). Черкаси: ЧДТУ, 2014. Т. 1. С. 135–136.
66. Бабенко В. Г., Стабецька Т. А. Операції матричного криптографічного декодування на основі логічних визначників. *Методи та засоби кодування, захисту й ущільнення інформації:* тези доп. Четвертої міжнар. наук.-практ. конф., (м. Вінниця, Україна, 23–25 квіт. 2013 р.). Вінниця: ТД Едельвейс і К, 2013. С. 135–137.
67. Бабенко В. Г., Лада Н. В. Синтез і аналіз мікрооперацій для криптографічного перетворення. *Проблеми інформатизації:* тези доп. Другої міжнар. наук.-техн. конф., (м. Черкаси, Україна – м. Тольятті, Росія, 25–26 листоп. 2014 р.). Черкаси: ЧДТУ; Тольятті: ТДУ, 2014. С. 9–10.
68. Ланських Є. В., Бабенко В. Г., Зажома В. М. Алгоритми вбудовування повідомлення для LSB методу. *Інформаційні технології в освіті, науці і техніці (ІТОНТ-2014):* тези доп. ІІ Міжнар. наук.-практ. конф., (м. Черкаси, Україна, 24–26 квіт. 2014 р.). Черкаси: ЧДТУ, 2014. Т. 1. С. 141–142.
69. Ланських Є. В., Бабенко В. Г., Зажома В. М. Технологія застосування ключового елементу стеганоконтейнера для LSB методу. *Інтегровані інтелектуальні робототехнічні комплекси (ІІРТК-2014):* тези доп. Сьомої міжнар. наук.-практ. конф., (19–20 трав. 2014 р.). Київ: НАУ, 2014. С. 312–313.
70. Ланських Є. В., Бабенко В. Г., Зажома В. М. Використання надлишковості систем числення в стеганографічних системах. *Інформаційні технології та комп'ютерна інженерія (ІТКІ-2014):* тези доп. Четвертої міжнар. наук.-практ. конф., (м. Вінниця, Україна, 27–30 трав. 2014 р.). Вінниця: ВНТУ, 2014. С. 161–162.

71. Гресько Є. І., Бабенко В. Г. Огляд стеганографічних методів приховування інформації. *Інформаційна безпека держави, суспільства та особистості:* зб. тез доп. Всеукр. наук.-практ. конф., (16 квіт. 2015 р.). Кіровоград: КНТУ, 2015. С. 87–89.

72. Бабенко В. Г., Рудницький С. В. Способи синтезу алгоритмів на основі операцій криптографічного перетворення інформації. *Проблеми інформатизації:* тези доп. Другої міжнар. наук.-техн. конф. (м. Черкаси, Україна – м. Тольятті, Росія, 25–26 листоп. 2014 р.). Черкаси: ЧДТУ; Тольятті: ТДУ, 2014. С. 10.

73. Бабенко В. Г. Синтез моделей реалізації багаторазового примітиву ковзного шифрування. *Сучасні напрями розвитку інформаційно-комунікаційних технологій та засобів управління:* матеріали П’ятої міжнар. наук.-техн. конф., (23–24 квіт. 2015 р.). Полтава: ПНТУ; Баку: ВА ЗС АР; Кіровоград: КЛА НАУ; Харків: ХНДІ ТМ, 2015. С. 59.

74. Бабенко В. Г., Лада Н. В. Аналіз результатів виконання модифікованих операцій додавання за модулем два з точністю до перестановки. *The Scientific Potential of the Present:* зб. наук. праць «ЛОГОΣ». 2016. С. 108–111.

75. Бабенко В. Г., Лада Н. В., Лада С. В. Взаємозв’язки між операціями в матричних моделях криптографічного перетворення. *Проблеми науково-технічного та правового забезпечення кібербезпеки у сучасному світі «ПНПЗК-2016»:* тези доп. Першої міжнар. наук.-практ. конф., (30 берез.–1 квіт. 2016 р.). Харків: Нац. техн. ун-т «ХПІ», 2016. С. 17.

76. Бабенко В. Г., Лада Н. В., Лада С. В. Аналіз множини операцій, синтезованих на основі додавання за модулем два. *Методи та засоби кодування, захисту й ущільнення інформації:* тези доп. П’ятої міжнар. наук.-практ. конф., (19–21 квіт. 2016 р.). Вінниця: ВНТУ, 2016. С. 54–57.

77. Бабенко В. Г., Висоцький С. В. Забезпечення захисту інформації для системи моніторингу та статистики web-ресурсів. *Інформаційні технології в освіті,*

науці й техніці (ІТОНТ-2016): тези доп. Третьої міжнар. наук.-практ. конф., (12–14 трав. 2016 р.). Черкаси: ЧДТУ, 2016. С. 85–86.

78. Бабенко В. Г., Ланських Є. В. Дослідження заміни операції для реалізації матричного криптографічного перетворення. *Інтегровані інтелектуальні робототехнічні комплекси (ІПРТК-2016):* тези доп. Дев'ятої міжнар. наук.-практ. конф., (17–18 трав. 2016 р.). Київ: НАУ, 2016. С. 246–248.
79. Бабенко В. Г., Стабецька Т. А. Синтез обернених операцій розширеного матричного криптографічного перетворення. *Проблеми інформатизації:* тези доп. Четвертої міжнар. наук.-техн. конф., (м. Черкаси, Україна, 3–4 листоп. 2016 р.). Черкаси: ЧДТУ; Баку: ВА ЗС АР; Бельсько-Бяла: УТіГН; Полтава: ПНТУ, 2016. С. 9.
80. Стабецька Т. А., Бабенко В. Г. Алгоритми побудови та застосування операцій розширеного матричного криптографічного перетворення. *Наукова думка інформаційного століття:* матеріали Міжнар. наук.-практ. конф., (м. Дніпропетровськ, Україна, 19 черв. 2017 р.). Одеса: Друкарня «Друкарик», 2017. Т. 6. С. 86–94.
81. Миронюк Т. В., Бабенко В. Г. Аналіз статистичних властивостей результатів криптографічного перетворення на основі операцій перестановок, керованих інформацією. *Інноваційні тенденції сьогодення у сфері природничих, гуманітарних та точних наук:* матеріали Міжнар. наук.-практ. конф., (м. Івано-Франківськ, Україна, 17 жовт. 2017 р.). Одеса: Друкарня «Друкарик», 2017. Т. 2. С. 41–47.
82. Бабенко В. Г., Лада Н. В. Потокові шифри з використанням групи модифікованих операцій криптографічного додавання за модулем два з точністю до перестановки. *Проблеми інформатизації:* тези доп. П'ятої міжнар. наук.-техн. конф., (м. Черкаси, Україна, 13–15 листоп. 2017 р.). Черкаси: ЧДТУ; Баку: ВА ЗС АР; Бельсько-Бяла: УТіГН; Полтава: ПНТУ, 2017. С. 12.

83. Стабецька Т. А., Бабенко В. Г. Порівняльна оцінка основних параметрів методу захисту інформації на основі операцій розширеного матричного криптографічного перетворення. *Наука у контексті сучасних глобалізаційних процесів: зб. наук. праць* «*ΛΌГОΣ*» з *матеріалами Міжнар. наук.-практ. конф.*, (м. Полтава, Україна, 19 листоп. 2017 р.) / відп. за вип. М. А. Голденблат; ГО «Європейська наукова платформа». Одеса: Друкарня «Друкарик», 2017. Т. 10. С. 81–84.

84. Бабенко В. Г., Нестеренко О. Б., Пустовіт М. О. Дослідження результатів багатораундового шифрування, реалізованого на основі операцій строгого стійкого кодування. *Проблеми інформатизації:* тези доп. Шостої міжнар. наук.-техн. конф., (м. Черкаси, Україна, 14–16 листоп. 2018 р.). Черкаси: ЧДТУ; Баку: ВА ЗС АР; Бельсько-Бяла: УТіГН; Полтава: ПНТУ, 2018. С. 9–10.

85. Сисоєнко С. В., Бабенко В. Г. Аналіз складності реалізації моделей операцій групового матричного криптографічного перетворення. *Naukowy i innowacyjny potencjał prezentacji:* kolekcja prac naukowych «ΛΌГОΣ» z materiałami Międzynar. nauk.-prakt. konf., (Opole, 18 listopada 2018 r.). Równe: Volynsky Oberegi, 2018. T. 7. S. 5–53.

86. Sysoienko S., Myronets I., Babenko V. Practical implementation effectiveness of the speed increasing method of group matrix cryptographic transformation. *Second International Workshop on Computer Modeling and Proceedings of the Second International Workshop on Computer Modeling and Intelligent Systems (CMIS-2019),* (Zaporizhzhia, Ukraine, April 15–19, 2019). P. 402–412. URL: http://ceur-ws.org/Vol-2353/paper32.pdf

87. Пристрій для виконання логічних операцій криптографічного перетворення: декларац. пат. на корисну модель 45916 Україна, МПК H03M 13/00 / Рудницький В. М., Паціра Є. В., Миронець І. В., Бабенко В. Г. № u200907997; заявл. 29.07.2009; опубл. 25.11.2009, Бюл. № 22. 3 с.

88. Пристрій для виконання логічних операцій криптографічного перетворення: деклараc. пат. на корисну модель 45917 Україна, МПК H03M 13/00 / Рудницький В. М., Паціра Є. В., Миронець І. В., Бабенко В. Г. № u200907998; заявл. 29.07.2009; опубл. 25.11.2009, Бюл. № 22. 3 с.

89. Пристрій для виконання логічних операцій криптографічного перетворення: деклара. пат. на корисну модель 46617 Україна, МПК H03M 13/00 / Рудницький В. М., Паціра Є. В., Миронець І. В., Бабенко В. Г. № u200908000; заявл. 29.07.2009; опубл. 25.12.2009, Бюл. № 24. 3 с.

90. Пристрій для виконання логічних операцій криптографічного перетворення: деклараc. пат. на корисну модель 46618 Україна, МПК H03M 13/00 / Рудницький В. М., Паціра Є. В., Миронець І. В., Бабенко В. Г. № u200908001; заявл. 29.07.2009; опубл. 25.12.2009, Бюл. № 24. 3 с.

91. Молдовян А.А. Криптография: учебник для вузов / А.А. Молдовян, Н.А. Молдовян, Б.Я. Советов. СПб.: Лань, 2000. 224 с.

92. Молдовян Н.А. Скоростные блочные шифры / Н.А. Молдовян. СПб.: СПбГУ, 1998. 230 с.

93. Нечаев В.И. Элементы криптографии. Основы теории защиты информации / В.И. Нечаев. М.: Высшая школа, 1999. 109 с.

94. Корченко О.Г. Спосіб шифрування інформації на основі шифру Файстеля / О.Г. Корченко, Є.В. Паціра, С.О. Гнатюк,. В.М. Кінзерявий // Вісник інженерної академії України. - №2, 2009. - С. 117-121.

95. Соколов А.В. Защита информации в распределенных корпоративных сетях и системах / А.В. Соколов, В.Ф. Шаньгин. М.: ДМК-Пресс, 2003. 656 с..

96. Корченко О.Г. Конвейерный криптографический вычислитель реального времени / О.Г. Корченко, А.В. Малофеев, Ю.Е. Хохлачева // Журн. «Захист інформації». – Вип. №2 (47). К.: ДУІКТ.– 2010. – С.30-36.

97. Логачев О.А. Булевы функции в теории кодирования и криптологии / О.А. Логачев, А.А. Сальников, В.В. Ященко. М.: МЦНМО, 2004 470 с.

98. Шнайер Брюс. Прикладная криптография. Протоколы, алгоритмы, исходные тексты на языке Си / Брюс Шнайер. М.: Триумф, 2002. 816 с.

99. Kerckhoffs A. La cryptographie militaire / A. Kerckhoffs // Journal des sciences militaires. Jan. 1883. vol. IX. P. 5-38 (P. 161-191, Feb. 1883).

100. Панасенко С.П. Защита информации в компьютерных сетях: шифрование / С.П. Панасенко // Мир ПК. 2002. № 2. С. 7073.

101. Галатенко В.А. Основы информационной безопасности / В.А. Галатенко. М.: Интернет-Университет Информационных технологий; БИНОМ; Лаборатория знаний, 2008. 205 с.

102. Борсуковський Ю.В., Борсуковська В.Ю. Прикладні аспекти захисту інформації в сучасних умовах. *Сучасний захист інформації*: наук.-техн. журнал. 2018. № 2(34). С. 6-11.

103. Information Resistance [Електронний ресурс] // Режим доступу: http://sprotyv.info/ru/news/kiev/es-utverdil-mery-po-usileniyu-svoey-kiberbezopasnosti.

104. Захист інформації в телефонних лініях та радіо діапазоні [Електронний ресурс]. Режим доступу: http://wiki.univ.uzhgorod.ua/index.php Захист_інформації_в_телефонних_лініях_та_радіо_діапазоні.

105. Бевз О. М., Квєтний Р. Н. Шифрування даних на основі високонелінійних булевих функцій та кодів з максимальною відстанню: монографія. Вінниця: ВНТУ, 2010. 96 с.

106. Кузьминов В.И. Криптографические методы защиты информации. Новосибирск: Высшая школа, 1998. 340 с.

107. Бабаш А.В., Шангин Г.П. Криптография. М.: СОЛОН-ПРЕСС, 2007. (Серия книг «Аспекты защиты»). 512 с.

108. Поповский В. В. Основы криптографической защиты информации в телекоммуникационных системах. Ч. 1 / В. В. Поповский, А. В. Персиков. Х.:Компания СМИТ, 2010. 352 с.

109. Горобцов В. О. Криптографічний захист інформації. Юридический словарь / В. О. Горобцов // zakony.com.ua від 11.02.2014. [Електронний ресурс]. Режим доступу: http://www.zakony.com.ua.

110. Швець О. Ю., Лазаренко В. В. Аналіз методів і засобів захисту інформації та сучасних вимог до них [Електронний ресурс]. URL: http://www.rusnauka.com/25_DN_2008/Informatica/28842.doc.htm

111. Бабак В.П. Теоретичні основи захисту інформації / В. П. Бабак: Підручник. Книжкове видавництво НАУ, 2008. 752 с.

112. Фергюсон Н., Шнайер Б. Практическая криптография / пер. с англ. М.: Издательский дом "Вильямс", 2005. 424 с.:ил. Парал. тит. англ.

113. Панасенко С.П. Алгоритмы шифрования / С.П. Панасенко. Специальный справочник. СПб.: БХВ-Петербург, 2009. 576 с.: ил.

114. Вельшенбах М. Криптография на Си и С++ в действии / М. Вельшенбах. Учебное пособие. М.:Издательство Триумф, 2004 464 с.

115. Рябко Б.Я., Фионов А.Н. Криптографические методы защиты информации / Б.Я. Рябко, А.Н. Фионов : Учебное пособие для вузов. М.: Горячая линия-Телеком, 2005. 229 с.: ил.

116. Задірака В.К. Олексик О. Комп‘ютерна криптологія / В. К. Задірака, О. Олексик. Київ, 2002. 505 с.

117. Алферов А.П. Основы криптографии / А.П. Алферов, А.Ю. Зубов, А.С. Кузьмин, А.В. Черемушкин. Учебн ое пособие, 2-е изд., испр. и доп. М.. Гелиос АРВ, 2002. 480 с., ил.

118. Н. Смарт. Криптография / Н. Смарт. Москва: Техносфера, 2005. 528 с.

119. Болотов А.А. Элементарное введение в эллиптическую криптографию: Протоколы криптографии на Эллиптических кривых / А.А. Болотов, С.Б. Гашков, А.Б. Фролов. М.: КомКнига, 2006. 280 с.

120. Василенко О.Н. Теоретико-числовые алгоритмы в криптографии / О.Н. Василенко. М.: МЦНМО, 2003. 328 с.

121. Горбенко І. Д., Горбенко Ю. І. Прикладна криптологія: монографія. Харків, ХНУРЕ, Форт, 2012. 868 с.

122. Положення про порядок розроблення, виготовлення та експлуатації засобів криптографічного захисту інформації, затверджене наказом Адміністрації Держспецзв'язку від 20.07.2007 р. № 141, зареєстроване в Міністерстві юстиції України 30 липня 2007 р. за № 862/14129.

123. Горбенко И. Д., Долгов В. И., Олейников Р. В, Руженцев В. И., Михайленко М. С., Горбенко Ю. И., Тоцкий А. С., Казмина С. В. Перспективный блочный шифр "Калина" основные положения и спецификация // Прикладная радиоэлектроника, 2007, №2.

124. Хоффман Л. Современные методы защиты информации / пер. с англ. М. Сов. радио, 1980. 264 с.

125. J. Daemen, R. Govaerts, J. Van Weak keys for IDEA // Advances in Cryptology. CRYPTO'93 (LNCS 773). 1994. P. 224231.

126. L.R. Knudsen Block Ciphers Analysis, Design and Applications. PhD thesis. Computer Science Department, Aarhus University, Denmark. 1994.

127. L.R. Knudsen A key-schedule weakness in SAFER-K64 // Advances in Cryptology. Proceedings Crypto'95. LNCS 963. 1995. P. 274286.

128. ISO/IEC 10116. Information technology Security techniques Modes of operation for an n-bit block cipher.

129. Бабаш А. В., Шангин Г. П. Криптография /под ред. В. П. Шестюка, Э. А. Применко. М.:СОЛОН-ПРЕСС, 2007. 512 с. (Серия книг «Аспекты защиты»).

130. Коблиц Н. Курс теории чисел и криптографии / Н. Коблиц. М. : Науч. изд-во ТВП, 2001. 254 с.

131. Черемушкин А. В. Лекции по арифметическим алгоритмам в криптографии / А. В. Черемушкин. М. : МЦНМО, 2002. 104 с.

132. Cryptology and computational number theory, Proc. of Symp. in Appl. Math., v. 42, 1990.

133. Мао Венбо. Современная криптография: теория и практика / Мао Венбо ; пер. с англ. Изд. дом «Вильямс», 2005. 768 с. : ил. Парал. тит. англ. ISBN 5-8459-0847-7 (рус.)

134. Ростовцев А. Г. Теоретическая криптография / А. Г. Ростовцев, Е. Б. Маховенко. М. : Профессионал, 2005. 490 с.

135. Черёмушкин А. В. Криптографические протоколы. Основные свойства и уязвимости / А. В. Черёмушкин. М. : Изд. дом «Академия», 2009. 272 с.

136. Тилборг Х. К. А. ван. Основы криптологии. Профессиональное руководство и интерактивный учебник / Х. К. А. ван Тилборг. М. : Мир, 2006. 471 с.

137. Жельников В. Криптография от папируса до компьютера / В. Жельников. М. : ABF, 1996. 335 с.

138. Хорошко В.А. Методи й засоби захисту інформації / В.А. Хорошко, А. А. Чекатков. К.: Юніор, 2003. 504 с.

139. Корченко О.Г. Сучасні квантові технології захисту інформації / О.Г. Корченко, Є.В. Васіліу, С.О. Гнатюк // Наук.-техн. журн. «Захист інформації». – Вип. №1 (46). К.: ДУІКТ.– 2010. – С. 77–89.

140. Логачев О.А. Булевы функции в теории кодирования и криптологии / О.А. Логачев, А.А. Сальников, В.В. Ященко. М.: МЦНМО, 2004 470 с.

141. Хемминг Р.В. Теория кодирования и теория информации / Р.В. Хемминг. М.: Радио и связь, 1983. 176 с.

142. Шнайер Брюс. Прикладная криптография. Протоколы, алгоритмы, исходные тексты на языке Си / Брюс Шнайер. М.: Триумф, 2002. 816 с.

143. Крысин А.В. Информационная безопасность: Практическое руководство / А.В. Крысин. М.: СПАРРК, К.: Век+, 2003. 320 с.

144. Тарасюк М.В. Защищенные информационные технологии. Проектирование и применение / М.В. Тарасюк. М.: Солон-Пресс, 2004. 192 с.

145. Панасенко С.П. Защита информации в компьютерных сетях: шифрование / С.П. Панасенко // Мир ПК. 2002. № 2. С. 7073.

146. Баутов А. Эффективность защиты информации / А. Баутов // Открытые системы. 2003. № 78. С. 24.

147. Вихорев С.В. Защита информации в сети Интернет / С.В. Вихорев // Электросвязь. 1999. №1. С. 67.

148. Галатенко В.А. Основы информационной безопасности / В.А. Галатенко. М.: Интернет-Университет Информационных технологий; БИНОМ; Лаборатория знаний, 2008. 205 с.

149. Фергюссон Н. Практическая криптография / Нильс Фергюссон, Брюсс Шнайер. М.: Вильямс, 2005. 424 с.

150. Рябко Б.Я. Основы современной криптографии для специалистов в информационных технологиях / Б.Я. Рябко, А.Н. Фионов. М.: Научный мир,

2004. 172 с.

151. Баричев С.Г. Основы современной криптографии / С.Г. Баричев, В.В. Гончаров, Р.Е. Серов. М.: Горячая линия - Телеком, 2002. 175 с.

152. Вельшенбах Михаэл. Криптография на Си и С++ в действии / Михаэл Вельшенбах. Под редакцией П.В. Семьянова. М.: Триумф, 2004. 464 с.

153. Бабаш А.В. Криптография. Аспекты защиты / А.В. Бабаш, Г.П. Шанкин. М.: Солон-Р, 2002. 512 с.

154. Чмора А.П. Современная прикладная криптография / А.П. Чмора. [2-е изд., стер.]. М.: Гелиос АРВ, 2002. 256 с.

155. Введение в криптографию / [Ященко В.В.,Варновский Н.П.,Нестеренко Ю.В. и др.]; под общ. ред. В. В. Ященко. [3-е изд., испр.]. СПб.: Питер, 2001. 288 с.

156. Молдовян Н.А. Криптография: от примитивов к синтезу алгоритмов / Н.А. Молдовян, А.А. Молдовян, М.А. Еремеев. СПб.: БХВ-Петербург, 2004. 446 с.

157. Молдовян Н.А. Проблематика и методы криптографии (монография) / Н.А. Молдовян СПб.: СПбГУ,1998. 212 с..

158. Лужецький В.А. Використання операції множення за модулем в симетричних блокових шифрах / В.А. Лужецький, О.В. Дмитришин //Системи обробки інформації. 2010. № 5. С. 9-14.

159. Бабенко В.Г. Метод підвищення швидкодії систем захисту інформації на основі використання спеціалізованих логічних функцій: Дис. канд. техн. наук: 05.13.21. Черкаси, 2009. 166 с..

160. Пантелєєва Н.М. Вибір наборів спеціалізованих логічних функцій для пристроїв захисту дискретної інформації / Н.М. Пантелєєва, В.Г. Бабенко // Проблеми інформатики та моделювання: матеріали восьмої міжнар. наук.-

техн. конф.: зб. наук. пр. Харк. ун-ту Повітряних Сил. Х.: НТУ «ХПИ», 2008. Вип. №3(18). С. 187.

161. Рудницький В.М. Визначення множини логічних функцій для синтезу цифрових пристроїв систем захисту інформації / В.М. Рудницький, Н.М. Пантелєєва, В.Г. Бабенко // Системи управління, навігації та зв'язку: зб. наук. пр. К.: ДП «Центральний науково-дослідний інститут навігації і управління», 2008. Вип. 4(8). С. 155-157.

162. Рудницький В.М. Модель уніфікованого пристрою криптографічного перетворення інформації / В.М. Рудницький, В.Г. Бабенко // Системи управління, навігації та зв'язку: зб. наук. пр. К.: ДП «Центральний науково-дослідний інститут навігації і управління», 2009. Вип. 1(9). С. 173-177.

163. Прикладная теория цифровых автоматов / [Самофалов К. Г., Романкевич А. М., Валуйский В. Н. и др.]. К. : Вища шк. Головное изд-во, 1987. 375 с.

164. Глушков В. М. Синтез цифровых автоматов / В. М. Глушков. М. : Физматгиз, 1962. 476 с.

165. Бабенко В. Г. Алгоритми вибору логічних функцій для криптографії / В. Г. Бабенко, Т. В. Дахно, В. М. Рудницький // Сучасні інформаційні системи. Проблеми та тенденції розвитку : зб. матеріалів 2-ї Міжнар. наук. конф. Х. : ХНУРЕ, 2007. С. 423-424.

166. Бардачов Ю. М. Дискретна математика. / Ю. М. Бардачов, Н. А. Соколова, В. Є. Ходаков; За ред. В. Є. Ходакова. К.: Вища шк., 2002. 287с.

167. Зубов А. Ю. Криптографические методы защиты информации. Совершенные шифры / А. Ю. Зубов. М. : Гелиос АРВ, 2005. 192 с.

168. Мухачев В.А. Методы практической криптографии / В.А. Мухачев, В.А. Хорошко. М.: Полиграф-Консалтинг, 2005. 209 с.

169 Гантмахер Ф.Р. Теория матриц / Ф.Р. Гантмахер. М.: Наука, 1966. 576 с.

170. Фомичев В. М. Дискретная математика и криптология. Курс лекций / Под общ. ред. д-ра физ.-мат. н. Н. Д. Подуфалова. М.: ДИАЛОГ-МИФИ, 2003. 400с.

171. Шеннон К. Теория связи в секретных системах // Работы по теории информации и кибернетике / К. Э. Шеннон. М. : ИЛ, 1963.

172. Киносита К., Асада К., Карацу О. Логическое проектирование СБИС /Под ред. Л.В. Поспелова.-М.:Мир, 1988.-309 с.

173. Лада Н. В., Козловська С. Г. Синтез та аналіз перестановочних схем побудови двохоперандних операцій криптоперетворення. Проблеми інформатизації: матеріали Шостої міжнар. наук.-техн. конф.: тези доп., (Черкаси – Баку – Бельсько-Бяла - Харків, 14-16 листоп. 2018 р.). Черкаси: ЧДТУ; Баку: ВА ЗС АР, Бельсько-Бяла: УТіГН, Харків: НТУ «ХПІ», 2018. С. 11.

174. Стабецька Т.А. Умови невиродженості нелінійних операцій розширеного матричного криптографічного перетворення, що містять неповні функції РМКП. «Системи обробки інформації»: зб. наук. пр. Харків: ХУПС ім. І. Кожедуба, 2016. Вип. 1(138). С.131-133.

175. Дахно Т.В. Оцінка придатності логічних функцій для криптографії на основі методу Жегалкіна / Т.В. Дахно //Проблеми інформатизації: Матеріали першої міжнародної науково-технічної конференції.- Черкаси: ЧДТУ; Київ: ДУТ; Тольятті: ТДУ; Полтава: ПНТУ, 2013. с. 26.

176. Koblitz N., Algebraic Aspects of Cryptography, Springer-Verlag, Berlin, 1998. 215 p.

177. Дмитришин О. В. Операція множення як базовий криптографічний примітив в симетричних блокових шифрах / О. В. Дмитришин // Системи обробки інформації. 2010. № 3. С. 112. ISNN 1681-7710.

178. Белецкий А. Я. Криптографические примитивы, основанные на методе скользящего кодирования / Белецкий А. Я., Белецкий А. А. // Вісник СумДУ, 2006. № 10. С. 33-42.

179. Лужецький В. А. Використання операції множення за модулем в симетричних блокових шифрах / В. А. Лужецький, О. В. Дмитришин // Системи обробки інформації. 2010. № 5. С. 9-14. ISSN 1681-7710.

180. Повідомлення організаційного комітету по проведенню відкритого конкурсу криптоалгоритмів про припинення прийому заявок на участь у конкурсі. [Електронний ресурс] Режим доступу: http://dstszi.gov.ua/dstszi/control/uk/publish/article?art_id=49027&cat_id=38710.

181. Белецкий А. Я. Примитивные полиномы в криптографических приложениях / Белецкий А.Я., Белецкий А.А., Навроцкий Д.А., Кандыба Р.Ю. // Сучасний захист інформації. 2011, № 4. С. 518.

182. В.А. Ильин, Э.Г. Позняк. Линейная алгебра: Учеб. для вузов. 4-е изд. М.: Нака. Физматлит, 1999. 296 с.

183. The Marsaglia Random Number CDROM including the Diehard Battery of Tests". [Електронний ресурс]. Доступно: http://stat.fsu.edu/pub/diehard/.

184. A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications [Електронний ресурс] / A. Rukhin, J. Soto, J. Nechvatal et al. Режим доступу : http://csrc.nist.gov/ publications/nistpubs/800-22-rev1a/SP800-22rev1a.pdf

185. Soto J., Randomness Testing of the Advanced Encryption Candidate Algorithms. NIST, 1999.

186. Потій А. В. Статистичне тестування генераторів випадкових і псевдовипадкових чисел з використанням набору статистичних тестів NIST STS [Електронний ресурс] / А. В. Потій, С. Ю. Орлова, Т. А. Гриненко.

Режим доступу : //www.kiev-security.org.ua

187. Иванов М. А. Теория, применение и оценка качества генераторов псевдослучайных последовательностей / М. А. Иванов, И. В. Чугунков. М. : КУДИЦ-ОБРАЗ, 2003. 240 с.

188. Вильданов Р. Р. Тесты псевдослучайных последовательностей и реализующее их программное средство / Р. Р. Вильданов, Р. В. Мещеряков, С. С. Бондарчук // Доклады ТУСУРа. 2012. № 1 (25), ч. 2. С. 108-111.

189. Богданов В. В. Навчальний комплекс статистичної оцінки псевдовипадкових і текстових послідовностей / В. В. Богданов, Н. А. Паламарчук // Збірник наукових праць Військового інституту телекомунікацій та інформатизації Національного технічного університету України «Київський політехнічний інститут». Вип. № 3. К. : ВІТІ НТУУ «КПІ», 2007. С. 17-26.

190. Саломаа А. Криптография с открытым ключом / А. Саломаа. М. : Мир, 1996. 318 с.

191. Юдін О. К. Захист інформації в мережах передачі даних : підруч. / Юдін О. К., Корченко О. Г., Конахович Г. Ф. К. : Вид-во ТОВ «НВП» ІНТЕРСЕРВІС», 2009. 716 с.

192. Романец Ю.В., Тимофеев П.А., Шаньгин В.Ф. Защита информации в компьютерных системах и сетях / Под ред. В.Ф. Шаньгина. 2-е изд., перераб. и доп. М.: Радио и связь, 2001. 376 с.

193. Чечельницький В. Я. Методологія підвищення ефективності телекомунікаційних систем на основі інтеграції канального кодування та шифрування даних : дис. докт. техн. наук : 05.12.02 / Чечельницький В. Я. Одеса, 2013. 407 с.

194. Ю. І. Горбенко, Р. С. Ганзя. Аналіз шляхів розвитку криптографії після появи квантових комп’ютерів. [Електронний ресурс] Режим доступу //

http://ena.lp.edu.ua:8080/bitstream/ntb/27194/1/8-40-48.pdf

195. Горбенко Ю. І. Аналіз стійкості популярних криптосистем проти квантового криптоаналізу на основі алгоритму Гровера / Ю. І. Горбенко, Р. С. Ганзя // Захист інформації: науково-практичний журнал. К., 2014. Том 16, No2. С. 106112.

196. Bernstein, D. Post-quantum cryptography [Text] / D. Bernstein, J. Buchmann, E. Dahmen. Berlin: Springer, 2009. 246 p.

197. Основы криптографии : учеб. пособие / А. П. Алферов, А. К. Зубов, А. С. Кузьмин, А. В. Черемушкин. [2-е изд., испр. и доп.]. М. : Гелиос АРВ, 2002. 480 с, ил. ISBN 5-85438-025-0.

198. Словарь криптографических терминов / [под ред. Б. А. Погорелова и В. Н. Сачкова]. М. : МЦНМО, 2006. 94 с.

199. Жданов О. Н. Методы и средства криптографической защиты информации : учеб. пособие / О. Н. Жданов, В. В. Золотарев ; СибГАУ. Красноярск, 2007. 217 с.

200. Кузьминов Т. В. Криптографические методы защиты информации / Т. В. Кузьминов. Новосибирск : Наука, 1998. 185 с.

201. Зубов А. Ю. Криптографические методы защиты информации. Совершенные шифры / А. Ю. Зубов. М. : Гелиос АРВ, 2005. 192 с.

202. Мухачев В.А. Методы практической криптографии / В.А. Мухачев, В.А. Хорошко. М.: Полиграф-Консалтинг, 2005. 209 с.

203. Программно-аппаратные средства обеспечения информационной безопасности. Защита программ и данных : учеб. пособие для вузов / [П. Ю. Белкин, О. О. Михальский, А. С. Першаков и др.]. М. : Радио и связь, 2000. 168 с.

204. Шаньгин В. Ф. Защита компьютерной информации. Эффективные методы и

средства / В. Ф. Шаньгин. М. : ДМК Пресс, 2008. 544 с.

205. Крысин А. В. Информационная безопасность : практ. руководство / А. В. Крысин. М. : СПАРРК, К. : Век+, 2003. 320 с.

206. Goldreich O., Foundations of cryptography. Volume 1 (Basic tools). Volume 2 (Basic applications). Cambridge University Press, Cambridge, United Kingdom, 2001 (v. 1), 2004 (v. 2).

207. Vergili I., Yücel M. D.Avalanche and Bit Independence Properties for the Ensembles of Randomly Chosen S-Boxes // Turk J Elec Engin. 2001. T. 9. No 2. C.137-145.

208. Соколов, А. В. Новые методы синтеза нелинейных преобразований современных шифров / А. В. Соколов. Lap Lambert Academic Publishing, Germany, 2015. 100 с.

209. Menezes A.J., Oorschot P.C., Vanstone S.A., Handbook of Applied Cryptography, Pub. CRC Press , 1996, 816 p.

210. Beker H., Piper F., Cipher System, Northwood Books, 1982. 144 p.

211. Мельников В. В. Защита информации в компьютерных системах / В. В. Мельников. М. : Финансы и статистика - Электроинформ, 1997. 368 с.

212. Грушо А. А. Теоретические основы защиты информации / А. А. Грушо, Е. Е. Тимонина. М. : Изд-во Агентства «Яхтсмен», 1996. 192 с.

213. Luby M., Pseudorandomness and cryptographic applications. Princeton University Press, Princeton, New Jersey, 1996.

214. Агафонова И. В. Криптографические свойства нелинейных булевых функций [Електронний ресурс] : материалы семинара по дискретному гармоническому анализу и геометрическому моделированию «DHA & CAGD» / И. В. Агафонова. Режим доступу : http://www.dha.spb.ru/

215. Токарева Н. Н. Нелинейные булевы функции: бент-функции и их обобщения

/ Н. Н. Токарева. Изд-во LAP LAMBERT Academic Publishing (Saarbrucken, Germany), 2011. 180 с. ISBN 978-3-8433-0904-2.

216. Carlisle Adams. The CAST-256 Encryption Algorithm. Режим доступу // http://www.mavi1.org/web_security/cryptography/aes-testing/cast/cast-256.pdf

217. C. Adams, H.M. Heys, S.E. Tavares, and M. Wiener. An Analysis of the CAST-256 Cipher Режим доступу //http://www.engr.mun.ca/~howard/PAPERS/cast256.pdf

218. Безбогов А. А. Криптографическая защита информации : учеб. пособие / Безбогов А. А., Яковлев А. Я., Шамкин В. Н. Тамбов : Изд-во Тамб. гос. техн. ун-та, 2006. 140 с.

219. Малюк А. А. Введение в защиту информации в автоматизированных системах / Малюк А. А., Пазизин С. В., Погожин Н. С. М. : Горячая линия-Телеком, 2001. 148 с.

220. Kocher P.C. Timing Attacks on Implementations of Diffie-Hellman, RSA, DSS, and Other Systems. // http://citeseer.ist.psu.edu Cryptography Research, Inc., San Francisco, USA.

221. Аутентификация. Теория и практика обеспечения безопасного доступа к информационным ресурсам. - Москва: Наука, 2012. 552 с.

222. Барабанова М.И., Кияев В.И. Информационные технологии: открытые системы, сети, безопасность в системах и сетях: Учебное пособие.- СПб.: Изд-во СПбГУЭФ, 2010. 267 с.

223. Шаньгин В.Ф. Защита информации в компьютерных системах и сетях [Текст] / В.Ф. Шаньгин. М.: ДМК Пресс, 2012. 592 с.: ил.

224. Katz J., Lindell Y., Introduction to Modern Cryptography: Principles and Protocols - Chapman and Hall/CRC, 2007, 552 p.

225. Stinson D.R., Cryptography: Theory and Practice, CRC Press, 2007, 616 p.

226. Van Tilborg H.C.A., Jajodia S., Encyclopedia of Cryptography and Security - Springer, 2011, 1457 p.

227. Goldreich O., Foundations of Cryptography. Basic Applications, Cambridge university press, 2004, 396 p.

228. Конхейм А. Г. Основы криптографии. М.: Радио и связь, 1987.

229. Щербаков А. Ю., Домашев А. В. Прикладная криптография: использование и синтез криптографических интерфейсов. М.: Русская Редакция, 2003. — 416 с.

230. Масленников М. Практическая криптография. СПб.: БХВ-Петербург, 2003. 464 с.

231. Столлингс В. Криптография и защита сетей: принципы и практика. 2-е изд. М.: Вильяме, 2001. 672 с.

232. Васильева, И. Н. Криптографические методы защиты информации : учебник и практикум для академического бакалавриата / И. Н. Васильева. Москва : Издательство Юрайт, 2018. 349 с.

233. Введение в криптографию / Под общ. ред. В. В. Ященко. 4-еизд., доп. М.: МЦНМО, 2012. 348 с.

234. Н. П. Варновский, “Криптография и теория сложности”, Матем. просв., сер. 3, 2, МЦНМО, М., 1998, 7186.

235. Зубов А.Ю. Совершенные шифры - М.: Гелиос АРВ, 2003. - 160 с.

236. Горбенко І.Д., Горбенко Ю.І. Прикладна криптологія: Теорія. Практика. Застосування: Підручник для ВНЗ Харків: «Форт», 2013. 880 с.

237. Richard A. Mollin, «Codes: the guide to secrecy from ancient to modern times», Chapman & Hall/CRC, 2005. С. 142.

238. Thomas W. Cusick, Pantelimon Stanica, Pantelimon Stănică. Cryptographic

Boolean Functions and Applications. — Academic Press, 2009. С. 25.

239. Інформаційна безпека (соціально-правові аспекти): підручник / Остроухов В. В., Петрик В. М., Присяжнюк М. М. та ін.; за ред. Є. Д. Скулиша. Київ: КНТ, 2010. 776 с.

240. Забезпечення інформаційної безпеки держави: іноземний та вітчизняний досвід: навч. посіб. / Петрик В. М., Панченко В. М., Мельник Д. С. та ін. Київ: Центр навч.-наук. та наук.-практ. вид. НА СБ України, 2014. 424 с.

241. Марущак А. І. Інформаційне право: регулювання інформаційної діяльності: навч.посіб. Київ: Видавничий дім «Скіф»; КНТ, 2008. 344 с.

242. Угрозы, уязвимости, атаки и подходы к защите / Запечников С. В., Милославская Н. Г., Толстой А. И., Ушаков Д. В. М.: Горячая Линия-Телеком, 2006. (Информационная безопасность открытых систем: в 2 томах). Т.1. 536 с.

243. ISO 15408-99. Общие критерии оценки безопасности информационных технологий. Ч. I.

244. ISO 15408-99. Общие критерии оценки безопасности информационных технологий. Ч. II.

245. ISO 15408-99. Общие критерии оценки безопасности информационных технологий. Ч. III.

246. Грицюк Ю. І., Малець І. О., Бабак В. П., Козловський В. В., Хорошко В. О., Чирков Д. В. Підготовка фахівців із захисту інформації в Україні. *Захист інформації*. 2001. № 4. С. 5769.

247. Закон України «Про інформацію»: затверджений і введений в дію Постановою Верховної Ради України № 2657-XII від 02.10.1992 р. *Відомості Верховної Ради України.* 1992, N 48, ст.650.

248. Закон України «Про державну таємницю» від 21 січня 1994 р. *Відомості*

Верховної Ради України. 1994, N 6, ст. 93.

249. Закон України «Про захист інформації в автоматизованих системах»: затверджений і введений в дію Постановою Верховної Ради України № 81/94-ВР від 05.07.1994 р. *Відомості Верховної Ради України.* 1994, N 31, ст.286.

250. Закон України «Про Національну програму інформатизації» від 04.02.1998 р. *Відомості Верховної Ради України*. 1998, N 27-28, ст. 181.

251. Закон України «Про електронні документи та електронний документообіг» від 22 травня 2003 р. №851-IV. *Відомості Верховної Ради України*. 2003, N 36, ст. 275.

252. Закон України «Про електронний цифровий підпис» від 22.05.2003 р. №852-IУ. *Відомості Верховної Ради України*. 2003. N 36, ст. 276.

253. Закон України «Про основи національної безпеки України» : затверджений і введений в дію Постановою Верховної Ради України № 964-IV від 19.06.2003 р. *Відомості Верховної Ради України*. 2003, N 39, ст.351.

254. Закон України «Про телекомунікації» від 18 листопада 2003 р. *Відомості Верховної Ради України*. 2004, N 12, ст.155.

255. Закон України «Про захист інформації в інформаційно- телекомунікаційних системах» від 31 травня 2005 р. *Відомості Верховної Ради України*. 2006, N 26, ст. 347.

256. Закон України «Про внесення змін до Закону України «Про ратифікацію Конвенції про кіберзлочинність» від 21 вересня 2010 р. № 2532-VI. *Урядовий кур'єр*. 2010 р., № 190. 13 жовт.

257. Закон України «Про захист персональних даних» : затверджений і введений в дію Постановою Верховної Ради України № 2297-VI від 01.06.2010 р. *Відомості Верховної Ради України*. 2010, N 34, ст. 481.

52. Постанова Кабінету Міністрів України «Про затвердження Концепції технічного захисту інформації в Україні» № 1126 від 08.10.1997 р. [Електронний ресурс]: Законодавство України: Офіційний сайт Верховної Ради України. URL: http:www. http://zakon2.rada.gov.ua

258. Указ Президента України «Про Положення про порядок здійснення криптографічного захисту інформації в Україні» № 505/98 від 22.05.1998 р. [Електронний ресурс]: Офіційне інтернет-представництво Президента України. URL: http://www.president.gov.ua /stateauthority/authofstate /prezidlist/ prezidentadmin

ДОДАТОК А

ДЕРЖАВНЕ ПІДПРИЄМСТВО
НАУКОВО-ВИРОБНИЧИЙ КОМПЛЕКС
«ФОТОПРИЛАД»
вул. Б. Вишневецького, 85, м. Черкаси, 18000
тел.:(0472) 36 03 08
факс: (0472) 37-45-31
телетайп: 147123 «Щука»
E-mail: photopribor@ic.ck.ua

ГОСУДАРСТВЕННОЕ ПРЕДПРИЯТИЕ
НАУЧНО-ПРОИЗВОДСТВЕННЫЙ
КОМПЛЕКС
«ФОТОПРИБОР»
ул. Б. Вишневецкого, 85, г. Черкассы,
Украина,18000
тел.:(0472) 36-03-08
факс: (0472) 37-45-31
телетайп: 147123 «Щука»
E-mail: photopribor@ic.ck.ua

_____ № _____
на № _____ від _____

ЗАТВЕРДЖУЮ
Генеральний директор
НВК "Фотоприлад"
_____ А.О. Бурківський
"21" листопада 2012 р.

АКТ
впровадження результатів дисертаційної роботи
Бабенко Віри Григорівни
в ЦКБ "Сокіл" НВК "Фотоприлад"

Для забезпечення конфіденційності та достовірності передачі команд в оптичній лінії зв'язку за допомогою виробу 1К118 були використані наступні наукові результати отримані Бабенко Вірою Григорівною, а саме:

- метод синтезу матричних операцій криптографічного перетворення на основі додавання за модулем два;
- метод синтезу базових операцій криптографічного перетворення на основі заміщення однієї або декількох елементарних функцій зі збереженням інформативності;
- математичні моделі та алгоритми побудови матричних операцій криптографічного перетворення інформації на основі спеціалізованих функцій.

Дані наукові результати реалізовані на основі спеціалізованого модуля операційної системи.

Начальник відділу ЦКБ "Сокіл"
НВК "Фотоприлад" _____ О.Я. Хомченко

ЗАТВЕРДЖУЮ
Директор Державного
підприємства "Науково-дослідний
інститут "Акорд"
_____ Онойко В.М.
«___» _____ 2015 р.

АКТ
впровадження результатів дисертаційної роботи
Бабенко Віри Григорівни

При виконанні ДП "НДІ "Акорд" НДДКР для забезпечення конфіденційності та достовірності передачі інформації в системі дистанційного контролю та управління віддаленими об'єктами були використані наступні наукові результати, одержані в дисертаційній роботі на здобуття наукового ступеня доктора технічних наук Бабенко Віри Григорівни, а саме:

- технологія криптографічного перетворення інформації на основі використання матричних операцій;
- метод підвищення стійкості алгоритмів до статистичного криптоаналізу на основі використання операцій матричного криптографічного перетворення та застосування методології синтезу криптографічних алгоритмів, основаних на виконанні матричних операцій;
- технологія підвищення швидкодії виконання примітивів ковзного шифрування на основі застосування матричних операцій криптографічного перетворення оптимізованої структури.

Впровадження вказаних результатів забезпечило можливість використання для матричних операцій криптографічного перетворення одного спеціалізованого процесора, що реалізує повну множину вказаних операцій та забезпечує наявність додаткового ресурсу продуктивності для виконання інших процесів.

Головний інженер
ДП "НДІ "Акорд" _____ Барсуков Є.О.

Провідний інженер _____ Олешко О.П.

25006, Україна, м. Кіровоград,
вул. Орджонікідзе 5, офіс 331
тел. (0522) 30-87-92,
e-mail: lumensgrop@ukr.net

ЛЮМЕНС-ГРУП

ТОВ "ЛЮМЕНС-ГРУП"
р/р 26006002023432
АТ «Дельта Банк»
МФО 380236

ЗАТВЕРДЖУЮ
Директор ТОВ «Люменс-груп»
_____С.В. Богачов
«10» 04 2014 р.

АКТ
впровадження результатів дисертаційної роботи
БАБЕНКО ВІРИ ГРИГОРІВНИ
на ТОВ «Люменс-груп»

Даний акт складено про те, що наукові результати БАБЕНКО ВІРИ ГРИГОРІВНИ, одержані в дисертаційній роботі на здобуття наукового ступеня доктора технічних наук, використано та впроваджено при виконанні ТОВ «Люменс-груп» робіт для забезпечення конфіденційності та достовірності передачі інформації в системі передачі даних, а саме:

- концепція побудови криптографічних алгоритмів на основі синтезу матричних операцій криптографічного перетворення інформації;
- метод захисту інформаційних ресурсів на основі застосування алгоритмів криптографічного перетворення синтезованих на базі комбінації матричних операцій криптографічного перетворення;
- метод підвищення стійкості алгоритмів до статистичного криптоаналізу на основі застосування розробленої технології криптографічного перетворення інформації на базі матричних операцій.

Впровадження вказаних результатів забезпечило можливість підвищення якості захисту електронних інформаційних ресурсів шляхом застосування ефективних криптографічних алгоритмів синтезованих на основі матричних операцій криптографічного перетворення, для побудови яких використано дискретні операції криптографічного перетворення з мінімальною складністю реалізації та водночас максимальною швидкодію.

Голова комісії:
Директор ТОВ «Люменс-груп» С.В. Богачов

Члени комісії:
провідний розробник О.В. Коваленко

провідний розробник Є.В. Мелешко

ЗАТВЕРДЖУЮ

Директор ПП «Сенсорна електроніка»
д.т.н., професор

_____ М.П. Мусієнко

«19» травня 2015 р.

АКТ

впровадження результатів дисертаційної роботи
Бабенко Віри Григорівни в
ПП «Сенсорна електроніка»

На приватному підприємстві «Сенсорна електроніка» для забезпечення захисту програмних продуктів, а також доступу до технічної і технологічної документації підприємства використані наукові результати дисертаційної роботи Бабенко Віри Григорівни, а саме метод захисту інформаційних ресурсів на основі застосування алгоритмів криптографічного перетворення синтезованих на базі комбінації матричних операцій криптографічного перетворення.

Технічну реалізацію отримали наступні практичні результати дисертаційної роботи:

- технологія побудови та використання криптопримітивів на основі синтезованих операцій криптографічного перетворення інформації з можливістю їх паралельного виконання, що дає виграш у швидкості та часі здійснення перетворення;
- алгоритми синтезу криптографічних операцій, що володіють властивостями афінності та нелінійності, зокрема матричного та розширеного матричного перетворення.

Дані результати реалізовані на програмному та апаратному рівнях.

Провідний спеціаліст О. О. Корецька

ЗАТВЕРДЖУЮ:
Проректор з наукової роботи
Кіровоградського національного
технічного університету

_____О.М. Левченко
26 12 2016 р.

АКТ

впровадження результатів дисертаційної роботи
Бабенко Віри Григорівни

Цей акт складено у тому, що під час роботи над держбюджетною темою № 36Б115 «Розробка методів синтезу тестових моделей поведінки програмних об'єктів, підвищення оперативності передачі та захисту інформації у телекомунікаційних системах» (№ДР 0115U003103), яка виконується у Кіровоградському національному технічному університеті, для забезпечення захисту програмних продуктів, а також доступу до технічної і технологічної документації використані наукові результати дисертаційної роботи Бабенко Віри Григорівни, а саме метод захисту інформаційних ресурсів на основі застосування алгоритмів криптографічного перетворення синтезованих на базі комбінації матричних операцій криптографічного перетворення.

При розробці спеціалізованих програмних та апаратних засобів використані вдосконалені примітиви ковзного шифрування шляхом впровадження мультиоперандних операцій криптографічного перетворення з точністю до перестановки.

Керівник ДБ № 36Б115 «Розробка методів синтезу тестових моделей поведінки програмних об'єктів, підвищення оперативності передачі та захисту інформації у телекомунікаційних системах»

доктор технічних наук, професор О.А. Смірнов

ЗАТВЕРДЖУЮ
Проректор з навчальної роботи
Черкаського державного
технологічного університету
_____О.О. Григор
«21» 10 2015 р.

АКТ

впровадження результатів дисертаційної роботи Бабенко Віри Григорівни в навчальний процес Черкаського державного технологічного університету

Комісія у складі декана факультету інформаційних технологій і систем к.т.н., доцента Ланських Є.В., к.т.н., доцента Фауре Е.В., к.ф.-м.н., доцента Півня О.Б., розглянувши дисертаційну роботу Бабенко Віри Григорівни, встановила наступне:

- в курсі лекцій з дисципліни «Захист інформації в комп'ютерних системах» використовується вдосконалений спосіб багаторазового застосування примітива ковзного шифрування;
- в курсі лекцій з дисципліни «Надійність і безпека комп'ютерних систем обробки інформації» використовуються підходи щодо реалізації криптопримітивів матричними операціями криптографічного перетворення, а саме оптимізаційні моделі матричних операцій ковзного шифрування реалізовані на основі рекурентних послідовностей.

Дані дисципліни викладаються при підготовці бакалаврів з напряму 6.050102- комп'ютерна інженерія.

При підготовці магістрів зі спеціальності 8.05010201 – комп'ютерні системи та мережі матеріали дисертаційного дослідження Бабенко В.Г. використані для розробки курсу лекцій з дисципліни «Інформаційна безпека комп'ютерних систем та мереж».

Голова комісії: Є.В. Ланських

Члени комісії: Е.В. Фауре

О.Б. Півень

ЗАТВЕРДЖУЮ
Проректор з наукової та
інноваційної діяльності Черкаського
національного університету імені
Богдана Хмельницького, професор
Корновенко С.В.

«20» 10 2015 р.

АКТ

впровадження результатів дисертаційної роботи
Бабенко Віри Григорівни в навчальний процес
Черкаського національного університету
ім. Богдана Хмельницького

Основні результати дисертаційного дослідження Бабенко Віри Григорівни використовуються при викладанні дисциплін «Захист інформації» та «Безпека програм та даних» бакалаврам напряму 6.050103 «Програмна інженерія». До лекційного курсу вказаних дисциплін включені такі результати, отримані Бабенко В.Г.: методи синтезу операцій криптографічного перетворення інформації шляхом побудови та перебудови функцій обмеження, що дало змогу синтезувати ці операції на основі поєднання елементарних функцій; технологія синтезу криптопримітивів на основі матричних операцій криптографічного перетворення.

При виконанні курсових та кваліфікаційних робіт використовуються принципи побудови алгоритмів шифрування із застосуванням криптопримітивів синтезованих на основі операцій матричного криптографічного перетворення, що дало можливість будувати системи криптографічного захисту інформації з новими якісними характеристиками.

Завідувач кафедри інтелектуальних систем прийняття рішень Черкаського національного університету імені Богдана Хмельницького к.т.н., доцент І.А. Осауленко

Професор кафедри інтелектуальних систем прийняття рішень Черкаського національного університету імені Богдана Хмельницького д.т.н., професор С.В. Голуб

Завідувач кафедри програмного забезпечення автоматизованих систем, к.т.н., доцент Б.О. Онищенко

Декан факультету обчислювальної техніки, інтелектуальних і управляючих систем, к.т.н., доцент В.І. Саланатов

ЗАТВЕРДЖУЮ
Проректор з НПР
Національного аерокосмічного
університету ім. М.Є. Жуковського
«ХАІ»
проф. Зайцев В.Є. _____
«12» 03 2015 р.

АКТ

**впровадження результатів дисертаційної роботи
Бабенко Віри Григорівни в навчальний процес
Національного аерокосмічного університету
ім. М.Є. Жуковського «ХАІ»**

При підготовці бакалаврів напряму 6.050103 «Програмна інженерія» в курсі лекцій з дисципліни «Безпека програм та даних» використані наступні результати дисертаційного дослідження, отримані Бабенко Вірою Григорівною:

- методологія дослідження і синтезу логічних операцій для криптографічного перетворення інформації;
- методи синтезу операцій матричного криптографічного перетворення;
- моделювання криптоалгоритмів підвищеної ефективності на основі операцій криптографічного перетворення інформації.

При курсовому проектуванні та виконанні кваліфікаційних робіт використовуються методи, моделі синтезу примітивів на основі операцій криптографічного перетворення інформації для побудови алгоритмів захисту інформації.

Завідувач кафедри
інженерії програмного забезпечення
Національного аерокосмічного
університету ім. М.Є. Жуковського «ХАІ»
д.т.н., професор І.Б. Туркін

ЗАТВЕРДЖУЮ
Проректор з наукової роботи
Кіровоградського національного
технічного університету
_____О.М. Левченко
«25» ____11_____ 2016 р.

АКТ
впровадження результатів дисертаційної роботи
Бабенко Віри Григорівни в навчальний процес
Кіровоградського національного технічного університету

Комісія у складі голови – завідувача кафедри програмування та захисту інформації доктора технічних наук, професора Смірнова О.А, членів комісії – доцента кафедри програмування та захисту інформації кандидата фізико-математичних наук, доцента Якименко Н.М., доцента кафедри програмування та захисту інформації кандидата технічних наук, доцента Коваленко О.В. розглянувши матеріали дисертаційної роботи Бабенко Віри Григорівни, встановила наступне:

1. При підготовці фахівців напряму 6.170103 Управління інформаційною безпекою в курсі лекцій з дисципліни «Проектування систем комплексного захисту інформації», «Основи криптографічного захисту інформації» використані наступні результати дисертаційного дослідження, отримані Бабенко Вірою Григорівною: технологія синтезу операцій для мультиопераційних матричних криптографічних примітивів, методи побудови нових груп операцій з точністю до перестановки шляхом використання запропонованої табличної моделі операції криптоперетворення, що дозволило збільшити кількість операцій за рахунок варіативності операцій криптопримітивів.

2. При курсовому проектуванні та виконанні кваліфікаційних робіт використовуються методи синтезу примітивів на основі моделей операцій матричного криптографічного перетворення інформації для побудови алгоритмів захисту інформації.

Голова комісії
Завідувач кафедри програмування та захисту інформації
Кіровоградського національного технічного університету
доктор технічних наук, професор О.А. Смірнов

Члени комісії:
доцент кафедри програмування та захисту інформації
кандидат фізико-математичних наук, доцент Н.М. Якименко

доцент кафедри програмування та захисту інформації
кандидат технічних наук, доцент О.В. Коваленко

ДОДАТОК Б

Результати тестування матричного перетворення невипадкової монотонно зростаючої послідовності з циклом повторення 64 байти

RESULTS FOR THE UNIFORMITY OF P-VALUES AND THE PROPORTION OF PASSING SEQUENCES

---

generator is <V_M_64.bin>

C1	C2	C3	C4	C5	C6	C7	C8	C9	C10	P-VALUE	PROPORTION	STATISTICAL TEST
6	11	6	11	12	9	13	9	11	12	0.798139	1.0000	Frequency
10	6	10	13	7	10	10	13	7	14	0.657933	0.9900	BlockFrequency
7	9	10	14	6	10	7	11	16	10	0.455937	1.0000	CumulativeSums
8	7	4	10	12	8	13	17	12	9	0.213309	1.0000	CumulativeSums
10	13	5	5	12	19	9	11	9	7	0.075719	0.9900	Runs
21	9	9	7	10	3	11	9	13	8	0.020548	0.9600	LongestRun
15	11	14	9	4	10	11	8	5	13	0.224821	0.9700	Rank
5	6	8	6	10	9	13	15	17	11	0.102526	1.0000	FFT
11	10	11	10	11	11	17	8	7	4	0.334538	0.9800	NonOverlappingTemplate
9	7	8	13	7	12	12	11	11	10	0.897763	1.0000	NonOverlappingTemplate
10	8	8	10	7	13	12	12	11	9	0.935716	0.9700	NonOverlappingTemplate
8	9	13	9	11	12	13	11	10	4	0.678686	0.9800	NonOverlappingTemplate
7	12	15	13	7	9	13	2	11	11	0.153763	0.9900	NonOverlappingTemplate
11	8	11	10	8	14	6	9	10	13	0.816537	0.9900	NonOverlappingTemplate
13	7	9	12	8	11	10	8	9	13	0.897763	0.9900	NonOverlappingTemplate
6	20	5	8	7	8	9	14	14	9	0.023545	1.0000	NonOverlappingTemplate
11	11	6	6	9	11	12	8	14	12	0.699313	1.0000	NonOverlappingTemplate
8	8	13	11	18	8	6	6	11	11	0.213309	1.0000	NonOverlappingTemplate
8	10	12	11	10	4	10	18	6	11	0.181557	0.9700	NonOverlappingTemplate
10	8	11	12	13	9	10	9	9	9	0.987896	1.0000	NonOverlappingTemplate
13	15	8	13	10	9	8	7	8	9	0.678686	1.0000	NonOverlappingTemplate
7	11	8	8	8	13	6	10	18	11	0.262249	1.0000	NonOverlappingTemplate
8	17	14	13	9	8	9	6	3	13	0.071177	1.0000	NonOverlappingTemplate
10	9	9	9	15	13	7	8	10	10	0.834308	1.0000	NonOverlappingTemplate
8	13	8	10	8	10	10	9	12	12	0.964295	0.9800	NonOverlappingTemplate
12	9	12	7	5	12	11	6	18	8	0.153763	0.9900	NonOverlappingTemplate
12	13	13	10	10	4	7	7	14	10	0.419021	0.9900	NonOverlappingTemplate
9	6	12	9	18	8	8	7	9	14	0.213309	1.0000	NonOverlappingTemplate
8	14	11	12	9	10	3	11	10	12	0.534146	0.9800	NonOverlappingTemplate
11	10	10	12	11	13	4	9	13	7	0.637119	0.9900	NonOverlappingTemplate
8	9	6	8	21	4	12	11	9	12	0.023545	0.9900	NonOverlappingTemplate
13	11	13	8	14	6	4	3	13	15	0.042808	1.0000	NonOverlappingTemplate
10	11	14	7	10	10	12	10	7	9	0.911413	0.9900	NonOverlappingTemplate
9	8	11	6	10	12	10	12	9	13	0.911413	1.0000	NonOverlappingTemplate
13	8	8	7	10	11	7	12	16	8	0.534146	0.9900	NonOverlappingTemplate
9	8	12	9	9	16	7	11	10	9	0.759756	0.9900	NonOverlappingTemplate
12	10	11	7	9	9	6	21	8	7	0.055361	0.9900	NonOverlappingTemplate
8	7	10	15	8	11	8	10	11	12	0.816537	1.0000	NonOverlappingTemplate
13	5	11	12	7	9	6	15	10	12	0.401199	1.0000	NonOverlappingTemplate
9	8	14	11	7	13	10	11	13	4	0.474986	0.9700	NonOverlappingTemplate
13	8	11	9	9	7	5	16	11	11	0.455937	0.9900	NonOverlappingTemplate
7	11	15	9	11	8	14	7	8	10	0.637119	1.0000	NonOverlappingTemplate
13	16	11	7	11	7	3	9	9	14	0.153763	0.9800	NonOverlappingTemplate
10	15	9	7	9	11	14	9	7	9	0.699313	1.0000	NonOverlappingTemplate
10	10	11	7	7	15	16	6	11	7	0.304126	1.0000	NonOverlappingTemplate
9	11	9	15	13	9	4	6	14	10	0.304126	0.9800	NonOverlappingTemplate
15	10	11	13	9	7	10	6	12	7	0.595549	0.9900	NonOverlappingTemplate
4	12	9	11	8	17	8	12	15	4	0.058984	1.0000	NonOverlappingTemplate
9	6	13	11	8	5	10	12	17	9	0.275709	1.0000	NonOverlappingTemplate
12	8	7	11	10	7	13	12	10	10	0.911413	0.9800	NonOverlappingTemplate
11	10	9	11	11	10	4	13	9	12	0.798139	0.9800	NonOverlappingTemplate
11	12	6	9	11	6	14	12	9	10	0.739918	0.9800	NonOverlappingTemplate
12	12	7	14	6	8	7	13	15	6	0.262249	0.9900	NonOverlappingTemplate
10	9	8	13	16	8	6	7	17	6	0.108791	0.9800	NonOverlappingTemplate

7	8	12	11	10	14	6	9	9	14	0.657933	0.9700	NonOverlappingTemplate
13	11	13	10	7	10	8	12	7	9	0.867692	0.9900	NonOverlappingTemplate
13	9	11	9	10	8	8	9	11	12	0.978072	0.9800	NonOverlappingTemplate
6	17	13	12	11	10	6	9	4	12	0.137282	0.9900	NonOverlappingTemplate
6	9	12	12	15	14	9	6	10	7	0.419021	0.9900	NonOverlappingTemplate
10	9	12	14	6	8	10	11	10	10	0.897763	1.0000	NonOverlappingTemplate
10	8	8	8	9	7	16	16	10	8	0.366918	0.9900	NonOverlappingTemplate
13	11	6	12	12	4	13	9	10	10	0.534146	0.9900	NonOverlappingTemplate
9	17	7	11	8	12	12	9	7	8	0.474986	0.9800	NonOverlappingTemplate
10	9	6	8	15	15	12	6	8	11	0.383827	1.0000	NonOverlappingTemplate
10	13	9	6	9	10	10	11	10	12	0.955835	0.9800	NonOverlappingTemplate
7	13	12	12	8	8	8	18	5	9	0.171867	0.9800	NonOverlappingTemplate
10	9	9	12	7	12	12	5	13	11	0.759756	0.9900	NonOverlappingTemplate
11	17	8	7	17	11	6	4	7	12	0.037566	1.0000	NonOverlappingTemplate
10	7	8	9	12	13	8	16	12	5	0.383827	0.9900	NonOverlappingTemplate
17	15	10	11	10	5	4	5	10	13	0.048716	0.9800	NonOverlappingTemplate
7	17	4	14	6	12	9	16	7	8	0.035174	1.0000	NonOverlappingTemplate
5	8	13	9	11	9	15	10	13	7	0.494392	1.0000	NonOverlappingTemplate
10	12	10	9	10	14	11	9	7	8	0.935716	0.9900	NonOverlappingTemplate
12	4	13	12	11	8	9	14	8	9	0.534146	0.9900	NonOverlappingTemplate
13	11	7	13	12	9	11	7	11	6	0.739918	0.9900	NonOverlappingTemplate
8	17	9	13	8	13	6	13	6	7	0.181557	1.0000	NonOverlappingTemplate
14	9	8	11	12	18	7	7	8	6	0.171867	0.9700	NonOverlappingTemplate
8	9	14	9	9	11	9	13	13	5	0.657933	0.9900	NonOverlappingTemplate
10	10	11	10	16	9	10	9	10	5	0.699313	0.9800	NonOverlappingTemplate
14	8	9	11	9	10	10	4	10	15	0.494392	0.9900	NonOverlappingTemplate
12	7	11	11	14	9	9	8	9	10	0.924076	0.9900	NonOverlappingTemplate
5	11	8	12	12	12	9	5	16	10	0.319084	0.9800	NonOverlappingTemplate
11	10	11	10	11	12	16	8	7	4	0.419021	0.9800	NonOverlappingTemplate
6	7	12	15	12	11	13	6	6	12	0.319084	1.0000	NonOverlappingTemplate
9	12	18	13	7	8	7	4	10	12	0.122325	0.9900	NonOverlappingTemplate
8	14	12	10	15	9	7	12	6	7	0.455937	0.9900	NonOverlappingTemplate
12	10	11	6	4	15	13	13	9	7	0.275709	1.0000	NonOverlappingTemplate
16	5	6	12	9	9	11	12	8	12	0.383827	0.9800	NonOverlappingTemplate
11	9	7	12	9	5	12	11	12	12	0.798139	0.9900	NonOverlappingTemplate
15	10	9	10	12	11	8	7	9	9	0.867692	1.0000	NonOverlappingTemplate
10	11	8	9	13	7	10	14	9	9	0.897763	0.9800	NonOverlappingTemplate
12	14	7	8	11	11	6	13	11	7	0.637119	0.9900	NonOverlappingTemplate
5	11	10	14	13	8	10	9	11	9	0.759756	0.9900	NonOverlappingTemplate
13	10	18	7	4	9	10	7	16	6	0.035174	0.9900	NonOverlappingTemplate
9	8	14	14	3	10	8	14	13	7	0.191687	0.9800	NonOverlappingTemplate
19	9	10	6	8	11	10	13	8	6	0.153763	1.0000	NonOverlappingTemplate
9	11	8	5	9	9	12	12	14	11	0.759756	1.0000	NonOverlappingTemplate
10	15	7	10	8	8	12	14	6	10	0.554420	0.9900	NonOverlappingTemplate
8	1	12	15	9	13	9	10	7	16	0.048716	1.0000	NonOverlappingTemplate
9	9	13	11	10	13	6	8	8	13	0.798139	0.9900	NonOverlappingTemplate
10	9	7	16	6	10	13	11	8	10	0.574903	1.0000	NonOverlappingTemplate
8	8	9	11	9	11	12	11	13	8	0.964295	1.0000	NonOverlappingTemplate
8	8	10	8	14	8	10	10	5	19	0.129620	0.9900	NonOverlappingTemplate
13	11	6	10	9	14	6	10	11	10	0.739918	0.9800	NonOverlappingTemplate
9	8	10	9	5	9	10	19	8	13	0.181557	0.9800	NonOverlappingTemplate
10	10	8	9	6	13	12	13	8	11	0.851383	1.0000	NonOverlappingTemplate
16	4	8	10	10	6	7	12	14	13	0.162606	0.9800	NonOverlappingTemplate
11	15	5	12	5	9	8	8	15	12	0.224821	0.9800	NonOverlappingTemplate
14	11	9	8	10	12	11	7	8	10	0.911413	0.9800	NonOverlappingTemplate
18	10	8	9	8	10	11	9	9	8	0.534146	0.9900	NonOverlappingTemplate
10	9	7	9	13	14	13	5	14	6	0.334538	1.0000	NonOverlappingTemplate
10	13	8	9	11	9	8	10	13	9	0.964295	1.0000	NonOverlappingTemplate
17	10	11	14	9	6	6	9	11	7	0.275709	0.9700	NonOverlappingTemplate
6	7	14	12	13	6	10	12	7	13	0.419021	1.0000	NonOverlappingTemplate
9	16	6	8	11	10	11	11	11	7	0.637119	0.9900	NonOverlappingTemplate
6	5	10	17	6	15	14	12	10	5	0.040108	1.0000	NonOverlappingTemplate
6	15	9	7	16	9	10	10	9	9	0.437274	0.9900	NonOverlappingTemplate
10	9	7	4	9	11	12	17	10	11	0.334538	0.9900	NonOverlappingTemplate
12	13	10	10	7	8	12	9	8	11	0.935716	0.9800	NonOverlappingTemplate
14	14	9	10	9	10	11	8	6	9	0.779188	0.9800	NonOverlappingTemplate
4	8	6	13	17	15	8	11	11	7	0.080519	1.0000	NonOverlappingTemplate
7	7	7	9	19	11	9	10	15	6	0.085587	0.9900	NonOverlappingTemplate
9	9	11	8	15	10	8	17	6	7	0.275709	0.9800	NonOverlappingTemplate
15	7	5	11	10	12	13	12	6	9	0.401199	0.9900	NonOverlappingTemplate

13	5	9	9	7	10	10	10	15	12	0.595549	0.9700	NonOverlappingTemplate
19	9	7	11	6	4	9	11	14	10	0.062821	0.9600	NonOverlappingTemplate
8	12	14	14	8	7	13	7	10	7	0.534146	0.9800	NonOverlappingTemplate
5	11	16	10	8	10	10	6	14	10	0.366918	1.0000	NonOverlappingTemplate
5	6	10	10	10	12	5	17	18	7	0.023545	0.9900	NonOverlappingTemplate
13	6	8	11	10	15	9	10	14	4	0.289667	0.9900	NonOverlappingTemplate
8	9	11	10	7	10	10	13	9	13	0.946308	0.9900	NonOverlappingTemplate
7	8	9	11	11	14	8	5	12	15	0.437274	0.9900	NonOverlappingTemplate
10	6	10	11	5	11	8	16	8	15	0.262249	0.9700	NonOverlappingTemplate
8	14	11	8	8	9	14	10	8	10	0.834308	0.9900	NonOverlappingTemplate
8	9	13	12	13	7	7	9	14	8	0.678686	1.0000	NonOverlappingTemplate
9	6	11	7	8	9	6	12	15	17	0.181557	0.9900	NonOverlappingTemplate
9	10	11	9	13	18	10	6	5	9	0.224821	0.9900	NonOverlappingTemplate
11	5	13	12	9	9	11	9	10	11	0.883171	0.9900	NonOverlappingTemplate
8	4	11	8	8	14	15	11	8	13	0.319084	1.0000	NonOverlappingTemplate
10	9	10	10	12	12	11	5	9	12	0.911413	0.9800	NonOverlappingTemplate
11	7	10	8	9	5	14	14	10	12	0.574903	1.0000	NonOverlappingTemplate
11	9	7	5	9	16	15	11	5	12	0.171867	1.0000	NonOverlappingTemplate
7	17	9	6	16	6	8	9	8	14	0.085587	0.9900	NonOverlappingTemplate
13	12	5	9	11	10	10	12	9	9	0.867692	0.9800	NonOverlappingTemplate
9	7	11	6	12	11	15	14	6	9	0.437274	0.9900	NonOverlappingTemplate
6	13	11	10	7	9	10	12	13	9	0.834308	0.9900	NonOverlappingTemplate
9	15	12	6	8	10	13	8	12	7	0.574903	1.0000	NonOverlappingTemplate
13	12	9	7	8	9	8	15	10	9	0.759756	0.9800	NonOverlappingTemplate
10	13	9	10	9	9	11	11	8	10	0.994250	0.9900	NonOverlappingTemplate
7	10	17	9	13	11	11	11	5	6	0.262249	0.9900	NonOverlappingTemplate
16	9	5	12	8	8	14	11	5	12	0.213309	0.9900	NonOverlappingTemplate
11	12	8	9	9	10	7	11	6	17	0.474986	0.9800	NonOverlappingTemplate
10	7	3	10	10	10	14	10	13	13	0.419021	0.9900	NonOverlappingTemplate
13	8	6	16	7	13	4	11	9	13	0.162606	0.9700	NonOverlappingTemplate
13	10	7	11	6	10	7	11	12	13	0.759756	0.9800	NonOverlappingTemplate
5	11	8	12	12	12	8	6	16	10	0.366918	0.9800	NonOverlappingTemplate
16	9	7	7	14	12	7	5	10	13	0.224821	0.9900	OverlappingTemplate
11	8	13	14	5	8	11	11	7	12	0.595549	1.0000	Universal
7	19	11	5	9	8	14	6	13	8	0.055361	0.9900	ApproximateEntropy
4	7	7	6	7	3	3	8	9	7	0.689019	1.0000	RandomExcursions
10	9	6	2	9	5	3	4	9	4	0.170294	1.0000	RandomExcursions
4	9	5	6	4	3	4	6	12	8	0.222869	1.0000	RandomExcursions
1	9	4	10	5	5	5	7	8	7	0.311542	1.0000	RandomExcursions
2	3	8	9	7	9	4	9	6	4	0.287306	1.0000	RandomExcursions
3	6	10	4	2	9	6	3	9	9	0.141256	1.0000	RandomExcursions
4	5	8	5	2	4	5	9	6	13	0.095617	1.0000	RandomExcursions
6	6	5	4	1	5	8	9	12	5	0.141256	1.0000	RandomExcursions
3	3	7	7	8	5	10	7	4	7	0.551026	1.0000	RandomExcursionsVariant
4	4	5	8	3	9	8	6	9	5	0.585209	1.0000	RandomExcursionsVariant
5	4	9	2	6	3	8	11	8	5	0.204076	1.0000	RandomExcursionsVariant
7	5	6	2	6	7	7	7	9	5	0.819544	1.0000	RandomExcursionsVariant
7	6	5	7	4	9	5	6	2	10	0.517442	0.9672	RandomExcursionsVariant
8	5	1	7	7	8	3	9	9	4	0.264458	0.9672	RandomExcursionsVariant
6	4	5	3	7	12	5	3	8	8	0.242986	0.9836	RandomExcursionsVariant
3	7	6	5	9	8	7	8	1	7	0.422034	1.0000	RandomExcursionsVariant
5	5	5	7	8	4	9	4	7	7	0.875539	1.0000	RandomExcursionsVariant
6	5	8	11	6	1	3	10	7	4	0.116519	1.0000	RandomExcursionsVariant
6	9	6	3	3	5	8	10	4	7	0.452799	0.9836	RandomExcursionsVariant
8	6	6	5	2	8	7	8	7	4	0.756476	0.9836	RandomExcursionsVariant
5	4	9	9	8	4	7	6	8	1	0.337162	0.9836	RandomExcursionsVariant
7	5	3	4	13	8	7	5	5	4	0.186566	0.9836	RandomExcursionsVariant
7	6	4	3	11	9	3	4	6	8	0.287306	0.9836	RandomExcursionsVariant
8	5	3	5	6	7	4	6	8	9	0.788728	0.9672	RandomExcursionsVariant
2	11	2	8	7	4	3	9	7	8	0.095617	0.9672	RandomExcursionsVariant
3	6	10	7	4	5	5	5	8	8	0.654467	0.9672	RandomExcursionsVariant
8	10	10	6	13	11	7	11	11	13	0.834308	0.9900	Serial
9	10	12	10	13	9	10	9	8	10	0.991468	0.9800	Serial
9	14	7	12	11	11	5	13	6	12	0.474986	0.9900	LinearComplexity

- -

The minimum pass rate for each statistical test with the exception of the random excursion (variant) test is approximately = 0.960150 for a sample size = 100 binary sequences.

The minimum pass rate for the random excursion (variant) test is approximately 0.951781 for a sample size = 61 binary sequences.

For further guidelines construct a probability table using the MAPLE program provided in the addendum section of the documentation.

Результати тестування матричного перетворення невипадкової монотонно зростаючої послідовності з циклом повторення 256 байти

RESULTS FOR THE UNIFORMITY OF P-VALUES AND THE PROPORTION OF PASSING SEQUENCES

---

generator is <V_M_256.bin>

C1	C2	C3	C4	C5	C6	C7	C8	C9	C10	P-VALUE	PROPORTION	STATISTICAL TEST
10	10	9	11	10	11	5	15	8	11	0.759756	0.9900	Frequency
12	12	9	13	4	13	6	9	12	10	0.494392	1.0000	BlockFrequency
9	10	12	8	7	10	10	11	6	17	0.494392	1.0000	CumulativeSums
11	8	12	9	11	6	8	11	11	13	0.897763	1.0000	CumulativeSums
7	5	11	16	11	11	8	12	12	7	0.401199	0.9900	Runs
9	8	8	11	13	11	6	13	11	10	0.867692	0.9800	LongestRun
7	12	17	7	7	10	15	10	5	10	0.162606	1.0000	Rank
3	7	9	7	12	9	15	12	12	14	0.202268	1.0000	FFT
6	14	9	16	11	8	11	8	8	9	0.494392	0.9700	NonOverlappingTemplate
12	9	13	8	9	9	9	10	13	8	0.946308	1.0000	NonOverlappingTemplate
14	16	10	9	9	11	5	6	10	10	0.383827	0.9700	NonOverlappingTemplate
16	13	9	9	9	9	7	12	11	5	0.455937	0.9700	NonOverlappingTemplate
11	14	6	11	5	11	13	11	7	11	0.534146	0.9900	NonOverlappingTemplate
10	11	8	8	9	12	13	10	10	9	0.983453	1.0000	NonOverlappingTemplate
12	12	8	9	10	4	11	12	13	9	0.699313	0.9800	NonOverlappingTemplate
6	11	13	14	7	9	9	6	13	12	0.514124	0.9800	NonOverlappingTemplate
12	9	10	4	9	12	12	9	10	13	0.739918	1.0000	NonOverlappingTemplate
8	9	10	6	6	13	13	12	14	9	0.574903	0.9900	NonOverlappingTemplate
12	13	11	5	15	12	6	10	11	5	0.275709	1.0000	NonOverlappingTemplate
12	10	10	9	13	6	8	10	9	13	0.883171	0.9800	NonOverlappingTemplate
8	6	17	11	11	8	11	6	10	12	0.383827	0.9900	NonOverlappingTemplate
11	11	19	9	11	8	8	10	8	5	0.202268	1.0000	NonOverlappingTemplate
6	3	11	15	5	15	16	11	7	11	0.026948	1.0000	NonOverlappingTemplate
12	8	7	12	13	15	9	7	10	7	0.595549	0.9900	NonOverlappingTemplate
12	10	6	7	13	15	8	5	12	12	0.350485	1.0000	NonOverlappingTemplate
12	13	18	7	9	8	9	13	4	7	0.102526	1.0000	NonOverlappingTemplate
9	15	8	8	9	8	11	12	14	6	0.574903	1.0000	NonOverlappingTemplate
8	8	11	4	11	8	14	13	10	13	0.494392	1.0000	NonOverlappingTemplate
11	12	10	13	10	5	10	10	10	9	0.911413	0.9900	NonOverlappingTemplate
7	10	11	10	11	5	9	10	16	11	0.595549	0.9700	NonOverlappingTemplate
12	11	10	8	2	10	8	17	11	11	0.171867	0.9900	NonOverlappingTemplate
8	8	9	8	4	7	16	9	15	16	0.075719	0.9900	NonOverlappingTemplate
8	8	13	10	8	12	9	12	12	8	0.924076	0.9900	NonOverlappingTemplate
11	9	15	8	8	9	10	12	9	9	0.897763	0.9800	NonOverlappingTemplate
4	14	13	12	5	8	9	13	9	13	0.249284	1.0000	NonOverlappingTemplate
5	10	5	14	16	12	8	9	10	11	0.262249	1.0000	NonOverlappingTemplate
12	7	11	8	8	9	14	10	8	13	0.816537	1.0000	NonOverlappingTemplate
10	14	9	9	6	10	8	13	12	9	0.816537	1.0000	NonOverlappingTemplate
5	13	14	7	13	9	8	13	10	8	0.474986	1.0000	NonOverlappingTemplate
14	6	7	15	8	9	7	14	12	8	0.319084	1.0000	NonOverlappingTemplate
13	9	10	7	10	6	10	17	11	7	0.401199	0.9900	NonOverlappingTemplate
9	13	8	15	14	6	11	5	12	7	0.275709	0.9700	NonOverlappingTemplate
12	5	10	10	7	4	15	10	14	13	0.191687	1.0000	NonOverlappingTemplate
9	7	14	9	14	12	9	12	6	8	0.616305	1.0000	NonOverlappingTemplate
11	14	11	10	8	10	10	9	9	8	0.971699	0.9800	NonOverlappingTemplate
5	11	8	9	11	10	14	13	5	14	0.366918	1.0000	NonOverlappingTemplate
9	7	3	13	9	8	8	17	16	10	0.062821	1.0000	NonOverlappingTemplate
10	6	10	7	8	13	10	13	13	10	0.779188	1.0000	NonOverlappingTemplate
7	11	14	7	9	4	10	13	9	16	0.224821	1.0000	NonOverlappingTemplate
10	12	4	9	8	12	8	13	16	8	0.334538	0.9900	NonOverlappingTemplate
9	10	9	9	13	14	6	13	7	10	0.719747	1.0000	NonOverlappingTemplate
7	10	2	10	14	10	10	9	15	13	0.191687	0.9800	NonOverlappingTemplate
12	5	10	15	10	15	10	7	11	5	0.249284	0.9700	NonOverlappingTemplate
8	7	14	9	10	11	9	9	9	14	0.834308	0.9900	NonOverlappingTemplate
6	9	10	10	10	9	14	9	13	10	0.883171	0.9900	NonOverlappingTemplate
8	14	17	9	12	9	8	6	12	5	0.191687	0.9900	NonOverlappingTemplate

8	14	9	15	6	11	4	13	11	9	0.275709	0.9800	NonOverlappingTemplate
8	13	4	17	10	9	15	6	7	11	0.090936	0.9900	NonOverlappingTemplate
4	15	7	13	14	13	11	12	8	3	0.062821	1.0000	NonOverlappingTemplate
10	6	9	10	10	13	6	13	10	13	0.739918	1.0000	NonOverlappingTemplate
7	8	13	9	7	9	13	15	7	12	0.534146	0.9900	NonOverlappingTemplate
6	15	9	9	5	13	10	12	10	11	0.514124	1.0000	NonOverlappingTemplate
11	6	9	11	7	8	11	10	12	15	0.719747	1.0000	NonOverlappingTemplate
8	7	9	14	7	11	12	12	14	6	0.534146	1.0000	NonOverlappingTemplate
14	12	9	8	13	11	9	6	11	7	0.719747	1.0000	NonOverlappingTemplate
14	10	10	12	10	9	4	10	10	11	0.759756	1.0000	NonOverlappingTemplate
9	12	7	10	12	9	9	10	10	12	0.983453	1.0000	NonOverlappingTemplate
13	6	7	10	8	11	15	17	7	6	0.129620	0.9900	NonOverlappingTemplate
4	8	12	14	9	9	10	19	8	7	0.075719	0.9900	NonOverlappingTemplate
12	7	10	7	14	14	10	7	10	9	0.699313	0.9900	NonOverlappingTemplate
5	5	6	8	14	10	18	14	7	13	0.030806	1.0000	NonOverlappingTemplate
11	5	11	12	11	15	11	5	5	14	0.191687	0.9800	NonOverlappingTemplate
7	12	13	4	15	9	11	6	11	12	0.304126	0.9900	NonOverlappingTemplate
14	9	11	10	6	7	9	12	15	7	0.514124	0.9700	NonOverlappingTemplate
6	6	6	5	10	14	7	13	12	21	0.005762	1.0000	NonOverlappingTemplate
15	6	7	12	6	9	13	14	12	6	0.236810	0.9900	NonOverlappingTemplate
13	10	7	14	8	10	12	12	8	6	0.678686	0.9800	NonOverlappingTemplate
5	7	10	12	7	11	16	9	15	8	0.249284	1.0000	NonOverlappingTemplate
6	8	8	14	5	8	18	7	12	14	0.062821	0.9900	NonOverlappingTemplate
10	12	8	9	10	12	11	11	11	6	0.955835	0.9900	NonOverlappingTemplate
13	14	7	6	12	12	12	9	7	8	0.574903	1.0000	NonOverlappingTemplate
4	11	16	13	8	12	10	8	8	10	0.366918	1.0000	NonOverlappingTemplate
6	14	9	16	11	8	11	8	8	9	0.494392	0.9700	NonOverlappingTemplate
7	14	10	8	7	10	11	12	17	4	0.171867	0.9800	NonOverlappingTemplate
6	10	14	9	7	13	15	7	8	11	0.437274	0.9900	NonOverlappingTemplate
5	11	15	12	7	7	17	7	13	6	0.075719	1.0000	NonOverlappingTemplate
10	8	16	13	7	11	11	6	11	7	0.474986	1.0000	NonOverlappingTemplate
11	5	5	14	12	7	9	13	15	9	0.236810	0.9900	NonOverlappingTemplate
10	10	13	10	6	7	14	4	15	11	0.262249	0.9800	NonOverlappingTemplate
8	15	10	13	4	5	12	7	13	13	0.162606	1.0000	NonOverlappingTemplate
6	12	11	11	13	10	10	12	9	6	0.816537	0.9900	NonOverlappingTemplate
11	7	7	15	4	6	18	13	12	7	0.032923	0.9700	NonOverlappingTemplate
7	11	11	11	14	12	6	7	10	11	0.759756	1.0000	NonOverlappingTemplate
9	9	7	10	14	15	7	15	6	8	0.304126	0.9900	NonOverlappingTemplate
12	8	11	10	8	9	14	5	10	13	0.699313	0.9700	NonOverlappingTemplate
12	9	9	8	12	9	7	15	9	10	0.834308	0.9900	NonOverlappingTemplate
11	9	8	9	5	10	12	12	10	14	0.779188	0.9900	NonOverlappingTemplate
12	12	8	10	4	10	9	10	14	11	0.678686	0.9900	NonOverlappingTemplate
17	4	11	8	11	10	9	11	12	7	0.304126	0.9900	NonOverlappingTemplate
11	14	12	11	6	13	7	7	9	10	0.678686	0.9900	NonOverlappingTemplate
12	4	14	14	9	4	12	13	9	9	0.191687	0.9900	NonOverlappingTemplate
14	10	9	13	7	10	13	6	4	14	0.262249	0.9900	NonOverlappingTemplate
15	4	9	13	11	6	7	10	12	13	0.275709	0.9900	NonOverlappingTemplate
13	12	7	12	7	11	12	13	8	5	0.554420	0.9800	NonOverlappingTemplate
9	13	11	14	5	9	6	12	12	9	0.554420	1.0000	NonOverlappingTemplate
12	8	6	13	9	10	13	12	11	6	0.699313	0.9800	NonOverlappingTemplate
8	14	5	10	14	5	6	17	12	9	0.075719	0.9900	NonOverlappingTemplate
9	12	13	7	8	11	8	10	12	10	0.935716	0.9800	NonOverlappingTemplate
14	10	6	17	10	10	9	9	5	10	0.289667	1.0000	NonOverlappingTemplate
14	12	11	9	11	7	8	10	8	10	0.911413	0.9900	NonOverlappingTemplate
5	8	12	4	17	8	14	13	6	13	0.045675	1.0000	NonOverlappingTemplate
15	12	13	8	11	8	10	9	6	8	0.657933	0.9900	NonOverlappingTemplate
10	12	17	6	9	6	8	10	14	8	0.275709	0.9900	NonOverlappingTemplate
10	12	6	11	8	11	12	13	7	10	0.851383	0.9800	NonOverlappingTemplate
6	8	17	8	10	10	12	10	12	7	0.437274	0.9900	NonOverlappingTemplate
17	9	11	10	10	9	10	11	5	8	0.514124	0.9900	NonOverlappingTemplate
10	10	11	8	9	10	12	9	11	10	0.998821	0.9700	NonOverlappingTemplate
6	6	9	14	13	7	11	10	16	8	0.289667	0.9700	NonOverlappingTemplate
4	11	7	13	9	17	8	11	9	11	0.262249	0.9900	NonOverlappingTemplate
8	13	20	10	11	8	8	10	6	6	0.080519	0.9900	NonOverlappingTemplate
15	6	7	8	10	13	8	11	10	12	0.616305	0.9800	NonOverlappingTemplate
8	15	4	13	3	10	7	13	10	17	0.025193	1.0000	NonOverlappingTemplate
9	7	10	4	10	10	15	10	16	9	0.289667	0.9900	NonOverlappingTemplate
10	13	13	6	5	15	8	12	5	13	0.181557	0.9600	NonOverlappingTemplate
5	8	9	10	11	16	12	9	10	10	0.616305	1.0000	NonOverlappingTemplate
10	13	11	4	9	11	15	9	10	8	0.554420	0.9900	NonOverlappingTemplate

```
 15   9  14   6   9  13  10   6   8  10  0.455937   0.9900    NonOverlappingTemplate
 11  13  11  10   8   9  12  16   3   7  0.249284   0.9900    NonOverlappingTemplate
  8  15  14   8   6   8   6  10  10  15  0.275709   0.9900    NonOverlappingTemplate
 10  10   8   8  14   9   8   9  10  14  0.867692   0.9900    NonOverlappingTemplate
 18   5  10  12  13   7  10   8   8   9  0.213309   0.9500 *  NonOverlappingTemplate
  6  13  10  10   9  17   6  13  10   6  0.236810   1.0000    NonOverlappingTemplate
  9   8  12   7  12  11  11   9  11  10  0.978072   0.9900    NonOverlappingTemplate
 11  11   9  12   8   9  11  13   9   7  0.955835   0.9900    NonOverlappingTemplate
  8  13   7   9   7  12  14   9   9  12  0.759756   0.9800    NonOverlappingTemplate
 10   6  11  12   9  17   4  13   8  10  0.213309   1.0000    NonOverlappingTemplate
  5   7   7   8   9  15  15  11   9  14  0.236810   1.0000    NonOverlappingTemplate
  7   6  15   7   7  11  11   8  11  17  0.191687   1.0000    NonOverlappingTemplate
 10   8   9  10  12   7  10  12  17   5  0.383827   1.0000    NonOverlappingTemplate
 20   8   8  12   5   9   7  13   9   9  0.071177   0.9600    NonOverlappingTemplate
 12   7  10   6   6   9  15  13  14   8  0.350485   0.9700    NonOverlappingTemplate
  9   7  14  12   7   8  15   7   6  15  0.224821   1.0000    NonOverlappingTemplate
 11  11   9   5  13  10  12  12   5  12  0.595549   1.0000    NonOverlappingTemplate
 11   9   7  11   9   8  11   9   9  16  0.779188   0.9800    NonOverlappingTemplate
 13   8   7  11   8   9  12  12  10  10  0.935716   0.9900    NonOverlappingTemplate
 10  10  11   6  13   9   9  11  11  10  0.964295   0.9900    NonOverlappingTemplate
 10  10  11   5  17   9   7   9  11  11  0.455937   0.9900    NonOverlappingTemplate
  6  11   9  15   5  12   8   5  11  18  0.055361   1.0000    NonOverlappingTemplate
 12  12  11   9   9   9  11   7  11   9  0.983453   0.9900    NonOverlappingTemplate
  7   5  15   8   8  13  10  11  12  11  0.514124   0.9800    NonOverlappingTemplate
  4  15  17  10   7   7   8  12  13   7  0.080519   1.0000    NonOverlappingTemplate
  6   8  12   7  13  13   8  14  10   9  0.616305   0.9800    NonOverlappingTemplate
 11   9   6  13  11   4   5  15  14  12  0.145326   0.9800    NonOverlappingTemplate
  9  13  11  12   8   9  13  12   5   8  0.719747   0.9900    NonOverlappingTemplate
 12  10  11   8  12   9  12  11   9   6  0.935716   0.9800    NonOverlappingTemplate
  4  11  16  13   8  12  10   8   8  10  0.366918   1.0000    NonOverlappingTemplate
  9   9  10   7  10  16  10  14   8   7  0.574903   0.9900    OverlappingTemplate
 12  14  10   6  17   9  12   7   6   7  0.191687   0.9800    Universal
 11   8  12   4  12  10  11   9   9  14  0.657933   0.9700    ApproximateEntropy
  6   6   9   5   4   7  10   9   5   5  0.637119   1.0000    RandomExcursions
  7   5   3   3   9  10   8   3   9   9  0.178278   0.9848    RandomExcursions
  5   7   6   8   5  11  10   6   6   2  0.299251   1.0000    RandomExcursions
  7   6   8  10   4   7   4   7   8   5  0.739918   1.0000    RandomExcursions
  8   3   4   8  14   5   8   4   9   3  0.028181   1.0000    RandomExcursions
  6   8   4   8   7   7   5  10   6   5  0.804337   0.9848    RandomExcursions
  3   5  10   6   7   5   7   9   3  11  0.213309   0.9848    RandomExcursions
  8   8   7  11   5   7   5   3   3   9  0.299251   0.9697    RandomExcursions
  7  11   6   4   9   4   7   4   6   8  0.468595   1.0000    RandomExcursionsVariant
  9  11   1   6  12   7   7   2   3   8  0.012650   1.0000    RandomExcursionsVariant
  9   8   6   5   8  11   4   6   3   6  0.407091   1.0000    RandomExcursionsVariant
 15   3   4  10   5   7   6   5   5   6  0.025193   1.0000    RandomExcursionsVariant
 11   6   7   4   7   6   6   5   5   9  0.637119   0.9848    RandomExcursionsVariant
  7   6   4   9  10   4   5   9   4   8  0.468595   0.9848    RandomExcursionsVariant
  7   4   7   4   8  10   9  10   2   5  0.213309   0.9848    RandomExcursionsVariant
  7   5   4   6   8   9   4   7   7   9  0.772760   0.9848    RandomExcursionsVariant
  5   6   2   9  12   5   4   9   4  10  0.066882   0.9848    RandomExcursionsVariant
  4   3   8   5   8  10   8   7   7   6  0.602458   0.9848    RandomExcursionsVariant
  3   6   4   7   4  10  11   9   4   8  0.178278   1.0000    RandomExcursionsVariant
  6  10   5   9   7   4   5   6   5   9  0.637119   1.0000    RandomExcursionsVariant
 10   8   9   6   2   5   9   7   4   6  0.350485   1.0000    RandomExcursionsVariant
 12   7   4   4   6   8   9   4   5   7  0.299251   1.0000    RandomExcursionsVariant
 12   8   5   2   8   6   3   6   7   9  0.148094   0.9848    RandomExcursionsVariant
  9  11   2   7   3   4   6  10   7   7  0.134686   1.0000    RandomExcursionsVariant
  8  10   5   5   5   4   6   7  10   6  0.602458   1.0000    RandomExcursionsVariant
  7   9   4   6  11   6   4   4   6   9  0.407091   1.0000    RandomExcursionsVariant
  9   6  16  11   5   7  16   8   8  14  0.096578   1.0000    Serial
  8   8  13   8  15  11   8  11  10   8  0.779188   0.9900    Serial
  9  11   7  12  11   3  11  12  17   7  0.171867   0.9900    LinearComplexity
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
The minimum pass rate for each statistical test with the exception of the
random excursion (variant) test is approximately = 0.960150 for a
sample size = 100 binary sequences.
The minimum pass rate for the random excursion (variant) test
is approximately 0.953258 for a sample size = 66 binary sequences.
For further guidelines construct a probability table using the MAPLE program
provided in the addendum section of the documentation.- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
```

Результати тестування модифікованого матричного перетворення невипадкової монотонно зростаючої послідовності з циклом повторення 256 байти

```
------------------------------------------------------------------------------
RESULTS FOR THE UNIFORMITY OF P-VALUES AND THE PROPORTION OF PASSING SEQUENCES
------------------------------------------------------------------------------
  generator is <V_My_256.bin>
------------------------------------------------------------------------------
 C1  C2  C3  C4  C5  C6  C7  C8  C9 C10  P-VALUE  PROPORTION  STATISTICAL TEST
------------------------------------------------------------------------------
 10  10  12   7  11   7  10  15   9   9 0.834308   1.0000    Frequency
 12  12   7   9   9  14   5  13   8  11 0.595549   1.0000    BlockFrequency
 10   7  12   7  14   9   9  12  11   9 0.867692   0.9800    CumulativeSums
 11   6  10  11   9   7  12  11  10  13 0.897763   1.0000    CumulativeSums
 10  12  13  15  11   9  10   5   6   9 0.514124   0.9900    Runs
  9   9  12  14  10  10   7  10  11   8 0.935716   1.0000    LongestRun
  6  11   7   9   9   8  13   6  14  17 0.202268   1.0000    Rank
  1  11   8   9   6  18   6  15  14  12 0.006661   1.0000    FFT
 15   8  15  10   9   7  16   7  10   3 0.071177   0.9800    NonOverlappingTemplate
 10  12   7   8  14  14  11   7  11   6 0.574903   1.0000    NonOverlappingTemplate
  4   9  12  11  17   6  12   8  12   9 0.213309   1.0000    NonOverlappingTemplate
 11  17   7   6  11  10   8   7  12  11 0.401199   0.9600    NonOverlappingTemplate
  8   8   9   9   9  10   9  16  12  10 0.816537   0.9800    NonOverlappingTemplate
 10  10  11   7   5  11  11  10  12  13 0.834308   0.9900    NonOverlappingTemplate
 12   7   6  10  10  13  12   8  10  12 0.834308   0.9900    NonOverlappingTemplate
  9  17  11  11   7   9  11   8   4  13 0.262249   0.9900    NonOverlappingTemplate
 12  11  12   9   7  14   4   9  15   7 0.304126   0.9900    NonOverlappingTemplate
  9   9  11  10   7   9  12  13  11   9 0.971699   1.0000    NonOverlappingTemplate
  9  10   9  10  13   6  14  11  10   8 0.851383   0.9900    NonOverlappingTemplate
  8  14   5  10   3  10  12  16  11  11 0.137282   1.0000    NonOverlappingTemplate
  4  11  15  11  13  13  12   8   6   7 0.249284   0.9900    NonOverlappingTemplate
 12   8   8  11  10  10  10   5   8  18 0.304126   0.9900    NonOverlappingTemplate
 12   8   8   8   7  16  13   9  15   4 0.153763   0.9900    NonOverlappingTemplate
  5  10  10  12   7  14  12  12  12   6 0.514124   0.9900    NonOverlappingTemplate
 10  13  10   9   8  12  12  13   6   7 0.779188   0.9700    NonOverlappingTemplate
 10   8  13  11  14  11  11   5   7  10 0.678686   0.9700    NonOverlappingTemplate
 10  12   9   6   9  11  11  11  17   4 0.275709   1.0000    NonOverlappingTemplate
  9  11   7   7  15   7  13   5  15  11 0.249284   1.0000    NonOverlappingTemplate
 14   9   8  10  11  14   9   6  10   9 0.779188   1.0000    NonOverlappingTemplate
 13  10  10  13   6   5  10  14  11   8 0.534146   0.9900    NonOverlappingTemplate
  8  14   9  10   9   9  14   7  13   7 0.678686   1.0000    NonOverlappingTemplate
 11  10  15  11  12   9  10   5   9   8 0.719747   0.9900    NonOverlappingTemplate
 10   9  11   8  14   7  11   9  11  10 0.946308   0.9800    NonOverlappingTemplate
 11  10   3  10  11   6  12  13  12  12 0.455937   0.9900    NonOverlappingTemplate
 12   4  13   7   9  13  11  10  11  10 0.637119   1.0000    NonOverlappingTemplate
  7  15   9  10  12   6  14   9   9   9 0.595549   0.9900    NonOverlappingTemplate
 10   9   8  17   6  12   8  13  11   6 0.319084   0.9900    NonOverlappingTemplate
 12   7  10  11  15  10   9   4  13   9 0.474986   0.9700    NonOverlappingTemplate
  5  16   8  12  12   8  12   9  11   7 0.419021   0.9700    NonOverlappingTemplate
 10  11  13  15   8   7   5  13   9   9 0.494392   0.9800    NonOverlappingTemplate
  7   9   8   5  11  10  10  13  16  11 0.474986   0.9900    NonOverlappingTemplate
  7  12  11  13   6  14  11   5  10  11 0.514124   0.9700    NonOverlappingTemplate
 10   9   5  14  10  15  11  10   7   9 0.554420   0.9900    NonOverlappingTemplate
 10  13  10  11  12   6  10   6   8  14 0.678686   0.9800    NonOverlappingTemplate
 10   9   6  15  12   6  10  11  12   9 0.657933   1.0000    NonOverlappingTemplate
 15   9   9   8   9   8  11  10  10  11 0.924076   1.0000    NonOverlappingTemplate
  8   8   7  14   9  10  13  11  12   8 0.816537   0.9700    NonOverlappingTemplate
 15  10   6  12   3  14  12  12  10   6 0.145326   0.9700    NonOverlappingTemplate
 12   6  10   8   8   5  11  14  17   9 0.213309   0.9900    NonOverlappingTemplate
  9  14   7   8  11   6  10  15  11   9 0.595549   0.9900    NonOverlappingTemplate
 13   3  11   8  14   9   9   9  12  12 0.437274   0.9900    NonOverlappingTemplate
 14   8   7  15  13  11   8   9   4  11 0.304126   1.0000    NonOverlappingTemplate
  9   9   7   9  15  12  13   5  14   7 0.350485   0.9900    NonOverlappingTemplate
  5   6   6  12  16  11   8  21   8   7 0.004981   1.0000    NonOverlappingTemplate
 10  13   9   9  14  10  14   3   8  10 0.383827   0.9700    NonOverlappingTemplate
 13   9   3   9  14  17   9  10   9   7 0.137282   0.9900    NonOverlappingTemplate
```

7	12	13	15	7	15	7	7	10	7	0.289667	1.0000	NonOverlappingTemplate
10	13	10	11	5	8	15	15	10	3	0.129620	1.0000	NonOverlappingTemplate
10	10	7	9	14	6	14	10	9	11	0.739918	0.9800	NonOverlappingTemplate
5	8	10	15	12	7	12	17	7	7	0.129620	1.0000	NonOverlappingTemplate
7	8	14	6	8	13	12	7	12	13	0.494392	1.0000	NonOverlappingTemplate
14	13	13	6	2	11	12	7	12	10	0.153763	1.0000	NonOverlappingTemplate
7	18	8	8	11	14	10	7	9	8	0.262249	0.9900	NonOverlappingTemplate
2	12	13	9	9	11	15	8	12	9	0.249284	0.9900	NonOverlappingTemplate
3	6	12	12	19	13	11	8	6	10	0.030806	1.0000	NonOverlappingTemplate
9	10	19	9	8	7	9	12	10	7	0.275709	0.9800	NonOverlappingTemplate
12	10	12	10	10	14	4	7	7	14	0.401199	0.9900	NonOverlappingTemplate
8	10	12	9	5	11	12	12	10	11	0.883171	0.9800	NonOverlappingTemplate
12	5	9	11	8	8	8	10	15	14	0.494392	0.9800	NonOverlappingTemplate
10	14	11	14	7	8	10	7	12	7	0.657933	1.0000	NonOverlappingTemplate
13	8	12	12	4	9	10	11	11	10	0.739918	0.9800	NonOverlappingTemplate
16	8	11	7	9	9	14	4	14	8	0.191687	0.9700	NonOverlappingTemplate
9	8	10	8	11	9	13	7	17	8	0.514124	0.9900	NonOverlappingTemplate
11	11	11	12	11	11	6	9	8	10	0.964295	0.9900	NonOverlappingTemplate
10	4	8	12	11	9	9	13	8	16	0.383827	0.9900	NonOverlappingTemplate
12	5	9	5	14	7	16	10	11	11	0.224821	0.9900	NonOverlappingTemplate
6	7	7	8	16	9	13	14	9	11	0.334538	1.0000	NonOverlappingTemplate
10	12	7	13	9	8	11	12	13	5	0.678686	0.9900	NonOverlappingTemplate
9	14	9	14	8	10	8	10	11	7	0.816537	1.0000	NonOverlappingTemplate
12	10	7	11	11	6	6	11	17	9	0.366918	0.9900	NonOverlappingTemplate
10	7	9	13	9	11	11	12	12	6	0.867692	1.0000	NonOverlappingTemplate
7	13	5	14	11	14	13	5	10	8	0.249284	1.0000	NonOverlappingTemplate
15	8	15	10	9	7	16	7	10	3	0.071177	0.9800	NonOverlappingTemplate
5	14	7	12	13	16	5	9	13	6	0.090936	0.9900	NonOverlappingTemplate
6	10	9	8	14	14	3	9	15	12	0.153763	0.9900	NonOverlappingTemplate
8	10	8	11	10	12	14	9	5	13	0.699313	0.9900	NonOverlappingTemplate
12	8	8	12	14	7	13	7	9	10	0.739918	0.9900	NonOverlappingTemplate
7	10	6	11	14	9	10	10	12	11	0.851383	1.0000	NonOverlappingTemplate
14	9	14	6	9	11	14	8	8	7	0.494392	1.0000	NonOverlappingTemplate
11	9	5	8	13	10	11	12	10	11	0.867692	1.0000	NonOverlappingTemplate
10	5	15	15	4	15	10	11	10	5	0.062821	1.0000	NonOverlappingTemplate
9	18	15	7	8	7	3	8	10	15	0.025193	0.9800	NonOverlappingTemplate
14	10	10	5	15	6	8	10	9	13	0.383827	0.9800	NonOverlappingTemplate
17	14	7	8	17	12	3	6	6	10	0.011791	0.9600	NonOverlappingTemplate
13	9	12	16	13	10	8	7	6	6	0.319084	0.9900	NonOverlappingTemplate
8	9	9	12	13	9	6	17	8	9	0.437274	0.9900	NonOverlappingTemplate
14	7	14	7	9	6	8	8	17	10	0.191687	0.9800	NonOverlappingTemplate
11	9	13	11	7	11	8	13	8	9	0.911413	1.0000	NonOverlappingTemplate
11	8	5	9	12	12	9	17	10	7	0.366918	1.0000	NonOverlappingTemplate
11	9	6	14	9	15	6	14	6	10	0.289667	0.9900	NonOverlappingTemplate
7	13	12	10	7	13	7	5	14	12	0.401199	1.0000	NonOverlappingTemplate
11	13	13	12	11	10	7	7	8	8	0.834308	0.9900	NonOverlappingTemplate
9	13	6	12	6	13	11	6	12	12	0.534146	0.9800	NonOverlappingTemplate
8	10	9	6	12	17	9	13	9	7	0.401199	0.9800	NonOverlappingTemplate
14	7	14	7	12	10	11	8	6	11	0.574903	0.9900	NonOverlappingTemplate
8	6	12	15	13	9	11	10	7	9	0.637119	1.0000	NonOverlappingTemplate
7	10	7	14	12	12	4	11	9	14	0.383827	1.0000	NonOverlappingTemplate
11	14	8	11	4	12	10	9	15	6	0.319084	0.9800	NonOverlappingTemplate
9	13	7	8	16	8	7	6	14	12	0.289667	0.9900	NonOverlappingTemplate
12	6	12	11	3	11	14	13	9	9	0.334538	0.9900	NonOverlappingTemplate
16	10	9	18	10	8	10	8	5	6	0.090936	1.0000	NonOverlappingTemplate
8	7	7	16	9	12	10	9	13	9	0.595549	0.9900	NonOverlappingTemplate
8	9	11	11	11	11	12	11	9	7	0.983453	0.9900	NonOverlappingTemplate
8	7	12	15	10	9	11	11	11	6	0.719747	0.9800	NonOverlappingTemplate
10	9	5	8	8	23	9	10	12	6	0.007694	0.9900	NonOverlappingTemplate
13	5	9	8	12	11	7	8	13	14	0.514124	0.9800	NonOverlappingTemplate
11	10	8	10	7	9	13	12	14	6	0.739918	0.9900	NonOverlappingTemplate
19	11	4	10	14	9	8	9	9	7	0.090936	0.9900	NonOverlappingTemplate
9	14	12	14	4	9	10	4	13	11	0.213309	0.9900	NonOverlappingTemplate
14	6	9	8	11	15	7	13	10	7	0.437274	0.9700	NonOverlappingTemplate
9	16	12	10	9	8	14	7	4	11	0.289667	0.9900	NonOverlappingTemplate
10	5	13	9	10	11	6	12	9	15	0.514124	1.0000	NonOverlappingTemplate
10	9	17	10	11	10	9	7	7	10	0.637119	1.0000	NonOverlappingTemplate
9	7	9	13	10	8	10	15	9	10	0.834308	0.9800	NonOverlappingTemplate
16	7	9	10	8	7	13	9	10	11	0.637119	0.9700	NonOverlappingTemplate
5	11	9	11	11	12	13	11	6	11	0.739918	0.9900	NonOverlappingTemplate

```
 12   7  20   7   6   6   8  13  11  10  0.051942   0.9800    NonOverlappingTemplate
  4  11  11  11  10  11  13  11   6  12  0.637119   1.0000    NonOverlappingTemplate
  9  11  11   6  19   5   9  10  10  10  0.181557   0.9900    NonOverlappingTemplate
  9  12  11  12   7   8   5  14  15   7  0.366918   0.9900    NonOverlappingTemplate
 12   9   9  12  17  10   8   8   6   9  0.494392   0.9800    NonOverlappingTemplate
  9   6  12  13   9  12   6   9  10  14  0.657933   1.0000    NonOverlappingTemplate
 11   8  11   5  12  10  17   7   6  13  0.224821   0.9800    NonOverlappingTemplate
  9  12  13   8   8  10   8  12   8  12  0.924076   0.9900    NonOverlappingTemplate
  9  10  14   9  12   7  13   9   6  11  0.759756   1.0000    NonOverlappingTemplate
 14  14   5  10  13   4  11  13   6  10  0.171867   1.0000    NonOverlappingTemplate
 10   9   8  12  12  11   6  18   8   6  0.249284   0.9900    NonOverlappingTemplate
 11  12  10  12  13   6  11   7   5  13  0.554420   0.9900    NonOverlappingTemplate
 16  11   8   6   6  16   6   8  14   9  0.102526   1.0000    NonOverlappingTemplate
 10  15  11  10   7   9   7   9  11  11  0.851383   1.0000    NonOverlappingTemplate
 11  15   9   7  10   9  13  10  10   6  0.719747   0.9900    NonOverlappingTemplate
 10   9   9   6  10  12  16  13   6   9  0.494392   1.0000    NonOverlappingTemplate
  8   8   9  20   7  11   4   8  14  11  0.040108   1.0000    NonOverlappingTemplate
  5   8   9  14  12  15   7  13   9   8  0.366918   0.9800    NonOverlappingTemplate
 13   8   7  12  10  11   5  10  11  13  0.719747   1.0000    NonOverlappingTemplate
 12   7  14   7  12  11   6  12   8  11  0.657933   0.9900    NonOverlappingTemplate
  9  11  12  11  11   7  10   8   8  13  0.946308   1.0000    NonOverlappingTemplate
 10   9   6  11  10   9  15  13   8   9  0.759756   0.9900    NonOverlappingTemplate
  9   8  10  10  10   9  13  13   8  10  0.971699   1.0000    NonOverlappingTemplate
  7   9  12  10  11   5   9  16  10  11  0.554420   0.9700    NonOverlappingTemplate
 12   5  13   6  13  11  10   5  14  11  0.304126   0.9900    NonOverlappingTemplate
  6  13  10   6  10   7  13  11  12  12  0.657933   1.0000    NonOverlappingTemplate
 12   7  10  10   9  13   4  15  12   8  0.419021   1.0000    NonOverlappingTemplate
 14  10   9  14   6   9  14   8   7   9  0.534146   0.9900    NonOverlappingTemplate
  7   8  11   9  10   9  14  10  11  11  0.946308   0.9900    NonOverlappingTemplate
  7  13   5  14  11  14  13   5  10   8  0.249284   1.0000    NonOverlappingTemplate
 12  12   8  11   6  14  10   6  11  10  0.719747   1.0000    OverlappingTemplate
  8   6   9  12  13   8   7  10  14  13  0.616305   0.9700    Universal
 17  11   7   8   8   4  12  15  10   8  0.137282   0.9900    ApproximateEntropy
  4   9   4   6  16   2  10   4   5   4  0.001801   1.0000    RandomExcursions
  7   9   8   4   6   5   5   6  10   4  0.671779   0.9688    RandomExcursions
  8  11   8   9   5   4   4   3   8   4  0.253551   1.0000    RandomExcursions
 10   5   7   8   1  11   8   3   6   5  0.110952   0.9844    RandomExcursions
  8   4   8   7   4   6   5  10   5   7  0.739918   0.9844    RandomExcursions
  5  14   8   2   6   6   6   8   6   3  0.060239   1.0000    RandomExcursions
  7   7  11   4   5   5   5   7   8   5  0.671779   0.9844    RandomExcursions
  7   6   3   7   9   8   4   6   7   7  0.834308   1.0000    RandomExcursions
  4   6   5   6   5  12   6   4   8   8  0.437274   1.0000    RandomExcursionsVariant
  7   4   7   2   5  13   4   8   9   5  0.090936   1.0000    RandomExcursionsVariant
  5   8   3   4   8  13   1   8   8   6  0.043745   1.0000    RandomExcursionsVariant
  3  11   1   9   9   8   5   8   8   2  0.039244   1.0000    RandomExcursionsVariant
  2   8   7  10   9   7   4   3   8   6  0.299251   1.0000    RandomExcursionsVariant
  0   5  11  10   6   7   6   7   4   8  0.100508   1.0000    RandomExcursionsVariant
  2   4   6  10   7   7  11   4   6   7  0.253551   1.0000    RandomExcursionsVariant
  3   7   9   5   9   7   5   8   7   4  0.671779   0.9844    RandomExcursionsVariant
 10   4  12   9   2   6   6   8   3   4  0.060239   0.9844    RandomExcursionsVariant
  9   6   7   5   8   6   5   4   8   6  0.911413   0.9844    RandomExcursionsVariant
  6   7   4   9   6   4   8   6   5   9  0.804337   0.9844    RandomExcursionsVariant
  5   4   6   9   6   7   6   8   6   7  0.949602   0.9844    RandomExcursionsVariant
  3  10   3   7   9   8   5   5   6   8  0.437274   0.9844    RandomExcursionsVariant
  5   5   4  10   5   6   6   5   8  10  0.602458   0.9844    RandomExcursionsVariant
  5   3   6   7   5   7   7   6   6  12  0.500934   0.9844    RandomExcursionsVariant
  5   4   3   7   9   6  10   6   8   6  0.602458   0.9844    RandomExcursionsVariant
  4   3   7   4  13   6   7   5   6   9  0.162606   0.9844    RandomExcursionsVariant
  3   6   4   7   9   7   7   4   7  10  0.568055   0.9844    RandomExcursionsVariant
 11  13  14  12   9  10   7   8   4  12  0.494392   0.9800    Serial
  8  13  11  14   7   8   9  12   9   9  0.834308   0.9800    Serial
 10   7  11  15  12   9  13   8  10   5  0.554420   1.0000    LinearComplexity
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
The minimum pass rate for each statistical test with the exception of the
random excursion (variant) test is approximately = 0.960150 for a
sample size = 100 binary sequences.
The minimum pass rate for the random excursion (variant) test
is approximately 0.952688 for a sample size = 64 binary sequences.
For further guidelines construct a probability table using the MAPLE program
provided in the addendum section of the documentation.- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
```

Результати тестування матричного перетворення константи зі значенням 150

RESULTS FOR THE UNIFORMITY OF P-VALUES AND THE PROPORTION OF PASSING SEQUENCES
---
generator is <V_MP_150.bin>

C1 C2 C3 C4 C5 C6 C7 C8 C9 C10 P-VALUE PROPORTION STATISTICAL TEST
---
9 7 13 8 14 7 13 14 9 6 0.437274 0.9800 Frequency
10 10 8 12 10 15 9 9 6 11 0.816537 0.9800 BlockFrequency
9 5 14 12 9 7 11 14 12 7 0.474986 0.9800 CumulativeSums
12 5 12 4 14 11 5 14 12 11 0.153763 0.9800 CumulativeSums
11 14 11 5 11 12 12 6 6 12 0.455937 1.0000 Runs
13 10 13 12 4 10 8 6 10 14 0.401199 1.0000 LongestRun
13 12 13 5 7 8 15 9 6 12 0.304126 0.9800 Rank
3 4 6 13 9 12 10 13 22 8 0.001296 1.0000 FFT
13 5 21 5 5 10 9 12 9 11 0.011791 0.9800 NonOverlappingTemplate
15 13 12 10 12 7 9 9 7 6 0.554420 0.9900 NonOverlappingTemplate
10 9 12 12 9 8 14 10 8 8 0.924076 1.0000 NonOverlappingTemplate
8 11 8 8 16 11 14 9 6 9 0.494392 0.9900 NonOverlappingTemplate
14 9 9 9 14 4 5 11 11 14 0.249284 0.9800 NonOverlappingTemplate
9 9 14 9 8 10 12 15 5 9 0.554420 0.9900 NonOverlappingTemplate
8 13 8 5 14 12 12 5 8 15 0.213309 0.9700 NonOverlappingTemplate
12 8 9 9 11 6 9 14 11 11 0.867692 0.9700 NonOverlappingTemplate
10 14 10 11 8 9 5 11 11 11 0.834308 0.9800 NonOverlappingTemplate
10 12 8 15 11 12 9 7 8 8 0.779188 1.0000 NonOverlappingTemplate
11 14 6 12 12 12 6 9 7 11 0.616305 1.0000 NonOverlappingTemplate
10 13 8 10 8 14 9 9 7 12 0.851383 0.9900 NonOverlappingTemplate
14 11 11 8 12 10 8 8 11 7 0.883171 1.0000 NonOverlappingTemplate
11 12 5 11 13 9 13 13 7 6 0.494392 0.9900 NonOverlappingTemplate
14 7 9 12 5 6 15 11 5 16 0.071177 0.9700 NonOverlappingTemplate
13 8 15 8 8 8 14 7 12 7 0.455937 1.0000 NonOverlappingTemplate
16 13 10 11 5 10 10 7 4 14 0.153763 0.9800 NonOverlappingTemplate
13 6 12 10 10 14 10 8 9 8 0.798139 0.9900 NonOverlappingTemplate
14 10 5 7 13 12 16 9 8 6 0.213309 0.9800 NonOverlappingTemplate
4 15 9 10 9 13 10 13 12 5 0.275709 0.9900 NonOverlappingTemplate
10 7 10 14 14 12 8 8 6 11 0.637119 0.9800 NonOverlappingTemplate
4 11 12 12 11 12 12 10 8 8 0.719747 1.0000 NonOverlappingTemplate
15 11 9 9 12 10 9 6 9 10 0.834308 0.9900 NonOverlappingTemplate
13 6 9 13 15 3 11 10 7 13 0.171867 0.9800 NonOverlappingTemplate
11 8 14 10 8 7 12 10 12 8 0.867692 0.9900 NonOverlappingTemplate
10 9 8 14 18 6 6 11 7 11 0.171867 0.9900 NonOverlappingTemplate
6 8 11 11 10 11 9 8 16 10 0.699313 1.0000 NonOverlappingTemplate
20 10 8 12 13 8 9 3 8 9 0.040108 1.0000 NonOverlappingTemplate
5 9 2 13 10 12 15 15 10 9 0.080519 0.9900 NonOverlappingTemplate
9 10 15 12 6 11 6 12 9 10 0.657933 1.0000 NonOverlappingTemplate
14 10 7 9 5 7 12 9 12 15 0.401199 1.0000 NonOverlappingTemplate
13 12 8 16 8 13 9 7 6 8 0.383827 0.9800 NonOverlappingTemplate
5 10 17 10 10 10 10 8 11 9 0.534146 1.0000 NonOverlappingTemplate
6 6 12 13 8 11 8 16 14 6 0.202268 0.9900 NonOverlappingTemplate
12 15 11 7 11 10 10 6 8 10 0.739918 0.9700 NonOverlappingTemplate
10 7 6 14 7 14 9 14 9 10 0.494392 0.9900 NonOverlappingTemplate
7 9 11 10 11 9 6 16 12 9 0.637119 1.0000 NonOverlappingTemplate
9 7 8 12 14 9 10 12 13 6 0.699313 1.0000 NonOverlappingTemplate
5 10 14 10 7 11 6 7 14 16 0.171867 1.0000 NonOverlappingTemplate
9 10 15 9 14 9 10 9 9 6 0.719747 0.9900 NonOverlappingTemplate
6 10 6 14 13 8 11 8 12 12 0.595549 0.9900 NonOverlappingTemplate
16 13 6 13 4 9 8 12 7 12 0.171867 0.9800 NonOverlappingTemplate
8 11 8 11 15 10 14 9 8 6 0.616305 1.0000 NonOverlappingTemplate
13 7 13 9 7 3 13 14 10 11 0.262249 0.9900 NonOverlappingTemplate
14 9 9 11 10 8 11 12 7 9 0.924076 0.9800 NonOverlappingTemplate
12 13 10 6 10 14 13 5 8 9 0.494392 1.0000 NonOverlappingTemplate
6 11 13 11 12 8 11 10 11 7 0.867692 1.0000 NonOverlappingTemplate
10 11 11 8 13 9 12 9 4 13 0.678686 0.9900 NonOverlappingTemplate
12 10 6 10 15 9 9 11 9 9 0.834308 0.9900 NonOverlappingTemplate

7	11	8	11	7	10	11	10	16	9	0.719747	0.9900	NonOverlappingTemplate
13	9	8	9	10	7	10	8	13	13	0.867692	0.9900	NonOverlappingTemplate
6	13	10	16	5	14	9	11	10	6	0.213309	1.0000	NonOverlappingTemplate
14	9	10	3	9	9	13	9	12	12	0.474986	0.9900	NonOverlappingTemplate
10	14	9	4	11	10	11	7	12	12	0.616305	1.0000	NonOverlappingTemplate
15	12	11	6	8	7	13	8	9	11	0.595549	0.9800	NonOverlappingTemplate
9	10	7	14	12	12	10	9	8	9	0.911413	1.0000	NonOverlappingTemplate
18	10	9	10	9	10	7	11	7	9	0.474986	0.9800	NonOverlappingTemplate
12	7	7	11	8	9	13	13	12	8	0.798139	0.9700	NonOverlappingTemplate
11	16	9	12	10	10	10	7	9	6	0.657933	0.9700	NonOverlappingTemplate
10	14	7	11	11	8	10	12	8	9	0.911413	0.9900	NonOverlappingTemplate
7	14	8	15	7	13	10	3	12	11	0.181557	0.9900	NonOverlappingTemplate
12	19	10	8	5	13	7	8	11	7	0.102526	0.9900	NonOverlappingTemplate
10	14	12	13	6	11	8	8	10	8	0.759756	0.9800	NonOverlappingTemplate
9	13	10	7	14	8	10	10	3	16	0.191687	1.0000	NonOverlappingTemplate
11	15	4	7	15	13	10	10	6	9	0.202268	1.0000	NonOverlappingTemplate
7	14	13	10	11	9	8	9	9	10	0.897763	1.0000	NonOverlappingTemplate
6	13	8	11	13	9	12	8	6	14	0.534146	1.0000	NonOverlappingTemplate
12	15	9	9	12	7	9	11	7	9	0.779188	1.0000	NonOverlappingTemplate
13	11	14	13	11	8	4	3	12	11	0.162606	0.9800	NonOverlappingTemplate
8	12	12	6	11	10	9	13	11	8	0.883171	0.9800	NonOverlappingTemplate
10	6	8	14	14	8	10	11	9	10	0.759756	0.9900	NonOverlappingTemplate
6	8	12	8	15	9	8	8	7	19	0.085587	1.0000	NonOverlappingTemplate
14	10	13	12	7	8	13	6	8	9	0.616305	1.0000	NonOverlappingTemplate
13	11	6	10	13	12	11	8	10	6	0.739918	0.9900	NonOverlappingTemplate
13	5	21	5	5	10	9	12	9	11	0.011791	0.9800	NonOverlappingTemplate
7	11	9	11	6	12	4	17	9	14	0.145326	1.0000	NonOverlappingTemplate
10	8	13	9	13	11	8	11	8	9	0.946308	1.0000	NonOverlappingTemplate
13	12	13	10	7	8	10	14	10	3	0.350485	1.0000	NonOverlappingTemplate
17	15	14	9	4	13	4	5	9	10	0.019188	0.9900	NonOverlappingTemplate
10	4	16	9	6	13	13	10	10	9	0.289667	0.9800	NonOverlappingTemplate
12	12	12	9	6	11	8	14	7	9	0.739918	0.9900	NonOverlappingTemplate
5	15	13	4	10	15	9	11	9	9	0.191687	1.0000	NonOverlappingTemplate
7	5	16	7	12	12	11	11	9	10	0.437274	1.0000	NonOverlappingTemplate
9	4	8	13	10	11	8	10	16	11	0.419021	0.9900	NonOverlappingTemplate
17	11	6	9	8	9	7	8	10	15	0.275709	1.0000	NonOverlappingTemplate
7	8	12	13	6	10	7	13	13	11	0.637119	1.0000	NonOverlappingTemplate
10	7	9	9	11	13	10	9	11	11	0.983453	0.9900	NonOverlappingTemplate
9	9	9	11	10	11	8	9	12	12	0.994250	0.9900	NonOverlappingTemplate
13	9	5	5	13	9	13	14	11	8	0.350485	1.0000	NonOverlappingTemplate
14	12	9	7	9	11	4	17	12	5	0.102526	0.9900	NonOverlappingTemplate
3	10	14	10	8	17	10	13	6	9	0.108791	1.0000	NonOverlappingTemplate
7	10	12	15	9	12	13	8	7	7	0.595549	1.0000	NonOverlappingTemplate
14	4	10	10	12	9	14	7	10	10	0.514124	0.9700	NonOverlappingTemplate
9	6	14	11	14	8	8	9	9	12	0.699313	0.9800	NonOverlappingTemplate
10	10	16	10	6	10	6	11	12	9	0.595549	0.9900	NonOverlappingTemplate
7	8	10	11	10	6	10	14	11	13	0.779188	1.0000	NonOverlappingTemplate
7	11	12	8	12	9	9	12	9	11	0.964295	0.9900	NonOverlappingTemplate
15	9	8	7	9	8	9	13	9	13	0.699313	1.0000	NonOverlappingTemplate
8	14	11	7	9	9	12	15	9	6	0.554420	0.9800	NonOverlappingTemplate
7	13	10	5	18	12	8	14	7	6	0.075719	1.0000	NonOverlappingTemplate
6	7	11	11	9	7	14	8	16	11	0.401199	1.0000	NonOverlappingTemplate
8	12	13	10	11	11	7	10	13	5	0.719747	0.9800	NonOverlappingTemplate
13	9	16	9	7	8	12	11	6	9	0.514124	0.9700	NonOverlappingTemplate
9	8	9	12	11	9	12	10	6	14	0.851383	1.0000	NonOverlappingTemplate
9	7	13	10	12	12	9	7	11	10	0.924076	0.9900	NonOverlappingTemplate
11	10	7	9	6	14	15	11	8	9	0.595549	0.9800	NonOverlappingTemplate
9	8	8	15	7	9	13	13	8	10	0.678686	1.0000	NonOverlappingTemplate
7	11	17	9	9	7	13	4	8	15	0.108791	0.9900	NonOverlappingTemplate
11	12	7	13	12	14	4	6	16	5	0.075719	0.9800	NonOverlappingTemplate
14	14	7	11	10	10	10	7	10	7	0.739918	0.9800	NonOverlappingTemplate
10	6	9	11	15	11	12	5	8	13	0.474986	1.0000	NonOverlappingTemplate
8	14	14	10	7	13	9	4	12	9	0.383827	0.9900	NonOverlappingTemplate
13	8	5	13	12	11	11	7	13	7	0.534146	1.0000	NonOverlappingTemplate
12	11	8	13	4	11	9	6	11	15	0.366918	0.9700	NonOverlappingTemplate
7	10	12	13	4	12	8	10	13	11	0.574903	0.9900	NonOverlappingTemplate
11	12	10	11	13	5	12	8	11	7	0.759756	0.9900	NonOverlappingTemplate
8	13	12	10	8	10	7	12	7	13	0.816537	1.0000	NonOverlappingTemplate
10	17	8	8	8	10	6	10	12	11	0.514124	0.9900	NonOverlappingTemplate
9	8	9	14	9	12	12	10	12	5	0.739918	1.0000	NonOverlappingTemplate

```
 16  10  11   9   5  12  10   9  12   6 0.455937   0.9800    NonOverlappingTemplate
 10   7   9  11  11  13   5  13  15   6 0.383827   0.9900    NonOverlappingTemplate
 14   9   8  15   9  10  12   7  10   6 0.574903   0.9700    NonOverlappingTemplate
 15   7  13  10   4   9  11   9  15   7 0.236810   0.9800    NonOverlappingTemplate
  9  10  11   8  13   5   7   7  17  13 0.236810   0.9900    NonOverlappingTemplate
  9   9  10  12   8  13   9   5  15  10 0.637119   0.9800    NonOverlappingTemplate
 16   6  12  12  14  11   6   8   6   9 0.249284   0.9900    NonOverlappingTemplate
 11  12  11  13  10   9  11   6   9   8 0.924076   1.0000    NonOverlappingTemplate
 11   8  12   4   8   9  14  13   8  13 0.455937   0.9800    NonOverlappingTemplate
 10  12   5  12   8   5  17  15   7   9 0.102526   1.0000    NonOverlappingTemplate
 11   7   8   9  10  11  16  13   9   6 0.554420   0.9900    NonOverlappingTemplate
 10  10   8  16  11   9  13   9   3  11 0.334538   1.0000    NonOverlappingTemplate
 10   9   9  14   4  16   9  11  10   8 0.383827   0.9800    NonOverlappingTemplate
 10   9  18   8  11   6  13  10  10   5 0.213309   1.0000    NonOverlappingTemplate
  3  16   9  12   9  10   9   9  10  13 0.334538   0.9900    NonOverlappingTemplate
  8  16  12  14   4   7   9  13   6  11 0.153763   0.9900    NonOverlappingTemplate
  7   8  14   8   8  14  11   9  12   9 0.739918   0.9900    NonOverlappingTemplate
  9  11   9   7   5  10  13  12  11  13 0.739918   1.0000    NonOverlappingTemplate
  8  11   7  14   3  12  10  14  14   7 0.191687   0.9900    NonOverlappingTemplate
 11  13  14   4  10  10  10  11  10   7 0.616305   0.9900    NonOverlappingTemplate
  9   5   5   8  19  11  17  11   4  11 0.007694   0.9900    NonOverlappingTemplate
  9   7   7  15   9  13   9  12  17   2 0.045675   0.9800    NonOverlappingTemplate
 11  11   6  12   9   8   8  16  11   8 0.616305   0.9900    NonOverlappingTemplate
 10   4  11  10  10  14   8  16   8   9 0.366918   1.0000    NonOverlappingTemplate
  6  13   6  14  13   7   8  11   8  14 0.350485   0.9700    NonOverlappingTemplate
 10   4  13  15   9  12   9   9  12   7 0.437274   1.0000    NonOverlappingTemplate
  8   9  10   8  12  10   7   8  16  12 0.678686   1.0000    NonOverlappingTemplate
  8   8  14   5  13  10   7  13   9  13 0.474986   1.0000    NonOverlappingTemplate
 14  10   6  10  13  12  11   8  10   6 0.678686   0.9900    NonOverlappingTemplate
 18  13   8  12  16   8   4   5   9   7 0.023545   0.9800    OverlappingTemplate
 10  12  10  15  10   6   9  13   6   9 0.616305   1.0000    Universal
  8  12  19   6   9  10  11   7  12   6 0.137282   0.9900    ApproximateEntropy
  4   6   8   3   6   5   3   4   2  10 0.275709   1.0000    RandomExcursions
  4   4   4   8   4   8   4   6   4   5 0.834308   0.9804    RandomExcursions
  5   3   9   3   4   5   9   6   5   2 0.334538   1.0000    RandomExcursions
  8   2   3   9   4   4   7   3   9   2 0.102526   1.0000    RandomExcursions
  2   5   5   7   6   3   5   7   7   4 0.798139   1.0000    RandomExcursions
  5   5   2   3   7   7   4   5   9   4 0.554420   0.9804    RandomExcursions
  4   6   2   8   7   3  10   6   3   2 0.145326   1.0000    RandomExcursions
  6   3   4   8   4   3   8   7   6   2 0.474986   1.0000    RandomExcursions
  3   6   3   4   3   9   4   7   7   5 0.554420   1.0000    RandomExcursionsVariant
  5   5   4   4   7   1   5   9   8   3 0.334538   1.0000    RandomExcursionsVariant
  6   5   8   3   4   4   4   5   7   5 0.897763   1.0000    RandomExcursionsVariant
  6   4   6   6   1   9   4   3   3   9 0.202268   1.0000    RandomExcursionsVariant
  5   2   3   4  10   8   6   3   4   6 0.275709   1.0000    RandomExcursionsVariant
  3   5   5   3   5  10   2   1   9   8 0.055361   1.0000    RandomExcursionsVariant
  6   6   1   6   4   9   6   4   1   8 0.181557   1.0000    RandomExcursionsVariant
  6   7   3   0   9   7   4   5   6   4 0.249284   1.0000    RandomExcursionsVariant
  7   3   5   4   5   6   7   6   2   6 0.834308   1.0000    RandomExcursionsVariant
  4   7   4   8   4   6   3   5   5   5 0.897763   1.0000    RandomExcursionsVariant
  4   3   2   9   5   7   7   4   5   5 0.554420   1.0000    RandomExcursionsVariant
  4   4   4   9   4   9   6   4   3   4 0.474986   0.9804    RandomExcursionsVariant
  4   6   1   9  10   5   3   7   4   2 0.080519   1.0000    RandomExcursionsVariant
  4   6   3   9   3   3   6   6   5   6 0.678686   1.0000    RandomExcursionsVariant
  4   5   2   8   7   4   3   6   5   7 0.678686   1.0000    RandomExcursionsVariant
  5   3   5   3   5   4   9   5   8   4 0.637119   1.0000    RandomExcursionsVariant
  7   3   4   3   7   7   4   3   8   5 0.637119   0.9804    RandomExcursionsVariant
  5   6   3   6   5   6   6   5   4   5 0.994250   0.9804    RandomExcursionsVariant
 11  11  20   9   9   7   7   9   8   9 0.171867   1.0000    Serial
 13   9  11  11  13   9  12   9   5   8 0.779188   0.9900    Serial
 10  12   9   9   7  16  11  11   8   7 0.678686   0.9800    LinearComplexity
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
The minimum pass rate for each statistical test with the exception of the
random excursion (variant) test is approximately = 0.960150 for a
sample size = 100 binary sequences.
The minimum pass rate for the random excursion (variant) test
is approximately 0.948202 for a sample size = 51 binary sequences.
For further guidelines construct a probability table using the MAPLE program
provided in the addendum section of the documentation.- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
```

Результати тестування застосування операцій матричного перетворення над текстовою інформацією

RESULTS FOR THE UNIFORMITY OF P-VALUES AND THE PROPORTION OF PASSING SEQUENCES

generator is <V_M_TXT.bin>

C1	C2	C3	C4	C5	C6	C7	C8	C9	C10	P-VALUE	PROPORTION	STATISTICAL TEST
9	12	8	10	10	13	12	11	7	8	0.935716	1.0000	Frequency
15	4	10	11	9	11	14	5	8	13	0.224821	1.0000	BlockFrequency
7	10	8	15	13	11	4	8	13	11	0.366918	1.0000	CumulativeSums
10	12	9	10	9	13	7	10	10	10	0.983453	0.9900	CumulativeSums
14	5	9	12	19	10	6	9	5	11	0.048716	0.9900	Runs
11	13	9	11	8	8	10	12	9	9	0.978072	0.9800	LongestRun
8	10	9	7	13	11	12	13	12	5	0.678686	0.9900	Rank
1	10	6	11	8	7	16	14	12	15	0.023545	1.0000	FFT
9	11	11	10	10	7	12	12	8	10	0.983453	0.9800	NonOverlappingTemplate
9	14	5	11	10	9	6	7	14	15	0.275709	0.9900	NonOverlappingTemplate
8	13	8	9	12	11	13	9	8	9	0.924076	0.9800	NonOverlappingTemplate
12	11	11	8	7	12	9	8	11	11	0.964295	1.0000	NonOverlappingTemplate
15	8	11	6	8	12	10	12	7	11	0.657933	0.9900	NonOverlappingTemplate
12	12	15	9	10	6	5	14	7	10	0.350485	0.9700	NonOverlappingTemplate
17	11	6	15	6	4	4	12	13	12	0.020548	0.9900	NonOverlappingTemplate
13	16	6	5	12	4	16	9	9	10	0.058984	0.9900	NonOverlappingTemplate
9	10	15	9	14	7	8	8	10	10	0.739918	0.9900	NonOverlappingTemplate
8	11	9	11	6	11	8	15	12	9	0.759756	1.0000	NonOverlappingTemplate
8	9	13	14	9	8	13	8	9	9	0.834308	1.0000	NonOverlappingTemplate
7	9	11	12	10	11	7	16	8	9	0.678686	0.9800	NonOverlappingTemplate
11	6	12	13	10	11	7	7	10	13	0.759756	0.9700	NonOverlappingTemplate
8	9	10	10	14	6	12	13	8	10	0.798139	0.9900	NonOverlappingTemplate
8	13	11	10	17	7	9	3	16	6	0.042808	0.9800	NonOverlappingTemplate
11	9	12	10	10	10	5	11	13	9	0.897763	0.9800	NonOverlappingTemplate
6	10	8	15	8	9	13	11	12	8	0.657933	1.0000	NonOverlappingTemplate
11	13	11	12	8	3	7	16	13	6	0.129620	1.0000	NonOverlappingTemplate
7	6	9	9	9	13	7	16	11	13	0.419021	0.9900	NonOverlappingTemplate
7	12	10	11	7	12	12	6	13	10	0.779188	1.0000	NonOverlappingTemplate
7	10	12	18	4	13	12	8	6	10	0.102526	1.0000	NonOverlappingTemplate
9	14	9	9	11	9	12	7	9	11	0.935716	0.9800	NonOverlappingTemplate
7	13	9	8	5	11	10	9	17	11	0.350485	0.9900	NonOverlappingTemplate
11	12	10	13	8	12	8	8	6	12	0.834308	0.9900	NonOverlappingTemplate
9	7	6	12	8	16	7	14	12	9	0.350485	0.9800	NonOverlappingTemplate
10	8	10	8	5	9	10	13	8	19	0.171867	0.9800	NonOverlappingTemplate
11	9	9	7	8	9	15	7	13	12	0.699313	1.0000	NonOverlappingTemplate
7	11	19	9	12	7	9	8	9	9	0.262249	1.0000	NonOverlappingTemplate
8	7	9	13	7	10	7	14	10	15	0.514124	1.0000	NonOverlappingTemplate
9	10	13	9	9	12	7	14	11	6	0.759756	0.9700	NonOverlappingTemplate
11	10	12	8	8	7	13	14	12	5	0.574903	1.0000	NonOverlappingTemplate
9	7	9	6	17	11	10	9	7	15	0.262249	0.9900	NonOverlappingTemplate
9	12	5	6	11	12	14	9	12	10	0.616305	0.9900	NonOverlappingTemplate
9	15	8	9	10	10	11	8	11	9	0.924076	0.9900	NonOverlappingTemplate
7	13	7	5	11	12	10	15	11	9	0.494392	0.9800	NonOverlappingTemplate
8	8	11	14	8	6	11	12	11	11	0.816537	0.9900	NonOverlappingTemplate
12	12	7	8	10	10	9	11	10	11	0.983453	0.9900	NonOverlappingTemplate
7	6	17	9	7	11	8	14	12	9	0.275709	1.0000	NonOverlappingTemplate
8	15	11	6	11	7	10	13	9	10	0.678686	1.0000	NonOverlappingTemplate
10	13	8	15	10	7	10	12	3	12	0.319084	0.9900	NonOverlappingTemplate
10	10	12	11	7	8	9	12	12	9	0.971699	0.9900	NonOverlappingTemplate
5	10	8	8	11	14	12	3	15	14	0.108791	0.9800	NonOverlappingTemplate
13	13	4	16	10	11	8	8	6	11	0.236810	0.9800	NonOverlappingTemplate
14	11	10	7	16	8	9	6	12	7	0.383827	0.9800	NonOverlappingTemplate
14	5	9	9	8	17	8	7	13	10	0.224821	1.0000	NonOverlappingTemplate
13	8	6	12	7	6	9	15	11	13	0.401199	0.9900	NonOverlappingTemplate
9	6	11	10	8	10	10	10	10	16	0.759756	1.0000	NonOverlappingTemplate
12	6	7	14	7	15	11	7	10	11	0.437274	0.9700	NonOverlappingTemplate
8	12	13	10	16	2	14	9	9	7	0.108791	0.9800	NonOverlappingTemplate
4	14	9	10	5	8	14	17	10	9	0.096578	0.9900	NonOverlappingTemplate
12	14	13	8	8	10	10	10	10	5	0.719747	1.0000	NonOverlappingTemplate

10	15	11	17	6	9	8	12	6	6	0.153763	0.9800	NonOverlappingTemplate
13	8	12	12	7	13	14	8	5	8	0.455937	0.9800	NonOverlappingTemplate
8	8	11	13	12	7	15	6	10	10	0.616305	1.0000	NonOverlappingTemplate
8	9	9	6	11	15	10	11	10	11	0.834308	1.0000	NonOverlappingTemplate
14	14	7	6	13	13	5	8	5	15	0.080519	0.9900	NonOverlappingTemplate
8	12	10	9	9	13	5	11	10	13	0.798139	1.0000	NonOverlappingTemplate
9	12	5	10	10	14	13	8	10	9	0.739918	1.0000	NonOverlappingTemplate
9	8	15	11	10	10	11	8	7	11	0.867692	0.9900	NonOverlappingTemplate
10	9	11	17	6	8	7	7	14	11	0.304126	0.9900	NonOverlappingTemplate
11	6	12	14	7	12	13	5	10	10	0.494392	0.9800	NonOverlappingTemplate
14	10	12	8	6	12	8	8	11	11	0.798139	1.0000	NonOverlappingTemplate
5	13	8	7	10	12	12	10	10	13	0.699313	1.0000	NonOverlappingTemplate
19	5	10	11	8	6	13	14	5	9	0.037566	0.9600	NonOverlappingTemplate
5	10	8	9	10	13	12	10	10	13	0.816537	0.9800	NonOverlappingTemplate
10	10	8	11	11	13	14	9	5	9	0.759756	0.9900	NonOverlappingTemplate
9	12	9	14	7	10	8	10	13	8	0.851383	0.9800	NonOverlappingTemplate
6	12	5	9	12	14	10	9	10	13	0.574903	1.0000	NonOverlappingTemplate
9	6	14	11	9	8	8	17	10	8	0.383827	0.9700	NonOverlappingTemplate
14	11	10	10	11	11	5	13	9	6	0.637119	0.9900	NonOverlappingTemplate
10	11	13	11	8	10	9	11	8	9	0.987896	0.9900	NonOverlappingTemplate
12	10	6	12	10	6	12	12	7	13	0.678686	0.9600	NonOverlappingTemplate
5	15	14	11	6	14	10	9	4	12	0.122325	1.0000	NonOverlappingTemplate
9	12	13	11	12	9	7	11	8	8	0.924076	1.0000	NonOverlappingTemplate
9	11	10	11	10	7	12	12	8	10	0.983453	0.9800	NonOverlappingTemplate
13	12	10	9	11	8	8	14	11	4	0.574903	0.9900	NonOverlappingTemplate
10	9	10	8	13	11	8	10	8	13	0.955835	0.9900	NonOverlappingTemplate
10	13	11	10	8	13	3	10	10	12	0.574903	0.9900	NonOverlappingTemplate
11	9	11	11	14	4	8	8	12	12	0.616305	0.9800	NonOverlappingTemplate
8	14	10	7	9	9	13	9	14	7	0.678686	1.0000	NonOverlappingTemplate
11	5	12	12	9	10	11	7	14	9	0.719747	0.9700	NonOverlappingTemplate
6	13	16	10	14	10	7	6	8	10	0.304126	0.9900	NonOverlappingTemplate
13	11	13	9	9	9	4	9	10	13	0.657933	1.0000	NonOverlappingTemplate
17	16	8	8	8	9	7	9	4	14	0.066882	0.9900	NonOverlappingTemplate
15	4	14	9	11	11	6	10	9	11	0.366918	1.0000	NonOverlappingTemplate
10	10	14	6	9	13	7	14	6	11	0.494392	0.9900	NonOverlappingTemplate
18	11	8	12	9	6	10	14	2	10	0.048716	0.9700	NonOverlappingTemplate
12	9	8	8	15	12	6	11	12	7	0.616305	0.9800	NonOverlappingTemplate
12	8	8	10	6	19	8	6	12	11	0.145326	0.9800	NonOverlappingTemplate
9	10	15	9	9	6	7	10	12	13	0.678686	1.0000	NonOverlappingTemplate
8	4	11	14	16	12	7	13	6	9	0.153763	0.9800	NonOverlappingTemplate
12	8	9	17	9	9	7	5	14	10	0.275709	0.9800	NonOverlappingTemplate
7	10	16	10	10	7	10	7	8	15	0.419021	0.9900	NonOverlappingTemplate
7	8	14	13	11	13	5	14	9	6	0.304126	1.0000	NonOverlappingTemplate
9	16	8	7	8	12	12	6	13	9	0.455937	0.9900	NonOverlappingTemplate
12	9	5	14	7	9	13	9	15	7	0.350485	1.0000	NonOverlappingTemplate
9	12	12	9	8	11	10	7	12	10	0.971699	0.9900	NonOverlappingTemplate
11	11	8	7	11	12	10	5	10	15	0.637119	0.9800	NonOverlappingTemplate
6	5	8	14	9	12	10	17	7	12	0.171867	1.0000	NonOverlappingTemplate
17	13	7	9	3	2	17	12	4	16	0.000347	0.9800	NonOverlappingTemplate
14	3	9	10	12	8	11	15	9	9	0.334538	0.9800	NonOverlappingTemplate
14	8	7	7	13	9	11	11	8	12	0.759756	0.9700	NonOverlappingTemplate
7	14	7	12	8	8	12	14	10	8	0.637119	0.9900	NonOverlappingTemplate
10	10	3	17	17	6	14	5	8	10	0.013569	0.9800	NonOverlappingTemplate
8	13	9	14	8	8	8	11	11	10	0.883171	0.9900	NonOverlappingTemplate
7	9	18	7	8	13	9	9	12	8	0.304126	0.9900	NonOverlappingTemplate
17	5	14	6	12	12	12	6	8	8	0.115387	0.9600	NonOverlappingTemplate
12	9	10	12	15	11	8	10	4	9	0.574903	1.0000	NonOverlappingTemplate
3	12	10	11	15	9	12	9	12	7	0.366918	1.0000	NonOverlappingTemplate
15	6	8	12	12	9	8	14	8	8	0.514124	0.9600	NonOverlappingTemplate
10	8	14	6	8	9	12	13	8	12	0.719747	1.0000	NonOverlappingTemplate
10	9	16	8	9	12	5	11	12	8	0.534146	0.9900	NonOverlappingTemplate
11	5	10	11	12	5	9	11	11	15	0.494392	0.9900	NonOverlappingTemplate
9	14	11	13	8	11	13	6	8	7	0.637119	1.0000	NonOverlappingTemplate
10	9	8	8	11	10	9	21	9	5	0.071177	0.9900	NonOverlappingTemplate
12	10	8	5	15	6	11	10	11	12	0.534146	0.9900	NonOverlappingTemplate
10	9	10	7	14	7	10	7	11	15	0.637119	0.9900	NonOverlappingTemplate
11	13	13	6	13	9	10	7	10	8	0.759756	0.9900	NonOverlappingTemplate
9	11	12	6	8	12	10	13	6	13	0.699313	0.9900	NonOverlappingTemplate
11	11	9	11	8	9	16	11	6	8	0.678686	0.9900	NonOverlappingTemplate
14	5	12	7	11	8	14	9	8	12	0.494392	1.0000	NonOverlappingTemplate
7	13	8	16	15	5	8	10	10	8	0.236810	0.9900	NonOverlappingTemplate

```
 12  12   7   7   7  12  11  10  13   9  0.834308   0.9900    NonOverlappingTemplate
  7   8  11   4  16   9   9  14  14   8  0.191687   0.9900    NonOverlappingTemplate
  7  14   7   9  13  12   9  13   7   9  0.657933   1.0000    NonOverlappingTemplate
  5  10  11   9  14  15   8  10   8  10  0.574903   1.0000    NonOverlappingTemplate
  7  12  13  11   7   5  14   7   8  16  0.202268   1.0000    NonOverlappingTemplate
  8  14  12  12   7   7   8  11   8  13  0.699313   0.9800    NonOverlappingTemplate
  9   8   8   6  13  13  14  10   6  13  0.494392   0.9900    NonOverlappingTemplate
 11  14   8   7   8  14   9   7   8  14  0.534146   0.9900    NonOverlappingTemplate
 11   8   7   9  12   9  11  11   7  15  0.779188   0.9900    NonOverlappingTemplate
 10  12   5  10  12  10  18  10   8   5  0.181557   0.9900    NonOverlappingTemplate
 13   8   7   8   9  13  12   9   9  12  0.867692   0.9800    NonOverlappingTemplate
 12   8  10  11  13  14  11   4   6  11  0.455937   0.9800    NonOverlappingTemplate
 12  13  13   5  10  10  11   8   9   9  0.798139   1.0000    NonOverlappingTemplate
  8  12  15   7   6   6  10  13  12  11  0.455937   0.9900    NonOverlappingTemplate
  6  12   5  10  12  11   4  15  14  11  0.171867   1.0000    NonOverlappingTemplate
 13   9   8  11  11  10  13   6   7  12  0.798139   0.9900    NonOverlappingTemplate
 11   8  11   8  13  10  13  10   7   9  0.924076   0.9900    NonOverlappingTemplate
 11   3  13  13  12   6  11  12   7  12  0.304126   1.0000    NonOverlappingTemplate
  8  15  11   5  15  10  12   7   9   8  0.366918   0.9900    NonOverlappingTemplate
  9   8  11  16   7  13   8  10  10   8  0.657933   0.9900    NonOverlappingTemplate
  8  12  13  17   2   8  14   7  10   9  0.066882   0.9900    NonOverlappingTemplate
 11  15   8  11   9  11   9   6  10  10  0.834308   0.9800    NonOverlappingTemplate
 12  14  13   7   9   6  11  10   7  11  0.678686   0.9900    NonOverlappingTemplate
 14  15   7  15  15   9   3   8  10   4  0.025193   1.0000    NonOverlappingTemplate
  7  15  11   8   9  10  14   8   8  10  0.699313   1.0000    NonOverlappingTemplate
 10  11  12  12  12   9   7  11   8   8  0.955835   1.0000    NonOverlappingTemplate
  6   6  11  15  10   8  15   6  12  11  0.289667   0.9900    OverlappingTemplate
 11  10  13   8  10  12   6   9  12   9  0.911413   1.0000    Universal
 15  10  13  12   8   5   8  13   7   9  0.437274   1.0000    ApproximateEntropy
  9   9   5   9   4   7   7   5   2   5  0.468595   0.9677    RandomExcursions
  3   4   4   7  14   8   6   4   6   6  0.090936   0.9839    RandomExcursions
  7   5   4  11  11   4   2   5   4   9  0.090936   1.0000    RandomExcursions
  1   5   5  11   8   7   8   4   4   9  0.162606   1.0000    RandomExcursions
  6   3   3   8   6   9   8   3  10   6  0.350485   0.9839    RandomExcursions
 11   7   5   0   9   0   7   7   7   9  0.017912   0.9677    RandomExcursions
  9   2   7   6   6   6  11   1   8   6  0.148094   0.9839    RandomExcursions
  7   6   6   5   5   7   5   7   7   7  0.998205   1.0000    RandomExcursions
  6   7   6   4   5   5   6  11   7   5  0.772760   0.9839    RandomExcursionsVariant
  7   3   8   5   6   6   1  11   6   9  0.195163   0.9839    RandomExcursionsVariant
  6   6   9   6   4   4   9   6   5   7  0.862344   0.9839    RandomExcursionsVariant
  7   7   6   4  12   6   4   5   7   4  0.468595   0.9839    RandomExcursionsVariant
 11   3   4  11   7   6   7   5   3   5  0.178278   0.9677    RandomExcursionsVariant
  8   7   6   6   7   6   6   6   6   4  0.995711   0.9839    RandomExcursionsVariant
  9   7   2   5   7   5   8   5   3  11  0.253551   1.0000    RandomExcursionsVariant
  9   3   6   5   3  11   7   3   8   7  0.253551   0.9839    RandomExcursionsVariant
  4   7   9   5   6   2  11   3   8   7  0.232760   1.0000    RandomExcursionsVariant
  4   9   7   6   4   6   7   4   9   6  0.804337   0.9677    RandomExcursionsVariant
  6   4   6   6  13   7   8   3   5   4  0.213309   0.9839    RandomExcursionsVariant
  7   5   5   8   7   5   7   6   8   4  0.964295   0.9839    RandomExcursionsVariant
  7   3   7   7   6   5   6   4   9   8  0.834308   0.9839    RandomExcursionsVariant
  5   5   7   9   4   4   8   6   7   7  0.888137   1.0000    RandomExcursionsVariant
  4   4   8   5  10   4   4   5  10   8  0.378138   1.0000    RandomExcursionsVariant
  6   3   5   8   4  10   5   7   6   8  0.671779   1.0000    RandomExcursionsVariant
  6   2   4   8   7   8   7   9   7   4  0.602458   1.0000    RandomExcursionsVariant
  6   1   8   3   8   7  15   5   3   6  0.007880   1.0000    RandomExcursionsVariant
  6   6  12   8  12  10   8  10  10  18  0.262249   1.0000    Serial
 10   6  10  12  14   9   5   8  12  14  0.474986   1.0000    Serial
  8  11   7  14   5   5  11  13  18   8  0.071177   1.0000    LinearComplexity
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
The minimum pass rate for each statistical test with the exception of the
random excursion (variant) test is approximately = 0.960150 for a
sample size = 100 binary sequences.
The minimum pass rate for the random excursion (variant) test
is approximately 0.952091 for a sample size = 62 binary sequences.
For further guidelines construct a probability table using the MAPLE program
provided in the addendum section of the documentation.
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
```

RESULTS FOR THE UNIFORMITY OF P-VALUES AND THE PROPORTION OF PASSING SEQUENCES

generator is <V_DI_DR.bin>

C1	C2	C3	C4	C5	C6	C7	C8	C9	C10	P-VALUE	PROPORTION	STATISTICAL TEST
17	11	14	7	12	8	4	9	9	9	0.202268	0.9800	Frequency
100	0	0	0	0	0	0	0	0	0	0.000000 *	0.0000 *	BlockFrequency
18	14	18	9	8	11	7	3	9	3	0.002203	0.9700	CumulativeSums
21	10	8	16	16	6	7	8	5	3	0.000439	0.9700	CumulativeSums
16	12	9	8	13	7	11	8	9	7	0.554420	0.9500 *	Runs
19	12	10	10	4	13	6	6	10	10	0.062821	0.9700	LongestRun
100	0	0	0	0	0	0	0	0	0	0.000000 *	0.0000 *	Rank
100	0	0	0	0	0	0	0	0	0	0.000000 *	0.0000 *	FFT
28	17	10	8	10	7	5	10	5	0	0.000000 *	0.9300 *	NonOverlappingTemplate
19	19	12	12	10	11	4	7	4	2	0.000233	0.9600	NonOverlappingTemplate
22	12	10	14	12	5	5	14	1	5	0.000089 *	0.9600	NonOverlappingTemplate
21	17	9	15	10	8	6	7	6	1	0.000184	0.9700	NonOverlappingTemplate
15	18	11	11	8	12	6	8	8	3	0.045675	0.9500 *	NonOverlappingTemplate
23	18	17	6	7	9	5	5	7	3	0.000004 *	0.9400 *	NonOverlappingTemplate
29	10	16	6	12	4	6	5	7	5	0.000000 *	0.9500 *	NonOverlappingTemplate
34	4	11	9	9	7	7	5	8	6	0.000000 *	0.9000 *	NonOverlappingTemplate
24	9	12	13	10	9	10	2	7	4	0.000199	0.9700	NonOverlappingTemplate
21	16	10	4	10	10	13	6	6	4	0.001399	0.9400 *	NonOverlappingTemplate
21	13	20	8	7	9	4	5	5	8	0.000114	0.9700	NonOverlappingTemplate
20	17	8	7	8	13	8	11	5	3	0.002559	0.9500 *	NonOverlappingTemplate
21	13	11	8	4	11	6	8	8	10	0.020548	0.9800	NonOverlappingTemplate
19	14	9	15	10	6	6	6	8	7	0.030806	0.9600	NonOverlappingTemplate
25	13	12	11	9	6	8	8	6	2	0.000076 *	0.9800	NonOverlappingTemplate
17	15	19	8	3	13	9	9	6	1	0.000233	0.9500 *	NonOverlappingTemplate
27	10	11	8	8	9	9	10	4	4	0.000024 *	0.9400 *	NonOverlappingTemplate
17	18	10	12	10	6	7	9	8	3	0.020548	0.9700	NonOverlappingTemplate
22	10	12	11	12	9	8	8	5	3	0.004981	0.9800	NonOverlappingTemplate
25	9	7	6	11	8	11	10	6	7	0.000883	0.9600	NonOverlappingTemplate
22	12	9	12	10	9	3	12	6	5	0.003201	0.9600	NonOverlappingTemplate
21	16	10	9	12	8	11	4	6	3	0.001509	0.9500 *	NonOverlappingTemplate
24	14	12	8	9	6	4	12	4	7	0.000184	0.9900	NonOverlappingTemplate
21	12	13	7	7	10	10	9	9	2	0.009535	0.9500 *	NonOverlappingTemplate
26	15	12	13	8	6	6	4	6	4	0.000004 *	0.9300 *	NonOverlappingTemplate
26	12	11	8	8	10	7	7	6	5	0.000145	0.9700	NonOverlappingTemplate
26	7	10	11	10	13	6	6	6	5	0.000065 *	0.9400 *	NonOverlappingTemplate
21	13	12	6	6	12	11	5	6	8	0.010237	0.9600	NonOverlappingTemplate
20	15	17	8	10	7	5	9	6	3	0.001030	0.9500 *	NonOverlappingTemplate
31	16	9	11	7	6	6	6	3	5	0.000000 *	0.9300 *	NonOverlappingTemplate
36	12	8	8	6	5	6	7	5	7	0.000000 *	0.8800 *	NonOverlappingTemplate
25	11	15	10	6	9	7	6	6	5	0.000114	0.9100 *	NonOverlappingTemplate
16	14	18	10	12	7	7	7	5	4	0.013569	0.9500 *	NonOverlappingTemplate
26	16	16	12	6	4	5	7	6	2	0.000000 *	0.9700	NonOverlappingTemplate
30	13	9	6	6	7	8	4	7	10	0.000000 *	0.9600	NonOverlappingTemplate
28	14	15	11	8	6	8	4	3	3	0.000000 *	0.9800	NonOverlappingTemplate
23	13	13	11	7	8	6	6	5	8	0.001895	0.9500 *	NonOverlappingTemplate
27	14	6	12	7	5	8	9	2	10	0.000002 *	0.9800	NonOverlappingTemplate
29	15	7	5	9	6	8	6	5	10	0.000000 *	0.9200 *	NonOverlappingTemplate
20	13	18	9	5	3	12	7	8	5	0.000648	0.9700	NonOverlappingTemplate
22	17	11	11	6	6	4	12	4	7	0.000274	0.9700	NonOverlappingTemplate
24	13	13	9	14	7	5	4	5	6	0.000082 *	0.9200 *	NonOverlappingTemplate
28	13	3	4	8	11	14	12	6	1	0.000000 *	0.9400 *	NonOverlappingTemplate
25	10	8	10	13	10	12	6	2	4	0.000043 *	0.9600	NonOverlappingTemplate
26	15	8	9	14	11	7	5	1	4	0.000001 *	0.9500 *	NonOverlappingTemplate
17	13	14	12	11	6	11	10	2	4	0.020548	0.9800	NonOverlappingTemplate
25	8	12	12	11	9	8	8	6	1	0.000076 *	0.9600	NonOverlappingTemplate
21	19	4	17	11	9	6	3	5	5	0.000006 *	0.9700	NonOverlappingTemplate
17	17	18	4	8	9	7	10	6	4	0.001757	0.9800	NonOverlappingTemplate
23	13	11	6	11	10	8	7	6	5	0.002971	0.9700	NonOverlappingTemplate
21	12	7	11	9	12	7	11	6	4	0.016717	0.9600	NonOverlappingTemplate
28	14	11	11	4	6	3	10	7	6	0.000000 *	0.9400 *	NonOverlappingTemplate
22	12	10	12	9	11	5	9	8	2	0.003201	0.9700	NonOverlappingTemplate
24	18	6	12	9	10	8	6	3	4	0.000014 *	0.9200 *	NonOverlappingTemplate
25	6	10	7	8	10	7	12	10	5	0.000600	0.9600	NonOverlappingTemplate
15	17	12	12	9	6	11	5	7	6	0.090936	0.9800	NonOverlappingTemplate
24	9	10	15	10	12	6	5	4	5	0.000145	0.9700	NonOverlappingTemplate

18	18	9	14	4	12	6	6	11	2	0.000883	0.9600	NonOverlappingTemplate
22	15	21	11	6	7	3	3	7	5	0.000001 *	0.9600	NonOverlappingTemplate
15	20	8	16	10	8	7	6	6	4	0.003447	0.9700	NonOverlappingTemplate
18	12	20	12	7	6	8	6	7	4	0.001895	0.9700	NonOverlappingTemplate
17	19	16	8	15	6	5	9	3	2	0.000060 *	0.9600	NonOverlappingTemplate
23	14	10	9	8	6	11	6	9	4	0.002043	0.9500 *	NonOverlappingTemplate
20	15	8	12	5	5	9	13	8	5	0.008266	0.9900	NonOverlappingTemplate
26	10	16	7	10	9	5	4	5	8	0.000011 *	0.9100 *	NonOverlappingTemplate
35	11	12	10	11	5	4	4	5	3	0.000000 *	0.9200 *	NonOverlappingTemplate
29	11	16	5	8	9	10	3	4	5	0.000000 *	0.9600	NonOverlappingTemplate
25	16	11	8	11	12	6	6	4	1	0.000003 *	0.9800	NonOverlappingTemplate
29	10	14	5	11	7	6	8	6	4	0.000000 *	0.9400 *	NonOverlappingTemplate
22	16	12	12	9	8	9	5	5	2	0.000320	0.9500 *	NonOverlappingTemplate
25	11	18	7	11	6	8	8	5	1	0.000002 *	0.9900	NonOverlappingTemplate
21	21	10	5	12	7	4	7	4	9	0.000037 *	0.9400 *	NonOverlappingTemplate
29	13	11	9	8	11	5	2	8	4	0.000000 *	0.9500 *	NonOverlappingTemplate
23	17	9	9	8	6	4	9	9	6	0.000555	0.9600	NonOverlappingTemplate
28	17	10	8	10	7	5	10	5	0	0.000000 *	0.9300 *	NonOverlappingTemplate
19	16	11	12	10	8	8	3	10	3	0.006661	0.9300 *	NonOverlappingTemplate
25	17	9	5	11	7	8	8	6	4	0.000026 *	0.9700	NonOverlappingTemplate
25	8	20	13	11	6	6	3	3	5	0.000000 *	0.9400 *	NonOverlappingTemplate
26	15	8	13	6	5	6	6	7	8	0.000017 *	0.9400 *	NonOverlappingTemplate
25	9	12	14	12	6	5	10	4	3	0.000021 *	0.9500 *	NonOverlappingTemplate
19	15	15	10	5	7	9	9	7	4	0.011791	0.9800	NonOverlappingTemplate
14	19	13	16	9	5	7	8	5	4	0.003996	0.9900	NonOverlappingTemplate
27	13	9	16	10	7	6	4	5	3	0.000000 *	0.9100 *	NonOverlappingTemplate
27	10	12	9	11	4	9	6	7	5	0.000016 *	0.9000 *	NonOverlappingTemplate
21	15	7	8	11	11	7	9	2	9	0.004981	0.9500 *	NonOverlappingTemplate
27	17	10	9	7	5	7	7	6	5	0.000002 *	0.9400 *	NonOverlappingTemplate
28	15	6	5	5	12	6	5	10	8	0.000001 *	0.9300 *	NonOverlappingTemplate
22	16	12	11	6	11	7	5	3	7	0.000555	0.9700	NonOverlappingTemplate
13	18	11	9	12	13	6	5	7	6	0.080519	0.9600	NonOverlappingTemplate
24	19	6	10	9	6	9	10	4	3	0.000009 *	0.9600	NonOverlappingTemplate
27	11	12	13	6	7	6	7	8	3	0.000006 *	0.9900	NonOverlappingTemplate
25	15	18	11	6	8	7	4	4	2	0.000000 *	0.9200 *	NonOverlappingTemplate
22	21	12	5	5	10	10	6	4	5	0.000009 *	0.9900	NonOverlappingTemplate
21	12	15	10	9	8	8	5	6	6	0.010237	0.9900	NonOverlappingTemplate
16	16	18	4	4	5	14	9	9	5	0.001112	0.9700	NonOverlappingTemplate
26	13	11	13	3	7	7	10	6	4	0.000010 *	0.9600	NonOverlappingTemplate
22	12	14	8	9	7	9	7	4	8	0.006661	0.9600	NonOverlappingTemplate
23	18	8	18	7	8	4	6	3	5	0.000001 *	0.9600	NonOverlappingTemplate
28	19	10	4	11	8	3	12	3	2	0.000000 *	0.9500 *	NonOverlappingTemplate
24	8	8	14	12	5	7	12	6	4	0.000253	0.9000 *	NonOverlappingTemplate
29	15	10	11	5	4	8	8	4	6	0.000000 *	0.9500 *	NonOverlappingTemplate
25	13	16	7	6	7	7	6	9	4	0.000031 *	0.9700	NonOverlappingTemplate
18	20	17	9	11	3	5	9	6	2	0.000026 *	0.9600	NonOverlappingTemplate
26	10	13	5	12	11	5	7	7	4	0.000022 *	0.9400 *	NonOverlappingTemplate
34	14	8	5	13	9	6	3	5	3	0.000000 *	0.9600	NonOverlappingTemplate
29	20	8	8	8	5	7	5	7	3	0.000000 *	0.9500 *	NonOverlappingTemplate
26	16	11	10	8	7	7	5	5	5	0.000012 *	0.9400 *	NonOverlappingTemplate
22	19	8	9	10	5	7	7	5	8	0.000406	0.9500 *	NonOverlappingTemplate
26	10	15	9	9	5	9	5	8	4	0.000022 *	0.9400 *	NonOverlappingTemplate
31	14	8	8	7	10	4	7	6	5	0.000000 *	0.9500 *	NonOverlappingTemplate
26	13	9	10	12	5	4	8	8	5	0.000034 *	0.9600	NonOverlappingTemplate
26	13	13	3	8	11	8	2	10	6	0.000005 *	0.9100 *	NonOverlappingTemplate
21	14	9	19	7	5	2	7	7	9	0.000105	0.9400 *	NonOverlappingTemplate
26	11	9	13	6	7	11	8	4	5	0.000043 *	0.9700	NonOverlappingTemplate
21	12	15	9	9	7	11	13	2	1	0.000233	0.9800	NonOverlappingTemplate
24	12	13	15	7	8	3	7	6	5	0.000070 *	0.9700	NonOverlappingTemplate
14	11	8	15	13	11	11	3	9	5	0.153763	0.9900	NonOverlappingTemplate
18	17	10	9	9	7	6	7	9	8	0.080519	0.9700	NonOverlappingTemplate
21	14	14	9	8	10	5	4	6	9	0.004981	0.9600	NonOverlappingTemplate
16	18	12	10	5	8	10	12	6	3	0.016717	0.9400 *	NonOverlappingTemplate
25	12	8	14	11	5	11	4	7	3	0.000026 *	0.9500 *	NonOverlappingTemplate
20	12	14	2	9	10	8	10	9	6	0.014550	0.9400 *	NonOverlappingTemplate
31	15	8	4	13	10	8	3	5	3	0.000000 *	0.9300 *	NonOverlappingTemplate
23	14	12	10	8	5	8	8	4	8	0.001628	0.9700	NonOverlappingTemplate
23	10	15	8	6	9	10	7	9	3	0.001201	0.9800	NonOverlappingTemplate
20	17	14	9	10	8	9	5	5	3	0.001399	0.9500 *	NonOverlappingTemplate
22	15	10	9	11	7	10	6	3	7	0.002559	0.9600	NonOverlappingTemplate
18	17	9	9	12	7	7	7	5	9	0.045675	0.9700	NonOverlappingTemplate

```
 27  12  14   8   8   8   8   5   6   4  0.000007 * 0.9700    NonOverlappingTemplate
 24  15  10  11   7   8   8   7   7   3  0.000347   0.9400 *  NonOverlappingTemplate
 27  16   9   9   9   3   6   5  10   6  0.000002 * 0.9300 *  NonOverlappingTemplate
 27  11   7  10   8  12   7   7   6   5  0.000031 * 0.9600    NonOverlappingTemplate
 27  20   6   2  10  11   4   6  10   4  0.000000 * 0.9700    NonOverlappingTemplate
 24  12  20   5  10   8   6   9   3   3  0.000001 * 0.9400 *  NonOverlappingTemplate
 27  10  16  11   8   8   7   6   6   1  0.000001 * 0.9000 *  NonOverlappingTemplate
 24  15  13   9   8  12   6   4   4   5  0.000055 * 0.9600    NonOverlappingTemplate
 24  18  10   7   6  10   7   5   6   7  0.000076 * 0.9600    NonOverlappingTemplate
 25  15  12  12   7   5  12   4   5   3  0.000006 * 0.9500 *  NonOverlappingTemplate
 27  13   8  14   9   8   9   5   2   5  0.000002 * 0.9600    NonOverlappingTemplate
 30   7  12   8  11   8  12   7   4   1  0.000000 * 0.9700    NonOverlappingTemplate
 25  14   8   9  11   9   9   9   2   4  0.000060 * 0.9300 *  NonOverlappingTemplate
 16  26  15   9  10   7   7   6   3   1  0.000000 * 0.9800    NonOverlappingTemplate
 22  11  11   8  13  12   5   5   6   7  0.004629   0.9400 *  NonOverlappingTemplate
 14   9  11  15  12   9   9   7   9   5  0.494392   0.9400 *  NonOverlappingTemplate
 23  17  11  11   8   9   4   8   3   6  0.000134   0.9400 *  NonOverlappingTemplate
 24  15  12  11   9   5   6  10   4   4  0.000089 * 0.9700    NonOverlappingTemplate
 19  14  10   8  11   7  15   6   7   3  0.012650   0.9400 *  NonOverlappingTemplate
 23  17   9   9   8   6   4   9   9   6  0.000555   0.9600    NonOverlappingTemplate
 62  14  10   6   3   2   1   2   0   0  0.000000 * 0.6800 *  OverlappingTemplate
 12   9  10  11  11   7  12   8  11   9  0.978072   0.9800    Universal
100   0   0   0   0   0   0   0   0   0  0.000000 * 0.0200 *  ApproximateEntropy
  9   6   3   8   4   4   6   6   7   3  0.494392   1.0000    RandomExcursions
  4   9   4   7   6   2   5   4  11   4  0.122325   0.9821    RandomExcursions
  4   8   3   6   4   8   7   6   3   7  0.574903   1.0000    RandomExcursions
  0   5   6   4  11   5   5   6  11   3  0.013569   1.0000    RandomExcursions
  4   6   4   6   5   2   9   6   8   6  0.534146   1.0000    RandomExcursions
  6   8   4   5   5   3   6   7   5   7  0.851383   1.0000    RandomExcursions
  4   4   8  12   2   4   6   5   3   8  0.051942   1.0000    RandomExcursions
  6   6   7   2   6   5   5   5  12   2  0.096578   0.9821    RandomExcursions
  5   4   5   8   3  11   7   7   2   4  0.137282   1.0000    RandomExcursionsVariant
  3   6   5   3   7   5  11   8   2   6  0.137282   0.9821    RandomExcursionsVariant
  2   7   4   7   6   7   4   5   7   7  0.699313   1.0000    RandomExcursionsVariant
  2   8   3   4   6   7   7   9   7   3  0.262249   1.0000    RandomExcursionsVariant
  3   3   3   6   9   6   7   5   6   8  0.455937   1.0000    RandomExcursionsVariant
  3   3   5   5   7   5   9   6   5   8  0.574903   1.0000    RandomExcursionsVariant
  4   6   5   5   8   5   6   9   3   5  0.699313   1.0000    RandomExcursionsVariant
  7   4   7   5   6   6   4   4   7   6  0.935716   1.0000    RandomExcursionsVariant
  6   6   6   6   3   4   4   3   7  11  0.289667   1.0000    RandomExcursionsVariant
  6   7   5   2   4   1   6  10   9   6  0.096578   0.9821    RandomExcursionsVariant
  4   5   8   7   6   7   6   3   5   5  0.851383   1.0000    RandomExcursionsVariant
  4   6   8   6   4   3   5   7   7   6  0.816537   1.0000    RandomExcursionsVariant
  3   4   9  11   6   4   4   6   5   4  0.191687   1.0000    RandomExcursionsVariant
  3   6   9   8  12   1   5   3   5   4  0.017912   1.0000    RandomExcursionsVariant
  5   5   3  14   5   7   3   6   3   5  0.020548   0.9821    RandomExcursionsVariant
  4   5   6  12   7   6   3   4   5   4  0.191687   0.9821    RandomExcursionsVariant
  5   4   7   3   8   9   7   4   4   5  0.534146   0.9821    RandomExcursionsVariant
  5   5   4   3   9   7   6   8   3   6  0.534146   0.9821    RandomExcursionsVariant
100   0   0   0   0   0   0   0   0   0  0.000000 * 0.0000 *  Serial
100   0   0   0   0   0   0   0   0   0  0.000000 * 0.0000 *  Serial
 12  12   8  13  12  10   6  12   6   9  0.719747   0.9800    LinearComplexity
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
The minimum pass rate for each statistical test with the exception of the
random excursion (variant) test is approximately = 0.960150 for a
sample size = 100 binary sequences.
The minimum pass rate for the random excursion (variant) test
is approximately 0.950112 for a sample size = 56 binary sequences.
For further guidelines construct a probability table using the MAPLE program
provided in the addendum section of the documentation.
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
```

Результати тестування розширеного матричного перетворення невипадкової монотонно зростаючої послідовності з циклом повторення 64 байти

RESULTS FOR THE UNIFORMITY OF P-VALUES AND THE PROPORTION OF PASSING SEQUENCES

generator is <V_R_64.bin>

C1	C2	C3	C4	C5	C6	C7	C8	C9	C10	P-VALUE	PROPORTION	STATISTICAL TEST
11	10	13	8	14	5	10	14	5	10	0.383827	0.9900	Frequency
10	15	13	5	7	13	9	10	8	10	0.514124	0.9900	BlockFrequency
10	9	14	14	6	10	9	11	6	11	0.657933	0.9900	CumulativeSums
10	13	8	12	13	11	7	11	8	7	0.834308	0.9800	CumulativeSums
11	4	11	10	8	11	10	11	14	10	0.739918	0.9900	Runs
15	11	5	11	13	8	5	15	10	7	0.191687	0.9800	LongestRun
13	7	7	8	12	9	8	15	10	11	0.678686	0.9800	Rank
2	7	12	6	9	9	17	14	14	10	0.040108	1.0000	FFT
6	10	9	13	9	11	7	7	13	15	0.534146	0.9800	NonOverlappingTemplate
14	6	7	10	12	8	16	7	9	11	0.383827	0.9800	NonOverlappingTemplate
11	10	14	4	8	15	9	10	10	9	0.494392	0.9900	NonOverlappingTemplate
7	9	11	6	9	6	11	13	11	17	0.319084	0.9900	NonOverlappingTemplate
10	6	10	4	13	10	12	15	12	8	0.366918	0.9900	NonOverlappingTemplate
9	15	12	10	10	13	9	9	8	5	0.637119	0.9800	NonOverlappingTemplate
7	12	6	13	12	9	7	14	9	11	0.637119	1.0000	NonOverlappingTemplate
11	8	17	10	14	12	5	9	7	7	0.224821	1.0000	NonOverlappingTemplate
12	10	12	8	8	8	13	10	6	13	0.798139	0.9900	NonOverlappingTemplate
11	8	9	7	9	15	12	11	7	11	0.779188	0.9900	NonOverlappingTemplate
5	13	13	12	12	13	10	7	8	7	0.514124	1.0000	NonOverlappingTemplate
7	9	17	9	6	10	8	12	8	14	0.319084	0.9900	NonOverlappingTemplate
8	11	18	11	8	6	7	9	17	5	0.042808	0.9900	NonOverlappingTemplate
8	10	7	13	14	10	14	4	8	12	0.366918	0.9900	NonOverlappingTemplate
9	8	6	19	11	11	13	5	8	10	0.115387	1.0000	NonOverlappingTemplate
8	14	7	7	11	8	11	13	6	15	0.401199	0.9800	NonOverlappingTemplate
15	8	11	12	6	16	7	4	8	13	0.108791	0.9700	NonOverlappingTemplate
7	4	12	6	11	16	13	13	6	12	0.122325	1.0000	NonOverlappingTemplate
9	10	11	10	8	9	12	10	11	10	0.998821	0.9800	NonOverlappingTemplate
16	3	11	12	11	11	9	10	5	12	0.202268	0.9700	NonOverlappingTemplate
11	8	10	7	7	16	12	16	8	5	0.171867	1.0000	NonOverlappingTemplate
11	11	12	7	12	9	8	7	15	8	0.719747	0.9900	NonOverlappingTemplate
10	12	7	13	11	15	7	5	8	12	0.437274	0.9900	NonOverlappingTemplate
8	12	5	9	15	8	12	11	10	10	0.657933	0.9900	NonOverlappingTemplate
9	18	10	6	7	14	8	9	14	5	0.085587	1.0000	NonOverlappingTemplate
10	11	14	6	5	13	9	3	17	12	0.048716	0.9800	NonOverlappingTemplate
13	10	10	6	10	6	11	13	14	7	0.574903	1.0000	NonOverlappingTemplate
9	10	9	16	12	9	10	9	9	7	0.798139	0.9900	NonOverlappingTemplate
10	10	14	3	14	13	8	9	9	10	0.383827	0.9800	NonOverlappingTemplate
15	4	9	12	11	7	6	10	11	15	0.224821	0.9800	NonOverlappingTemplate
11	8	11	12	9	12	10	8	9	10	0.991468	1.0000	NonOverlappingTemplate
13	11	10	10	15	7	9	3	8	14	0.249284	1.0000	NonOverlappingTemplate
11	12	7	10	10	9	11	11	9	10	0.994250	0.9900	NonOverlappingTemplate
10	11	12	12	7	9	12	11	9	7	0.946308	1.0000	NonOverlappingTemplate
11	5	11	15	8	10	8	9	8	15	0.437274	0.9900	NonOverlappingTemplate
11	7	9	8	7	11	5	15	14	13	0.350485	0.9800	NonOverlappingTemplate
8	13	8	11	12	11	13	13	8	3	0.401199	1.0000	NonOverlappingTemplate
12	10	7	11	10	9	13	10	11	7	0.946308	0.9800	NonOverlappingTemplate
10	8	12	8	13	15	4	7	14	9	0.289667	0.9900	NonOverlappingTemplate
10	15	10	8	11	7	11	7	12	9	0.798139	0.9900	NonOverlappingTemplate
7	8	12	12	13	7	12	9	10	10	0.883171	1.0000	NonOverlappingTemplate
6	13	12	6	11	13	6	7	9	17	0.162606	1.0000	NonOverlappingTemplate
8	9	11	11	14	11	15	5	8	8	0.514124	0.9900	NonOverlappingTemplate
6	4	13	10	15	12	8	9	10	13	0.319084	1.0000	NonOverlappingTemplate
11	11	11	9	9	14	12	4	11	8	0.678686	0.9900	NonOverlappingTemplate
10	13	11	10	6	8	8	8	10	16	0.595549	0.9900	NonOverlappingTemplate
10	14	13	11	10	7	10	13	4	8	0.494392	0.9900	NonOverlappingTemplate
7	12	6	11	13	12	12	10	8	9	0.816537	0.9900	NonOverlappingTemplate
7	13	7	14	6	13	9	11	8	12	0.554420	0.9900	NonOverlappingTemplate
7	8	12	10	16	6	9	8	10	14	0.437274	1.0000	NonOverlappingTemplate
8	9	15	11	12	6	12	7	10	10	0.699313	0.9900	NonOverlappingTemplate

10	9	10	10	9	10	11	12	11	8	0.998821	0.9800	NonOverlappingTemplate
4	8	11	13	9	8	11	10	12	14	0.574903	1.0000	NonOverlappingTemplate
11	12	8	8	9	12	13	9	13	5	0.719747	0.9900	NonOverlappingTemplate
9	12	11	10	13	9	8	8	12	8	0.955835	0.9600	NonOverlappingTemplate
8	11	16	9	15	7	10	9	8	7	0.437274	0.9900	NonOverlappingTemplate
10	8	8	13	4	12	11	9	12	13	0.616305	0.9900	NonOverlappingTemplate
10	13	10	10	6	9	13	8	9	12	0.883171	1.0000	NonOverlappingTemplate
12	4	9	10	10	12	9	10	13	11	0.779188	0.9900	NonOverlappingTemplate
9	7	14	9	12	7	7	16	10	9	0.474986	1.0000	NonOverlappingTemplate
12	6	11	12	7	12	15	12	9	4	0.319084	1.0000	NonOverlappingTemplate
5	5	11	15	11	8	16	7	8	14	0.102526	1.0000	NonOverlappingTemplate
9	10	12	6	6	14	12	11	9	11	0.739918	0.9800	NonOverlappingTemplate
13	7	9	12	11	6	8	16	9	9	0.514124	0.9600	NonOverlappingTemplate
9	10	12	6	15	11	8	9	6	14	0.494392	0.9900	NonOverlappingTemplate
7	11	10	11	9	12	15	8	9	8	0.834308	1.0000	NonOverlappingTemplate
8	11	10	13	12	11	10	9	5	11	0.867692	0.9800	NonOverlappingTemplate
9	8	19	12	7	7	6	14	9	9	0.115387	1.0000	NonOverlappingTemplate
7	8	13	14	10	7	11	8	6	16	0.319084	1.0000	NonOverlappingTemplate
8	12	7	10	7	9	11	18	11	7	0.334538	0.9900	NonOverlappingTemplate
10	14	9	13	4	12	9	10	12	7	0.534146	1.0000	NonOverlappingTemplate
15	14	10	13	9	8	2	6	13	10	0.108791	1.0000	NonOverlappingTemplate
6	9	10	9	11	10	16	10	11	8	0.739918	0.9900	NonOverlappingTemplate
10	14	12	7	10	9	10	8	9	11	0.935716	0.9800	NonOverlappingTemplate
6	10	9	13	9	11	7	7	13	15	0.534146	0.9800	NonOverlappingTemplate
8	6	11	14	11	15	9	6	10	10	0.534146	0.9900	NonOverlappingTemplate
14	9	10	10	13	9	7	12	11	5	0.678686	0.9900	NonOverlappingTemplate
9	12	6	11	16	14	8	10	6	8	0.366918	0.9900	NonOverlappingTemplate
12	7	13	12	9	12	8	9	9	9	0.924076	0.9900	NonOverlappingTemplate
14	9	9	8	7	8	12	13	8	12	0.779188	0.9900	NonOverlappingTemplate
5	15	17	9	8	8	9	10	15	4	0.048716	1.0000	NonOverlappingTemplate
10	11	11	12	8	12	12	5	10	9	0.883171	0.9900	NonOverlappingTemplate
16	12	9	10	11	5	7	13	10	7	0.401199	0.9900	NonOverlappingTemplate
10	11	9	11	12	8	11	9	11	8	0.994250	1.0000	NonOverlappingTemplate
9	8	11	12	10	9	13	12	8	8	0.955835	0.9800	NonOverlappingTemplate
10	9	9	9	15	5	8	10	10	15	0.514124	1.0000	NonOverlappingTemplate
10	13	9	8	8	15	5	15	8	9	0.366918	1.0000	NonOverlappingTemplate
12	9	12	6	8	12	6	8	10	17	0.334538	0.9800	NonOverlappingTemplate
10	12	9	8	7	13	11	12	15	3	0.304126	0.9900	NonOverlappingTemplate
8	7	8	10	9	15	11	10	18	4	0.108791	0.9800	NonOverlappingTemplate
6	10	8	10	15	7	11	4	10	19	0.045675	1.0000	NonOverlappingTemplate
14	6	12	7	13	9	7	20	5	7	0.019188	1.0000	NonOverlappingTemplate
12	9	13	15	7	11	9	5	7	12	0.455937	0.9800	NonOverlappingTemplate
13	10	11	9	11	9	12	8	5	12	0.834308	0.9900	NonOverlappingTemplate
10	12	9	9	15	6	9	11	10	9	0.834308	1.0000	NonOverlappingTemplate
17	10	12	11	7	10	10	5	8	10	0.419021	0.9900	NonOverlappingTemplate
7	10	7	9	10	13	6	10	15	13	0.554420	1.0000	NonOverlappingTemplate
9	8	11	7	13	13	11	11	6	11	0.816537	0.9800	NonOverlappingTemplate
6	10	12	6	11	15	10	10	11	9	0.699313	1.0000	NonOverlappingTemplate
8	6	9	13	13	13	10	8	16	4	0.191687	0.9900	NonOverlappingTemplate
10	10	7	12	8	14	12	5	11	11	0.699313	1.0000	NonOverlappingTemplate
9	10	6	10	15	7	14	10	10	9	0.657933	0.9800	NonOverlappingTemplate
8	12	12	12	6	7	12	9	12	10	0.834308	0.9900	NonOverlappingTemplate
11	7	8	10	13	11	11	14	8	7	0.798139	0.9900	NonOverlappingTemplate
10	8	8	10	9	15	10	9	10	11	0.935716	0.9700	NonOverlappingTemplate
9	9	10	11	8	14	14	10	6	9	0.779188	0.9700	NonOverlappingTemplate
10	8	9	9	18	8	15	10	5	8	0.171867	1.0000	NonOverlappingTemplate
6	12	14	11	10	8	10	7	8	14	0.637119	1.0000	NonOverlappingTemplate
9	4	8	12	11	11	13	10	7	15	0.437274	0.9900	NonOverlappingTemplate
10	11	15	15	7	7	8	6	14	7	0.249284	1.0000	NonOverlappingTemplate
8	12	8	8	9	12	12	7	11	13	0.883171	1.0000	NonOverlappingTemplate
8	12	12	13	10	13	8	9	6	9	0.816537	0.9800	NonOverlappingTemplate
14	13	7	7	12	15	8	13	8	3	0.129620	0.9900	NonOverlappingTemplate
7	6	5	10	8	11	18	7	17	11	0.037566	0.9900	NonOverlappingTemplate
7	7	11	9	7	12	10	11	13	13	0.816537	1.0000	NonOverlappingTemplate
15	8	11	9	9	9	9	11	8	11	0.911413	0.9800	NonOverlappingTemplate
10	8	9	13	9	9	11	8	9	14	0.924076	0.9900	NonOverlappingTemplate
16	7	13	14	9	4	8	9	9	11	0.249284	0.9900	NonOverlappingTemplate
10	8	8	6	10	11	12	12	11	12	0.924076	0.9900	NonOverlappingTemplate
13	7	9	10	9	13	8	12	10	9	0.924076	0.9900	NonOverlappingTemplate
12	10	4	9	15	10	10	7	8	15	0.319084	0.9700	NonOverlappingTemplate
12	11	8	9	12	11	13	8	9	7	0.924076	0.9800	NonOverlappingTemplate

```
 10   9  11   8  10  10  13   7  11  11  0.978072   1.0000    NonOverlappingTemplate
 14   7   6  11  12  12  11   9   9   9  0.798139   0.9900    NonOverlappingTemplate
 11   8   5  15  16  10   6   8  10  11  0.262249   0.9900    NonOverlappingTemplate
 15   6  11   8  10  12  11   8   6  13  0.534146   0.9600    NonOverlappingTemplate
  5   8   9  13  10   8   6  13  13  15  0.334538   0.9900    NonOverlappingTemplate
 10  10  14   7  10  10   7  11  11  10  0.935716   0.9900    NonOverlappingTemplate
  5  13   7   9  11   8  11  11  13  12  0.699313   0.9900    NonOverlappingTemplate
 14  11   4  14   5  12   6   9  14  11  0.153763   0.9800    NonOverlappingTemplate
  7  19  10   8   6  12  10  13   8   7  0.137282   0.9700    NonOverlappingTemplate
  9   6   6  16   9   8  10  14  13   9  0.350485   1.0000    NonOverlappingTemplate
  7   8  13  12  12   7   8   6   9  18  0.191687   0.9800    NonOverlappingTemplate
  7  13   9   8  13   8  10  10  15   7  0.637119   1.0000    NonOverlappingTemplate
 16   4  12  14   9   9  15   7   8   6  0.096578   0.9700    NonOverlappingTemplate
 10   8  11   8  11  18   5  11  12   6  0.213309   1.0000    NonOverlappingTemplate
 11   6   7   8   9  11   9  13  10  16  0.554420   0.9800    NonOverlappingTemplate
 11   9  19   9   6   8   8   9  11  10  0.275709   0.9800    NonOverlappingTemplate
  9  12   8  10  10  12  16   4  12   7  0.366918   0.9900    NonOverlappingTemplate
 11  12  10  10   8   7  10   6  11  15  0.739918   1.0000    NonOverlappingTemplate
  8   7   9  10  16   8  11   9  15   7  0.437274   0.9700    NonOverlappingTemplate
 13   8  10   8  12   7  12   6  16   8  0.437274   1.0000    NonOverlappingTemplate
 10  10  10   9   7  13  17   6   9   9  0.474986   1.0000    NonOverlappingTemplate
 11  12  12  14   6   8  10  11   3  13  0.319084   0.9900    NonOverlappingTemplate
 11   9   9  10   7  11  16  10   4  13  0.401199   1.0000    NonOverlappingTemplate
 15  12   8   9   7  13   6  12   9   9  0.595549   1.0000    NonOverlappingTemplate
 11   8  15  11  12  10   8   7   9   9  0.834308   0.9900    NonOverlappingTemplate
 10  14  13   6  10   8  11   8   8  12  0.759756   0.9800    NonOverlappingTemplate
 11  12   7   9   9  11   9   8  10  14  0.924076   1.0000    OverlappingTemplate
  6   8  11  10   8  12   7  10  13  15  0.616305   1.0000    Universal
  9  11  16  10  13   8   7  12   8   6  0.494392   0.9900    ApproximateEntropy
  9   7   5   8   4   3   9   5   3   5  0.289667   0.9655    RandomExcursions
  4   6  13   6   5   3   9   3   5   4  0.030806   1.0000    RandomExcursions
  4   3   6   5   9   6   6   8   3   8  0.419021   1.0000    RandomExcursions
  6   8   6   5   4   7   8   7   1   6  0.419021   0.9828    RandomExcursions
  5   6   6   7   5   4   5   4   6  10  0.657933   1.0000    RandomExcursions
  8   6   4   7   7   6   7   8   2   3  0.419021   1.0000    RandomExcursions
  9   3   6   6   6   5   1   9   7   6  0.213309   0.9828    RandomExcursions
  9   4   5   8   4   3   3   4  10   8  0.122325   0.9655    RandomExcursions
  5   8   3   6   1  10   6   5   5   9  0.108791   1.0000    RandomExcursionsVariant
  5   3   5  14   1   6  11   4   4   5  0.000954   1.0000    RandomExcursionsVariant
  2  11   6   5   8   5   5   7   6   3  0.171867   0.9828    RandomExcursionsVariant
  4   7   9   7   5   6   7   5   3   5  0.657933   0.9828    RandomExcursionsVariant
  5   8  11   4   6   6   6   3   5   4  0.289667   1.0000    RandomExcursionsVariant
  2  12   6   7   5   8   4   6   5   3  0.075719   1.0000    RandomExcursionsVariant
  5   5   7   5  10   8   4   5   3   6  0.455937   1.0000    RandomExcursionsVariant
  4   6   8   3   4   5   9   6   6   7  0.574903   1.0000    RandomExcursionsVariant
  4   8   7   2   3   8   3   9   8   6  0.153763   1.0000    RandomExcursionsVariant
  8   6   5   4   6   7   2  10   5   5  0.350485   0.9828    RandomExcursionsVariant
  7   3   4   9   4   9   4   5   3  10  0.108791   1.0000    RandomExcursionsVariant
  3   6   5   6  10   9   4   5   5   5  0.383827   1.0000    RandomExcursionsVariant
  4   6   4   5   4   6   9  10   5   5  0.419021   1.0000    RandomExcursionsVariant
  5   3   7   5   4  11   7   6   7   3  0.236810   1.0000    RandomExcursionsVariant
  5   3   7   6   7   9   4   4   5   8  0.534146   1.0000    RandomExcursionsVariant
  4   6   3   9   2   8   3   9   5   9  0.085587   1.0000    RandomExcursionsVariant
  5   5   4   4   7   5   6   8   4  10  0.494392   1.0000    RandomExcursionsVariant
  6   3   5   7   6   6   8   8   6   3  0.657933   1.0000    RandomExcursionsVariant
 14   9  11   8   4   6  12  14   8  14  0.249284   0.9700    Serial
 12  11   7   5  10  14  10   9   6  16  0.289667   0.9900    Serial
  9   8   5  13  13   9  12  14   8   9  0.595549   0.9800    LinearComplexity
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
The minimum pass rate for each statistical test with the exception of the
random excursion (variant) test is approximately = 0.960150 for a
sample size = 100 binary sequences.
The minimum pass rate for the random excursion (variant) test
is approximately 0.950806 for a sample size = 58 binary sequences.
For further guidelines construct a probability table using the MAPLE program
provided in the addendum section of the documentation.
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
```

Результати тестування розширеного матричного перетворення невипадкової монотонно зростаючої послідовності з циклом повторення 256 байти

RESULTS FOR THE UNIFORMITY OF P-VALUES AND THE PROPORTION OF PASSING SEQUENCES

generator is <V_R_256.bin>

C1	C2	C3	C4	C5	C6	C7	C8	C9	C10	P-VALUE	PROPORTION	STATISTICAL TEST
5	11	7	8	8	9	12	9	14	17	0.249284	1.0000	Frequency
13	7	8	9	8	12	14	14	4	11	0.350485	0.9900	BlockFrequency
7	8	9	9	8	17	9	11	11	11	0.616305	1.0000	CumulativeSums
4	10	17	6	14	8	6	16	11	8	0.037566	1.0000	CumulativeSums
12	11	16	8	10	13	10	2	12	6	0.129620	0.9900	Runs
14	11	11	11	12	6	9	8	8	10	0.851383	0.9800	LongestRun
14	10	13	4	9	6	8	12	12	12	0.401199	0.9700	Rank
0	6	5	7	12	16	11	12	19	12	0.000954	1.0000	FFT
8	14	13	14	7	7	7	10	8	12	0.534146	1.0000	NonOverlappingTemplate
9	8	9	11	9	5	12	15	8	14	0.514124	1.0000	NonOverlappingTemplate
13	9	9	9	7	10	16	7	11	9	0.657933	0.9900	NonOverlappingTemplate
8	10	13	11	16	10	8	3	13	8	0.236810	0.9900	NonOverlappingTemplate
6	18	8	7	4	7	9	10	16	15	0.017912	1.0000	NonOverlappingTemplate
8	10	9	8	10	11	9	8	14	13	0.911413	0.9800	NonOverlappingTemplate
12	13	10	10	5	11	12	9	11	7	0.798139	0.9800	NonOverlappingTemplate
13	13	10	8	4	11	12	7	11	11	0.595549	0.9900	NonOverlappingTemplate
11	11	11	7	9	12	13	11	3	12	0.534146	0.9900	NonOverlappingTemplate
6	7	15	10	11	5	7	13	15	11	0.213309	1.0000	NonOverlappingTemplate
9	11	13	6	8	10	11	13	9	10	0.897763	1.0000	NonOverlappingTemplate
10	12	11	15	10	4	7	8	13	10	0.455937	1.0000	NonOverlappingTemplate
9	9	7	7	11	10	12	16	7	12	0.595549	1.0000	NonOverlappingTemplate
7	10	14	12	8	7	8	15	9	10	0.616305	0.9900	NonOverlappingTemplate
14	10	11	16	11	9	8	6	7	8	0.455937	1.0000	NonOverlappingTemplate
5	9	16	11	11	10	6	9	10	13	0.437274	1.0000	NonOverlappingTemplate
11	13	11	13	7	6	14	9	5	11	0.455937	0.9800	NonOverlappingTemplate
16	7	13	5	8	13	12	11	7	8	0.275709	1.0000	NonOverlappingTemplate
10	10	9	12	14	12	6	7	7	13	0.657933	1.0000	NonOverlappingTemplate
7	5	13	7	12	8	13	13	10	12	0.514124	0.9900	NonOverlappingTemplate
12	9	12	5	11	6	13	8	11	13	0.595549	1.0000	NonOverlappingTemplate
14	10	12	8	12	8	8	11	7	10	0.867692	0.9700	NonOverlappingTemplate
7	7	10	11	10	12	8	14	8	13	0.779188	1.0000	NonOverlappingTemplate
6	8	10	9	11	13	13	10	11	9	0.897763	0.9900	NonOverlappingTemplate
17	6	10	10	10	8	9	10	10	10	0.637119	0.9700	NonOverlappingTemplate
10	10	10	5	9	8	15	16	7	10	0.350485	0.9900	NonOverlappingTemplate
4	11	8	15	10	6	11	8	12	15	0.236810	0.9900	NonOverlappingTemplate
13	11	10	6	8	10	4	16	11	11	0.319084	0.9900	NonOverlappingTemplate
9	10	8	8	12	11	9	12	16	5	0.534146	1.0000	NonOverlappingTemplate
7	5	10	8	10	11	13	17	9	10	0.366918	0.9900	NonOverlappingTemplate
14	7	12	8	8	18	10	6	9	8	0.202268	0.9900	NonOverlappingTemplate
7	13	12	11	9	13	4	13	13	5	0.262249	1.0000	NonOverlappingTemplate
18	5	10	8	11	7	9	15	6	11	0.102526	0.9800	NonOverlappingTemplate
14	16	16	7	5	10	11	6	9	6	0.075719	1.0000	NonOverlappingTemplate
7	6	12	11	9	8	15	10	10	12	0.699313	0.9800	NonOverlappingTemplate
13	13	7	8	11	8	17	9	6	8	0.304126	0.9800	NonOverlappingTemplate
9	15	8	10	13	5	14	8	6	12	0.319084	0.9800	NonOverlappingTemplate
12	11	10	14	6	10	8	9	11	9	0.883171	1.0000	NonOverlappingTemplate
9	8	9	11	8	9	14	9	11	12	0.946308	1.0000	NonOverlappingTemplate
8	15	11	15	8	6	10	7	10	10	0.494392	0.9900	NonOverlappingTemplate
13	7	11	12	13	4	11	11	10	8	0.595549	1.0000	NonOverlappingTemplate
10	9	14	13	11	13	4	10	7	9	0.514124	1.0000	NonOverlappingTemplate
17	12	12	9	11	9	11	8	3	8	0.224821	0.9600	NonOverlappingTemplate
7	8	10	13	9	10	8	12	12	11	0.935716	0.9900	NonOverlappingTemplate
11	9	7	10	5	17	9	11	10	11	0.455937	1.0000	NonOverlappingTemplate
10	10	7	10	19	12	2	10	12	8	0.055361	0.9900	NonOverlappingTemplate
8	8	10	10	12	13	12	7	9	11	0.935716	0.9900	NonOverlappingTemplate
9	13	11	6	12	13	7	12	9	8	0.759756	1.0000	NonOverlappingTemplate
8	13	12	5	10	11	8	8	14	11	0.657933	1.0000	NonOverlappingTemplate
7	11	18	9	7	9	16	11	3	9	0.045675	1.0000	NonOverlappingTemplate
5	6	11	7	18	8	8	12	15	10	0.085587	1.0000	NonOverlappingTemplate

8	12	6	11	8	9	11	9	15	11	0.759756	0.9800	NonOverlappingTemplate
13	9	7	11	10	12	9	6	13	10	0.834308	1.0000	NonOverlappingTemplate
14	9	14	10	3	13	17	7	5	8	0.037566	1.0000	NonOverlappingTemplate
9	9	12	7	13	13	9	10	9	9	0.935716	0.9900	NonOverlappingTemplate
11	9	10	9	5	13	11	12	10	10	0.897763	0.9900	NonOverlappingTemplate
18	7	11	8	4	9	12	13	12	6	0.096578	0.9900	NonOverlappingTemplate
17	10	10	17	6	9	5	12	7	7	0.062821	0.9700	NonOverlappingTemplate
13	10	5	9	10	5	9	13	13	13	0.455937	0.9900	NonOverlappingTemplate
6	12	15	7	8	11	14	9	7	11	0.474986	1.0000	NonOverlappingTemplate
12	10	10	3	12	10	16	10	12	5	0.202268	0.9900	NonOverlappingTemplate
11	9	12	8	10	9	8	13	8	12	0.955835	0.9800	NonOverlappingTemplate
6	11	12	8	17	8	11	12	6	9	0.350485	1.0000	NonOverlappingTemplate
7	5	15	11	10	13	9	11	9	10	0.616305	0.9900	NonOverlappingTemplate
14	10	9	8	7	13	12	7	4	16	0.191687	0.9700	NonOverlappingTemplate
6	13	15	8	16	7	8	9	8	10	0.289667	0.9900	NonOverlappingTemplate
8	12	12	13	11	8	10	10	5	11	0.816537	1.0000	NonOverlappingTemplate
10	8	15	12	10	8	4	11	14	8	0.401199	0.9900	NonOverlappingTemplate
6	10	15	9	10	12	12	11	6	9	0.657933	0.9900	NonOverlappingTemplate
6	12	6	10	15	7	11	12	10	11	0.574903	0.9900	NonOverlappingTemplate
7	8	6	9	10	10	14	9	16	11	0.494392	1.0000	NonOverlappingTemplate
6	11	10	10	10	11	9	10	8	15	0.851383	1.0000	NonOverlappingTemplate
9	12	9	13	6	10	10	12	12	7	0.851383	0.9600	NonOverlappingTemplate
8	10	9	4	10	12	14	10	14	9	0.554420	1.0000	NonOverlappingTemplate
8	14	13	14	7	7	7	10	8	12	0.534146	1.0000	NonOverlappingTemplate
9	11	10	8	10	13	8	8	13	10	0.955835	1.0000	NonOverlappingTemplate
15	9	6	4	11	11	17	9	9	9	0.153763	0.9700	NonOverlappingTemplate
10	14	11	7	13	16	5	8	9	7	0.275709	0.9900	NonOverlappingTemplate
9	8	12	10	5	10	9	11	11	15	0.719747	0.9900	NonOverlappingTemplate
10	9	11	12	11	12	11	10	8	6	0.955835	1.0000	NonOverlappingTemplate
11	11	8	11	13	13	9	11	8	5	0.779188	0.9900	NonOverlappingTemplate
8	15	13	10	9	9	7	8	5	16	0.249284	1.0000	NonOverlappingTemplate
8	11	8	18	9	8	12	8	4	14	0.129620	0.9900	NonOverlappingTemplate
8	15	14	14	7	9	5	11	4	13	0.115387	0.9900	NonOverlappingTemplate
12	10	17	8	13	7	10	11	5	7	0.275709	0.9900	NonOverlappingTemplate
5	13	9	14	13	7	16	7	6	10	0.162606	0.9900	NonOverlappingTemplate
14	7	13	10	20	6	4	9	10	7	0.020548	0.9700	NonOverlappingTemplate
12	9	15	11	5	12	10	12	5	9	0.437274	0.9800	NonOverlappingTemplate
15	10	7	9	13	13	10	2	10	11	0.224821	0.9800	NonOverlappingTemplate
10	10	6	16	8	8	6	13	13	10	0.401199	1.0000	NonOverlappingTemplate
6	10	11	11	10	13	13	7	13	6	0.637119	0.9900	NonOverlappingTemplate
10	8	11	11	9	7	11	10	10	13	0.978072	1.0000	NonOverlappingTemplate
11	13	7	10	9	5	11	11	11	12	0.816537	0.9900	NonOverlappingTemplate
10	17	8	11	9	4	9	10	10	12	0.383827	0.9900	NonOverlappingTemplate
12	10	8	8	11	12	13	11	5	10	0.816537	1.0000	NonOverlappingTemplate
13	9	7	12	14	8	7	5	11	14	0.401199	0.9800	NonOverlappingTemplate
11	12	6	12	14	5	8	11	12	9	0.574903	0.9900	NonOverlappingTemplate
7	11	19	13	12	9	10	7	8	4	0.080519	1.0000	NonOverlappingTemplate
11	9	10	8	11	8	13	8	10	12	0.971699	0.9900	NonOverlappingTemplate
8	9	13	8	7	13	5	14	11	12	0.514124	0.9800	NonOverlappingTemplate
8	7	13	17	11	6	9	10	12	7	0.334538	0.9900	NonOverlappingTemplate
10	9	11	17	10	11	8	7	2	15	0.080519	1.0000	NonOverlappingTemplate
7	10	13	13	10	11	8	10	8	10	0.935716	1.0000	NonOverlappingTemplate
6	14	13	9	6	12	11	6	13	10	0.455937	1.0000	NonOverlappingTemplate
8	5	11	16	9	9	10	14	9	9	0.474986	0.9900	NonOverlappingTemplate
10	14	3	9	14	13	10	7	12	8	0.289667	0.9900	NonOverlappingTemplate
7	12	15	8	12	10	7	8	9	12	0.699313	1.0000	NonOverlappingTemplate
11	11	17	5	7	10	11	11	6	11	0.319084	0.9800	NonOverlappingTemplate
14	17	7	7	11	11	9	9	4	11	0.191687	0.9700	NonOverlappingTemplate
6	13	10	9	11	9	16	13	8	5	0.334538	0.9800	NonOverlappingTemplate
9	13	11	12	9	7	7	6	9	17	0.350485	1.0000	NonOverlappingTemplate
10	12	13	13	6	9	7	9	14	7	0.595549	0.9900	NonOverlappingTemplate
9	13	5	14	9	11	13	9	8	9	0.657933	0.9900	NonOverlappingTemplate
6	8	7	9	12	13	10	10	16	9	0.534146	1.0000	NonOverlappingTemplate
10	4	11	12	7	10	9	16	16	5	0.096578	1.0000	NonOverlappingTemplate
9	13	8	10	10	16	5	8	13	8	0.419021	1.0000	NonOverlappingTemplate
7	8	9	11	14	7	12	12	9	11	0.834308	1.0000	NonOverlappingTemplate
15	4	9	11	11	7	9	9	15	10	0.350485	1.0000	NonOverlappingTemplate
10	11	14	9	10	9	13	8	8	8	0.911413	0.9900	NonOverlappingTemplate
11	12	13	7	11	9	12	16	4	5	0.181557	0.9900	NonOverlappingTemplate
11	7	12	10	10	12	12	10	9	7	0.955835	0.9800	NonOverlappingTemplate
11	10	10	10	10	11	7	12	10	9	0.996335	0.9800	NonOverlappingTemplate

```
 14   8  11   7  13   8  11   7  13   8  0.678686   1.0000    NonOverlappingTemplate
 10   5  16   9  10   9   6   9  11  15  0.304126   0.9900    NonOverlappingTemplate
 12   9  13   6  11   9  12  10  10   8  0.911413   0.9900    NonOverlappingTemplate
  9   7   7  14   8  13  12  10  13   7  0.637119   0.9900    NonOverlappingTemplate
 13   9  15  15  11   9   4  11  10   3  0.096578   1.0000    NonOverlappingTemplate
 16   9   8  13  11  12  10   3   7  11  0.249284   0.9800    NonOverlappingTemplate
  5   7  13   8   9   8  15  14  14   7  0.224821   0.9900    NonOverlappingTemplate
 11  11   5  15   8   8  13   9  12   8  0.554420   0.9800    NonOverlappingTemplate
  8   5  12  13  14  12   8   8  11   9  0.616305   0.9900    NonOverlappingTemplate
 13  12   7  12   8   6  11   9  10  12  0.816537   0.9800    NonOverlappingTemplate
  8   8  11  13  11  11   9   9  13   7  0.911413   0.9900    NonOverlappingTemplate
 13   7  10   7  12   8  11  13  13   6  0.637119   0.9700    NonOverlappingTemplate
 11  11  14   9  10   6   9  12   7  11  0.834308   0.9900    NonOverlappingTemplate
 12  10   9  15   5   8  12  10  11   8  0.657933   0.9900    NonOverlappingTemplate
  9  14  10  10   6  11  13  11   3  13  0.334538   0.9700    NonOverlappingTemplate
 11  10  12   4   9   9  11  11  11  12  0.834308   1.0000    NonOverlappingTemplate
 12   9   8  11   9  14  15   3  10   9  0.334538   0.9900    NonOverlappingTemplate
 13   9  10   9   8   9  11  11  11   9  0.991468   0.9700    NonOverlappingTemplate
 15   6   7  10   5  13  13  10  14   7  0.224821   0.9900    NonOverlappingTemplate
  9  12  11   7  11   9   7  12  10  12  0.946308   0.9900    NonOverlappingTemplate
  9   7  10  14  15  11  11   9   7   7  0.616305   0.9900    NonOverlappingTemplate
  7   9  15  14   6  13   8  11  13   4  0.181557   0.9800    NonOverlappingTemplate
  6   8  11  11   8   6  11  11  15  13  0.554420   0.9800    NonOverlappingTemplate
 11  12  12  13   7   8   9  11   5  12  0.719747   0.9800    NonOverlappingTemplate
  3  11  13  12   8  18   8   8   8  11  0.108791   0.9900    NonOverlappingTemplate
  8  10   9   4  10  12  14  10  14   9  0.554420   1.0000    NonOverlappingTemplate
 13  10  13   7   6  16  10   8   8   9  0.455937   0.9900    OverlappingTemplate
 11  10  10   8  11  14  10   5   9  12  0.816537   0.9900    Universal
 10  11   8  13  12   5  10  11   8  12  0.816537   1.0000    ApproximateEntropy
  7   8   7   4   6   4   7   8  10   7  0.739918   0.9853    RandomExcursions
  7   7   7   4   5  10   8  11   5   4  0.378138   0.9706    RandomExcursions
  5   6  10  10   9   7   4   7   3   7  0.378138   0.9853    RandomExcursions
  7   4   7   7  13   3   5  11   8   3  0.043745   1.0000    RandomExcursions
  5   5   7   5   6   9   8  10   8   5  0.706149   1.0000    RandomExcursions
  5   5   9   3   6   8  10   7   8   7  0.568055   0.9853    RandomExcursions
  7   1  13   6   9   9   3   7   7   6  0.043745   0.9853    RandomExcursions
  5   4   8   5  10   5   9   7   7   8  0.637119   0.9853    RandomExcursions
  6  10   5   4   7   6   7   9  10   4  0.468595   0.9853    RandomExcursionsVariant
  6  10   6   7   5   7   5   7   8   7  0.888137   0.9853    RandomExcursionsVariant
  6   9   7   9   6   3   8  11   3   6  0.275709   0.9853    RandomExcursionsVariant
  8  10   5   7   9   2   7   6   8   6  0.468595   1.0000    RandomExcursionsVariant
  9  10   6   5   6   6   5   7   7   7  0.834308   1.0000    RandomExcursionsVariant
 10  10   7   2   7   6   6  10   4   6  0.232760   1.0000    RandomExcursionsVariant
  7  11   6   4   9   3   6   6   4  12  0.100508   0.9853    RandomExcursionsVariant
  8  11   3   7   5  10   6   6   6   6  0.407091   1.0000    RandomExcursionsVariant
  4  13   5   5   8   6   9   6   7   5  0.232760   0.9853    RandomExcursionsVariant
  6   5   8   9   6   5   5  11   8   5  0.568055   1.0000    RandomExcursionsVariant
 11   4   1   6  11   5   7   5  12   6  0.020085   0.9853    RandomExcursionsVariant
 10   5   4   5   8   3  16   5   5   7  0.006196   0.9853    RandomExcursionsVariant
  8   5   7   8   6   6   3   9   6  10  0.602458   1.0000    RandomExcursionsVariant
  6   8   9   4   7   6   4   9   6   9  0.671779   1.0000    RandomExcursionsVariant
  8   3  10   9   6   6   2   9  10   5  0.148094   1.0000    RandomExcursionsVariant
  8   7   7   5  11   6   6   5   7   6  0.772760   0.9853    RandomExcursionsVariant
  7   8   9   5   7   7   8   7   6   4  0.888137   0.9853    RandomExcursionsVariant
  5   9   9   7   6   6   5   8   8   5  0.834308   0.9853    RandomExcursionsVariant
 12   9  17  12   8  11   6  12   5   8  0.262249   0.9800    Serial
 11  16  11  11  12   9   8   5   9   8  0.554420   0.9800    Serial
  9   7  10   9  12  11   9   8  15  10  0.867692   1.0000    LinearComplexity
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
The minimum pass rate for each statistical test with the exception of the
random excursion (variant) test is approximately = 0.960150 for a
sample size = 100 binary sequences.
The minimum pass rate for the random excursion (variant) test
is approximately 0.953802 for a sample size = 68 binary sequences.
For further guidelines construct a probability table using the MAPLE program
provided in the addendum section of the documentation.
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
```

Результати тестування розширеного матричного перетворення константи зі значенням 150

RESULTS FOR THE UNIFORMITY OF P-VALUES AND THE PROPORTION OF PASSING SEQUENCES

generator is <V_R_150.bin>

C1	C2	C3	C4	C5	C6	C7	C8	C9	C10	P-VALUE	PROPORTION	STATISTICAL TEST
6	9	9	18	14	11	7	9	11	6	0.181557	1.0000	Frequency
15	9	8	12	13	8	10	12	9	4	0.455937	1.0000	BlockFrequency
7	11	9	13	17	9	11	8	6	9	0.419021	1.0000	CumulativeSums
5	12	16	10	6	9	14	11	7	10	0.289667	1.0000	CumulativeSums
10	11	15	11	6	9	11	11	8	8	0.798139	0.9900	Runs
11	13	13	12	9	8	10	6	13	5	0.554420	0.9700	LongestRun
10	14	8	10	13	8	6	15	7	9	0.494392	1.0000	Rank
3	4	7	8	12	15	12	12	12	15	0.058984	1.0000	FFT
5	9	9	11	11	11	11	6	15	12	0.574903	0.9900	NonOverlappingTemplate
11	13	11	10	8	7	14	13	7	6	0.595549	0.9700	NonOverlappingTemplate
12	9	6	10	10	5	10	11	15	12	0.574903	0.9800	NonOverlappingTemplate
7	7	12	14	9	12	14	10	8	7	0.616305	0.9800	NonOverlappingTemplate
13	11	12	9	11	8	7	9	8	12	0.924076	0.9800	NonOverlappingTemplate
10	9	11	8	10	11	8	13	6	14	0.816537	0.9900	NonOverlappingTemplate
11	13	12	11	9	9	8	8	10	9	0.978072	0.9700	NonOverlappingTemplate
7	9	12	6	10	12	8	14	14	8	0.595549	1.0000	NonOverlappingTemplate
11	12	9	2	12	11	15	9	6	13	0.181557	0.9900	NonOverlappingTemplate
15	6	10	11	10	14	9	6	13	6	0.350485	0.9800	NonOverlappingTemplate
9	13	9	5	12	14	9	7	10	12	0.637119	0.9800	NonOverlappingTemplate
11	5	7	12	13	7	16	7	13	9	0.262249	0.9800	NonOverlappingTemplate
12	9	9	9	9	11	12	12	4	13	0.719747	0.9900	NonOverlappingTemplate
13	5	11	10	13	9	8	14	9	8	0.637119	1.0000	NonOverlappingTemplate
7	12	9	9	11	12	9	9	11	11	0.983453	1.0000	NonOverlappingTemplate
13	6	11	11	7	7	13	17	9	6	0.213309	0.9900	NonOverlappingTemplate
5	12	8	13	8	10	14	10	11	9	0.699313	1.0000	NonOverlappingTemplate
13	4	13	12	11	14	8	6	14	5	0.137282	0.9900	NonOverlappingTemplate
13	8	7	10	6	13	11	8	12	12	0.739918	0.9800	NonOverlappingTemplate
3	12	16	10	12	11	9	5	13	9	0.162606	1.0000	NonOverlappingTemplate
10	6	9	14	7	11	7	16	12	8	0.383827	0.9900	NonOverlappingTemplate
7	15	10	9	14	10	8	10	6	11	0.616305	1.0000	NonOverlappingTemplate
11	8	4	11	7	11	9	7	15	17	0.137282	0.9900	NonOverlappingTemplate
15	7	10	6	13	15	3	11	6	14	0.055361	0.9900	NonOverlappingTemplate
8	8	12	9	13	10	13	8	9	10	0.935716	0.9900	NonOverlappingTemplate
17	19	8	7	8	9	11	9	4	8	0.025193	0.9900	NonOverlappingTemplate
8	13	7	9	13	8	13	12	9	8	0.798139	1.0000	NonOverlappingTemplate
7	18	9	11	18	11	8	3	7	8	0.014550	0.9800	NonOverlappingTemplate
15	8	10	14	9	9	10	6	8	11	0.657933	1.0000	NonOverlappingTemplate
7	7	16	12	10	14	7	11	8	8	0.419021	1.0000	NonOverlappingTemplate
8	17	5	20	5	13	5	10	8	9	0.003996	0.9800	NonOverlappingTemplate
11	15	11	14	8	9	13	4	9	6	0.275709	0.9800	NonOverlappingTemplate
5	7	9	8	12	13	11	9	19	7	0.108791	1.0000	NonOverlappingTemplate
10	12	8	10	8	9	9	9	12	13	0.971699	0.9900	NonOverlappingTemplate
12	9	7	12	16	6	8	9	12	9	0.534146	1.0000	NonOverlappingTemplate
15	8	10	7	13	12	5	7	16	7	0.162606	1.0000	NonOverlappingTemplate
5	13	14	10	11	13	7	7	6	14	0.275709	0.9900	NonOverlappingTemplate
10	15	13	7	8	11	8	8	12	8	0.699313	0.9900	NonOverlappingTemplate
12	12	11	7	8	9	14	8	13	6	0.657933	0.9600	NonOverlappingTemplate
11	10	11	7	8	8	7	12	10	16	0.657933	1.0000	NonOverlappingTemplate
15	9	10	5	10	12	15	3	13	8	0.115387	0.9800	NonOverlappingTemplate
15	7	4	9	7	12	9	10	15	12	0.249284	0.9800	NonOverlappingTemplate
6	12	10	7	7	13	13	15	10	7	0.437274	1.0000	NonOverlappingTemplate
22	4	14	10	9	7	8	10	9	7	0.008879	0.9700	NonOverlappingTemplate
5	8	18	12	6	13	5	11	12	10	0.085587	1.0000	NonOverlappingTemplate
9	7	8	12	9	19	11	9	8	8	0.275709	1.0000	NonOverlappingTemplate
18	19	9	8	10	6	8	6	5	11	0.011791	0.9600	NonOverlappingTemplate
10	13	9	14	8	7	14	7	6	12	0.494392	0.9800	NonOverlappingTemplate
8	7	10	12	8	6	14	13	8	14	0.514124	1.0000	NonOverlappingTemplate
12	11	7	20	7	13	8	7	9	6	0.062821	0.9900	NonOverlappingTemplate
7	7	5	14	17	9	10	11	12	8	0.224821	0.9900	NonOverlappingTemplate

7	7	9	17	12	9	11	10	7	11	0.494392	0.9800	NonOverlappingTemplate
10	13	13	13	8	6	7	14	8	8	0.534146	0.9800	NonOverlappingTemplate
19	9	14	8	7	11	4	10	10	8	0.085587	0.9900	NonOverlappingTemplate
13	14	10	12	10	7	9	9	9	7	0.834308	0.9900	NonOverlappingTemplate
9	8	11	8	11	13	10	9	10	11	0.987896	0.9800	NonOverlappingTemplate
14	8	12	9	6	9	14	9	10	9	0.739918	0.9800	NonOverlappingTemplate
10	8	14	7	7	6	11	18	6	13	0.108791	0.9900	NonOverlappingTemplate
12	11	14	7	10	7	8	12	7	12	0.739918	1.0000	NonOverlappingTemplate
10	10	5	9	11	8	9	9	19	10	0.249284	1.0000	NonOverlappingTemplate
7	12	8	10	12	10	11	10	10	10	0.987896	1.0000	NonOverlappingTemplate
10	9	13	8	8	7	13	13	8	11	0.834308	1.0000	NonOverlappingTemplate
9	7	10	8	10	20	11	14	3	8	0.030806	1.0000	NonOverlappingTemplate
11	10	13	11	13	8	7	11	8	8	0.897763	1.0000	NonOverlappingTemplate
7	10	14	12	13	13	7	8	6	10	0.574903	0.9700	NonOverlappingTemplate
11	7	13	10	9	7	7	12	9	15	0.657933	0.9900	NonOverlappingTemplate
10	9	11	11	12	5	11	11	9	11	0.935716	0.9900	NonOverlappingTemplate
10	8	9	11	12	5	10	16	11	8	0.574903	1.0000	NonOverlappingTemplate
9	16	13	7	12	8	6	10	10	9	0.534146	0.9900	NonOverlappingTemplate
9	11	9	16	10	8	10	7	12	8	0.739918	0.9700	NonOverlappingTemplate
9	8	15	10	11	8	17	13	4	5	0.080519	0.9800	NonOverlappingTemplate
16	12	10	11	12	8	7	12	7	5	0.383827	0.9900	NonOverlappingTemplate
6	5	9	16	10	14	11	7	7	15	0.129620	0.9900	NonOverlappingTemplate
9	12	10	9	9	10	11	7	11	12	0.987896	0.9900	NonOverlappingTemplate
5	9	9	11	11	12	10	6	15	12	0.554420	0.9900	NonOverlappingTemplate
10	13	10	11	9	13	11	6	10	7	0.867692	1.0000	NonOverlappingTemplate
5	8	9	14	9	12	10	11	10	12	0.779188	1.0000	NonOverlappingTemplate
7	9	8	16	12	11	7	11	11	8	0.637119	0.9900	NonOverlappingTemplate
12	6	10	3	11	6	16	10	11	15	0.096578	1.0000	NonOverlappingTemplate
8	14	15	9	11	10	13	7	6	7	0.437274	0.9800	NonOverlappingTemplate
12	6	9	8	14	11	15	7	7	11	0.474986	0.9900	NonOverlappingTemplate
13	9	7	11	10	5	7	21	12	5	0.015598	0.9900	NonOverlappingTemplate
7	9	7	12	14	9	8	9	6	19	0.115387	1.0000	NonOverlappingTemplate
14	5	7	12	6	17	11	6	11	11	0.129620	0.9900	NonOverlappingTemplate
10	13	6	8	9	8	9	10	13	14	0.739918	0.9900	NonOverlappingTemplate
5	10	8	9	10	7	12	11	16	12	0.494392	1.0000	NonOverlappingTemplate
10	11	12	13	6	10	10	12	9	7	0.883171	0.9900	NonOverlappingTemplate
5	15	7	15	6	10	11	11	10	10	0.334538	1.0000	NonOverlappingTemplate
13	8	13	9	9	7	9	14	10	8	0.798139	0.9900	NonOverlappingTemplate
10	7	7	14	12	13	12	6	9	10	0.657933	0.9900	NonOverlappingTemplate
10	11	13	11	7	10	12	15	7	4	0.401199	0.9900	NonOverlappingTemplate
7	11	10	6	11	8	18	8	10	11	0.350485	1.0000	NonOverlappingTemplate
5	15	9	12	9	14	9	8	6	13	0.334538	1.0000	NonOverlappingTemplate
8	11	12	12	1	8	22	14	7	5	0.000600	0.9800	NonOverlappingTemplate
8	13	9	9	14	4	10	11	12	10	0.616305	0.9900	NonOverlappingTemplate
9	15	10	7	9	9	11	12	10	8	0.867692	0.9900	NonOverlappingTemplate
13	7	9	10	11	15	8	9	8	10	0.798139	0.9700	NonOverlappingTemplate
10	12	4	9	7	9	11	7	17	14	0.181557	1.0000	NonOverlappingTemplate
11	10	9	9	10	9	10	12	15	5	0.759756	1.0000	NonOverlappingTemplate
12	10	7	11	13	11	7	8	13	8	0.834308	0.9800	NonOverlappingTemplate
11	11	10	11	5	10	7	8	13	14	0.678686	0.9800	NonOverlappingTemplate
10	7	8	14	9	14	15	6	6	11	0.319084	0.9800	NonOverlappingTemplate
11	4	17	7	11	7	19	10	9	5	0.011791	0.9700	NonOverlappingTemplate
5	7	16	11	9	10	8	12	10	12	0.494392	1.0000	NonOverlappingTemplate
7	9	3	10	8	8	16	12	11	16	0.108791	1.0000	NonOverlappingTemplate
12	10	13	13	11	9	8	8	4	12	0.616305	0.9900	NonOverlappingTemplate
8	9	9	13	7	9	11	12	8	14	0.834308	1.0000	NonOverlappingTemplate
10	9	8	8	7	9	5	13	20	11	0.080519	1.0000	NonOverlappingTemplate
7	9	3	10	10	10	12	10	16	13	0.289667	0.9900	NonOverlappingTemplate
10	6	6	11	20	7	6	11	15	8	0.026948	1.0000	NonOverlappingTemplate
8	8	4	6	8	9	25	12	9	11	0.000513	0.9900	NonOverlappingTemplate
13	13	9	9	9	11	9	12	11	4	0.699313	0.9800	NonOverlappingTemplate
8	8	12	13	13	9	8	9	10	10	0.935716	0.9700	NonOverlappingTemplate
15	12	10	8	5	13	11	8	10	8	0.574903	0.9900	NonOverlappingTemplate
13	13	3	9	17	12	9	12	3	9	0.040108	0.9700	NonOverlappingTemplate
7	5	12	17	14	10	8	11	7	9	0.224821	0.9800	NonOverlappingTemplate
5	11	12	11	11	9	13	10	9	9	0.883171	0.9800	NonOverlappingTemplate
10	9	9	10	13	7	6	11	14	11	0.798139	0.9900	NonOverlappingTemplate
8	9	10	8	13	7	8	12	8	17	0.455937	0.9900	NonOverlappingTemplate
9	9	11	6	11	11	10	11	11	11	0.983453	1.0000	NonOverlappingTemplate
7	11	11	6	18	9	10	11	8	9	0.366918	0.9900	NonOverlappingTemplate
12	6	15	8	17	8	13	5	9	7	0.102526	0.9900	NonOverlappingTemplate

```
  8   8  15  10  13  11   7   8   9  11  0.759756   0.9900    NonOverlappingTemplate
 11   6   7  10   8  15  11  12   9  11  0.719747   1.0000    NonOverlappingTemplate
  8   9  14   7  11   7   8  14  14   8  0.534146   1.0000    NonOverlappingTemplate
  8  10   5  11  10   9   9  12  10  16  0.616305   0.9900    NonOverlappingTemplate
  9   5  10  11   8   7  14  13   9  14  0.514124   0.9900    NonOverlappingTemplate
 14   8  10  14   8   6   7  13   9  11  0.574903   0.9800    NonOverlappingTemplate
 19   7  10  14   8   7   5  11   7  12  0.071177   0.9700    NonOverlappingTemplate
  6   6  21   7  14  15   3  10  10   8  0.002374   1.0000    NonOverlappingTemplate
 16  14   9  12   9   8  12   5   7   8  0.319084   1.0000    NonOverlappingTemplate
  9   9  10   6   7  13   7  17  13   9  0.319084   0.9700    NonOverlappingTemplate
 11   8  13  10   6   8  15   9  13   7  0.554420   1.0000    NonOverlappingTemplate
 13  11  10  11   8   9   7   8  11  12  0.946308   0.9800    NonOverlappingTemplate
 19   8   6  12  14  10   8   9   8   6  0.102526   0.9600    NonOverlappingTemplate
  9  14  11   8   5  16  12   6   9  10  0.319084   0.9900    NonOverlappingTemplate
  9  15   7  10   8  11  12   7  14   7  0.554420   1.0000    NonOverlappingTemplate
  7  15  10   8   8   8  10  12   9  13  0.739918   1.0000    NonOverlappingTemplate
  8   5   6  10  21   9  12  13   6  10  0.020548   1.0000    NonOverlappingTemplate
 12  12  14   9   5  12   7   6  14   9  0.383827   0.9900    NonOverlappingTemplate
  9  11  10   6  13  16   9   8   8  10  0.616305   0.9700    NonOverlappingTemplate
 19  10   5   8   7  11   7  15   7  11  0.058984   0.9600    NonOverlappingTemplate
  7   7   8  11  11   8  15   9  12  12  0.719747   0.9800    NonOverlappingTemplate
  6  10  11   9  11  11  12   6  10  14  0.779188   1.0000    NonOverlappingTemplate
  9  10   8   9  13  14   6  11   7  13  0.678686   1.0000    NonOverlappingTemplate
  8   8  16   6   6  11  14  11   9  11  0.383827   0.9900    NonOverlappingTemplate
  7   7  16  11  12  10  10  10   7  10  0.657933   0.9900    NonOverlappingTemplate
  9  12   9  10   9   9  12   7  11  12  0.978072   0.9900    NonOverlappingTemplate
 10  12  12   9  12   9   9   6  10  11  0.955835   1.0000    OverlappingTemplate
 11  11  10  11   8   6  10   7  15  11  0.759756   0.9900    Universal
 10   8  11  10   7  11   9  10  13  11  0.978072   0.9700    ApproximateEntropy
 10   3   2   1   5   5   6  10  10   4  0.011791   0.9643    RandomExcursions
  9   9   5   5   7   7   5   3   3   3  0.319084   0.9821    RandomExcursions
  4   5   6   2  15   3   3   6   9   3  0.000954   1.0000    RandomExcursions
 10   7   6   1   5   5   2   6   7   7  0.171867   0.9464 *  RandomExcursions
  5   6   6   5   6   5   4   9   4   6  0.883171   1.0000    RandomExcursions
  6   7   3   5  10   2   4   7   8   4  0.236810   1.0000    RandomExcursions
  4   4   7   2   5   5  11   5   3  10  0.066882   1.0000    RandomExcursions
  4   3   5   4   6   7   7   5   6   9  0.699313   1.0000    RandomExcursions
  2  10  11   4   6   5   5   2   8   3  0.026948   1.0000    RandomExcursionsVariant
  5   9  10   5   1   8   4   5   5   4  0.137282   1.0000    RandomExcursionsVariant
  7   6  15   3   1   5   6   7   1   5  0.000600   0.9821    RandomExcursionsVariant
  8   6   7   7   2   6   6   4   5   5  0.739918   0.9643    RandomExcursionsVariant
  8   7   6   7   4   2   2   5   9   6  0.289667   1.0000    RandomExcursionsVariant
  6   9   5   4   8   4   6   6   4   4  0.699313   1.0000    RandomExcursionsVariant
  3   7   3   7   7  12   9   5   1   2  0.008879   0.9821    RandomExcursionsVariant
  3   5   5   8   8   7   4   8   4   4  0.574903   0.9821    RandomExcursionsVariant
  3   8   2   9   6   4   7   6   3   8  0.236810   1.0000    RandomExcursionsVariant
  6   7   5   6   2   6   9   4   5   6  0.657933   0.9821    RandomExcursionsVariant
  7   6   6   4   1   6   6   4   7   9  0.419021   1.0000    RandomExcursionsVariant
  2   8   7   7   7   3   4   5   3  10  0.171867   1.0000    RandomExcursionsVariant
  3   8   1   8   4   5   5   4  14   4  0.003712   1.0000    RandomExcursionsVariant
  3   7   4   5   3   9   6   4   9   6  0.383827   1.0000    RandomExcursionsVariant
  4   7   1   3   8   8   8   8   3   6  0.153763   1.0000    RandomExcursionsVariant
  5   2   5   6   4   7   9   4   7   7  0.534146   1.0000    RandomExcursionsVariant
  4   4   7   4  10   0   8   8   3   8  0.040108   1.0000    RandomExcursionsVariant
  5   4   7   4   4   6   7   8   6   5  0.883171   1.0000    RandomExcursionsVariant
  7   8  11  10  13  13   9  11   8  10  0.924076   1.0000    Serial
  2  11  12  12   7  14  13  14   6   9  0.122325   1.0000    Serial
  7  10  10   7  13  15  15   8   4  11  0.224821   0.9800    LinearComplexity
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
The minimum pass rate for each statistical test with the exception of the
random excursion (variant) test is approximately = 0.960150 for a
sample size = 100 binary sequences.
The minimum pass rate for the random excursion (variant) test
is approximately 0.950112 for a sample size = 56 binary sequences.
For further guidelines construct a probability table using the MAPLE program
provided in the addendum section of the documentation.
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
```

Результати тестування розширеного матричного перетворення над текстовою інформацією

RESULTS FOR THE UNIFORMITY OF P-VALUES AND THE PROPORTION OF PASSING SEQUENCES

generator is <V_R_TXT.bin>

C1	C2	C3	C4	C5	C6	C7	C8	C9	C10	P-VALUE	PROPORTION	STATISTICAL TEST
8	9	6	13	11	11	12	9	10	11	0.924076	1.0000	Frequency
10	12	5	6	8	17	11	15	9	7	0.145326	0.9800	BlockFrequency
6	15	11	10	8	8	16	9	13	4	0.153763	0.9900	CumulativeSums
9	12	3	10	12	9	11	13	13	8	0.514124	1.0000	CumulativeSums
16	14	8	12	7	9	5	9	11	9	0.366918	0.9800	Runs
10	13	13	12	7	11	13	6	9	6	0.595549	0.9900	LongestRun
10	7	8	10	12	14	14	7	11	7	0.657933	0.9900	Rank
0	3	6	11	15	7	15	20	10	13	0.000114	1.0000	FFT
8	13	10	7	10	12	7	7	13	13	0.719747	1.0000	NonOverlappingTemplate
4	11	7	10	13	12	9	12	9	13	0.595549	0.9900	NonOverlappingTemplate
15	4	13	7	7	12	9	11	16	6	0.102526	1.0000	NonOverlappingTemplate
10	10	6	11	8	8	8	10	17	12	0.514124	0.9900	NonOverlappingTemplate
11	5	5	13	11	11	10	10	11	13	0.616305	1.0000	NonOverlappingTemplate
13	11	13	15	9	6	8	6	4	15	0.115387	0.9900	NonOverlappingTemplate
8	9	8	9	14	11	16	14	5	6	0.213309	1.0000	NonOverlappingTemplate
5	13	11	11	10	6	14	11	9	10	0.637119	0.9900	NonOverlappingTemplate
8	5	10	17	5	15	9	9	14	8	0.090936	0.9600	NonOverlappingTemplate
7	11	12	5	9	17	8	11	8	12	0.334538	0.9900	NonOverlappingTemplate
8	15	11	9	8	13	6	9	14	7	0.474986	1.0000	NonOverlappingTemplate
9	8	4	16	7	9	13	10	12	12	0.319084	0.9800	NonOverlappingTemplate
12	12	9	11	8	8	9	11	12	8	0.971699	0.9700	NonOverlappingTemplate
12	11	8	15	11	7	7	8	6	15	0.366918	1.0000	NonOverlappingTemplate
9	7	13	6	8	11	14	12	8	12	0.657933	0.9800	NonOverlappingTemplate
7	10	9	11	13	7	11	13	8	11	0.883171	0.9900	NonOverlappingTemplate
8	10	8	9	7	15	9	11	10	13	0.798139	0.9800	NonOverlappingTemplate
8	7	11	13	11	8	12	9	9	12	0.924076	0.9700	NonOverlappingTemplate
10	5	10	14	12	7	5	10	10	17	0.171867	0.9900	NonOverlappingTemplate
9	5	17	11	10	12	11	5	8	12	0.249284	0.9900	NonOverlappingTemplate
8	13	11	10	14	11	5	8	8	12	0.657933	0.9900	NonOverlappingTemplate
16	5	12	13	6	7	13	8	11	9	0.249284	0.9800	NonOverlappingTemplate
9	13	11	12	9	12	10	10	7	7	0.924076	1.0000	NonOverlappingTemplate
11	10	9	11	13	7	13	5	9	12	0.739918	0.9900	NonOverlappingTemplate
12	8	15	8	8	11	13	11	5	9	0.554420	0.9800	NonOverlappingTemplate
14	6	13	11	9	13	15	6	4	9	0.162606	0.9800	NonOverlappingTemplate
11	6	10	10	7	12	9	13	10	12	0.883171	1.0000	NonOverlappingTemplate
8	14	11	8	17	13	8	12	3	6	0.075719	1.0000	NonOverlappingTemplate
11	10	7	9	10	14	5	14	7	13	0.474986	1.0000	NonOverlappingTemplate
12	4	6	10	11	8	12	10	14	13	0.437274	0.9700	NonOverlappingTemplate
12	13	11	5	9	13	10	7	12	8	0.678686	1.0000	NonOverlappingTemplate
8	11	14	15	8	8	8	8	8	12	0.637119	0.9900	NonOverlappingTemplate
7	9	9	9	12	12	4	11	12	15	0.474986	1.0000	NonOverlappingTemplate
6	15	10	11	12	12	8	7	9	10	0.699313	0.9900	NonOverlappingTemplate
10	9	8	7	8	8	19	9	10	12	0.289667	0.9800	NonOverlappingTemplate
7	12	7	12	6	7	13	15	9	12	0.437274	0.9900	NonOverlappingTemplate
13	6	7	8	12	10	10	14	7	13	0.574903	0.9600	NonOverlappingTemplate
13	8	8	11	11	10	12	7	10	10	0.955835	0.9800	NonOverlappingTemplate
16	8	6	11	3	13	12	9	11	11	0.202268	0.9900	NonOverlappingTemplate
11	9	9	8	9	7	13	8	12	14	0.834308	0.9800	NonOverlappingTemplate
9	7	13	12	9	15	9	8	9	9	0.779188	1.0000	NonOverlappingTemplate
7	18	10	13	10	8	6	10	9	9	0.319084	1.0000	NonOverlappingTemplate
6	15	6	9	8	11	11	12	9	13	0.554420	1.0000	NonOverlappingTemplate
8	13	11	11	13	12	4	7	9	12	0.554420	0.9900	NonOverlappingTemplate
11	11	9	12	6	8	10	9	12	12	0.935716	0.9800	NonOverlappingTemplate
6	9	14	12	13	9	9	9	6	13	0.595549	1.0000	NonOverlappingTemplate
9	9	9	6	11	7	14	13	9	13	0.699313	1.0000	NonOverlappingTemplate
9	10	9	7	8	15	11	13	10	8	0.798139	1.0000	NonOverlappingTemplate
9	12	9	6	12	12	13	7	11	9	0.834308	0.9900	NonOverlappingTemplate
8	10	11	11	11	10	12	6	8	13	0.911413	1.0000	NonOverlappingTemplate

7	12	7	5	16	9	12	5	13	14	0.129620	1.0000	NonOverlappingTemplate
8	11	9	11	12	8	5	15	8	13	0.554420	0.9900	NonOverlappingTemplate
9	10	7	12	6	14	12	8	11	11	0.779188	0.9900	NonOverlappingTemplate
14	8	6	12	12	11	10	14	10	3	0.275709	0.9800	NonOverlappingTemplate
11	11	9	13	11	9	11	9	6	10	0.955835	0.9900	NonOverlappingTemplate
8	6	9	5	7	17	9	13	16	10	0.090936	1.0000	NonOverlappingTemplate
12	7	10	20	9	12	4	9	9	8	0.066882	0.9900	NonOverlappingTemplate
9	7	13	10	7	10	15	8	9	12	0.719747	0.9900	NonOverlappingTemplate
6	13	9	14	10	10	12	11	6	9	0.699313	0.9900	NonOverlappingTemplate
7	11	15	8	7	9	8	10	16	9	0.437274	1.0000	NonOverlappingTemplate
9	14	13	8	10	4	11	14	7	10	0.419021	1.0000	NonOverlappingTemplate
8	11	15	13	10	9	6	9	11	8	0.719747	1.0000	NonOverlappingTemplate
8	10	10	13	11	10	10	10	7	11	0.983453	0.9900	NonOverlappingTemplate
6	12	7	7	16	12	11	13	10	6	0.319084	0.9900	NonOverlappingTemplate
7	11	11	11	12	6	14	10	7	11	0.759756	0.9900	NonOverlappingTemplate
15	10	7	13	9	10	8	12	10	6	0.657933	1.0000	NonOverlappingTemplate
8	10	7	8	10	13	13	8	10	13	0.851383	0.9900	NonOverlappingTemplate
16	14	12	7	7	7	7	7	14	9	0.224821	0.9800	NonOverlappingTemplate
9	8	11	15	6	14	9	7	4	17	0.071177	1.0000	NonOverlappingTemplate
6	14	10	9	7	13	4	12	6	19	0.026948	0.9900	NonOverlappingTemplate
6	12	10	6	11	10	11	10	16	8	0.554420	1.0000	NonOverlappingTemplate
12	10	12	11	6	12	10	9	5	13	0.699313	0.9800	NonOverlappingTemplate
11	14	11	12	8	3	8	13	11	9	0.437274	1.0000	NonOverlappingTemplate
11	7	14	15	11	5	8	10	13	6	0.304126	0.9500 *	NonOverlappingTemplate
8	13	10	7	10	12	7	7	13	13	0.719747	1.0000	NonOverlappingTemplate
14	12	4	6	16	13	11	4	11	9	0.075719	0.9900	NonOverlappingTemplate
9	7	15	15	9	10	8	11	4	12	0.304126	1.0000	NonOverlappingTemplate
10	9	8	12	8	10	12	11	9	11	0.991468	0.9700	NonOverlappingTemplate
15	5	16	8	13	10	8	6	6	13	0.108791	0.9900	NonOverlappingTemplate
3	16	14	10	11	12	10	6	6	12	0.115387	0.9900	NonOverlappingTemplate
7	13	11	12	8	11	12	9	9	8	0.924076	0.9900	NonOverlappingTemplate
11	10	12	10	7	8	13	6	14	9	0.739918	1.0000	NonOverlappingTemplate
12	12	13	6	8	11	10	5	9	14	0.534146	1.0000	NonOverlappingTemplate
4	8	16	12	12	13	8	9	9	9	0.350485	0.9900	NonOverlappingTemplate
16	6	8	7	7	11	12	13	8	12	0.383827	0.9800	NonOverlappingTemplate
13	11	13	11	6	13	9	9	7	8	0.739918	0.9800	NonOverlappingTemplate
12	9	6	13	13	7	13	10	7	10	0.678686	0.9800	NonOverlappingTemplate
7	9	11	6	7	16	10	12	9	13	0.474986	0.9900	NonOverlappingTemplate
12	11	7	10	9	14	11	11	5	10	0.759756	0.9800	NonOverlappingTemplate
11	12	7	19	10	8	9	11	8	5	0.162606	0.9800	NonOverlappingTemplate
12	16	8	11	8	14	6	10	3	12	0.145326	0.9900	NonOverlappingTemplate
9	18	9	11	9	5	12	6	9	12	0.224821	0.9900	NonOverlappingTemplate
11	7	5	11	15	7	14	12	10	8	0.401199	0.9900	NonOverlappingTemplate
10	6	10	9	15	9	14	7	11	9	0.637119	1.0000	NonOverlappingTemplate
8	10	16	9	7	8	16	8	5	13	0.171867	1.0000	NonOverlappingTemplate
14	9	15	8	7	7	10	11	7	12	0.554420	0.9900	NonOverlappingTemplate
11	7	10	1	13	13	9	12	10	14	0.162606	0.9900	NonOverlappingTemplate
9	15	13	5	7	12	11	11	9	8	0.534146	1.0000	NonOverlappingTemplate
9	12	11	14	14	6	9	7	12	6	0.494392	0.9900	NonOverlappingTemplate
9	15	12	6	9	10	13	12	5	9	0.474986	0.9900	NonOverlappingTemplate
13	13	9	9	5	10	10	10	10	11	0.867692	1.0000	NonOverlappingTemplate
12	13	7	12	10	5	11	15	9	6	0.401199	0.9700	NonOverlappingTemplate
9	12	15	8	10	8	9	14	8	7	0.657933	0.9900	NonOverlappingTemplate
13	12	15	14	15	5	6	14	5	1	0.003996	0.9900	NonOverlappingTemplate
15	7	7	7	7	12	10	12	13	10	0.554420	0.9900	NonOverlappingTemplate
7	10	5	9	9	12	14	9	14	11	0.595549	1.0000	NonOverlappingTemplate
12	13	9	6	13	8	4	12	9	14	0.350485	0.9800	NonOverlappingTemplate
10	9	8	11	7	8	19	6	10	12	0.213309	0.9900	NonOverlappingTemplate
9	7	7	7	11	12	12	14	13	8	0.678686	1.0000	NonOverlappingTemplate
11	6	6	8	21	9	10	7	12	10	0.045675	0.9900	NonOverlappingTemplate
9	10	9	16	9	8	13	10	8	8	0.739918	0.9900	NonOverlappingTemplate
7	10	14	6	11	10	12	12	10	8	0.798139	0.9800	NonOverlappingTemplate
16	15	6	6	5	9	13	10	8	12	0.137282	0.9500 *	NonOverlappingTemplate
13	20	9	7	6	10	8	10	7	10	0.096578	0.9900	NonOverlappingTemplate
13	8	11	7	11	6	14	10	7	13	0.595549	0.9900	NonOverlappingTemplate
16	11	16	8	8	10	7	12	6	6	0.181557	0.9900	NonOverlappingTemplate
13	11	12	11	8	10	11	9	10	5	0.867692	0.9900	NonOverlappingTemplate
9	8	8	10	8	13	9	9	11	15	0.834308	0.9800	NonOverlappingTemplate
11	13	11	12	8	10	11	5	10	9	0.867692	0.9900	NonOverlappingTemplate
6	8	10	12	17	11	4	13	11	8	0.191687	1.0000	NonOverlappingTemplate
13	5	15	13	7	4	10	12	9	12	0.202268	1.0000	NonOverlappingTemplate

```
 10   8   8  11   7   9  11  16  11   9  0.759756   0.9700    NonOverlappingTemplate
 17   6   9  11  11   8   9  14   6   9  0.304126   0.9800    NonOverlappingTemplate
  5  12  11  16   9  14   7   7  11   8  0.304126   1.0000    NonOverlappingTemplate
 14   9   8  10   7   8   9   9   8  18  0.319084   0.9800    NonOverlappingTemplate
 11  10   5  10   8  12   9  11   9  15  0.719747   1.0000    NonOverlappingTemplate
 11  10   9  10   9   7  11  11  10  12  0.994250   1.0000    NonOverlappingTemplate
  8   5   9  12   7   5  11  14  17  12  0.129620   0.9900    NonOverlappingTemplate
  5  13   7   8  16  11  13   6  10  11  0.275709   0.9900    NonOverlappingTemplate
 15  11   8  12   8  12  10   5  12   7  0.534146   0.9900    NonOverlappingTemplate
  8  13   9  18   9  10   6  13   7   7  0.202268   0.9800    NonOverlappingTemplate
  9  10  12   9  14  13  12   3  11   7  0.401199   1.0000    NonOverlappingTemplate
 11  12  10  12  13   9   7   8  10   8  0.935716   0.9900    NonOverlappingTemplate
 16  10  13   8   6  10   7   9  10  11  0.574903   0.9900    NonOverlappingTemplate
  6   5  10  10  10  12   9  11  13  14  0.616305   1.0000    NonOverlappingTemplate
  6   9  14  10  10  14   7   8   8  14  0.514124   1.0000    NonOverlappingTemplate
  4  11  11   6  12   7  11  18  11   9  0.145326   0.9900    NonOverlappingTemplate
  7  12  15   9  10  14   8  10   7   8  0.616305   1.0000    NonOverlappingTemplate
  8   5  14  16   8  13   8  11   7  10  0.289667   1.0000    NonOverlappingTemplate
  7  15  11  12   6  10  10  14   9   6  0.455937   0.9700    NonOverlappingTemplate
 14   8  13  11  12  16   9   4   9   4  0.108791   0.9900    NonOverlappingTemplate
  8   7  12  14   9   9   7  13   9  12  0.759756   0.9800    NonOverlappingTemplate
 10  11   6  12   7  13  12  10  11   8  0.851383   1.0000    NonOverlappingTemplate
  9  14   7  13  10  12  11   9   8   7  0.798139   1.0000    NonOverlappingTemplate
  4  13  15  10  13  11  13   5   8   8  0.202268   1.0000    NonOverlappingTemplate
 10   5  11  16  10  14   6   6  11  11  0.262249   1.0000    NonOverlappingTemplate
 15   8   8  12   7  12   8  13  10   7  0.616305   1.0000    NonOverlappingTemplate
 11   7  14  15  11   5   8  10  13   6  0.304126   0.9600    NonOverlappingTemplate
 11  11  11   6  13  10  10  12  11   5  0.759756   0.9900    OverlappingTemplate
 11  12   9   9  15   8  11  12   5   8  0.637119   1.0000    Universal
 12   7  10  10   8  13  12  12   8   8  0.897763   0.9700    ApproximateEntropy
 11   6   9   8   8   4   3   1   6   7  0.141256   0.9841    RandomExcursions
  7  10   5   9   5   3   5   8   7   4  0.551026   0.9683    RandomExcursions
  4   7  13   5   6   5   6   6   5   6  0.392456   0.9841    RandomExcursions
  4   9  10   3   8   3   7   7   6   6  0.452799   1.0000    RandomExcursions
  8   5   4   5  11   9   7   5   6   3  0.422034   0.9841    RandomExcursions
 11   6   3   3   5   9   4   8   8   6  0.287306   1.0000    RandomExcursions
  4   5   6  11   5   6   7  10   5   4  0.452799   0.9683    RandomExcursions
  4   4   4   9   5   7   5   8  11   6  0.452799   0.9841    RandomExcursions
  7   7  10   8   6   3   5   5   5   7  0.756476   0.9841    RandomExcursionsVariant
  4  14   6   5   7   4   4  10   3   6  0.046169   0.9841    RandomExcursionsVariant
  7   6   9   5   5   9   5   3   7   7  0.788728   0.9841    RandomExcursionsVariant
  6   9   5   7   4   6   7   7   6   6  0.970538   1.0000    RandomExcursionsVariant
  5   7  10   3   8   4   4   5  11   6  0.287306   1.0000    RandomExcursionsVariant
  6   4   5   6   8   7   6  11   3   7  0.585209   0.9841    RandomExcursionsVariant
  6   4   5   9   4   9   6   6   6   8  0.819544   1.0000    RandomExcursionsVariant
  6  10   6   4   5  10   6   6   5   5  0.689019   1.0000    RandomExcursionsVariant
  5   8  14   7   7   1  10   7   2   2  0.004045   0.9683    RandomExcursionsVariant
  7   6   8   7   3   7   8   6   4   7  0.900104   1.0000    RandomExcursionsVariant
  6   2   9   4   4   9   7   7   9   6  0.452799   1.0000    RandomExcursionsVariant
  5   3   5   5   7  10   5   9   9   5  0.517442   1.0000    RandomExcursionsVariant
  4   5   5   8   7  11   7   2   5   9  0.311542   0.9841    RandomExcursionsVariant
  4   8   7   6   5   9   7   3   5   9  0.689019   0.9841    RandomExcursionsVariant
  5   7   9   5   6   5   3   7  10   6  0.689019   0.9841    RandomExcursionsVariant
  5   7   8   8   4   6   9   3   5   8  0.723129   0.9841    RandomExcursionsVariant
  6   3  10   6   6   8   9   5   5   5  0.654467   1.0000    RandomExcursionsVariant
  7   5   5   6   6   8   9   4   8   5  0.900104   1.0000    RandomExcursionsVariant
 13  12  11  11   8  13   6   4  12  10  0.494392   0.9900    Serial
 16  13  12   8   7   5   9  13   7  10  0.304126   0.9600    Serial
  5   9   7  12  10  10   8  17  10  12  0.383827   0.9900    LinearComplexity
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
The minimum pass rate for each statistical test with the exception of the
random excursion (variant) test is approximately = 0.960150 for a
sample size = 100 binary sequences.
The minimum pass rate for the random excursion (variant) test
is approximately 0.952393 for a sample size = 63 binary sequences.
For further guidelines construct a probability table using the MAPLE program
provided in the addendum section of the documentation.
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
```

Результати тестування перетворення невипадкової монотонно зростаючої послідовності з циклом повторення 64 байти на основі алгоритму на основі комбінації матричних та розширених матричних операцій

RESULTS FOR THE UNIFORMITY OF P-VALUES AND THE PROPORTION OF PASSING SEQUENCES

generator is <V_MR_64.bin>

C1	C2	C3	C4	C5	C6	C7	C8	C9	C10	P-VALUE	PROPORTION	STATISTICAL TEST
4	11	13	13	10	15	9	5	14	6	0.129620	1.0000	Frequency
13	11	7	9	10	6	13	6	10	15	0.474986	0.9900	BlockFrequency
7	6	10	14	12	14	6	5	16	10	0.129620	1.0000	CumulativeSums
8	9	7	13	14	14	10	12	7	6	0.494392	1.0000	CumulativeSums
11	8	8	7	11	12	13	10	9	11	0.946308	0.9900	Runs
14	8	8	4	9	8	9	17	11	12	0.213309	0.9900	LongestRun
8	10	10	13	11	7	10	11	9	11	0.978072	1.0000	Rank
1	7	14	9	11	16	11	10	10	11	0.102526	1.0000	FFT
10	17	12	9	11	5	12	8	11	5	0.249284	0.9700	NonOverlappingTemplate
8	6	9	10	19	6	13	13	7	9	0.102526	1.0000	NonOverlappingTemplate
8	13	6	9	10	6	15	11	12	10	0.574903	0.9800	NonOverlappingTemplate
11	13	5	8	11	8	10	14	9	11	0.719747	1.0000	NonOverlappingTemplate
9	12	10	10	9	5	12	14	7	12	0.699313	1.0000	NonOverlappingTemplate
8	6	8	11	10	9	10	9	14	15	0.657933	1.0000	NonOverlappingTemplate
13	15	6	6	12	13	7	10	9	9	0.437274	0.9700	NonOverlappingTemplate
11	9	6	13	7	14	11	7	12	10	0.678686	0.9900	NonOverlappingTemplate
10	10	9	9	15	8	8	11	9	11	0.924076	0.9800	NonOverlappingTemplate
7	14	11	10	7	8	7	12	8	16	0.419021	1.0000	NonOverlappingTemplate
12	6	14	11	11	11	10	6	8	11	0.739918	0.9800	NonOverlappingTemplate
5	9	14	8	13	6	11	12	9	13	0.474986	1.0000	NonOverlappingTemplate
9	7	10	11	9	10	8	12	14	10	0.935716	0.9900	NonOverlappingTemplate
8	6	17	11	13	11	10	7	6	11	0.304126	0.9800	NonOverlappingTemplate
11	7	13	13	8	6	13	9	11	9	0.739918	0.9800	NonOverlappingTemplate
13	10	8	5	14	7	15	4	12	12	0.153763	0.9900	NonOverlappingTemplate
12	8	8	11	10	11	12	7	15	6	0.657933	0.9900	NonOverlappingTemplate
10	15	11	6	4	10	13	9	8	14	0.289667	0.9600	NonOverlappingTemplate
8	14	9	10	11	11	8	8	8	13	0.883171	1.0000	NonOverlappingTemplate
6	6	12	9	13	11	9	16	7	11	0.401199	1.0000	NonOverlappingTemplate
11	8	11	9	14	6	15	7	9	10	0.595549	1.0000	NonOverlappingTemplate
15	8	13	11	7	11	9	12	8	6	0.595549	0.9800	NonOverlappingTemplate
5	6	10	9	13	12	10	12	11	12	0.699313	0.9900	NonOverlappingTemplate
14	7	10	10	11	10	7	4	15	12	0.350485	0.9800	NonOverlappingTemplate
9	10	16	8	15	6	8	8	9	11	0.419021	1.0000	NonOverlappingTemplate
7	12	11	9	16	12	9	6	11	7	0.514124	0.9900	NonOverlappingTemplate
9	12	12	6	13	12	10	9	8	9	0.883171	0.9900	NonOverlappingTemplate
15	8	8	9	10	12	12	9	11	6	0.739918	1.0000	NonOverlappingTemplate
8	7	14	8	9	9	10	17	8	10	0.455937	0.9700	NonOverlappingTemplate
7	7	14	6	9	11	10	9	11	16	0.437274	0.9900	NonOverlappingTemplate
12	14	11	9	7	9	14	9	6	9	0.678686	0.9900	NonOverlappingTemplate
8	10	14	11	14	11	5	10	10	7	0.616305	0.9900	NonOverlappingTemplate
10	9	8	12	8	8	11	18	7	9	0.419021	0.9900	NonOverlappingTemplate
16	10	6	7	9	11	8	8	18	7	0.108791	0.9900	NonOverlappingTemplate
9	9	12	15	11	13	9	8	9	5	0.616305	1.0000	NonOverlappingTemplate
10	12	17	8	6	5	11	11	11	9	0.334538	0.9600	NonOverlappingTemplate
9	6	6	9	8	13	15	18	10	6	0.085587	0.9900	NonOverlappingTemplate
8	14	8	11	8	8	16	13	8	6	0.366918	1.0000	NonOverlappingTemplate
7	9	10	9	10	15	9	10	15	6	0.554420	0.9800	NonOverlappingTemplate
7	11	11	14	6	11	6	9	12	13	0.595549	1.0000	NonOverlappingTemplate
11	7	11	5	8	10	15	8	13	12	0.514124	0.9800	NonOverlappingTemplate
6	6	10	13	8	15	10	13	7	12	0.419021	0.9900	NonOverlappingTemplate
3	10	9	8	15	12	18	7	8	10	0.066882	1.0000	NonOverlappingTemplate
12	13	6	10	8	5	11	11	14	10	0.574903	1.0000	NonOverlappingTemplate
16	7	10	15	10	11	8	12	6	5	0.213309	1.0000	NonOverlappingTemplate
8	18	13	7	6	11	11	8	11	7	0.224821	1.0000	NonOverlappingTemplate
9	7	9	12	14	9	7	12	11	10	0.867692	1.0000	NonOverlappingTemplate
11	14	10	13	11	3	9	11	11	7	0.455937	1.0000	NonOverlappingTemplate
10	8	6	13	11	9	13	11	12	7	0.798139	0.9900	NonOverlappingTemplate

9	10	11	8	9	12	7	9	9	16	0.759756	0.9800	NonOverlappingTemplate
10	13	10	7	14	8	6	9	12	11	0.739918	0.9900	NonOverlappingTemplate
5	12	7	8	12	11	14	7	16	8	0.262249	1.0000	NonOverlappingTemplate
9	13	14	9	7	8	6	13	10	11	0.678686	1.0000	NonOverlappingTemplate
12	11	11	12	9	6	9	11	7	12	0.897763	0.9800	NonOverlappingTemplate
6	7	20	6	5	9	11	14	17	5	0.002203	1.0000	NonOverlappingTemplate
5	6	12	18	8	16	5	4	13	13	0.006661	0.9900	NonOverlappingTemplate
16	10	8	14	14	5	8	8	14	3	0.048716	0.9900	NonOverlappingTemplate
13	5	10	12	10	6	13	11	8	12	0.616305	1.0000	NonOverlappingTemplate
13	11	8	2	11	10	10	9	17	9	0.162606	0.9900	NonOverlappingTemplate
11	17	12	11	9	10	8	7	9	6	0.474986	1.0000	NonOverlappingTemplate
6	5	10	19	10	8	11	16	6	9	0.035174	0.9900	NonOverlappingTemplate
13	15	2	7	15	9	9	10	10	10	0.145326	0.9700	NonOverlappingTemplate
9	10	14	10	11	8	10	12	4	12	0.678686	0.9900	NonOverlappingTemplate
10	6	15	12	8	10	11	9	7	12	0.699313	1.0000	NonOverlappingTemplate
13	7	13	7	14	5	10	6	15	10	0.224821	1.0000	NonOverlappingTemplate
7	12	9	8	13	9	16	11	7	8	0.554420	1.0000	NonOverlappingTemplate
9	12	7	7	6	11	9	12	10	17	0.401199	0.9900	NonOverlappingTemplate
9	11	14	6	7	10	7	11	16	9	0.437274	0.9900	NonOverlappingTemplate
9	10	11	9	8	7	7	14	10	15	0.678686	0.9900	NonOverlappingTemplate
7	13	11	7	4	9	13	13	13	10	0.419021	0.9900	NonOverlappingTemplate
8	10	7	13	6	14	10	13	12	7	0.574903	1.0000	NonOverlappingTemplate
7	6	15	9	10	10	11	9	13	10	0.719747	0.9900	NonOverlappingTemplate
11	6	8	5	17	15	8	6	11	13	0.090936	0.9700	NonOverlappingTemplate
3	11	11	7	11	10	14	13	6	14	0.224821	1.0000	NonOverlappingTemplate
10	17	12	9	11	5	12	8	11	5	0.249284	0.9700	NonOverlappingTemplate
7	17	13	13	7	9	9	8	9	8	0.383827	1.0000	NonOverlappingTemplate
9	10	8	12	9	11	6	12	15	8	0.739918	0.9800	NonOverlappingTemplate
7	13	8	5	15	8	11	16	11	6	0.162606	0.9800	NonOverlappingTemplate
17	11	10	9	7	13	10	12	7	4	0.224821	0.9600	NonOverlappingTemplate
11	11	9	9	8	7	11	8	17	9	0.616305	1.0000	NonOverlappingTemplate
12	9	8	13	11	6	10	9	16	6	0.455937	0.9700	NonOverlappingTemplate
11	14	5	11	6	9	9	10	7	18	0.145326	0.9900	NonOverlappingTemplate
10	8	12	7	17	11	10	6	7	12	0.383827	1.0000	NonOverlappingTemplate
10	9	8	10	8	14	9	8	16	8	0.637119	0.9700	NonOverlappingTemplate
7	7	13	10	7	14	7	13	12	10	0.595549	0.9800	NonOverlappingTemplate
7	10	11	7	9	10	8	13	11	14	0.834308	1.0000	NonOverlappingTemplate
15	5	7	12	9	15	11	12	8	6	0.249284	0.9900	NonOverlappingTemplate
14	8	6	12	9	7	8	10	8	18	0.202268	0.9700	NonOverlappingTemplate
6	6	14	13	9	7	13	17	6	9	0.115387	0.9900	NonOverlappingTemplate
12	13	10	9	8	12	6	13	7	10	0.779188	0.9900	NonOverlappingTemplate
9	10	12	5	19	12	8	9	5	11	0.102526	0.9900	NonOverlappingTemplate
10	9	7	13	9	11	11	6	15	9	0.699313	0.9800	NonOverlappingTemplate
9	9	15	5	15	12	7	13	6	9	0.236810	1.0000	NonOverlappingTemplate
14	11	6	8	11	8	10	17	6	9	0.289667	1.0000	NonOverlappingTemplate
5	9	8	11	11	14	11	7	12	12	0.678686	0.9900	NonOverlappingTemplate
11	13	12	10	8	7	6	12	11	10	0.851383	1.0000	NonOverlappingTemplate
15	8	11	7	14	9	10	15	4	7	0.181557	0.9900	NonOverlappingTemplate
11	8	13	9	9	11	9	11	8	11	0.983453	1.0000	NonOverlappingTemplate
12	8	9	11	13	10	11	9	7	10	0.964295	0.9900	NonOverlappingTemplate
8	13	9	7	11	8	11	10	16	7	0.595549	0.9900	NonOverlappingTemplate
8	6	7	19	9	7	12	7	9	16	0.048716	0.9800	NonOverlappingTemplate
8	9	14	12	14	9	6	10	10	8	0.719747	0.9900	NonOverlappingTemplate
11	10	7	9	7	13	12	11	11	9	0.935716	1.0000	NonOverlappingTemplate
12	13	8	10	8	10	5	12	13	9	0.739918	0.9800	NonOverlappingTemplate
10	9	16	5	11	6	13	10	10	10	0.455937	0.9900	NonOverlappingTemplate
12	13	8	9	7	12	10	10	9	10	0.955835	0.9900	NonOverlappingTemplate
7	8	6	9	14	10	10	10	14	12	0.678686	1.0000	NonOverlappingTemplate
15	12	8	7	6	8	13	9	11	11	0.595549	0.9800	NonOverlappingTemplate
16	9	12	10	6	9	9	8	9	12	0.657933	0.9700	NonOverlappingTemplate
11	7	16	8	7	9	11	8	14	9	0.514124	0.9900	NonOverlappingTemplate
7	8	5	16	16	8	10	9	11	10	0.236810	1.0000	NonOverlappingTemplate
11	11	9	5	11	13	9	9	14	8	0.739918	0.9800	NonOverlappingTemplate
7	11	11	8	6	16	12	10	10	9	0.616305	0.9900	NonOverlappingTemplate
7	15	9	11	8	11	10	9	11	9	0.883171	0.9900	NonOverlappingTemplate
12	7	17	9	8	11	8	10	11	7	0.514124	0.9900	NonOverlappingTemplate
15	12	5	10	8	13	11	11	9	6	0.474986	0.9700	NonOverlappingTemplate
11	15	8	10	14	7	10	9	8	8	0.699313	0.9900	NonOverlappingTemplate
11	9	9	11	11	7	12	12	10	8	0.978072	0.9800	NonOverlappingTemplate
7	11	5	13	9	15	8	8	10	14	0.401199	1.0000	NonOverlappingTemplate
10	7	9	10	9	12	13	10	8	12	0.955835	1.0000	NonOverlappingTemplate

11	13	13	7	9	14	8	10	6	9	0.678686	1.0000	NonOverlappingTemplate
8	10	12	7	10	13	9	7	9	15	0.719747	1.0000	NonOverlappingTemplate
8	12	13	14	8	14	6	9	8	8	0.554420	0.9900	NonOverlappingTemplate
10	9	13	11	3	9	13	9	12	11	0.574903	0.9800	NonOverlappingTemplate
7	13	7	9	11	13	7	9	12	12	0.779188	1.0000	NonOverlappingTemplate
10	14	7	13	9	11	5	9	10	12	0.678686	0.9800	NonOverlappingTemplate
7	15	11	13	5	10	7	8	15	9	0.289667	1.0000	NonOverlappingTemplate
13	14	11	10	5	9	8	11	11	8	0.719747	0.9600	NonOverlappingTemplate
5	9	12	10	11	12	9	6	15	11	0.554420	1.0000	NonOverlappingTemplate
11	9	6	11	10	9	11	12	14	7	0.834308	0.9900	NonOverlappingTemplate
11	18	10	12	6	11	5	8	11	8	0.213309	1.0000	NonOverlappingTemplate
9	13	10	15	9	5	10	8	11	10	0.678686	0.9900	NonOverlappingTemplate
11	9	2	17	15	8	12	9	10	7	0.071177	0.9800	NonOverlappingTemplate
18	9	5	7	9	10	8	7	11	16	0.090936	1.0000	NonOverlappingTemplate
11	12	5	5	11	11	13	8	9	15	0.383827	0.9900	NonOverlappingTemplate
12	11	9	11	8	15	8	6	11	9	0.759756	1.0000	NonOverlappingTemplate
12	7	9	14	6	10	6	11	11	14	0.534146	0.9900	NonOverlappingTemplate
10	12	7	10	11	7	9	11	12	11	0.964295	1.0000	NonOverlappingTemplate
10	7	13	9	11	14	8	10	8	10	0.883171	1.0000	NonOverlappingTemplate
9	11	8	6	12	9	11	6	17	11	0.401199	1.0000	NonOverlappingTemplate
6	8	20	6	11	12	16	2	7	12	0.002559	0.9800	NonOverlappingTemplate
16	9	9	8	8	14	7	9	11	9	0.595549	0.9800	NonOverlappingTemplate
7	11	13	8	8	16	7	10	6	14	0.319084	0.9900	NonOverlappingTemplate
13	7	10	12	14	7	9	9	11	8	0.798139	0.9700	NonOverlappingTemplate
14	5	16	12	7	10	10	10	6	10	0.304126	0.9900	NonOverlappingTemplate
10	12	11	10	8	13	12	9	9	6	0.911413	0.9800	NonOverlappingTemplate
13	9	15	11	6	13	5	8	8	12	0.366918	0.9900	NonOverlappingTemplate
3	11	11	7	11	10	14	13	6	14	0.224821	1.0000	NonOverlappingTemplate
10	9	7	6	9	10	12	12	10	15	0.739918	0.9900	OverlappingTemplate
14	8	9	12	13	7	12	8	10	7	0.739918	1.0000	Universal
12	9	10	8	17	8	6	7	14	9	0.319084	0.9800	ApproximateEntropy
8	9	8	6	5	8	7	7	5	6	0.900104	1.0000	RandomExcursions
6	5	6	6	12	10	5	6	5	8	0.364146	1.0000	RandomExcursions
8	4	4	5	3	8	12	9	8	8	0.155209	0.9710	RandomExcursions
6	6	10	3	9	3	10	5	13	4	0.026648	1.0000	RandomExcursions
8	5	5	7	7	8	4	10	6	9	0.654467	1.0000	RandomExcursions
12	4	8	8	5	6	7	8	6	5	0.422034	1.0000	RandomExcursions
5	10	8	10	7	5	3	4	10	7	0.242986	1.0000	RandomExcursions
11	6	5	6	5	6	5	11	6	8	0.392456	0.9855	RandomExcursions
11	6	7	10	4	9	8	8	4	2	0.128379	1.0000	RandomExcursionsVariant
10	6	9	9	12	7	6	3	3	4	0.078086	0.9855	RandomExcursionsVariant
8	12	7	7	11	8	4	5	5	2	0.078086	0.9855	RandomExcursionsVariant
9	7	11	6	8	11	5	5	4	3	0.155209	0.9710	RandomExcursionsVariant
6	11	13	6	8	6	7	2	4	6	0.057146	0.9855	RandomExcursionsVariant
9	9	11	4	10	5	5	7	4	5	0.222869	1.0000	RandomExcursionsVariant
7	13	5	9	5	4	8	7	6	5	0.222869	1.0000	RandomExcursionsVariant
6	5	15	1	8	9	8	5	4	8	0.008366	1.0000	RandomExcursionsVariant
2	8	9	5	8	3	6	6	10	12	0.070445	1.0000	RandomExcursionsVariant
5	6	10	9	8	7	4	6	9	5	0.585209	0.9710	RandomExcursionsVariant
9	1	7	7	9	9	6	8	11	2	0.057146	1.0000	RandomExcursionsVariant
7	5	6	8	5	4	9	8	7	10	0.654467	1.0000	RandomExcursionsVariant
4	8	7	9	9	5	6	4	3	14	0.041438	1.0000	RandomExcursionsVariant
4	7	7	8	8	5	5	10	8	7	0.723129	0.9710	RandomExcursionsVariant
5	8	5	10	4	10	4	7	5	11	0.204076	0.9710	RandomExcursionsVariant
5	4	10	9	8	4	5	8	6	10	0.364146	0.9710	RandomExcursionsVariant
6	3	8	8	4	7	10	6	6	11	0.311542	0.9855	RandomExcursionsVariant
7	2	6	7	6	5	7	9	10	10	0.337162	0.9855	RandomExcursionsVariant
12	13	5	7	11	17	8	8	8	11	0.275709	0.9800	Serial
13	9	7	10	10	12	11	7	9	12	0.924076	0.9900	Serial
10	9	8	11	10	14	13	8	8	9	0.911413	0.9900	LinearComplexity

- -

The minimum pass rate for each statistical test with the exception of the random excursion (variant) test is approximately = 0.960150 for a sample size = 100 binary sequences.
The minimum pass rate for the random excursion (variant) test is approximately 0.954065 for a sample size = 69 binary sequences.
For further guidelines construct a probability table using the MAPLE program provided in the addendum section of the documentation.

- -

Результати тестування комбінації матричних та розширених матричних операцій перетворення невипадкової монотонно зростаючої послідовності з циклом повторення 256 байти

RESULTS FOR THE UNIFORMITY OF P-VALUES AND THE PROPORTION OF PASSING SEQUENCES

generator is <V_MR_256.bin>

C1	C2	C3	C4	C5	C6	C7	C8	C9	C10	P-VALUE	PROPORTION	STATISTICAL TEST
12	13	7	8	8	4	12	13	15	8	0.289667	0.9900	Frequency
8	8	12	11	7	14	12	10	7	11	0.816537	1.0000	BlockFrequency
11	17	5	8	6	11	8	14	8	12	0.191687	1.0000	CumulativeSums
12	8	11	12	9	9	10	8	9	12	0.983453	1.0000	CumulativeSums
14	6	10	11	14	10	12	10	6	7	0.554420	0.9900	Runs
12	9	9	15	4	14	14	8	10	5	0.171867	0.9900	LongestRun
6	11	11	12	11	9	6	14	13	7	0.595549	1.0000	Rank
3	3	11	9	14	14	13	8	14	11	0.062821	0.9900	FFT
17	14	12	8	9	6	8	5	12	9	0.191687	0.9700	NonOverlappingTemplate
14	9	13	11	9	10	5	11	7	11	0.699313	1.0000	NonOverlappingTemplate
12	11	9	7	12	13	12	5	8	11	0.719747	1.0000	NonOverlappingTemplate
8	11	10	9	15	7	7	15	13	5	0.289667	0.9800	NonOverlappingTemplate
12	15	11	8	2	12	6	9	12	13	0.153763	0.9800	NonOverlappingTemplate
10	7	13	14	3	10	12	8	13	10	0.350485	1.0000	NonOverlappingTemplate
11	11	14	9	11	12	11	10	8	3	0.554420	1.0000	NonOverlappingTemplate
7	11	11	12	9	14	11	7	8	10	0.867692	0.9900	NonOverlappingTemplate
13	5	7	14	10	7	7	10	17	10	0.181557	0.9900	NonOverlappingTemplate
13	13	11	12	9	6	12	12	5	7	0.514124	1.0000	NonOverlappingTemplate
10	12	11	8	8	7	8	10	14	12	0.867692	0.9800	NonOverlappingTemplate
11	10	7	10	17	8	8	11	10	8	0.616305	0.9900	NonOverlappingTemplate
11	13	8	10	7	12	7	12	13	7	0.759756	1.0000	NonOverlappingTemplate
8	9	14	14	11	8	10	8	7	11	0.779188	0.9900	NonOverlappingTemplate
14	12	10	6	8	6	12	10	10	12	0.699313	0.9700	NonOverlappingTemplate
10	12	8	15	9	4	11	12	7	12	0.455937	0.9800	NonOverlappingTemplate
8	5	12	10	12	9	10	11	13	10	0.851383	0.9900	NonOverlappingTemplate
8	9	13	12	10	14	11	5	8	10	0.699313	0.9900	NonOverlappingTemplate
11	11	13	10	10	8	11	9	11	6	0.946308	0.9900	NonOverlappingTemplate
10	9	7	12	10	12	9	8	11	12	0.971699	1.0000	NonOverlappingTemplate
14	14	8	10	9	6	7	10	11	11	0.699313	0.9900	NonOverlappingTemplate
12	6	9	10	11	10	10	9	9	14	0.911413	0.9900	NonOverlappingTemplate
9	5	10	11	11	13	14	8	6	13	0.514124	0.9800	NonOverlappingTemplate
6	9	15	6	10	7	10	17	8	12	0.191687	0.9900	NonOverlappingTemplate
12	10	6	13	4	12	6	12	15	10	0.249284	0.9800	NonOverlappingTemplate
7	11	14	14	8	8	12	9	10	7	0.699313	1.0000	NonOverlappingTemplate
9	12	7	12	10	9	13	9	6	13	0.798139	0.9900	NonOverlappingTemplate
13	13	9	10	7	11	16	8	3	10	0.224821	0.9900	NonOverlappingTemplate
11	11	7	12	10	12	7	14	7	9	0.798139	0.9800	NonOverlappingTemplate
4	8	9	12	9	13	15	11	9	10	0.514124	1.0000	NonOverlappingTemplate
7	9	18	8	9	11	5	13	11	9	0.236810	0.9900	NonOverlappingTemplate
8	8	7	10	14	12	8	15	9	9	0.657933	1.0000	NonOverlappingTemplate
12	6	12	11	8	10	13	11	9	8	0.883171	0.9800	NonOverlappingTemplate
6	13	9	8	17	15	11	6	8	7	0.145326	0.9800	NonOverlappingTemplate
9	9	11	10	9	12	13	12	5	10	0.867692	0.9900	NonOverlappingTemplate
15	14	5	9	8	5	15	13	5	11	0.075719	0.9700	NonOverlappingTemplate
14	9	4	12	8	9	11	12	9	12	0.616305	0.9900	NonOverlappingTemplate
7	10	11	5	15	8	17	9	6	12	0.145326	0.9900	NonOverlappingTemplate
17	9	11	4	7	10	11	11	10	10	0.366918	1.0000	NonOverlappingTemplate
8	8	6	11	13	14	9	7	12	12	0.657933	1.0000	NonOverlappingTemplate
10	15	12	12	3	4	9	13	10	12	0.153763	0.9800	NonOverlappingTemplate
10	14	8	7	12	6	15	5	14	9	0.236810	0.9900	NonOverlappingTemplate
10	10	14	11	10	16	9	6	6	8	0.437274	0.9900	NonOverlappingTemplate
9	8	14	7	15	6	15	6	10	10	0.262249	0.9900	NonOverlappingTemplate
8	11	11	11	14	13	4	11	5	12	0.366918	0.9800	NonOverlappingTemplate
12	11	12	6	7	8	14	8	12	10	0.719747	0.9900	NonOverlappingTemplate
11	9	11	15	11	6	11	9	7	10	0.779188	0.9800	NonOverlappingTemplate
8	9	12	9	11	13	8	11	8	11	0.964295	1.0000	NonOverlappingTemplate
12	11	8	9	16	10	14	4	8	8	0.304126	1.0000	NonOverlappingTemplate

8	8	13	9	10	15	14	9	10	4	0.383827	1.0000	NonOverlappingTemplate
12	5	8	12	8	7	10	13	13	12	0.616305	1.0000	NonOverlappingTemplate
11	14	10	12	11	11	7	5	12	7	0.637119	1.0000	NonOverlappingTemplate
10	14	12	10	9	11	7	6	14	7	0.616305	0.9900	NonOverlappingTemplate
11	12	13	7	9	14	12	10	9	3	0.401199	0.9900	NonOverlappingTemplate
12	7	9	9	10	6	13	14	8	12	0.699313	0.9800	NonOverlappingTemplate
6	15	6	11	9	13	15	10	10	5	0.224821	0.9900	NonOverlappingTemplate
13	11	14	8	10	10	9	9	9	7	0.897763	1.0000	NonOverlappingTemplate
10	11	12	9	7	12	10	12	9	8	0.971699	0.9800	NonOverlappingTemplate
9	11	10	11	5	13	15	7	9	10	0.616305	0.9900	NonOverlappingTemplate
10	10	14	11	7	10	7	8	14	9	0.779188	1.0000	NonOverlappingTemplate
10	9	12	16	13	8	8	8	11	5	0.455937	0.9900	NonOverlappingTemplate
12	7	10	15	9	9	14	7	10	7	0.595549	1.0000	NonOverlappingTemplate
11	9	9	16	8	3	7	8	16	13	0.090936	1.0000	NonOverlappingTemplate
7	11	13	7	16	12	11	11	7	5	0.319084	1.0000	NonOverlappingTemplate
11	10	13	12	9	8	7	6	14	10	0.739918	1.0000	NonOverlappingTemplate
9	17	9	7	15	11	8	5	12	7	0.171867	1.0000	NonOverlappingTemplate
13	10	8	14	7	4	10	13	11	10	0.494392	0.9900	NonOverlappingTemplate
13	9	11	6	13	13	12	9	6	8	0.637119	0.9900	NonOverlappingTemplate
6	11	8	9	10	9	10	15	10	12	0.816537	0.9700	NonOverlappingTemplate
8	17	6	7	11	7	12	12	7	13	0.249284	0.9800	NonOverlappingTemplate
13	12	7	6	12	10	4	11	7	18	0.085587	0.9800	NonOverlappingTemplate
10	10	9	10	6	7	11	15	9	13	0.719747	0.9700	NonOverlappingTemplate
9	4	8	9	12	13	13	10	11	11	0.678686	0.9900	NonOverlappingTemplate
12	11	10	15	8	10	8	9	7	10	0.851383	0.9900	NonOverlappingTemplate
17	14	12	8	9	6	8	5	12	9	0.191687	0.9700	NonOverlappingTemplate
6	10	11	13	11	10	10	9	10	10	0.971699	1.0000	NonOverlappingTemplate
12	9	12	11	9	12	6	7	8	14	0.739918	0.9700	NonOverlappingTemplate
11	13	2	10	12	7	10	11	9	15	0.249284	0.9800	NonOverlappingTemplate
11	13	5	10	10	11	13	8	9	10	0.834308	0.9900	NonOverlappingTemplate
9	9	11	12	9	8	14	9	9	10	0.964295	1.0000	NonOverlappingTemplate
4	7	11	10	12	14	12	10	8	12	0.554420	1.0000	NonOverlappingTemplate
14	11	9	12	7	10	9	7	10	11	0.897763	0.9900	NonOverlappingTemplate
5	11	6	11	7	9	15	13	12	11	0.419021	0.9900	NonOverlappingTemplate
11	8	6	14	3	9	12	9	13	15	0.181557	1.0000	NonOverlappingTemplate
7	12	8	14	11	5	10	10	12	11	0.699313	0.9900	NonOverlappingTemplate
18	9	14	10	9	6	8	9	8	9	0.289667	0.9900	NonOverlappingTemplate
11	14	12	5	10	14	6	8	10	10	0.514124	1.0000	NonOverlappingTemplate
10	7	16	8	10	11	16	8	7	7	0.289667	0.9900	NonOverlappingTemplate
9	9	19	5	8	11	12	10	9	8	0.202268	0.9800	NonOverlappingTemplate
12	10	12	10	9	7	15	12	4	9	0.494392	0.9900	NonOverlappingTemplate
8	10	12	6	11	12	13	7	14	7	0.616305	1.0000	NonOverlappingTemplate
10	9	13	15	8	9	7	10	8	11	0.798139	0.9900	NonOverlappingTemplate
14	7	8	7	6	13	9	16	9	11	0.334538	0.9800	NonOverlappingTemplate
8	12	9	18	11	8	11	11	2	10	0.108791	0.9900	NonOverlappingTemplate
12	8	11	12	11	9	4	11	12	10	0.779188	0.9900	NonOverlappingTemplate
10	16	12	7	6	8	10	9	10	12	0.595549	0.9900	NonOverlappingTemplate
10	8	12	9	11	14	10	8	7	11	0.911413	0.9900	NonOverlappingTemplate
13	12	10	5	13	8	11	7	10	11	0.719747	0.9900	NonOverlappingTemplate
9	10	8	12	6	14	6	15	12	8	0.437274	0.9700	NonOverlappingTemplate
12	7	8	11	10	11	8	14	12	7	0.816537	0.9800	NonOverlappingTemplate
14	11	8	4	10	8	11	10	14	10	0.554420	0.9900	NonOverlappingTemplate
10	7	12	12	5	16	12	10	13	3	0.122325	0.9800	NonOverlappingTemplate
11	9	12	10	10	13	10	9	10	6	0.955835	0.9800	NonOverlappingTemplate
12	11	11	12	9	7	18	10	6	4	0.137282	0.9900	NonOverlappingTemplate
4	14	5	11	16	11	9	8	17	5	0.021999	1.0000	NonOverlappingTemplate
9	6	5	10	9	11	14	17	13	6	0.145326	0.9900	NonOverlappingTemplate
11	9	3	8	6	12	10	20	11	10	0.040108	0.9900	NonOverlappingTemplate
5	6	11	8	10	10	10	18	13	9	0.213309	1.0000	NonOverlappingTemplate
4	12	12	13	8	6	8	15	11	11	0.319084	1.0000	NonOverlappingTemplate
12	11	9	10	12	13	6	10	10	7	0.883171	0.9800	NonOverlappingTemplate
18	14	9	9	12	9	12	4	5	8	0.075719	0.9800	NonOverlappingTemplate
5	11	15	7	10	9	14	14	9	6	0.275709	1.0000	NonOverlappingTemplate
13	12	15	4	10	12	9	8	8	9	0.455937	0.9800	NonOverlappingTemplate
15	9	8	11	14	6	7	10	10	10	0.616305	0.9800	NonOverlappingTemplate
9	5	10	6	21	16	9	9	9	6	0.009535	0.9900	NonOverlappingTemplate
16	16	11	10	11	5	7	7	4	13	0.062821	0.9900	NonOverlappingTemplate
12	15	9	8	8	6	7	8	15	12	0.383827	1.0000	NonOverlappingTemplate
11	16	9	9	5	8	11	15	9	7	0.319084	0.9700	NonOverlappingTemplate
10	9	13	13	9	9	11	6	8	12	0.867692	0.9900	NonOverlappingTemplate
9	9	11	8	11	11	12	10	9	10	0.997823	1.0000	NonOverlappingTemplate

```
 12   8  12  10  10  12   8  13   9   6  0.867692   1.0000    NonOverlappingTemplate
 11   9  13   7  10  17   7   7   7  12  0.350485   0.9800    NonOverlappingTemplate
 13   7  11   8   7  10  15   7  14   8  0.474986   0.9700    NonOverlappingTemplate
 17  15  11   9  12   8   9  12   2   5  0.037566   0.9900    NonOverlappingTemplate
  6   8   9  14   5  16   9  16  12   5  0.058984   1.0000    NonOverlappingTemplate
 10  13  11  13   9   9   9   6  10  10  0.924076   0.9900    NonOverlappingTemplate
  9   9  10   8  10  12   9   6  14  13  0.816537   0.9900    NonOverlappingTemplate
 14   9  11  13   9   8   9  10  10   7  0.897763   0.9800    NonOverlappingTemplate
 13   9   7  14  12   9   7  13   4  12  0.366918   0.9900    NonOverlappingTemplate
 12  16   9  11   9   7   4  14   7  11  0.249284   1.0000    NonOverlappingTemplate
  9   9   9  14  13   8   8   9   6  15  0.554420   0.9900    NonOverlappingTemplate
 15   9   9  10  11   8  15   9   8   6  0.554420   0.9900    NonOverlappingTemplate
  9   7   9  14  13  10  10  16   5   7  0.304126   1.0000    NonOverlappingTemplate
  6  11   9   9  11  10  10  10   9  15  0.867692   1.0000    NonOverlappingTemplate
  9  11  14  12   5  11  11  15   6   6  0.304126   1.0000    NonOverlappingTemplate
  9  13  12  13  11  10   6   6   8  12  0.699313   0.9900    NonOverlappingTemplate
  9  12   8  11   6   9  15  12  11   7  0.678686   0.9800    NonOverlappingTemplate
 15  10  12  13   7   6   8   3  14  12  0.137282   0.9900    NonOverlappingTemplate
 17   7   7  11  10  10  13  10   4  11  0.249284   0.9900    NonOverlappingTemplate
 13   6  12   9   9   9   9  12  11  10  0.924076   1.0000    NonOverlappingTemplate
  6  10   5  12  11  13  10   6  11  16  0.289667   1.0000    NonOverlappingTemplate
 11   5   9  14   7  14   9  14   7  10  0.401199   0.9900    NonOverlappingTemplate
  7  15   8  15   3   9  10  11   9  13  0.191687   1.0000    NonOverlappingTemplate
 12  11  12   6  14  12   6  10   9   8  0.678686   0.9800    NonOverlappingTemplate
  6  11   9  12  10  14   6   8   9  15  0.494392   0.9900    NonOverlappingTemplate
 10   8  13  10   9  12  11  12   8   7  0.935716   0.9900    NonOverlappingTemplate
 11  16  10   5   7  17   6  10   6  12  0.075719   1.0000    NonOverlappingTemplate
 12  11  10  15   7  11   8   9   7  10  0.798139   0.9900    NonOverlappingTemplate
  8   8  10   9  15  16  10   7  12   5  0.289667   1.0000    OverlappingTemplate
  7  11  16  10  11   8   9   7  12   9  0.678686   0.9900    Universal
  9  10   5  12  14  13   6   9  11  11  0.595549   0.9900    ApproximateEntropy
  7   4   5   9   8   2   7  11   5   6  0.324180   0.9688    RandomExcursions
  4   7   6   2   6  11   9  11   3   5  0.090936   1.0000    RandomExcursions
  3   9   5   9   2   7   7   8   6   8  0.437274   1.0000    RandomExcursions
  3  10  11   4   7  10   6   5   2   6  0.100508   0.9844    RandomExcursions
  5   7   4  11   8   5   9   7   5   3  0.407091   0.9844    RandomExcursions
  8   6   6   5   8   6   2   8   6   9  0.706149   0.9844    RandomExcursions
 12   5   6   5   7   8   4   8   3   6  0.350485   0.9688    RandomExcursions
  3  11   6   4   3   9   8   3  11   6  0.074177   0.9844    RandomExcursions
  8   7  10   7   5   7   2   5   8   5  0.568055   0.9688    RandomExcursionsVariant
  7   8   8   6   8   4   4   6   4   9  0.772760   0.9844    RandomExcursionsVariant
  7   8   7   6   3   6   6   8   7   6  0.949602   1.0000    RandomExcursionsVariant
  7  10   4   4   5   6   5  12   4   7  0.253551   1.0000    RandomExcursionsVariant
  9   3   7   5   6   8   7   4   7   8  0.772760   1.0000    RandomExcursionsVariant
 10   4   4  10   6   9   5   5   8   3  0.299251   0.9844    RandomExcursionsVariant
  6   7   7  13   4   7   4   7   4   5  0.275709   0.9844    RandomExcursionsVariant
  6   6  10   8  10   4   5   2   8   5  0.324180   0.9844    RandomExcursionsVariant
  8   7   6   7   6   5   8  10   5   2  0.602458   0.9844    RandomExcursionsVariant
  7  10   9   5   6   5   5   6   4   7  0.772760   1.0000    RandomExcursionsVariant
  7  11   7   6   5   2   6   4  11   5  0.195163   1.0000    RandomExcursionsVariant
 12   3   6   7   6   6   7   2   7   8  0.253551   0.9844    RandomExcursionsVariant
 10   6   7   9   3   4   4   4   7  10  0.299251   0.9844    RandomExcursionsVariant
 12   6   8   2   6   6  10   5   8   1  0.048716   0.9844    RandomExcursionsVariant
  9   9   4   9   7   3   9   5   5   4  0.407091   1.0000    RandomExcursionsVariant
  7   8   8  10   4   5   6   7   4   5  0.739918   1.0000    RandomExcursionsVariant
  9   3  10   8   6   8   5   5   5   5  0.568055   1.0000    RandomExcursionsVariant
  8   4  10   7   8   3   6   5   9   4  0.468595   1.0000    RandomExcursionsVariant
  9   9  10  11  10   6  11  10  10  14  0.935716   0.9900    Serial
 13   8   9   7   9  11   7   8  14  14  0.637119   0.9900    Serial
 13  10   7  12  12  12   9   5  13   7  0.595549   0.9700    LinearComplexity
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
The minimum pass rate for each statistical test with the exception of the
random excursion (variant) test is approximately = 0.960150 for a
sample size = 100 binary sequences.
The minimum pass rate for the random excursion (variant) test
is approximately 0.952688 for a sample size = 64 binary sequences.
For further guidelines construct a probability table using the MAPLE program
provided in the addendum section of the documentation.
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
```

Результати тестування застосування комбінації операцій матричного та розширеного матричного перетворення над текстовою інформацією

RESULTS FOR THE UNIFORMITY OF P-VALUES AND THE PROPORTION OF PASSING SEQUENCES

generator is <V_MR_TXT.bin>

C1	C2	C3	C4	C5	C6	C7	C8	C9	C10	P-VALUE	PROPORTION	STATISTICAL TEST
5	9	16	15	7	16	10	7	8	7	0.080519	1.0000	Frequency
6	12	11	11	9	11	14	11	6	9	0.759756	0.9900	BlockFrequency
8	11	10	10	14	10	8	10	7	12	0.924076	1.0000	CumulativeSums
7	8	9	13	16	10	7	12	12	6	0.419021	1.0000	CumulativeSums
9	10	11	10	12	11	5	10	13	9	0.897763	1.0000	Runs
11	7	11	9	11	9	5	11	11	15	0.678686	0.9700	LongestRun
12	10	10	8	8	4	11	16	8	13	0.366918	0.9900	Rank
3	1	4	8	20	9	13	15	15	12	0.000114	1.0000	FFT
9	10	6	16	9	13	10	7	6	14	0.319084	0.9900	NonOverlappingTemplate
9	14	8	6	11	9	6	12	11	14	0.574903	1.0000	NonOverlappingTemplate
14	8	15	11	11	14	3	6	9	9	0.162606	0.9800	NonOverlappingTemplate
8	6	7	9	12	14	12	11	14	7	0.534146	0.9900	NonOverlappingTemplate
7	12	4	16	13	11	9	12	8	8	0.289667	1.0000	NonOverlappingTemplate
10	6	9	11	15	10	11	11	8	9	0.834308	0.9800	NonOverlappingTemplate
4	10	14	10	16	7	9	9	11	10	0.350485	1.0000	NonOverlappingTemplate
3	14	9	11	10	14	8	16	9	6	0.122325	1.0000	NonOverlappingTemplate
14	11	11	8	11	6	10	13	10	6	0.699313	0.9800	NonOverlappingTemplate
13	14	10	7	12	11	6	5	11	11	0.514124	0.9800	NonOverlappingTemplate
10	10	11	12	10	10	6	9	14	8	0.897763	0.9800	NonOverlappingTemplate
15	15	10	8	9	6	4	15	7	11	0.115387	0.9700	NonOverlappingTemplate
6	11	12	8	10	9	12	8	13	11	0.883171	1.0000	NonOverlappingTemplate
11	8	11	10	14	9	10	7	6	14	0.699313	0.9900	NonOverlappingTemplate
10	13	11	13	8	8	10	10	8	9	0.955835	0.9800	NonOverlappingTemplate
5	3	12	12	13	16	9	12	11	7	0.115387	0.9800	NonOverlappingTemplate
12	5	13	11	8	15	11	7	10	8	0.514124	0.9800	NonOverlappingTemplate
7	11	8	8	14	12	10	8	12	10	0.867692	0.9700	NonOverlappingTemplate
12	10	11	11	11	7	6	4	13	15	0.334538	1.0000	NonOverlappingTemplate
10	9	5	12	18	7	8	8	14	9	0.171867	1.0000	NonOverlappingTemplate
7	12	10	10	14	8	10	10	11	8	0.924076	0.9900	NonOverlappingTemplate
7	11	9	7	14	16	11	7	8	10	0.474986	1.0000	NonOverlappingTemplate
8	19	8	10	10	9	9	14	7	6	0.153763	0.9900	NonOverlappingTemplate
11	11	13	7	10	12	11	12	7	6	0.798139	0.9800	NonOverlappingTemplate
7	11	9	14	9	12	11	9	11	7	0.883171	0.9900	NonOverlappingTemplate
12	9	11	7	8	11	7	9	14	12	0.834308	0.9900	NonOverlappingTemplate
10	11	14	13	3	15	5	9	12	8	0.145326	0.9900	NonOverlappingTemplate
8	6	8	15	11	12	11	12	7	10	0.657933	0.9900	NonOverlappingTemplate
8	7	11	9	6	18	12	11	10	8	0.319084	0.9800	NonOverlappingTemplate
11	10	12	8	8	9	12	12	8	10	0.978072	1.0000	NonOverlappingTemplate
11	15	8	6	8	6	14	14	9	9	0.350485	0.9800	NonOverlappingTemplate
13	8	6	11	8	11	8	10	9	16	0.574903	0.9700	NonOverlappingTemplate
11	14	10	8	13	10	10	12	6	6	0.678686	0.9900	NonOverlappingTemplate
13	10	6	11	13	15	9	8	10	5	0.437274	0.9800	NonOverlappingTemplate
12	4	13	14	12	14	5	9	8	9	0.236810	1.0000	NonOverlappingTemplate
12	10	13	5	6	12	12	11	7	12	0.574903	0.9900	NonOverlappingTemplate
4	10	12	12	15	9	12	6	10	10	0.437274	1.0000	NonOverlappingTemplate
14	10	11	10	4	10	15	8	11	7	0.419021	0.9800	NonOverlappingTemplate
8	9	11	9	15	14	8	7	10	9	0.719747	0.9900	NonOverlappingTemplate
13	6	13	7	9	14	9	12	10	7	0.595549	0.9900	NonOverlappingTemplate
11	9	10	11	14	8	10	9	10	8	0.971699	0.9700	NonOverlappingTemplate
8	10	9	7	11	18	6	9	6	16	0.096578	0.9800	NonOverlappingTemplate
8	8	8	14	15	7	10	10	11	9	0.699313	0.9800	NonOverlappingTemplate
11	13	12	13	8	7	10	13	9	4	0.514124	0.9700	NonOverlappingTemplate
13	15	13	9	7	10	10	8	10	5	0.514124	0.9800	NonOverlappingTemplate
6	4	10	6	11	13	10	13	8	19	0.045675	1.0000	NonOverlappingTemplate
9	11	8	9	9	6	14	14	9	11	0.759756	0.9900	NonOverlappingTemplate
15	12	8	12	8	8	13	7	7	10	0.616305	0.9900	NonOverlappingTemplate
6	7	9	12	9	10	14	8	13	12	0.699313	1.0000	NonOverlappingTemplate
7	8	11	15	8	7	12	10	9	13	0.678686	0.9900	NonOverlappingTemplate
11	12	13	8	12	8	7	11	8	10	0.911413	0.9800	NonOverlappingTemplate

8	10	15	7	11	6	10	10	10	13	0.699313	0.9900	NonOverlappingTemplate
7	12	8	6	15	11	9	9	13	10	0.637119	0.9800	NonOverlappingTemplate
10	14	9	4	10	12	11	18	5	7	0.075719	0.9900	NonOverlappingTemplate
8	7	7	9	14	14	5	16	7	13	0.145326	1.0000	NonOverlappingTemplate
15	11	11	15	11	8	7	11	6	5	0.289667	0.9700	NonOverlappingTemplate
6	10	14	9	11	9	10	13	13	5	0.554420	1.0000	NonOverlappingTemplate
9	11	12	11	11	13	6	5	9	13	0.657933	0.9800	NonOverlappingTemplate
8	9	7	6	12	15	15	6	13	9	0.275709	1.0000	NonOverlappingTemplate
12	12	8	11	7	11	10	13	7	9	0.897763	0.9800	NonOverlappingTemplate
13	13	9	8	8	15	5	9	12	8	0.474986	0.9800	NonOverlappingTemplate
11	12	7	9	10	15	9	9	8	10	0.867692	1.0000	NonOverlappingTemplate
11	8	6	15	19	8	7	10	10	6	0.075719	0.9700	NonOverlappingTemplate
10	9	14	5	11	8	8	7	14	14	0.419021	0.9800	NonOverlappingTemplate
6	9	10	13	12	15	10	7	9	9	0.678686	0.9900	NonOverlappingTemplate
11	9	13	10	13	3	6	9	15	11	0.262249	0.9900	NonOverlappingTemplate
10	7	9	11	8	13	6	16	12	8	0.494392	1.0000	NonOverlappingTemplate
7	7	12	14	7	11	7	11	12	12	0.678686	1.0000	NonOverlappingTemplate
11	7	8	5	18	13	10	8	13	7	0.145326	0.9900	NonOverlappingTemplate
14	13	11	9	8	10	6	7	12	10	0.739918	0.9900	NonOverlappingTemplate
7	11	11	10	10	9	13	9	12	8	0.964295	0.9800	NonOverlappingTemplate
8	7	14	7	10	11	14	9	11	9	0.759756	1.0000	NonOverlappingTemplate
8	14	10	9	12	5	11	14	8	9	0.616305	0.9900	NonOverlappingTemplate
9	11	6	11	12	13	10	11	10	7	0.897763	0.9900	NonOverlappingTemplate
9	10	6	16	9	13	10	7	6	14	0.319084	0.9900	NonOverlappingTemplate
6	10	13	11	10	12	12	7	6	13	0.657933	0.9800	NonOverlappingTemplate
8	4	8	10	11	10	15	11	14	9	0.455937	0.9800	NonOverlappingTemplate
13	8	7	13	13	10	8	14	6	8	0.534146	0.9700	NonOverlappingTemplate
9	9	13	12	10	10	7	9	16	5	0.474986	1.0000	NonOverlappingTemplate
8	4	6	11	9	20	7	10	13	12	0.035174	1.0000	NonOverlappingTemplate
8	7	15	10	11	12	10	6	11	10	0.739918	1.0000	NonOverlappingTemplate
7	14	9	10	14	7	13	13	9	4	0.304126	0.9900	NonOverlappingTemplate
10	12	10	9	6	7	8	15	8	15	0.455937	1.0000	NonOverlappingTemplate
13	9	11	12	5	10	13	8	10	9	0.798139	0.9900	NonOverlappingTemplate
9	13	3	13	15	9	12	9	8	9	0.319084	0.9900	NonOverlappingTemplate
5	12	11	11	10	11	11	11	10	8	0.924076	1.0000	NonOverlappingTemplate
11	12	7	8	7	6	6	16	9	18	0.066882	0.9600	NonOverlappingTemplate
7	13	7	14	11	8	14	8	9	9	0.637119	0.9900	NonOverlappingTemplate
11	10	12	7	11	10	10	10	10	9	0.996335	0.9800	NonOverlappingTemplate
15	10	8	13	9	8	14	10	6	7	0.494392	0.9900	NonOverlappingTemplate
8	13	11	10	9	6	14	5	9	15	0.366918	1.0000	NonOverlappingTemplate
15	4	11	9	6	7	8	12	15	13	0.162606	1.0000	NonOverlappingTemplate
10	16	5	9	12	6	6	9	13	14	0.191687	0.9900	NonOverlappingTemplate
13	6	9	7	13	9	12	9	10	12	0.798139	0.9700	NonOverlappingTemplate
7	6	12	11	9	12	5	12	18	8	0.153763	0.9900	NonOverlappingTemplate
15	4	10	7	14	9	8	11	13	9	0.334538	0.9900	NonOverlappingTemplate
12	9	11	7	9	18	9	7	9	9	0.419021	0.9800	NonOverlappingTemplate
10	9	7	13	13	11	7	10	12	8	0.867692	0.9800	NonOverlappingTemplate
6	7	9	9	16	12	6	10	11	14	0.350485	1.0000	NonOverlappingTemplate
13	5	9	10	9	16	11	8	11	8	0.514124	0.9900	NonOverlappingTemplate
11	8	8	6	11	15	15	6	3	17	0.025193	0.9800	NonOverlappingTemplate
8	8	10	9	15	9	13	6	12	10	0.699313	1.0000	NonOverlappingTemplate
6	8	12	16	16	10	10	6	11	5	0.129620	0.9900	NonOverlappingTemplate
10	10	12	6	12	9	8	14	7	12	0.759756	0.9900	NonOverlappingTemplate
9	11	8	8	8	11	8	11	12	14	0.911413	0.9900	NonOverlappingTemplate
8	8	12	12	11	14	9	10	6	10	0.834308	1.0000	NonOverlappingTemplate
12	11	13	15	9	6	8	13	5	8	0.366918	1.0000	NonOverlappingTemplate
16	11	7	6	11	5	11	14	11	8	0.275709	1.0000	NonOverlappingTemplate
8	14	3	7	13	12	11	12	5	15	0.102526	1.0000	NonOverlappingTemplate
9	12	10	8	16	4	9	12	11	9	0.455937	0.9800	NonOverlappingTemplate
7	14	8	11	8	7	15	11	12	7	0.514124	1.0000	NonOverlappingTemplate
9	10	10	11	10	8	8	14	12	8	0.946308	0.9800	NonOverlappingTemplate
12	8	7	19	8	5	13	7	14	7	0.048716	0.9800	NonOverlappingTemplate
8	10	13	13	13	11	7	10	4	11	0.554420	1.0000	NonOverlappingTemplate
7	12	11	11	10	6	10	6	14	13	0.616305	1.0000	NonOverlappingTemplate
11	12	9	14	12	1	8	10	16	7	0.075719	0.9700	NonOverlappingTemplate
14	10	18	10	11	8	7	8	10	4	0.145326	0.9800	NonOverlappingTemplate
10	14	11	6	16	6	9	11	5	12	0.236810	0.9900	NonOverlappingTemplate
15	9	9	9	17	6	8	12	7	8	0.249284	0.9800	NonOverlappingTemplate
9	4	12	11	15	14	8	10	7	10	0.383827	1.0000	NonOverlappingTemplate
7	9	14	12	11	12	9	4	12	10	0.574903	0.9900	NonOverlappingTemplate
9	7	13	16	12	5	14	10	5	9	0.181557	0.9800	NonOverlappingTemplate

```
 11  11  11  15   7   8   9   9  12   7  0.779188   1.0000    NonOverlappingTemplate
 19   7   7   8  11   6  10  13  12   7  0.115387   0.9600    NonOverlappingTemplate
  7  13   9  11   7   8   8   9  11  17  0.455937   1.0000    NonOverlappingTemplate
  6  13  13  10  10  12   8  13   6   9  0.657933   1.0000    NonOverlappingTemplate
 10   7  11   8  13  14  12   8  12   5  0.574903   0.9900    NonOverlappingTemplate
  9  19   8  10  13  10   5   8  10   8  0.171867   0.9800    NonOverlappingTemplate
  9   9  11   9  13   6  12  11  13   7  0.816537   0.9900    NonOverlappingTemplate
  9   8  17  11  10   5  14   5  12   9  0.181557   0.9900    NonOverlappingTemplate
 10  12   7   7  14   8  13  12   6  11  0.616305   0.9800    NonOverlappingTemplate
  7   8  11   8  15  13  12   7  10   9  0.678686   1.0000    NonOverlappingTemplate
 17  11  11   7  11  11  12   7   1  12  0.066882   1.0000    NonOverlappingTemplate
  9   9   9  10   9  10   7  12  11  14  0.946308   1.0000    NonOverlappingTemplate
  9  12   6  11   9  12  13  13   3  12  0.366918   1.0000    NonOverlappingTemplate
  9  11  14  11   8  13   8   8   3  15  0.249284   0.9900    NonOverlappingTemplate
  8  11   6  12  14   9  10   9  12   9  0.851383   1.0000    NonOverlappingTemplate
 15   6  15   7  11  11  11   7   6  11  0.319084   0.9900    NonOverlappingTemplate
 14   8  11  11   6  14  11   8   6  11  0.574903   0.9800    NonOverlappingTemplate
 10  10   9  11  11  14  10  11   7   7  0.924076   0.9900    NonOverlappingTemplate
 13   8   5  12  13  11  11  10   8   9  0.759756   1.0000    NonOverlappingTemplate
 11  10   9  14   7  13  13  10   7   6  0.637119   1.0000    NonOverlappingTemplate
 11  10   8  10   7  11   9  11   7  16  0.719747   0.9900    NonOverlappingTemplate
 12  14   9   7   6   9   6  11  15  11  0.437274   0.9800    NonOverlappingTemplate
  8  10  16   6  10   5   7  13  11  14  0.236810   0.9900    NonOverlappingTemplate
  9  13   9  11  13  13   5   9   8  10  0.739918   1.0000    NonOverlappingTemplate
  6  14  15  11   5  10  10   7  13   9  0.334538   0.9900    NonOverlappingTemplate
  9  11   6  11  11  15   9  11  10   7  0.779188   0.9900    NonOverlappingTemplate
 14   4  14   8  10  10  11   8  13   8  0.437274   1.0000    OverlappingTemplate
 15  10  10  10   8   9  11   8  12   7  0.851383   0.9900    Universal
  9  12  13   9  14   6   9  11   8   9  0.798139   0.9900    ApproximateEntropy
  6   6   5   7   5   5   7   7   5   5  0.971699   1.0000    RandomExcursions
  3   4   6   5   4   9   9   6   4   8  0.350485   1.0000    RandomExcursions
  5   2   7   5   8   4  10   4   8   5  0.236810   1.0000    RandomExcursions
  4   8   5   7   7  10   3   7   6   1  0.137282   1.0000    RandomExcursions
  6   4   5   7   3  11   6   5   5   6  0.383827   1.0000    RandomExcursions
  4   4   6   4  11   3   9   2   7   8  0.058984   0.9655    RandomExcursions
  5   3   1   9   9   8  14   2   6   1  0.000105   0.9828    RandomExcursions
  9   4   4   5   2   8   8   5   9   4  0.191687   0.9828    RandomExcursions
  5   5   5   4  10   4   8   5   5   7  0.534146   1.0000    RandomExcursionsVariant
  4   6   4   4  10   6   7   6   4   7  0.534146   1.0000    RandomExcursionsVariant
  2   7   6   8   6   6   6   5   8   4  0.616305   1.0000    RandomExcursionsVariant
  2   7   9   9   6   9   5   5   2   4  0.108791   1.0000    RandomExcursionsVariant
  1  13   8   5   7   8   5   3   3   5  0.008879   1.0000    RandomExcursionsVariant
  5  11   6   4   6  11   2   6   4   3  0.035174   1.0000    RandomExcursionsVariant
  7   5   8   7   8   6   5   2   6   4  0.574903   0.9828    RandomExcursionsVariant
  7   7   6   9   2   7   5   5   6   4  0.534146   0.9828    RandomExcursionsVariant
  8   5   4   8   6   4   6   4   5   8  0.699313   0.9828    RandomExcursionsVariant
  5   5   5  10   3   5   3   5   8   9  0.236810   1.0000    RandomExcursionsVariant
  4   5   5   0   5   3   9   7  12   8  0.010237   0.9828    RandomExcursionsVariant
  6   2   0   3   8  10   6   9   7   7  0.020548   1.0000    RandomExcursionsVariant
  4   6   7   9   6   5   6   8   4   3  0.574903   1.0000    RandomExcursionsVariant
  7   5   6   8   7   4   5   7   3   6  0.779188   1.0000    RandomExcursionsVariant
  6   2   9   8   3   6   5   7   6   6  0.419021   1.0000    RandomExcursionsVariant
  4   8   7   3   6   0   4   9   9   8  0.045675   0.9828    RandomExcursionsVariant
  4   8   5   6   3   3   9   7   6   7  0.455937   0.9655    RandomExcursionsVariant
  4   5   6   6   5   6   5  13   5   3  0.108791   0.9655    RandomExcursionsVariant
  9   8   8  10  12  20   4   9   7  13  0.051942   0.9900    Serial
 16   3   6  12   5   9  15  10  16   8  0.020548   0.9900    Serial
 12  10  13  10  12   8   9   9  10   7  0.955835   1.0000    LinearComplexity
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
The minimum pass rate for each statistical test with the exception of the
random excursion (variant) test is approximately = 0.960150 for a
sample size = 100 binary sequences.
The minimum pass rate for the random excursion (variant) test
is approximately 0.950806 for a sample size = 58 binary sequences.
For further guidelines construct a probability table using the MAPLE program
provided in the addendum section of the documentation.
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
```

Результати тестування невипадкової монотонно зростаючої послідовності з циклом повторення 64 байти комбінацією розширених матричних та матричних операцій перетворення

RESULTS FOR THE UNIFORMITY OF P-VALUES AND THE PROPORTION OF PASSING SEQUENCES

generator is <V_RM_64.bin>

C1	C2	C3	C4	C5	C6	C7	C8	C9	C10	P-VALUE	PROPORTION	STATISTICAL TEST
16	6	15	11	9	8	9	12	8	6	0.289667	0.9900	Frequency
14	12	3	7	7	14	6	13	14	10	0.108791	0.9800	BlockFrequency
14	11	12	8	11	11	8	6	11	8	0.816537	1.0000	CumulativeSums
11	13	9	14	5	7	13	8	12	8	0.514124	0.9900	CumulativeSums
15	3	12	11	7	8	11	9	8	16	0.145326	0.9800	Runs
12	9	14	12	7	9	11	10	6	10	0.816537	0.9900	LongestRun
11	13	10	7	3	6	6	15	17	12	0.037566	0.9900	Rank
1	7	11	13	11	10	11	10	14	12	0.202268	1.0000	FFT
13	9	9	9	7	15	6	12	9	11	0.657933	0.9800	NonOverlappingTemplate
13	8	6	8	12	9	10	12	9	13	0.816537	0.9700	NonOverlappingTemplate
10	12	8	5	15	13	10	7	10	10	0.574903	0.9900	NonOverlappingTemplate
9	8	8	13	10	11	6	12	9	14	0.779188	0.9900	NonOverlappingTemplate
8	13	11	10	5	10	15	11	8	9	0.637119	1.0000	NonOverlappingTemplate
12	10	9	5	8	13	11	11	10	11	0.867692	0.9900	NonOverlappingTemplate
12	10	9	9	12	7	14	12	6	9	0.779188	1.0000	NonOverlappingTemplate
12	8	10	11	10	15	11	7	7	9	0.798139	0.9900	NonOverlappingTemplate
10	10	7	13	6	15	11	13	9	6	0.474986	0.9900	NonOverlappingTemplate
12	6	10	12	8	9	9	10	12	12	0.924076	1.0000	NonOverlappingTemplate
11	9	8	12	11	14	11	8	6	10	0.851383	0.9800	NonOverlappingTemplate
14	11	10	8	5	10	9	12	10	11	0.816537	0.9900	NonOverlappingTemplate
14	10	16	8	11	7	13	8	7	6	0.319084	0.9900	NonOverlappingTemplate
9	12	12	16	10	9	9	5	9	9	0.595549	0.9900	NonOverlappingTemplate
7	7	11	10	7	11	10	15	14	8	0.595549	1.0000	NonOverlappingTemplate
9	9	8	6	9	15	11	13	11	9	0.739918	0.9900	NonOverlappingTemplate
12	8	13	8	11	12	4	11	14	7	0.455937	1.0000	NonOverlappingTemplate
14	8	10	3	10	8	12	12	12	11	0.474986	1.0000	NonOverlappingTemplate
11	9	6	9	14	13	8	10	9	11	0.834308	0.9800	NonOverlappingTemplate
9	13	8	7	9	9	10	11	12	12	0.946308	0.9800	NonOverlappingTemplate
11	14	19	9	4	10	9	6	8	10	0.075719	0.9700	NonOverlappingTemplate
12	13	14	11	6	8	10	11	9	6	0.657933	0.9800	NonOverlappingTemplate
5	8	16	9	15	8	6	8	12	13	0.171867	1.0000	NonOverlappingTemplate
10	18	8	11	11	5	5	10	12	10	0.191687	1.0000	NonOverlappingTemplate
9	5	9	8	15	11	12	11	6	14	0.401199	1.0000	NonOverlappingTemplate
14	13	6	7	6	9	9	11	17	8	0.202268	0.9900	NonOverlappingTemplate
4	12	7	6	15	14	9	8	13	12	0.191687	0.9900	NonOverlappingTemplate
11	9	11	6	5	11	11	16	8	12	0.437274	0.9800	NonOverlappingTemplate
12	18	11	5	11	5	9	9	9	11	0.191687	0.9800	NonOverlappingTemplate
8	9	9	7	12	10	13	9	10	13	0.924076	1.0000	NonOverlappingTemplate
8	8	13	9	13	8	6	15	14	6	0.319084	1.0000	NonOverlappingTemplate
12	7	11	10	11	9	9	10	10	11	0.994250	1.0000	NonOverlappingTemplate
21	6	4	10	12	17	8	5	7	10	0.001757	0.9900	NonOverlappingTemplate
10	10	7	11	8	10	7	12	11	14	0.883171	1.0000	NonOverlappingTemplate
8	12	7	14	10	12	7	13	8	9	0.739918	0.9900	NonOverlappingTemplate
11	15	11	5	12	11	6	10	12	7	0.474986	0.9800	NonOverlappingTemplate
5	13	9	11	13	12	7	10	7	13	0.574903	1.0000	NonOverlappingTemplate
13	14	9	12	13	8	6	9	7	9	0.637119	0.9900	NonOverlappingTemplate
7	10	8	9	13	13	11	12	7	10	0.867692	1.0000	NonOverlappingTemplate
10	7	14	8	12	16	11	11	5	6	0.262249	1.0000	NonOverlappingTemplate
10	11	3	12	8	15	9	14	10	8	0.319084	0.9900	NonOverlappingTemplate
6	10	7	12	9	16	12	9	11	8	0.574903	1.0000	NonOverlappingTemplate
13	11	10	10	15	10	8	2	6	15	0.108791	0.9900	NonOverlappingTemplate
7	8	10	12	11	14	10	11	6	11	0.816537	1.0000	NonOverlappingTemplate
10	11	10	10	9	16	6	12	8	8	0.678686	0.9900	NonOverlappingTemplate
9	11	7	8	11	10	8	9	17	10	0.637119	1.0000	NonOverlappingTemplate
8	8	6	15	10	7	14	10	13	9	0.494392	0.9900	NonOverlappingTemplate
14	8	9	8	9	13	13	7	14	5	0.401199	0.9600	NonOverlappingTemplate
13	12	7	7	13	8	9	11	8	12	0.798139	0.9800	NonOverlappingTemplate

11	6	10	9	12	10	5	14	9	14	0.534146	0.9800	NonOverlappingTemplate
10	15	10	13	10	10	9	8	10	5	0.699313	0.9900	NonOverlappingTemplate
10	11	6	12	8	7	10	9	16	11	0.616305	0.9900	NonOverlappingTemplate
13	6	9	8	11	7	12	14	10	10	0.739918	0.9700	NonOverlappingTemplate
6	11	15	12	5	10	9	10	10	12	0.574903	1.0000	NonOverlappingTemplate
13	11	7	12	10	12	8	10	12	5	0.739918	0.9900	NonOverlappingTemplate
11	8	9	12	9	7	8	9	16	11	0.719747	0.9900	NonOverlappingTemplate
6	7	10	12	12	10	8	12	12	11	0.867692	0.9900	NonOverlappingTemplate
8	11	11	12	7	12	12	8	12	7	0.883171	0.9900	NonOverlappingTemplate
13	6	11	8	10	11	14	8	10	9	0.816537	0.9900	NonOverlappingTemplate
8	10	10	12	11	11	8	11	7	12	0.971699	1.0000	NonOverlappingTemplate
14	11	10	11	10	12	7	5	8	12	0.699313	1.0000	NonOverlappingTemplate
5	7	6	13	10	7	13	18	11	10	0.115387	1.0000	NonOverlappingTemplate
11	12	11	11	12	9	7	7	11	9	0.955835	1.0000	NonOverlappingTemplate
5	10	19	7	10	9	13	8	7	12	0.115387	1.0000	NonOverlappingTemplate
8	12	8	13	9	14	8	14	8	6	0.554420	0.9900	NonOverlappingTemplate
10	9	8	15	11	8	8	13	10	8	0.816537	0.9800	NonOverlappingTemplate
9	14	7	10	15	9	7	8	11	10	0.678686	1.0000	NonOverlappingTemplate
7	8	6	9	12	13	15	9	11	10	0.637119	1.0000	NonOverlappingTemplate
5	16	10	7	13	11	5	7	12	14	0.145326	1.0000	NonOverlappingTemplate
8	10	9	12	7	9	5	15	8	17	0.202268	0.9900	NonOverlappingTemplate
8	10	10	8	13	13	12	5	10	11	0.779188	0.9800	NonOverlappingTemplate
5	6	9	12	8	16	13	9	12	10	0.350485	0.9900	NonOverlappingTemplate
8	7	10	12	11	9	12	8	13	10	0.935716	0.9900	NonOverlappingTemplate
8	2	8	10	12	12	14	11	11	12	0.334538	0.9900	NonOverlappingTemplate
13	9	9	9	7	15	6	12	9	11	0.657933	0.9800	NonOverlappingTemplate
9	12	14	9	7	10	10	14	7	8	0.739918	1.0000	NonOverlappingTemplate
6	14	9	11	13	14	7	8	11	7	0.514124	1.0000	NonOverlappingTemplate
9	9	7	15	14	11	6	11	9	9	0.616305	0.9800	NonOverlappingTemplate
7	13	14	8	11	8	9	10	11	9	0.867692	0.9900	NonOverlappingTemplate
9	11	11	11	15	6	12	5	7	13	0.419021	0.9900	NonOverlappingTemplate
9	8	8	14	13	9	14	9	7	9	0.719747	0.9700	NonOverlappingTemplate
10	16	7	13	9	5	12	11	6	11	0.334538	0.9900	NonOverlappingTemplate
11	11	11	7	11	8	8	18	4	11	0.202268	1.0000	NonOverlappingTemplate
7	10	6	7	13	11	13	11	8	14	0.595549	1.0000	NonOverlappingTemplate
10	9	10	7	13	15	2	9	14	11	0.181557	0.9900	NonOverlappingTemplate
11	8	8	14	9	8	13	7	15	7	0.514124	1.0000	NonOverlappingTemplate
9	14	9	6	9	12	8	14	12	7	0.616305	1.0000	NonOverlappingTemplate
11	6	11	12	8	7	5	14	14	12	0.383827	0.9800	NonOverlappingTemplate
11	9	7	10	9	11	15	10	6	12	0.759756	0.9700	NonOverlappingTemplate
11	11	9	7	11	10	7	11	13	10	0.955835	0.9700	NonOverlappingTemplate
12	16	10	12	8	5	7	9	12	9	0.455937	1.0000	NonOverlappingTemplate
8	11	14	15	12	8	11	7	5	9	0.437274	1.0000	NonOverlappingTemplate
15	9	6	8	5	11	9	12	17	8	0.162606	0.9900	NonOverlappingTemplate
8	7	15	13	10	6	13	10	13	5	0.304126	0.9900	NonOverlappingTemplate
13	8	12	7	8	16	8	11	9	8	0.574903	0.9900	NonOverlappingTemplate
10	14	6	10	12	14	7	13	6	8	0.437274	1.0000	NonOverlappingTemplate
9	9	11	11	14	8	4	12	12	10	0.657933	1.0000	NonOverlappingTemplate
10	7	8	13	8	11	13	12	11	7	0.834308	0.9900	NonOverlappingTemplate
9	10	7	11	15	10	9	10	10	9	0.924076	1.0000	NonOverlappingTemplate
8	6	10	11	13	9	12	8	10	13	0.851383	1.0000	NonOverlappingTemplate
11	17	9	9	11	8	11	7	10	7	0.574903	0.9800	NonOverlappingTemplate
6	10	8	6	11	7	8	16	17	11	0.137282	0.9900	NonOverlappingTemplate
8	11	12	8	9	9	11	9	8	15	0.867692	0.9900	NonOverlappingTemplate
11	9	14	6	12	8	10	9	8	13	0.779188	0.9900	NonOverlappingTemplate
11	14	5	7	7	11	7	11	14	13	0.383827	0.9900	NonOverlappingTemplate
12	6	7	17	13	11	10	9	8	7	0.334538	0.9800	NonOverlappingTemplate
13	10	10	11	9	11	6	11	8	11	0.946308	0.9900	NonOverlappingTemplate
10	8	8	13	8	5	13	9	16	10	0.419021	0.9800	NonOverlappingTemplate
7	19	7	6	10	12	12	11	9	7	0.145326	1.0000	NonOverlappingTemplate
11	8	8	4	7	17	8	15	15	7	0.055361	1.0000	NonOverlappingTemplate
8	10	9	11	12	12	6	11	10	11	0.955835	1.0000	NonOverlappingTemplate
13	10	6	9	9	16	8	9	10	10	0.657933	0.9900	NonOverlappingTemplate
10	11	8	13	10	8	11	11	8	10	0.983453	1.0000	NonOverlappingTemplate
5	10	8	8	9	12	14	11	12	11	0.739918	1.0000	NonOverlappingTemplate
11	8	10	6	10	13	8	11	13	10	0.883171	0.9900	NonOverlappingTemplate
11	9	8	7	10	9	10	10	15	11	0.897763	1.0000	NonOverlappingTemplate
9	10	8	15	12	7	10	8	10	11	0.851383	0.9700	NonOverlappingTemplate
17	7	10	8	8	11	10	11	5	13	0.334538	0.9800	NonOverlappingTemplate
13	12	12	11	5	11	8	11	9	8	0.798139	0.9900	NonOverlappingTemplate
8	7	9	10	6	13	10	17	3	17	0.028817	1.0000	NonOverlappingTemplate

```
 9  11   8  18  14   4  11   7   7  11  0.115387   0.9900    NonOverlappingTemplate
10  13  14   6   7  11   8  11   7  13  0.595549   0.9900    NonOverlappingTemplate
 6  19   8   7  11   5  12   9  14   9  0.071177   0.9900    NonOverlappingTemplate
12  10   6  11   7   9   9  12  14  10  0.816537   0.9900    NonOverlappingTemplate
12   7  16   5   8   7  15  13   8   9  0.181557   0.9700    NonOverlappingTemplate
 7   9   8  10  15  10  14   7   9  11  0.678686   0.9800    NonOverlappingTemplate
11   7  11  14   9  14   5   8  11  10  0.595549   0.9800    NonOverlappingTemplate
 9  12  11   6  10  11   6  11  12  12  0.851383   1.0000    NonOverlappingTemplate
 7  14  13   6   8   7  11  11  12  11  0.637119   0.9900    NonOverlappingTemplate
11   6   8  13  10  11  13   9   8  11  0.867692   0.9900    NonOverlappingTemplate
11  12  11  10   5   8  12  10  12   9  0.883171   0.9900    NonOverlappingTemplate
 8   5  10   9  11  14   7  13  17   6  0.162606   1.0000    NonOverlappingTemplate
15  11   7  10   7  10  12  10  11   7  0.759756   0.9900    NonOverlappingTemplate
10  10  12  10   8   9  14   7   8  12  0.897763   0.9900    NonOverlappingTemplate
 7  14  13   5   8   9  14  11  10   9  0.514124   0.9900    NonOverlappingTemplate
 8  10   6  14  11  11  12   9   8  11  0.851383   1.0000    NonOverlappingTemplate
11  13   9   5   9   7  11  14  11  10  0.699313   1.0000    NonOverlappingTemplate
10  11   6   6  10   8  15  10  12  12  0.637119   0.9800    NonOverlappingTemplate
13   9   7  12   6  11   9   7  17   9  0.350485   0.9900    NonOverlappingTemplate
 6   8   7   8   9  11  15  16  10  10  0.383827   0.9900    NonOverlappingTemplate
13  12   7  10  11   1  14  10  11  11  0.202268   0.9700    NonOverlappingTemplate
 7   7  10  12  12   8  12  14   9   9  0.816537   0.9800    NonOverlappingTemplate
10  12   9  11  13   6  10   9   8  12  0.911413   1.0000    NonOverlappingTemplate
 7  10   7  16  10   9   4  17  10  10  0.122325   1.0000    NonOverlappingTemplate
 6   8  13   7   5  13  12   9  18   9  0.115387   1.0000    NonOverlappingTemplate
 8  13  12  11  10  10   9   9   8  10  0.983453   0.9900    NonOverlappingTemplate
 4  17   6   7  10  17  11  13   3  12  0.008266   0.9900    NonOverlappingTemplate
 8   2   8  10  12  12  14  11  11  12  0.334538   0.9900    NonOverlappingTemplate
11  10   8   7   6  13   9  10  12  14  0.739918   0.9800    OverlappingTemplate
14  11   7   6   9   7  17   6  11  12  0.202268   0.9700    Universal
 8  11   5   8  12   7  13  11  11  14  0.595549   1.0000    ApproximateEntropy
 6   4   3   4   7   7   3  10   6   8  0.289667   0.9828    RandomExcursions
10   6   5   3   4   2   8   6   4  10  0.085587   1.0000    RandomExcursions
 6   5   2   8   5   7   7   7   4   7  0.616305   1.0000    RandomExcursions
 7   7   4   4   3   8   4   3  11   7  0.137282   0.9828    RandomExcursions
 7   9   2   4   6   6   3   8  10   3  0.096578   1.0000    RandomExcursions
 8   8   6   4   4   5   2   8   7   6  0.455937   0.9828    RandomExcursions
 6   5   3   7   5  12   2   5   2  11  0.007694   0.9828    RandomExcursions
11   6   5   5   4   6   7   2   6   6  0.289667   0.9655    RandomExcursions
 9   4   7   0   7   8   5   6   5   7  0.171867   0.9655    RandomExcursionsVariant
11   2   5   5   4   5   3  10   4   9  0.030806   0.9828    RandomExcursionsVariant
10   4   3   5   4   4   6   8   6   8  0.319084   0.9828    RandomExcursionsVariant
10   3   4   4   4   6   7   6   4  10  0.171867   1.0000    RandomExcursionsVariant
 7   4   4   6   4   3   6   9   5  10  0.289667   1.0000    RandomExcursionsVariant
 7   2   3   5   5   9   5   7   8   7  0.350485   1.0000    RandomExcursionsVariant
 7   2   4   6   6   6   3   8   6  10  0.262249   1.0000    RandomExcursionsVariant
 6   5   6   6   3   6   7   5   5   9  0.779188   0.9828    RandomExcursionsVariant
 6   4   4   7   1   6   5   8   6  11  0.122325   0.9828    RandomExcursionsVariant
 5   7   6   7   2   4   5   7  10   5  0.383827   0.9828    RandomExcursionsVariant
 7   4   5   3   3   8   5   5  11   7  0.191687   0.9828    RandomExcursionsVariant
 5   4   8   3   8   2   8   4  10   6  0.137282   0.9828    RandomExcursionsVariant
 4   1  11   3   9   3  14   5   3   5  0.000170   0.9828    RandomExcursionsVariant
 5   3   6   4   9   8   8   6   8   1  0.153763   0.9828    RandomExcursionsVariant
 6   6   5   4   4  10   3  10   5   5  0.236810   0.9828    RandomExcursionsVariant
 9   4   6   8   2   5  12   3   4   5  0.035174   1.0000    RandomExcursionsVariant
 7   5   5  10   7   5   2  10   6   1  0.051942   1.0000    RandomExcursionsVariant
 6   9   5   2   7   7   3   6   4   9  0.262249   1.0000    RandomExcursionsVariant
10   7   7   5   6  10  12  11  13  19  0.080519   0.9800    Serial
15   7  10   9   5  13   7  10   8  16  0.224821   0.9800    Serial
13   8   5  14  10   9   7  12  14   8  0.455937   0.9900    LinearComplexity
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
The minimum pass rate for each statistical test with the exception of the
random excursion (variant) test is approximately = 0.960150 for a
sample size = 100 binary sequences.
The minimum pass rate for the random excursion (variant) test
is approximately 0.950806 for a sample size = 58 binary sequences.
For further guidelines construct a probability table using the MAPLE program
provided in the addendum section of the documentation.
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
```

Результати тестування невипадкової монотонно зростаючої послідовності з циклом повторення 256 байти комбінацією розширених матричних та матричних операцій перетворення

RESULTS FOR THE UNIFORMITY OF P-VALUES AND THE PROPORTION OF PASSING SEQUENCES

generator is <V_RM_256.bin>

C1	C2	C3	C4	C5	C6	C7	C8	C9	C10	P-VALUE	PROPORTION	STATISTICAL TEST
8	15	11	12	6	8	8	10	9	13	0.657933	0.9900	Frequency
10	7	8	11	13	11	10	13	10	7	0.897763	0.9800	BlockFrequency
9	10	12	12	10	9	7	11	14	6	0.816537	0.9900	CumulativeSums
7	11	11	13	10	7	12	10	8	11	0.924076	0.9900	CumulativeSums
15	8	8	12	9	11	7	8	11	11	0.798139	0.9900	Runs
10	10	8	5	10	14	7	11	11	14	0.616305	1.0000	LongestRun
6	12	10	12	14	4	4	8	17	13	0.042808	0.9900	Rank
3	7	7	14	9	11	8	16	13	12	0.129620	1.0000	FFT
16	13	15	3	5	13	12	5	9	9	0.030806	1.0000	NonOverlappingTemplate
12	15	16	9	7	8	7	10	9	7	0.366918	1.0000	NonOverlappingTemplate
10	9	6	9	10	6	14	11	13	12	0.699313	0.9900	NonOverlappingTemplate
9	16	12	6	12	10	13	6	8	8	0.401199	0.9800	NonOverlappingTemplate
12	7	14	11	15	11	6	5	11	8	0.334538	0.9900	NonOverlappingTemplate
11	7	13	9	7	4	12	6	18	13	0.071177	0.9900	NonOverlappingTemplate
9	13	10	11	7	16	14	8	7	5	0.275709	0.9900	NonOverlappingTemplate
8	11	5	13	13	7	12	8	14	9	0.514124	0.9900	NonOverlappingTemplate
8	14	6	11	12	9	12	15	9	4	0.289667	1.0000	NonOverlappingTemplate
15	14	11	4	5	12	12	7	10	10	0.213309	0.9700	NonOverlappingTemplate
15	12	11	10	4	9	6	12	12	9	0.419021	1.0000	NonOverlappingTemplate
11	12	9	4	9	9	5	14	15	12	0.249284	0.9800	NonOverlappingTemplate
5	9	8	7	14	11	8	15	15	8	0.249284	0.9900	NonOverlappingTemplate
10	11	8	11	10	11	9	8	5	17	0.474986	0.9900	NonOverlappingTemplate
9	9	10	12	9	17	11	8	7	8	0.595549	0.9900	NonOverlappingTemplate
7	6	14	11	9	13	10	10	8	12	0.739918	1.0000	NonOverlappingTemplate
13	8	9	8	11	12	8	10	7	14	0.816537	1.0000	NonOverlappingTemplate
11	14	10	9	15	8	7	11	8	7	0.637119	0.9900	NonOverlappingTemplate
16	9	8	14	8	9	5	12	10	9	0.419021	0.9800	NonOverlappingTemplate
7	10	9	9	10	16	8	7	13	11	0.637119	0.9900	NonOverlappingTemplate
12	9	11	12	6	10	13	14	6	7	0.574903	0.9800	NonOverlappingTemplate
6	14	10	8	9	11	18	10	5	9	0.171867	0.9900	NonOverlappingTemplate
10	10	10	14	11	6	9	9	9	12	0.911413	1.0000	NonOverlappingTemplate
12	11	6	8	7	9	12	13	12	10	0.816537	0.9900	NonOverlappingTemplate
11	7	11	6	9	21	7	11	11	6	0.040108	0.9600	NonOverlappingTemplate
11	9	13	13	11	6	11	8	9	9	0.883171	1.0000	NonOverlappingTemplate
10	9	14	12	10	5	12	10	8	10	0.798139	0.9800	NonOverlappingTemplate
11	8	8	12	10	6	10	10	10	15	0.798139	0.9900	NonOverlappingTemplate
15	9	7	6	13	10	5	9	14	12	0.304126	0.9900	NonOverlappingTemplate
10	7	13	7	7	11	13	13	14	5	0.383827	1.0000	NonOverlappingTemplate
12	14	18	6	9	10	5	8	7	11	0.122325	1.0000	NonOverlappingTemplate
12	5	7	13	13	12	8	9	12	9	0.637119	0.9600	NonOverlappingTemplate
13	5	10	5	10	10	16	16	5	10	0.075719	0.9900	NonOverlappingTemplate
12	7	13	12	7	8	7	9	15	10	0.595549	0.9900	NonOverlappingTemplate
17	7	14	6	8	7	9	12	10	10	0.289667	0.9900	NonOverlappingTemplate
10	14	10	10	9	5	11	10	12	9	0.851383	1.0000	NonOverlappingTemplate
11	7	9	14	10	7	11	10	13	8	0.834308	0.9800	NonOverlappingTemplate
5	12	11	10	9	9	11	6	14	13	0.595549	1.0000	NonOverlappingTemplate
9	12	9	11	14	7	9	8	7	14	0.719747	1.0000	NonOverlappingTemplate
13	14	8	7	11	11	18	5	7	6	0.080519	0.9800	NonOverlappingTemplate
10	11	8	8	8	3	6	17	13	16	0.045675	0.9900	NonOverlappingTemplate
4	13	10	13	16	7	12	11	8	6	0.191687	1.0000	NonOverlappingTemplate
13	12	15	4	10	13	6	8	10	9	0.319084	0.9800	NonOverlappingTemplate
8	7	9	9	7	12	16	9	15	8	0.401199	1.0000	NonOverlappingTemplate
13	15	9	14	11	8	5	7	9	9	0.419021	1.0000	NonOverlappingTemplate
7	10	15	6	13	10	13	10	9	7	0.554420	1.0000	NonOverlappingTemplate
9	8	7	12	14	10	7	14	6	13	0.494392	1.0000	NonOverlappingTemplate
11	7	13	10	12	13	11	9	7	7	0.816537	1.0000	NonOverlappingTemplate
9	14	10	9	10	8	8	9	20	3	0.040108	0.9900	NonOverlappingTemplate

10	6	10	14	8	9	12	7	13	11	0.739918	0.9600	NonOverlappingTemplate
9	14	9	8	7	11	8	11	13	10	0.867692	0.9900	NonOverlappingTemplate
13	6	14	9	10	8	9	12	10	9	0.816537	0.9800	NonOverlappingTemplate
5	15	11	12	10	12	8	11	6	10	0.534146	1.0000	NonOverlappingTemplate
12	15	12	12	11	9	9	10	3	7	0.366918	0.9900	NonOverlappingTemplate
11	6	16	5	12	12	7	9	13	9	0.304126	0.9900	NonOverlappingTemplate
6	9	12	13	5	10	12	11	7	15	0.401199	0.9800	NonOverlappingTemplate
7	9	5	16	10	7	10	9	14	13	0.304126	1.0000	NonOverlappingTemplate
13	11	7	12	10	12	7	11	6	11	0.798139	1.0000	NonOverlappingTemplate
14	11	7	14	4	7	11	11	12	9	0.401199	0.9800	NonOverlappingTemplate
14	6	16	10	10	5	12	7	10	10	0.304126	0.9700	NonOverlappingTemplate
6	8	11	9	10	14	12	5	10	15	0.419021	1.0000	NonOverlappingTemplate
7	7	16	6	14	11	9	10	7	13	0.304126	0.9800	NonOverlappingTemplate
6	15	10	8	5	11	14	15	7	9	0.202268	0.9900	NonOverlappingTemplate
11	10	10	11	8	13	11	7	10	9	0.978072	0.9900	NonOverlappingTemplate
9	7	10	10	11	8	13	6	8	18	0.289667	0.9600	NonOverlappingTemplate
7	12	9	8	8	13	9	9	7	18	0.304126	0.9900	NonOverlappingTemplate
11	9	12	8	14	8	12	7	9	10	0.883171	1.0000	NonOverlappingTemplate
6	11	13	8	16	12	5	11	8	10	0.350485	1.0000	NonOverlappingTemplate
8	10	8	13	6	19	10	9	10	7	0.191687	1.0000	NonOverlappingTemplate
8	7	8	8	14	13	9	12	10	11	0.816537	1.0000	NonOverlappingTemplate
12	13	9	15	9	12	7	7	7	9	0.616305	0.9700	NonOverlappingTemplate
10	10	7	12	10	15	5	8	11	12	0.616305	1.0000	NonOverlappingTemplate
6	11	10	8	10	7	14	15	5	14	0.262249	1.0000	NonOverlappingTemplate
12	12	10	8	8	11	10	14	6	9	0.834308	0.9900	NonOverlappingTemplate
16	13	15	3	5	13	12	5	9	9	0.030806	1.0000	NonOverlappingTemplate
13	9	9	12	9	10	14	7	9	8	0.867692	0.9600	NonOverlappingTemplate
12	10	10	15	13	6	4	10	7	13	0.289667	0.9700	NonOverlappingTemplate
11	6	10	8	10	11	12	10	15	7	0.739918	0.9600	NonOverlappingTemplate
14	17	5	14	13	7	7	6	4	13	0.021999	0.9700	NonOverlappingTemplate
11	8	6	12	12	9	6	12	16	8	0.437274	0.9800	NonOverlappingTemplate
8	10	6	9	12	4	9	11	20	11	0.058984	1.0000	NonOverlappingTemplate
11	11	15	7	11	6	6	12	14	7	0.366918	0.9900	NonOverlappingTemplate
9	16	6	7	12	9	11	14	10	6	0.350485	0.9800	NonOverlappingTemplate
14	12	7	10	11	5	9	12	11	9	0.719747	1.0000	NonOverlappingTemplate
10	5	10	9	9	12	12	9	16	8	0.574903	1.0000	NonOverlappingTemplate
8	11	10	16	6	8	13	11	10	7	0.534146	1.0000	NonOverlappingTemplate
10	6	9	9	13	15	10	9	10	9	0.798139	0.9900	NonOverlappingTemplate
10	11	14	8	11	6	11	13	6	10	0.699313	0.9900	NonOverlappingTemplate
9	14	8	14	8	6	12	13	6	10	0.474986	1.0000	NonOverlappingTemplate
5	14	13	8	7	12	10	10	12	9	0.616305	1.0000	NonOverlappingTemplate
10	8	12	8	8	7	11	8	16	12	0.637119	0.9800	NonOverlappingTemplate
10	7	7	7	14	11	6	16	12	10	0.350485	0.9900	NonOverlappingTemplate
5	9	11	16	14	7	6	7	9	16	0.090936	0.9900	NonOverlappingTemplate
11	8	14	13	15	10	6	6	9	8	0.419021	0.9900	NonOverlappingTemplate
6	4	10	12	11	15	9	8	13	12	0.350485	1.0000	NonOverlappingTemplate
8	7	13	9	10	10	10	14	11	8	0.883171	1.0000	NonOverlappingTemplate
9	10	8	12	6	8	12	16	9	10	0.637119	1.0000	NonOverlappingTemplate
13	8	8	2	8	7	15	15	13	11	0.080519	0.9900	NonOverlappingTemplate
9	9	12	13	11	8	14	8	11	5	0.678686	1.0000	NonOverlappingTemplate
11	11	9	6	9	11	6	14	13	10	0.719747	0.9900	NonOverlappingTemplate
13	11	9	11	3	13	11	11	8	10	0.574903	1.0000	NonOverlappingTemplate
10	10	11	9	8	15	11	7	6	13	0.678686	0.9900	NonOverlappingTemplate
10	11	10	13	8	13	5	4	15	11	0.275709	1.0000	NonOverlappingTemplate
13	10	9	6	11	11	12	9	9	10	0.946308	0.9900	NonOverlappingTemplate
6	11	13	8	11	8	14	10	9	10	0.816537	0.9700	NonOverlappingTemplate
14	12	12	9	9	7	14	7	6	10	0.574903	0.9900	NonOverlappingTemplate
11	8	10	9	15	5	9	12	11	10	0.719747	0.9900	NonOverlappingTemplate
12	11	14	14	10	5	7	7	6	14	0.262249	0.9900	NonOverlappingTemplate
10	11	13	12	8	15	7	9	6	9	0.637119	0.9800	NonOverlappingTemplate
9	9	15	11	8	4	14	12	8	10	0.419021	0.9800	NonOverlappingTemplate
12	9	13	11	10	9	10	5	8	13	0.798139	0.9700	NonOverlappingTemplate
12	8	7	11	15	7	8	8	12	12	0.657933	0.9800	NonOverlappingTemplate
10	8	9	13	12	9	12	7	8	12	0.911413	0.9800	NonOverlappingTemplate
15	9	10	8	10	13	5	10	11	9	0.678686	0.9700	NonOverlappingTemplate
10	8	9	14	12	11	8	9	10	9	0.955835	0.9900	NonOverlappingTemplate
11	10	9	8	11	9	11	11	8	12	0.994250	0.9800	NonOverlappingTemplate
16	6	14	15	5	6	9	13	8	8	0.085587	1.0000	NonOverlappingTemplate
9	8	8	9	13	13	10	12	12	6	0.816537	0.9900	NonOverlappingTemplate
7	12	13	9	10	10	9	14	11	5	0.678686	1.0000	NonOverlappingTemplate
9	15	14	12	7	8	8	8	11	8	0.616305	0.9900	NonOverlappingTemplate

```
 12  11  11  10  11   8  11   9   7  10  0.987896   1.0000    NonOverlappingTemplate
  9  13   6  10  13  10   9   9   9  12  0.897763   0.9900    NonOverlappingTemplate
  9   8   8  13  12   7   7  12  13  11  0.798139   1.0000    NonOverlappingTemplate
 13  11  10  12  10   6  10   9  10   9  0.955835   1.0000    NonOverlappingTemplate
 10   9   9   9   8  12  11  10   7  15  0.867692   0.9800    NonOverlappingTemplate
 13   7   8  11  11   9  10  13  11   7  0.883171   1.0000    NonOverlappingTemplate
 15   9   7   8  12  10  11   8  11   9  0.834308   1.0000    NonOverlappingTemplate
  3   9  13  13   8  10  13   8  11  12  0.437274   0.9900    NonOverlappingTemplate
 11  10   9  10   9  10  12   8  11  10  0.998821   0.9900    NonOverlappingTemplate
 14   9  12  11  10  12   2   8   5  17  0.051942   0.9900    NonOverlappingTemplate
 10   5   9  13   9  11  17  11   5  10  0.262249   1.0000    NonOverlappingTemplate
  6  12   9   7   9  18  10  10   8  11  0.350485   0.9900    NonOverlappingTemplate
 17   9   7   7  15  10   3  13  12   7  0.058984   0.9700    NonOverlappingTemplate
 11  10   9   8   8  13  12   7  12  10  0.935716   1.0000    NonOverlappingTemplate
 10  17  11  11   8   6   9  11  12   5  0.334538   1.0000    NonOverlappingTemplate
 11  10  10   8  12   8  15   7  10   9  0.851383   0.9800    NonOverlappingTemplate
 10  15   5   8  14   6   9   8  13  12  0.319084   0.9900    NonOverlappingTemplate
 11   9   5  10  10  11   8  13   8  15  0.637119   1.0000    NonOverlappingTemplate
  8   5  16   4  12  13  11   9  14   8  0.137282   0.9700    NonOverlappingTemplate
 11   8   8   8  10  11   8  11  11  14  0.935716   0.9900    NonOverlappingTemplate
 15  11   7   6  10  11   7   5  18  10  0.090936   0.9900    NonOverlappingTemplate
 16  10   5   7   9  11   9   9   8  16  0.249284   0.9300 *  NonOverlappingTemplate
  4  10   9  11  13  12  10   9  12  10  0.779188   1.0000    NonOverlappingTemplate
 16   6  12  12  11   7  10  10   7   9  0.534146   0.9800    NonOverlappingTemplate
  5  11   8  12   6   9  11  14  18   6  0.096578   1.0000    NonOverlappingTemplate
  8  11  11  11  10   8   9  13  11   8  0.978072   0.9900    NonOverlappingTemplate
 10   9  14   5   5  13  12  11  12   9  0.474986   1.0000    NonOverlappingTemplate
 12  12  10   9   7  11  10  14   6   9  0.816537   0.9900    NonOverlappingTemplate
 10  14   6  11   8  15   5   5  13  13  0.162606   1.0000    OverlappingTemplate
 11   9   8  12   6  13  17   5   9  10  0.275709   1.0000    Universal
 10   6   7   8  13   7  13  15   9  12  0.474986   0.9800    ApproximateEntropy
  6   3   8   6   6   5   6   9   8   8  0.819544   1.0000    RandomExcursions
  9   8   2  12   3   5   6   3   4  13  0.006582   1.0000    RandomExcursions
  4   7   8  10   6   3  10   4  11   2  0.070445   1.0000    RandomExcursions
 12   8   5   5   5   6   4   3  10   7  0.204076   1.0000    RandomExcursions
  4  10   5  10   2   2  10  11   2   9  0.007422   1.0000    RandomExcursions
  6   7   8   4   5   7   6   9   5   8  0.900104   1.0000    RandomExcursions
  3   9   5   8   5   2   9   7   8   9  0.311542   0.9846    RandomExcursions
  6   6  10   6   4   6   5   7   9   6  0.819544   0.9846    RandomExcursions
  6   7   7   6  10   7   9   4   6   3  0.654467   0.9846    RandomExcursionsVariant
  6   6  10   7   7  12   6   5   2   4  0.186566   0.9846    RandomExcursionsVariant
  7   5  10   7   7  10   5   4   6   4  0.585209   0.9846    RandomExcursionsVariant
  8   4   8   9   8   5   4   5   7   7  0.788728   0.9846    RandomExcursionsVariant
  8   3   8   5   5   6  11   7   9   3  0.311542   0.9846    RandomExcursionsVariant
  7   4   7   6   4   7  12   5   4   9  0.337162   0.9846    RandomExcursionsVariant
  8   6   8   5   4   4   4  10   7   9  0.551026   0.9692    RandomExcursionsVariant
  9   6   4   7   8   5   6   9   6   5  0.848588   0.9846    RandomExcursionsVariant
 10   5  10   5   7   6   4   3   8   7  0.452799   0.9692    RandomExcursionsVariant
  7   7   7   3   7   6   4   6   9   9  0.756476   0.9846    RandomExcursionsVariant
  6   7   7   3   7   6   3   8   7  11  0.484646   1.0000    RandomExcursionsVariant
  5   9   8   3   7   4   4  10   6   9  0.392456   1.0000    RandomExcursionsVariant
  6   7   9   7   7   8  10   2   2   7  0.287306   1.0000    RandomExcursionsVariant
  5   2  10  14  10   3   5   8   5   3  0.006582   1.0000    RandomExcursionsVariant
  5   2   9   9   9   8   5   2   8   8  0.204076   1.0000    RandomExcursionsVariant
  6   2   8   6   5   7  11   6   6   8  0.484646   1.0000    RandomExcursionsVariant
  3   6   9   2   9   7   5   7   7  10  0.311542   0.9846    RandomExcursionsVariant
  5   5   8   9   3   3  10   4   8  10  0.204076   0.9846    RandomExcursionsVariant
  6  10  12   9  16   7  12   7  17   4  0.058984   1.0000    Serial
  9  12   6   8   7   7  15  16   9  11  0.304126   0.9900    Serial
 12  14  13   7  12  11   3  11   8   9  0.366918   0.9900    LinearComplexity
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
The minimum pass rate for each statistical test with the exception of the
random excursion (variant) test is approximately = 0.960150 for a
sample size = 100 binary sequences.
The minimum pass rate for the random excursion (variant) test
is approximately 0.952976 for a sample size = 65 binary sequences.
For further guidelines construct a probability table using the MAPLE program
provided in the addendum section of the documentation.
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
```

Результати тестування комбінації розширених матричних та матричних операцій перетворення послідовності із константи зі значенням 150

RESULTS FOR THE UNIFORMITY OF P-VALUES AND THE PROPORTION OF PASSING SEQUENCES

generator is <V_RM_150.bin>

C1	C2	C3	C4	C5	C6	C7	C8	C9	C10	P-VALUE	PROPORTION	STATISTICAL TEST
5	15	7	14	7	15	10	11	9	7	0.213309	0.9900	Frequency
8	10	10	11	12	11	7	9	7	15	0.798139	0.9900	BlockFrequency
9	6	11	12	11	9	13	16	7	6	0.401199	0.9800	CumulativeSums
7	5	11	13	13	14	10	13	8	6	0.366918	1.0000	CumulativeSums
11	7	8	10	11	14	9	10	6	14	0.699313	0.9900	Runs
8	14	9	11	10	10	11	6	9	12	0.883171	0.9900	LongestRun
5	14	10	17	5	8	9	13	8	11	0.145326	1.0000	Rank
1	10	9	11	11	12	10	15	11	10	0.249284	1.0000	FFT
9	10	14	8	13	6	11	9	10	10	0.851383	0.9700	NonOverlappingTemplate
12	8	9	8	14	13	7	7	9	13	0.678686	0.9800	NonOverlappingTemplate
17	11	8	10	11	13	6	9	6	9	0.366918	0.9900	NonOverlappingTemplate
8	17	9	11	10	7	9	9	8	12	0.595549	1.0000	NonOverlappingTemplate
6	12	7	12	15	12	9	10	7	10	0.616305	0.9900	NonOverlappingTemplate
8	12	7	14	15	11	10	8	5	10	0.455937	1.0000	NonOverlappingTemplate
5	7	13	11	8	10	9	11	12	14	0.637119	1.0000	NonOverlappingTemplate
4	7	11	9	12	10	14	12	12	9	0.574903	0.9900	NonOverlappingTemplate
11	11	15	11	12	11	7	11	8	3	0.383827	1.0000	NonOverlappingTemplate
10	12	7	14	11	8	9	10	11	8	0.911413	0.9900	NonOverlappingTemplate
10	7	17	10	14	6	10	7	11	8	0.319084	0.9900	NonOverlappingTemplate
11	10	10	11	11	7	12	12	7	9	0.964295	0.9900	NonOverlappingTemplate
12	11	12	10	7	11	9	8	8	12	0.955835	0.9800	NonOverlappingTemplate
12	14	15	8	4	9	9	9	11	9	0.437274	0.9800	NonOverlappingTemplate
11	8	10	15	10	14	6	7	8	11	0.574903	1.0000	NonOverlappingTemplate
13	5	11	10	11	6	11	14	13	6	0.401199	1.0000	NonOverlappingTemplate
9	11	8	16	10	8	10	3	16	9	0.153763	1.0000	NonOverlappingTemplate
6	9	9	9	14	10	12	11	9	11	0.897763	0.9900	NonOverlappingTemplate
9	11	13	9	10	5	13	8	9	13	0.739918	0.9900	NonOverlappingTemplate
12	10	15	11	8	12	11	4	6	11	0.419021	0.9900	NonOverlappingTemplate
7	13	12	10	7	7	12	16	7	9	0.437274	1.0000	NonOverlappingTemplate
9	8	11	10	15	18	6	7	9	7	0.162606	0.9900	NonOverlappingTemplate
11	10	13	7	9	10	6	10	12	12	0.883171	1.0000	NonOverlappingTemplate
12	13	12	11	8	10	9	7	6	12	0.816537	0.9900	NonOverlappingTemplate
5	10	17	9	10	11	10	8	15	5	0.162606	1.0000	NonOverlappingTemplate
15	8	8	8	8	9	10	12	13	9	0.779188	0.9900	NonOverlappingTemplate
11	7	8	5	16	11	12	9	13	8	0.401199	1.0000	NonOverlappingTemplate
10	5	14	7	11	10	12	7	14	10	0.534146	1.0000	NonOverlappingTemplate
12	7	9	9	8	11	14	13	8	9	0.834308	0.9900	NonOverlappingTemplate
12	7	7	11	11	10	8	7	12	15	0.678686	0.9900	NonOverlappingTemplate
7	6	16	9	10	11	10	8	11	12	0.616305	1.0000	NonOverlappingTemplate
14	12	5	12	10	8	7	8	16	8	0.304126	0.9900	NonOverlappingTemplate
13	9	7	6	6	14	12	10	12	11	0.574903	0.9800	NonOverlappingTemplate
9	9	9	14	12	7	5	13	12	10	0.637119	1.0000	NonOverlappingTemplate
8	11	14	8	11	8	11	13	11	5	0.678686	0.9800	NonOverlappingTemplate
9	7	8	10	14	13	9	10	10	10	0.911413	1.0000	NonOverlappingTemplate
10	18	13	13	6	9	8	11	6	6	0.137282	0.9900	NonOverlappingTemplate
11	12	9	6	12	9	8	11	5	17	0.304126	0.9900	NonOverlappingTemplate
7	8	9	8	10	14	14	12	12	6	0.595549	1.0000	NonOverlappingTemplate
8	11	12	12	10	12	11	5	12	7	0.779188	0.9900	NonOverlappingTemplate
3	17	15	14	12	9	4	8	12	6	0.015598	1.0000	NonOverlappingTemplate
11	5	14	7	8	10	15	8	7	15	0.224821	0.9900	NonOverlappingTemplate
5	12	9	7	15	7	12	9	17	7	0.137282	1.0000	NonOverlappingTemplate
17	10	8	9	12	8	5	17	7	7	0.080519	0.9800	NonOverlappingTemplate
7	9	8	11	18	7	15	7	8	10	0.181557	1.0000	NonOverlappingTemplate
9	10	11	15	10	9	7	8	8	13	0.798139	1.0000	NonOverlappingTemplate
6	8	16	6	13	11	9	15	4	12	0.096578	1.0000	NonOverlappingTemplate
16	6	11	8	12	8	12	13	4	10	0.249284	0.9800	NonOverlappingTemplate
10	11	9	11	10	12	17	5	5	10	0.304126	1.0000	NonOverlappingTemplate
9	5	11	5	9	10	12	10	13	16	0.334538	1.0000	NonOverlappingTemplate
5	12	10	7	10	14	14	9	9	10	0.616305	0.9900	NonOverlappingTemplate

8	14	8	7	13	11	6	11	7	15	0.401199	0.9900	NonOverlappingTemplate
8	10	8	13	7	10	9	8	13	14	0.779188	1.0000	NonOverlappingTemplate
7	6	14	8	14	10	10	8	13	10	0.595549	1.0000	NonOverlappingTemplate
7	16	14	12	4	8	11	12	5	11	0.137282	0.9900	NonOverlappingTemplate
7	11	11	10	7	9	13	9	12	11	0.935716	0.9900	NonOverlappingTemplate
8	4	14	11	11	12	10	12	12	6	0.474986	1.0000	NonOverlappingTemplate
9	11	6	10	10	6	13	13	13	9	0.719747	1.0000	NonOverlappingTemplate
11	10	8	12	8	9	9	8	12	13	0.955835	0.9800	NonOverlappingTemplate
9	14	7	6	8	9	12	7	17	11	0.275709	1.0000	NonOverlappingTemplate
6	10	6	17	13	11	7	12	7	11	0.249284	0.9900	NonOverlappingTemplate
23	13	8	10	4	7	9	8	9	9	0.005358	0.9800	NonOverlappingTemplate
14	8	6	8	11	5	12	12	8	16	0.249284	1.0000	NonOverlappingTemplate
12	11	12	10	10	11	12	4	7	11	0.739918	1.0000	NonOverlappingTemplate
13	9	12	11	7	8	6	15	7	12	0.514124	0.9700	NonOverlappingTemplate
12	8	12	17	8	9	7	9	7	11	0.474986	0.9900	NonOverlappingTemplate
12	7	14	12	9	9	7	10	15	5	0.401199	0.9700	NonOverlappingTemplate
9	7	10	13	10	8	8	9	8	18	0.383827	0.9700	NonOverlappingTemplate
8	11	16	11	11	12	5	8	9	9	0.554420	1.0000	NonOverlappingTemplate
10	10	12	11	11	8	5	10	13	10	0.883171	0.9800	NonOverlappingTemplate
10	6	10	10	9	6	13	16	8	12	0.474986	1.0000	NonOverlappingTemplate
10	12	13	10	9	10	6	9	9	12	0.935716	0.9900	NonOverlappingTemplate
16	12	5	12	8	9	14	10	9	5	0.236810	0.9900	NonOverlappingTemplate
10	8	9	16	8	16	11	9	8	5	0.262249	0.9900	NonOverlappingTemplate
10	9	15	7	13	6	11	9	10	10	0.719747	0.9700	NonOverlappingTemplate
8	10	6	10	15	14	8	9	12	8	0.595549	1.0000	NonOverlappingTemplate
7	16	13	11	7	12	11	7	8	8	0.474986	0.9900	NonOverlappingTemplate
11	14	8	10	8	9	11	8	10	11	0.955835	0.9800	NonOverlappingTemplate
10	6	6	12	14	13	12	12	7	8	0.514124	0.9900	NonOverlappingTemplate
13	14	13	10	11	12	7	10	5	5	0.366918	0.9800	NonOverlappingTemplate
7	9	11	7	10	10	11	12	15	8	0.798139	0.9900	NonOverlappingTemplate
14	11	12	10	8	10	4	5	9	17	0.137282	0.9900	NonOverlappingTemplate
15	9	8	5	9	10	8	16	11	9	0.366918	1.0000	NonOverlappingTemplate
9	11	14	5	13	11	7	9	12	9	0.657933	0.9900	NonOverlappingTemplate
12	10	11	10	4	6	11	11	11	14	0.574903	1.0000	NonOverlappingTemplate
11	14	13	10	13	7	8	8	8	8	0.739918	0.9500 *	NonOverlappingTemplate
8	8	6	8	8	12	12	12	15	11	0.637119	0.9900	NonOverlappingTemplate
9	13	9	3	13	7	11	14	8	13	0.289667	0.9900	NonOverlappingTemplate
10	13	9	12	6	11	5	10	12	12	0.699313	0.9900	NonOverlappingTemplate
7	9	12	10	10	14	10	10	11	7	0.911413	1.0000	NonOverlappingTemplate
13	17	8	11	10	11	11	4	9	6	0.224821	0.9900	NonOverlappingTemplate
10	10	12	3	11	11	12	13	10	8	0.616305	1.0000	NonOverlappingTemplate
9	13	9	6	13	12	9	13	8	8	0.759756	0.9800	NonOverlappingTemplate
6	14	10	12	17	5	6	13	6	11	0.085587	1.0000	NonOverlappingTemplate
11	10	10	9	7	6	13	14	11	9	0.798139	0.9800	NonOverlappingTemplate
9	12	6	7	11	8	14	13	13	7	0.554420	1.0000	NonOverlappingTemplate
11	8	10	15	8	8	12	10	7	11	0.816537	0.9600	NonOverlappingTemplate
16	14	9	5	12	10	11	7	7	9	0.334538	0.9800	NonOverlappingTemplate
10	15	6	12	11	7	8	7	14	10	0.494392	0.9900	NonOverlappingTemplate
15	10	6	8	10	11	7	14	7	12	0.494392	0.9900	NonOverlappingTemplate
11	10	14	9	16	7	5	7	12	9	0.334538	1.0000	NonOverlappingTemplate
9	15	11	9	13	9	8	11	8	7	0.779188	1.0000	NonOverlappingTemplate
12	6	8	7	8	12	9	13	12	13	0.699313	0.9800	NonOverlappingTemplate
11	6	5	11	16	10	9	12	10	10	0.494392	1.0000	NonOverlappingTemplate
12	14	11	9	11	8	7	10	8	10	0.911413	0.9800	NonOverlappingTemplate
14	11	4	11	10	9	10	13	8	10	0.657933	0.9700	NonOverlappingTemplate
11	9	7	9	10	11	10	13	8	12	0.964295	0.9900	NonOverlappingTemplate
8	14	11	10	9	10	11	2	8	17	0.122325	1.0000	NonOverlappingTemplate
11	9	9	7	16	5	12	9	13	9	0.455937	0.9800	NonOverlappingTemplate
7	11	15	10	9	2	9	11	6	20	0.009535	0.9900	NonOverlappingTemplate
12	12	12	4	5	11	12	10	12	10	0.514124	0.9700	NonOverlappingTemplate
10	13	10	5	10	6	13	5	10	18	0.096578	1.0000	NonOverlappingTemplate
14	12	9	9	6	13	10	11	7	9	0.759756	0.9800	NonOverlappingTemplate
11	10	8	10	7	8	13	8	14	11	0.851383	1.0000	NonOverlappingTemplate
10	13	13	10	11	11	10	8	4	10	0.739918	0.9900	NonOverlappingTemplate
12	11	11	10	9	7	11	12	9	8	0.978072	0.9900	NonOverlappingTemplate
10	11	12	7	7	9	11	8	10	15	0.798139	1.0000	NonOverlappingTemplate
10	12	12	7	8	11	8	10	14	8	0.867692	1.0000	NonOverlappingTemplate
17	7	10	5	13	10	10	8	9	11	0.366918	1.0000	NonOverlappingTemplate
15	8	12	11	5	10	9	11	4	15	0.202268	0.9800	NonOverlappingTemplate
11	6	12	9	12	7	13	5	9	16	0.304126	1.0000	NonOverlappingTemplate
5	10	11	13	11	6	7	8	19	10	0.102526	0.9900	NonOverlappingTemplate

```
  8  11  10   8  11  13  14  11   5   9  0.719747   1.0000    NonOverlappingTemplate
  9  10   8   6  11  14  14  10   9   9  0.779188   0.9900    NonOverlappingTemplate
 15   9   7   7   9   8  14   8  14   9  0.474986   0.9900    NonOverlappingTemplate
 11   8   7  13   8  10   9  11   8  15  0.759756   1.0000    NonOverlappingTemplate
 12   9  10  13  12   9   9   8   8  10  0.971699   0.9800    NonOverlappingTemplate
  7   9   6  15  14  10   5   5  16  13  0.062821   1.0000    NonOverlappingTemplate
 13  16  10   7  11  12   7   4   4  16  0.040108   1.0000    NonOverlappingTemplate
 12   8   9  12   8   4  12  10  14  11  0.595549   0.9700    NonOverlappingTemplate
  9  11  15  11   9  13   8   9   7   8  0.779188   0.9900    NonOverlappingTemplate
  6   9  11  12  11   9   7  12  15   8  0.678686   0.9900    NonOverlappingTemplate
  5   9   9   8  11  10  14   9  10  15  0.595549   0.9900    NonOverlappingTemplate
  8   8  14   8   9  12   8  12   9  12  0.867692   0.9900    NonOverlappingTemplate
 14  11  14   6   6   8  11  12  14   4  0.181557   0.9900    NonOverlappingTemplate
  7  13  10  11   7  12  12   4  13  11  0.514124   0.9800    NonOverlappingTemplate
 10  11  14   4  12   5  13  10  11  10  0.419021   0.9800    NonOverlappingTemplate
  9  13  12   7   7  12   9   6   8  17  0.304126   1.0000    NonOverlappingTemplate
  9  13  10  14   8   8   9   8  10  11  0.911413   1.0000    NonOverlappingTemplate
  6  11  11  10  11   9  13   5  12  12  0.719747   1.0000    NonOverlappingTemplate
  9  19  10  10   6  10   7   4  11  14  0.066882   0.9800    NonOverlappingTemplate
 10  14  12   9   9   6   6  10  12  12  0.719747   1.0000    NonOverlappingTemplate
  9  14   8  11  11  10  10  10   9   8  0.971699   0.9900    NonOverlappingTemplate
  5   7  13  10  16  13   9   7   7  13  0.236810   1.0000    NonOverlappingTemplate
  8  14   7   8  17  10   6   6  12  12  0.202268   1.0000    NonOverlappingTemplate
 13  10   8  10   7   7  14  11  13   7  0.678686   0.9800    NonOverlappingTemplate
 14   8   5   7  10   5  13  13  11  14  0.249284   1.0000    NonOverlappingTemplate
 10   8  10  15   8  17  10   9   8   5  0.262249   0.9900    NonOverlappingTemplate
 10   7  10   8  15   8   9  12  11  10  0.851383   0.9900    OverlappingTemplate
 11  11   9   8  12   8   6  14   9  12  0.816537   0.9900    Universal
  2  14  10   9  11  10  11   9  11  13  0.401199   0.9900    ApproximateEntropy
  7   5   6  10   2  12  10   5   4   3  0.054199   0.9688    RandomExcursions
  4   7   1   8  13   6   9   2  10   4  0.011250   0.9844    RandomExcursions
  4   7   5  12   5   6   7   2   5  11  0.110952   1.0000    RandomExcursions
 10   8   8   5   6   3   5   2   7  10  0.253551   1.0000    RandomExcursions
  9   5   2   3  12   9   6   7   4   7  0.110952   0.9844    RandomExcursions
  9   7   4  12   2   5   5   4   6  10  0.100508   1.0000    RandomExcursions
  6   7   7   5   4   9   8   5   6   7  0.931952   1.0000    RandomExcursions
  6   2   7   5  11   5   9   5   6   8  0.378138   1.0000    RandomExcursions
  8   4   9   6   8   4   7   7   7   4  0.804337   1.0000    RandomExcursionsVariant
  8   6   6   4   6   4   9   5  10   6  0.706149   1.0000    RandomExcursionsVariant
  7   7   5   5   4  10   6   7   4   9  0.706149   1.0000    RandomExcursionsVariant
  7   5   4   7   3   8   6  11  10   3  0.232760   0.9844    RandomExcursionsVariant
  5   8   6   5   4   4   6   9   9   8  0.739918   1.0000    RandomExcursionsVariant
  4   8   5   8   6   6   7   6   6   8  0.964295   1.0000    RandomExcursionsVariant
  4   5   4  13   5   4  10   5   5   9  0.090936   1.0000    RandomExcursionsVariant
  5   3   9   8   7  11   3   8   6   4  0.275709   1.0000    RandomExcursionsVariant
  5   9   5   7   5  10   5   6   9   3  0.534146   1.0000    RandomExcursionsVariant
  6   6   9   5  11   5   3   6   3  10  0.232760   1.0000    RandomExcursionsVariant
  4   3  11   6   5  10   9   8   5   3  0.162606   1.0000    RandomExcursionsVariant
  4   2   9   6   7   8   7  14   5   2  0.022503   0.9844    RandomExcursionsVariant
  6   5   7   6   3  11   9   3   6   8  0.378138   1.0000    RandomExcursionsVariant
  6   9   4   6   4   6   7   6   5  11  0.602458   0.9688    RandomExcursionsVariant
  5   6   8   3  12   5   7   2   4  12  0.035174   0.9688    RandomExcursionsVariant
  5   7   8   4   6   7   5   9   5   8  0.888137   0.9688    RandomExcursionsVariant
  8   6   5   5   4  12   7   3   6   8  0.350485   0.9688    RandomExcursionsVariant
  5  10   5   5   5   8   8   9   3   6  0.568055   0.9688    RandomExcursionsVariant
 10   7  14   8  14   6  12  15   5   9  0.236810   0.9900    Serial
  9  14  11  10   7  11   7  13  10   8  0.834308   0.9900    Serial
 10  12  13   9   8  10   7  10  12   9  0.955835   0.9800    LinearComplexity
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
The minimum pass rate for each statistical test with the exception of the
random excursion (variant) test is approximately = 0.960150 for a
sample size = 100 binary sequences.
The minimum pass rate for the random excursion (variant) test
is approximately 0.952688 for a sample size = 64 binary sequences.
For further guidelines construct a probability table using the MAPLE program
provided in the addendum section of the documentation.
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
```

Результати тестування застосування комбінації операцій розширеного матричного та матричного перетворення над текстовою інформацією

RESULTS FOR THE UNIFORMITY OF P-VALUES AND THE PROPORTION OF PASSING SEQUENCES

generator is <V_RM_TXT.bin>

C1	C2	C3	C4	C5	C6	C7	C8	C9	C10	P-VALUE		PROPORTION	STATISTICAL TEST
18	10	9	9	11	12	9	6	10	6	0.319084		0.9800	Frequency
16	9	13	10	12	4	14	4	7	11	0.096578		0.9900	BlockFrequency
16	12	8	8	10	10	4	13	11	8	0.366918		0.9800	CumulativeSums
15	11	8	5	10	12	6	11	13	9	0.474986		0.9800	CumulativeSums
8	7	8	16	9	11	8	9	12	12	0.657933		1.0000	Runs
7	8	6	8	5	15	10	12	16	13	0.153763		0.9900	LongestRun
12	11	13	10	8	10	8	11	5	12	0.816537		0.9900	Rank
2	4	6	13	13	22	6	9	7	18	0.000029	*	0.9900	FFT
11	10	9	12	10	8	10	10	11	9	0.998821		1.0000	NonOverlappingTemplate
12	6	10	8	10	9	13	14	7	11	0.739918		1.0000	NonOverlappingTemplate
9	7	13	10	11	13	10	9	7	11	0.911413		0.9800	NonOverlappingTemplate
6	9	11	9	10	11	10	11	12	11	0.978072		0.9900	NonOverlappingTemplate
12	7	15	6	9	7	9	14	10	11	0.514124		0.9900	NonOverlappingTemplate
12	10	8	9	12	5	15	12	7	10	0.574903		0.9600	NonOverlappingTemplate
8	11	12	12	8	11	10	12	8	8	0.964295		1.0000	NonOverlappingTemplate
16	11	4	11	8	11	10	9	9	11	0.514124		0.9900	NonOverlappingTemplate
6	11	7	10	9	13	13	12	9	10	0.834308		1.0000	NonOverlappingTemplate
7	11	10	13	7	11	10	8	10	13	0.897763		0.9900	NonOverlappingTemplate
15	9	13	7	14	13	5	9	4	11	0.153763		0.9800	NonOverlappingTemplate
13	11	8	8	12	11	10	10	11	6	0.911413		1.0000	NonOverlappingTemplate
13	15	10	5	6	14	13	8	12	4	0.108791		0.9700	NonOverlappingTemplate
8	10	7	9	6	10	14	11	12	13	0.739918		0.9900	NonOverlappingTemplate
12	10	12	7	9	15	14	10	2	9	0.191687		1.0000	NonOverlappingTemplate
15	9	10	7	11	5	17	14	8	4	0.055361		1.0000	NonOverlappingTemplate
7	7	9	12	12	9	11	15	9	9	0.779188		0.9900	NonOverlappingTemplate
6	13	11	17	9	7	7	13	10	7	0.262249		1.0000	NonOverlappingTemplate
7	7	8	15	10	8	14	14	4	13	0.171867		0.9900	NonOverlappingTemplate
5	7	15	10	11	13	10	7	6	16	0.162606		1.0000	NonOverlappingTemplate
4	22	13	4	13	8	7	7	13	9	0.001628		1.0000	NonOverlappingTemplate
14	13	6	9	13	14	10	5	12	4	0.153763		0.9900	NonOverlappingTemplate
7	8	15	11	13	6	15	13	4	8	0.129620		1.0000	NonOverlappingTemplate
12	10	9	11	10	17	9	8	7	7	0.554420		0.9800	NonOverlappingTemplate
9	7	9	11	8	13	10	10	12	11	0.964295		0.9900	NonOverlappingTemplate
14	9	7	16	10	4	7	8	10	15	0.137282		0.9900	NonOverlappingTemplate
12	15	5	5	12	6	6	13	16	10	0.066882		0.9800	NonOverlappingTemplate
12	10	7	13	10	9	8	10	8	13	0.911413		0.9700	NonOverlappingTemplate
7	7	19	6	12	12	10	5	15	7	0.032923		0.9900	NonOverlappingTemplate
13	13	14	6	6	2	7	14	16	9	0.023545		0.9900	NonOverlappingTemplate
9	9	17	6	12	12	6	7	11	11	0.334538		1.0000	NonOverlappingTemplate
10	9	17	9	13	16	6	6	7	7	0.102526		1.0000	NonOverlappingTemplate
5	9	9	7	10	8	10	9	14	19	0.129620		1.0000	NonOverlappingTemplate
12	9	16	12	6	9	9	8	14	5	0.289667		1.0000	NonOverlappingTemplate
16	5	7	7	8	14	12	8	10	13	0.236810		1.0000	NonOverlappingTemplate
9	9	11	13	8	6	6	16	12	10	0.455937		0.9900	NonOverlappingTemplate
11	6	10	11	13	8	10	8	7	16	0.534146		0.9600	NonOverlappingTemplate
16	6	7	12	9	7	11	13	10	9	0.474986		0.9600	NonOverlappingTemplate
9	12	13	11	11	10	9	10	8	7	0.964295		0.9900	NonOverlappingTemplate
6	10	5	14	8	14	8	18	10	7	0.080519		0.9900	NonOverlappingTemplate
6	11	11	9	15	10	5	12	8	13	0.474986		1.0000	NonOverlappingTemplate
8	7	13	14	11	10	7	9	13	8	0.719747		1.0000	NonOverlappingTemplate
15	9	11	7	9	9	12	14	2	12	0.181557		0.9900	NonOverlappingTemplate
12	10	11	9	11	7	10	11	7	12	0.964295		0.9900	NonOverlappingTemplate
7	7	18	14	7	8	12	10	8	9	0.213309		1.0000	NonOverlappingTemplate
12	12	14	11	4	10	12	7	10	8	0.554420		0.9900	NonOverlappingTemplate
8	8	10	10	10	10	7	11	16	10	0.798139		0.9900	NonOverlappingTemplate
14	6	11	10	9	6	10	8	17	9	0.319084		0.9900	NonOverlappingTemplate
8	9	9	10	10	11	9	13	12	9	0.987896		0.9800	NonOverlappingTemplate
11	12	7	6	16	5	8	14	7	14	0.137282		0.9600	NonOverlappingTemplate
10	14	4	13	13	9	8	9	10	10	0.574903		1.0000	NonOverlappingTemplate

15	9	9	7	13	7	7	9	16	8	0.319084	0.9700	NonOverlappingTemplate
14	8	11	7	8	10	11	14	8	9	0.779188	1.0000	NonOverlappingTemplate
11	8	10	10	5	12	6	18	11	9	0.236810	0.9900	NonOverlappingTemplate
7	9	10	17	5	13	4	11	15	9	0.075719	1.0000	NonOverlappingTemplate
12	10	14	4	6	14	14	9	9	8	0.275709	0.9700	NonOverlappingTemplate
5	14	11	15	10	10	9	11	6	9	0.474986	1.0000	NonOverlappingTemplate
13	10	12	11	10	9	7	7	8	13	0.867692	0.9900	NonOverlappingTemplate
13	11	5	12	7	8	12	11	9	12	0.719747	0.9900	NonOverlappingTemplate
8	7	14	10	9	15	7	11	9	10	0.678686	0.9900	NonOverlappingTemplate
12	9	11	9	13	9	10	7	10	10	0.978072	1.0000	NonOverlappingTemplate
6	7	9	16	7	14	10	8	11	12	0.383827	1.0000	NonOverlappingTemplate
9	7	9	8	8	19	8	9	10	13	0.249284	0.9900	NonOverlappingTemplate
8	17	9	13	7	7	12	7	10	10	0.401199	0.9900	NonOverlappingTemplate
11	14	9	5	11	12	12	12	11	3	0.304126	0.9900	NonOverlappingTemplate
14	5	4	14	11	14	8	11	11	8	0.213309	1.0000	NonOverlappingTemplate
15	5	12	8	13	11	6	11	9	10	0.474986	0.9800	NonOverlappingTemplate
12	10	5	10	9	11	6	19	7	11	0.129620	0.9900	NonOverlappingTemplate
8	9	11	12	6	10	13	11	9	11	0.924076	1.0000	NonOverlappingTemplate
12	6	8	10	11	11	10	9	10	13	0.935716	0.9800	NonOverlappingTemplate
9	12	9	7	11	8	11	8	12	13	0.924076	0.9900	NonOverlappingTemplate
13	9	10	8	6	13	10	15	6	10	0.534146	0.9900	NonOverlappingTemplate
14	8	13	6	13	6	7	8	13	12	0.383827	0.9700	NonOverlappingTemplate
18	6	8	9	13	10	7	10	11	8	0.289667	0.9900	NonOverlappingTemplate
11	10	9	12	10	8	10	10	11	9	0.998821	1.0000	NonOverlappingTemplate
8	10	8	14	9	10	13	10	8	10	0.924076	1.0000	NonOverlappingTemplate
9	13	10	7	10	11	11	11	12	6	0.897763	0.9900	NonOverlappingTemplate
10	7	12	10	10	13	10	7	12	9	0.935716	1.0000	NonOverlappingTemplate
16	10	7	14	11	10	12	7	6	7	0.350485	0.9900	NonOverlappingTemplate
11	4	12	9	11	8	13	6	15	11	0.366918	0.9900	NonOverlappingTemplate
16	8	10	9	6	10	16	9	9	7	0.319084	0.9700	NonOverlappingTemplate
6	13	15	13	7	10	6	4	15	11	0.102526	1.0000	NonOverlappingTemplate
8	9	10	11	9	12	12	11	9	9	0.994250	1.0000	NonOverlappingTemplate
17	6	8	13	9	7	14	10	7	9	0.249284	1.0000	NonOverlappingTemplate
6	11	6	13	10	13	11	12	11	7	0.678686	1.0000	NonOverlappingTemplate
13	12	6	10	9	14	7	12	7	10	0.657933	0.9800	NonOverlappingTemplate
14	8	15	9	7	5	10	9	9	14	0.366918	0.9800	NonOverlappingTemplate
8	4	12	10	13	11	8	14	12	8	0.514124	1.0000	NonOverlappingTemplate
13	7	7	12	10	8	7	15	9	12	0.595549	1.0000	NonOverlappingTemplate
12	8	10	5	9	9	9	13	12	13	0.759756	0.9900	NonOverlappingTemplate
4	10	9	6	13	8	15	16	10	9	0.171867	0.9900	NonOverlappingTemplate
8	11	10	7	16	7	6	15	12	8	0.289667	0.9900	NonOverlappingTemplate
9	10	9	6	10	10	15	11	14	6	0.574903	0.9900	NonOverlappingTemplate
12	10	10	13	11	7	10	13	8	6	0.816537	0.9900	NonOverlappingTemplate
9	7	7	16	13	9	13	6	9	11	0.419021	1.0000	NonOverlappingTemplate
11	13	11	9	7	7	9	9	14	10	0.851383	1.0000	NonOverlappingTemplate
8	13	10	11	10	9	9	10	6	14	0.851383	1.0000	NonOverlappingTemplate
9	10	9	12	14	10	8	8	7	13	0.851383	1.0000	NonOverlappingTemplate
12	8	9	11	9	8	11	9	11	12	0.987896	0.9600	NonOverlappingTemplate
7	9	13	6	10	7	11	8	13	16	0.401199	1.0000	NonOverlappingTemplate
12	7	11	16	15	10	6	9	5	9	0.224821	1.0000	NonOverlappingTemplate
11	10	6	16	6	7	12	12	11	9	0.455937	0.9900	NonOverlappingTemplate
9	8	10	11	11	17	8	12	5	9	0.437274	0.9900	NonOverlappingTemplate
12	12	7	6	9	12	13	14	8	7	0.574903	1.0000	NonOverlappingTemplate
17	8	13	8	11	11	7	6	11	8	0.366918	0.9900	NonOverlappingTemplate
8	10	7	9	11	12	11	12	8	12	0.955835	0.9900	NonOverlappingTemplate
11	16	11	8	13	8	9	9	11	4	0.401199	0.9700	NonOverlappingTemplate
11	10	16	3	8	8	6	10	18	10	0.042808	0.9800	NonOverlappingTemplate
7	14	15	12	14	14	4	6	6	8	0.071177	1.0000	NonOverlappingTemplate
10	10	17	7	14	8	6	8	11	9	0.350485	0.9900	NonOverlappingTemplate
12	12	15	8	11	12	5	2	10	13	0.122325	0.9900	NonOverlappingTemplate
10	13	8	3	4	7	11	11	14	19	0.014550	1.0000	NonOverlappingTemplate
6	14	11	12	7	10	11	12	7	10	0.739918	1.0000	NonOverlappingTemplate
11	9	12	10	12	9	7	11	10	9	0.987896	0.9800	NonOverlappingTemplate
8	9	13	7	8	13	12	11	12	7	0.798139	0.9900	NonOverlappingTemplate
9	8	8	5	10	7	11	19	10	13	0.145326	0.9700	NonOverlappingTemplate
15	12	13	10	8	5	12	5	7	13	0.249284	0.9900	NonOverlappingTemplate
11	9	10	9	14	7	9	10	15	6	0.637119	0.9900	NonOverlappingTemplate
4	3	18	9	11	11	15	12	12	5	0.012650	1.0000	NonOverlappingTemplate
11	4	3	13	13	14	10	13	9	10	0.162606	0.9700	NonOverlappingTemplate
11	9	12	12	8	12	10	9	10	7	0.971699	1.0000	NonOverlappingTemplate
10	11	9	14	12	10	11	7	6	10	0.851383	1.0000	NonOverlappingTemplate

```
  9  10   6   9  10  13  18  11   9   5  0.224821   1.0000    NonOverlappingTemplate
  7   9   9  12  12  14   9   7  11  10  0.867692   1.0000    NonOverlappingTemplate
 14  13   7  12   7   9  10  10   9   9  0.834308   0.9700    NonOverlappingTemplate
 14  12   7   8  11   5  12  12  14   5  0.289667   1.0000    NonOverlappingTemplate
  6   8   9  11  11   7   8  11  14  15  0.554420   1.0000    NonOverlappingTemplate
 10  10   5   8  11  15   9   6  16  10  0.289667   0.9900    NonOverlappingTemplate
  9  11   5   7  16   7  12  12  12   9  0.401199   0.9900    NonOverlappingTemplate
  9  12   5  17  13   8  11   7   8  10  0.304126   0.9500 *  NonOverlappingTemplate
  5  11  11   9  18   7   7  10  12  10  0.249284   1.0000    NonOverlappingTemplate
 12   9  11   4   9   9  13  14  11   8  0.595549   0.9900    NonOverlappingTemplate
  6  12  13   8  13   9   8  10   9  12  0.816537   1.0000    NonOverlappingTemplate
 15   9  10   8  14   9   4  12   8  11  0.419021   0.9900    NonOverlappingTemplate
 14  10  12   8   4   5   9   9  14  15  0.171867   0.9900    NonOverlappingTemplate
 17   7   9  13   8   7   9   8  13   9  0.383827   0.9900    NonOverlappingTemplate
 13  12   7   6  10   8  11  12  10  11  0.851383   0.9800    NonOverlappingTemplate
  5  10   9   6  14   7  15   9   6  19  0.025193   0.9900    NonOverlappingTemplate
 11  10   6  12  12  15   8  11   7   8  0.657933   0.9900    NonOverlappingTemplate
 13  13  16   8   4   9  12   9   6  10  0.236810   0.9800    NonOverlappingTemplate
  4  13  18   9   5   7  13  12  11   8  0.062821   1.0000    NonOverlappingTemplate
 10  11  14   9   8   8   7  11  14   8  0.779188   1.0000    NonOverlappingTemplate
 10   9  12   9   9   8   8   9  18   8  0.494392   1.0000    NonOverlappingTemplate
  5  14   9  10   9  11   5   9  14  14  0.334538   1.0000    NonOverlappingTemplate
 12  10  10  13  11  11  11   8   8   6  0.911413   0.9800    NonOverlappingTemplate
  7   9  11  13   4  11  11  16  11   7  0.319084   1.0000    NonOverlappingTemplate
 10   7  15   7   9  11   7   8  19   7  0.096578   0.9900    NonOverlappingTemplate
 18   6   8   9  13  10   7  11  10   8  0.289667   0.9900    NonOverlappingTemplate
  6   3  16  12  10  14  16   9   8   6  0.037566   0.9800    OverlappingTemplate
  9  10  15   9   8  10  11   8   8  12  0.883171   0.9700    Universal
 11  12  11  13   9  10   9  12   6   7  0.867692   1.0000    ApproximateEntropy
  5   6   4   9   6   3   5   4  10   6  0.350485   1.0000    RandomExcursions
  4   3   4   9   5  11   6   5   7   4  0.171867   0.9828    RandomExcursions
  5   5   9   8   1   8   3   6   6   7  0.213309   1.0000    RandomExcursions
  6   6   4   8   2   9   7   3   7   6  0.350485   1.0000    RandomExcursions
  8   6   8   5   7   5   2   3   4  10  0.191687   1.0000    RandomExcursions
  6   5   4   7   4   9   6   8   5   4  0.657933   1.0000    RandomExcursions
  7   5   6   4   6   5   5   5  10   5  0.699313   0.9655    RandomExcursions
  3   7   9   2   8   3   7   5   4  10  0.085587   0.9828    RandomExcursions
  3   2   9   3   9   3   8   7   8   6  0.085587   1.0000    RandomExcursionsVariant
  2   4   7   4  10   2   8   7  10   4  0.040108   1.0000    RandomExcursionsVariant
  3   5   4   6   6   8   8   8   4   6  0.616305   0.9828    RandomExcursionsVariant
  3   5   6   7   7   6   8   7   5   4  0.779188   0.9828    RandomExcursionsVariant
  6   1  11   4   8   7   8   5   4   4  0.075719   1.0000    RandomExcursionsVariant
  3   8   9   6   6   8   7   5   3   3  0.319084   1.0000    RandomExcursionsVariant
  7   2   5   9   5   8   7   7   5   3  0.350485   1.0000    RandomExcursionsVariant
  6   6   2   3   8   9   9   5   2   8  0.096578   0.9828    RandomExcursionsVariant
  7   6   3   4   5  13   3   4   8   5  0.040108   0.9655    RandomExcursionsVariant
  3   9   5   5   4   7  12   3   3   7  0.045675   1.0000    RandomExcursionsVariant
  5   5   6   4   6   9   9   4   6   4  0.574903   1.0000    RandomExcursionsVariant
  3   7   4   5   2   7   8   7   6   9  0.319084   1.0000    RandomExcursionsVariant
  4   3   5   6   6   7  10   3   9   5  0.262249   1.0000    RandomExcursionsVariant
  5   1   6   8   6   4   9   4   9   6  0.191687   0.9828    RandomExcursionsVariant
  3   5   6   7   5   5   4   7   9   7  0.657933   0.9828    RandomExcursionsVariant
  3   4   8   5   6   6   7   9   6   4  0.574903   0.9828    RandomExcursionsVariant
  4   5   4  10   3   9   4   8   6   5  0.236810   0.9828    RandomExcursionsVariant
  6   4   5   8   6   5   8   1   8   7  0.350485   0.9828    RandomExcursionsVariant
  6  12  12  14   9   7   8   8  14  10  0.595549   1.0000    Serial
  8  11  12   6  11  14  11   6  11  10  0.739918   0.9900    Serial
  8  12  10  10  12  14  10  11   5   8  0.759756   0.9900    LinearComplexity
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
The minimum pass rate for each statistical test with the exception of the
random excursion (variant) test is approximately = 0.960150 for a
sample size = 100 binary sequences.
The minimum pass rate for the random excursion (variant) test
is approximately 0.950806 for a sample size = 58 binary sequences.
For further guidelines construct a probability table using the MAPLE program
provided in the addendum section of the documentation.
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
```

Результати тестування вбудованого програмного датчика random з додатковою обробкою результатів матричними операціями криптографічного перетворення

RESULTS FOR THE UNIFORMITY OF P-VALUES AND THE PROPORTION OF PASSING SEQUENCES

generator is <V_M_ROND.bin>

C1	C2	C3	C4	C5	C6	C7	C8	C9	C10	P-VALUE	PROPORTION	STATISTICAL TEST
6	16	9	12	13	9	11	8	5	11	0.366918	1.0000	Frequency
8	8	14	11	6	11	8	10	10	14	0.719747	0.9900	BlockFrequency
7	15	11	7	5	15	12	7	10	11	0.289667	1.0000	CumulativeSums
10	11	13	12	7	13	5	10	9	10	0.759756	1.0000	CumulativeSums
7	10	13	6	10	12	9	17	4	12	0.171867	1.0000	Runs
15	10	10	16	5	6	13	9	9	7	0.202268	0.9700	LongestRun
11	9	18	7	8	8	9	8	11	11	0.437274	0.9900	Rank
2	10	6	10	12	14	12	11	14	9	0.202268	1.0000	FFT
3	7	11	18	10	12	8	11	12	8	0.122325	1.0000	NonOverlappingTemplate
5	14	5	11	11	13	7	15	9	10	0.262249	1.0000	NonOverlappingTemplate
11	10	13	13	9	7	13	5	13	6	0.455937	1.0000	NonOverlappingTemplate
12	9	9	8	10	16	7	11	8	10	0.739918	1.0000	NonOverlappingTemplate
13	9	12	11	14	6	10	6	6	13	0.455937	1.0000	NonOverlappingTemplate
8	7	11	16	12	9	10	15	4	8	0.213309	1.0000	NonOverlappingTemplate
17	4	9	16	9	13	7	9	7	9	0.085587	1.0000	NonOverlappingTemplate
15	10	12	6	6	9	9	11	10	12	0.657933	0.9700	NonOverlappingTemplate
7	12	8	9	16	7	9	10	9	13	0.595549	0.9700	NonOverlappingTemplate
11	9	8	12	13	9	7	9	15	7	0.699313	1.0000	NonOverlappingTemplate
10	7	15	9	10	9	12	12	13	3	0.334538	0.9700	NonOverlappingTemplate
13	13	12	11	6	10	11	4	8	12	0.494392	0.9800	NonOverlappingTemplate
13	5	3	16	14	11	14	12	4	8	0.020548	1.0000	NonOverlappingTemplate
11	6	16	9	9	7	6	21	10	5	0.007160	0.9900	NonOverlappingTemplate
16	9	11	7	10	9	9	6	9	14	0.514124	0.9700	NonOverlappingTemplate
9	16	8	9	13	10	6	12	7	10	0.534146	0.9900	NonOverlappingTemplate
13	9	8	13	8	9	10	12	6	12	0.816537	1.0000	NonOverlappingTemplate
9	13	10	7	11	7	10	9	14	10	0.867692	1.0000	NonOverlappingTemplate
4	10	10	6	13	11	12	10	7	17	0.191687	0.9800	NonOverlappingTemplate
10	10	5	17	7	7	8	11	12	13	0.275709	1.0000	NonOverlappingTemplate
9	19	9	8	7	8	10	10	5	15	0.090936	0.9900	NonOverlappingTemplate
13	10	12	12	12	9	8	9	5	10	0.816537	0.9900	NonOverlappingTemplate
11	17	8	11	8	11	6	9	9	10	0.554420	1.0000	NonOverlappingTemplate
11	11	14	11	9	12	9	5	9	9	0.816537	1.0000	NonOverlappingTemplate
11	14	13	7	12	6	9	9	12	7	0.637119	1.0000	NonOverlappingTemplate
15	4	6	9	9	12	9	10	12	14	0.319084	0.9800	NonOverlappingTemplate
6	7	8	16	8	8	13	10	9	15	0.289667	0.9900	NonOverlappingTemplate
16	8	10	9	13	11	8	12	9	4	0.383827	0.9900	NonOverlappingTemplate
13	10	9	8	7	6	16	11	11	9	0.554420	1.0000	NonOverlappingTemplate
10	14	9	15	8	9	3	12	11	9	0.334538	0.9800	NonOverlappingTemplate
9	6	16	11	14	9	6	7	15	7	0.162606	0.9800	NonOverlappingTemplate
17	9	9	9	8	7	13	11	11	6	0.419021	0.9600	NonOverlappingTemplate
6	14	7	12	12	10	9	10	14	6	0.514124	0.9800	NonOverlappingTemplate
8	10	11	9	13	3	19	12	6	9	0.055361	1.0000	NonOverlappingTemplate
13	12	10	11	10	9	11	8	10	6	0.935716	1.0000	NonOverlappingTemplate
12	4	13	8	9	11	8	16	10	9	0.383827	0.9900	NonOverlappingTemplate
6	10	11	11	17	10	11	7	6	11	0.401199	1.0000	NonOverlappingTemplate
14	11	14	9	11	4	12	10	6	9	0.419021	0.9900	NonOverlappingTemplate
10	8	6	8	10	11	8	14	12	13	0.759756	0.9800	NonOverlappingTemplate
13	14	7	11	7	9	11	12	7	9	0.739918	0.9800	NonOverlappingTemplate
14	11	6	9	10	17	13	8	6	6	0.171867	0.9900	NonOverlappingTemplate
9	10	9	7	11	11	14	7	15	7	0.616305	0.9900	NonOverlappingTemplate
9	15	4	11	14	15	5	11	7	9	0.122325	0.9900	NonOverlappingTemplate
7	16	11	12	8	6	8	11	13	8	0.455937	0.9900	NonOverlappingTemplate
7	12	13	6	18	5	15	8	10	6	0.045675	1.0000	NonOverlappingTemplate
12	6	9	14	15	13	8	7	8	8	0.419021	0.9800	NonOverlappingTemplate
15	12	8	12	10	5	7	9	11	11	0.595549	0.9700	NonOverlappingTemplate
11	11	9	11	11	12	9	8	10	8	0.994250	0.9800	NonOverlappingTemplate
7	9	6	13	11	8	6	14	13	13	0.437274	0.9900	NonOverlappingTemplate
12	12	5	8	17	4	11	9	14	8	0.108791	0.9900	NonOverlappingTemplate

13	12	12	7	15	8	9	5	10	9	0.514124	1.0000	NonOverlappingTemplate
10	14	8	14	8	12	9	8	13	4	0.401199	0.9900	NonOverlappingTemplate
8	13	11	8	11	9	12	10	12	6	0.883171	0.9900	NonOverlappingTemplate
11	8	10	6	9	10	8	18	13	7	0.289667	0.9800	NonOverlappingTemplate
13	11	11	13	11	7	10	8	8	8	0.897763	0.9700	NonOverlappingTemplate
17	10	11	10	5	4	12	10	10	11	0.236810	1.0000	NonOverlappingTemplate
7	10	16	8	10	9	6	9	9	16	0.319084	1.0000	NonOverlappingTemplate
12	8	6	10	14	7	8	10	13	12	0.678686	0.9900	NonOverlappingTemplate
17	11	11	9	8	12	5	8	17	2	0.016717	0.9800	NonOverlappingTemplate
9	10	9	7	15	12	9	8	12	9	0.834308	1.0000	NonOverlappingTemplate
11	10	9	4	11	14	10	10	10	11	0.779188	1.0000	NonOverlappingTemplate
11	7	6	11	9	7	12	12	15	10	0.637119	1.0000	NonOverlappingTemplate
14	13	7	11	10	13	5	10	9	8	0.595549	1.0000	NonOverlappingTemplate
8	10	7	11	9	14	9	13	12	7	0.798139	0.9900	NonOverlappingTemplate
15	3	5	12	7	9	14	11	7	17	0.026948	0.9800	NonOverlappingTemplate
5	11	8	14	10	15	12	7	11	7	0.401199	0.9900	NonOverlappingTemplate
14	13	7	8	13	8	6	5	9	17	0.115387	1.0000	NonOverlappingTemplate
8	11	10	12	15	5	12	9	8	10	0.657933	1.0000	NonOverlappingTemplate
6	11	7	10	12	12	12	5	13	12	0.574903	1.0000	NonOverlappingTemplate
6	12	5	13	8	16	10	9	14	7	0.213309	1.0000	NonOverlappingTemplate
7	9	7	12	12	8	11	12	12	10	0.911413	0.9800	NonOverlappingTemplate
14	5	14	14	11	9	10	7	5	11	0.275709	0.9900	NonOverlappingTemplate
6	10	6	11	11	11	14	7	16	8	0.350485	0.9900	NonOverlappingTemplate
8	15	13	11	11	14	5	8	7	8	0.366918	0.9900	NonOverlappingTemplate
3	7	11	18	10	12	8	11	12	8	0.122325	1.0000	NonOverlappingTemplate
11	13	9	12	5	9	14	8	12	7	0.595549	1.0000	NonOverlappingTemplate
7	12	7	15	9	10	10	13	11	6	0.595549	0.9900	NonOverlappingTemplate
10	9	7	10	9	6	14	12	16	7	0.419021	0.9800	NonOverlappingTemplate
15	7	10	10	10	12	8	6	11	11	0.739918	0.9800	NonOverlappingTemplate
8	9	7	13	5	9	9	11	11	18	0.236810	1.0000	NonOverlappingTemplate
7	16	10	9	7	8	11	9	15	8	0.437274	0.9700	NonOverlappingTemplate
9	5	8	11	17	17	7	11	5	10	0.058984	0.9800	NonOverlappingTemplate
14	7	6	13	7	7	9	11	15	11	0.383827	1.0000	NonOverlappingTemplate
6	5	8	13	11	20	7	9	11	10	0.055361	0.9900	NonOverlappingTemplate
9	12	10	17	2	8	13	10	8	11	0.137282	1.0000	NonOverlappingTemplate
18	7	10	7	9	7	10	12	10	10	0.383827	0.9600	NonOverlappingTemplate
6	13	13	11	10	7	10	11	12	7	0.759756	0.9800	NonOverlappingTemplate
9	10	5	12	10	11	12	4	15	12	0.350485	1.0000	NonOverlappingTemplate
12	9	4	14	15	10	8	7	8	13	0.289667	0.9800	NonOverlappingTemplate
10	8	7	14	9	10	9	18	10	5	0.213309	1.0000	NonOverlappingTemplate
15	8	9	10	11	9	12	8	7	11	0.834308	1.0000	NonOverlappingTemplate
15	11	12	9	10	10	7	11	8	7	0.798139	0.9700	NonOverlappingTemplate
14	9	7	9	10	6	9	13	15	8	0.514124	0.9900	NonOverlappingTemplate
5	11	6	12	14	9	9	8	13	13	0.474986	1.0000	NonOverlappingTemplate
15	9	12	8	9	5	9	5	10	18	0.090936	0.9800	NonOverlappingTemplate
7	5	10	5	12	13	11	10	10	17	0.202268	0.9900	NonOverlappingTemplate
10	13	6	11	7	12	6	11	15	9	0.514124	0.9700	NonOverlappingTemplate
9	12	10	13	7	12	7	8	13	9	0.834308	0.9800	NonOverlappingTemplate
7	11	3	13	11	9	11	8	10	17	0.191687	1.0000	NonOverlappingTemplate
9	8	14	15	10	7	14	4	4	15	0.051942	0.9900	NonOverlappingTemplate
9	7	16	7	12	11	7	7	12	12	0.474986	0.9800	NonOverlappingTemplate
9	11	10	9	9	15	11	7	10	9	0.911413	1.0000	NonOverlappingTemplate
10	12	4	6	12	7	11	13	12	13	0.419021	0.9900	NonOverlappingTemplate
14	8	7	9	14	9	9	9	11	10	0.834308	0.9700	NonOverlappingTemplate
12	14	12	15	6	9	9	5	10	8	0.383827	0.9900	NonOverlappingTemplate
6	9	12	15	10	5	10	15	13	5	0.162606	0.9900	NonOverlappingTemplate
11	9	15	9	7	10	12	11	8	8	0.834308	1.0000	NonOverlappingTemplate
9	14	8	14	3	6	10	10	11	15	0.171867	0.9900	NonOverlappingTemplate
8	10	10	15	9	11	11	10	10	6	0.851383	1.0000	NonOverlappingTemplate
10	11	12	10	8	11	9	9	12	8	0.991468	0.9900	NonOverlappingTemplate
13	6	11	5	11	11	12	7	10	14	0.514124	1.0000	NonOverlappingTemplate
9	7	12	12	13	3	10	13	11	10	0.474986	1.0000	NonOverlappingTemplate
17	10	6	10	13	9	11	8	10	6	0.383827	0.9900	NonOverlappingTemplate
13	12	13	8	7	9	4	12	9	13	0.474986	0.9900	NonOverlappingTemplate
10	15	7	11	6	14	11	13	6	7	0.334538	1.0000	NonOverlappingTemplate
10	8	11	12	8	8	12	13	8	10	0.946308	1.0000	NonOverlappingTemplate
9	10	11	9	16	5	14	4	7	15	0.090936	0.9800	NonOverlappingTemplate
9	5	10	16	12	6	11	7	11	13	0.334538	1.0000	NonOverlappingTemplate
6	7	9	9	6	14	12	10	14	13	0.455937	0.9900	NonOverlappingTemplate
10	5	7	10	10	10	9	9	14	16	0.455937	0.9900	NonOverlappingTemplate
1	6	8	14	12	11	11	11	15	11	0.090936	1.0000	NonOverlappingTemplate

```
  7   6   8  13   9  12  15   7  10  13  0.474986   1.0000    NonOverlappingTemplate
  5  11   5   7  11  16  10  15   9  11  0.191687   0.9900    NonOverlappingTemplate
 10   8  21   9  11   4   8  16   6   7  0.006661   0.9900    NonOverlappingTemplate
 12  12   8   7  13  10  10  12   7   9  0.883171   0.9900    NonOverlappingTemplate
  8  11  12  13  12   7   7  14   5  11  0.514124   1.0000    NonOverlappingTemplate
  6  16   9  16   8  10   8  12   7   8  0.249284   0.9900    NonOverlappingTemplate
 17   6  13  12   6  12   7   3  14  10  0.045675   0.9600    NonOverlappingTemplate
 10   9  10   8  17   8  17   7   7   7  0.145326   0.9900    NonOverlappingTemplate
 10   9  11  11   7  10   8  17  10   7  0.595549   1.0000    NonOverlappingTemplate
 12   9  15   4   9   7   9  13  14   8  0.304126   1.0000    NonOverlappingTemplate
 14   1  12   8   6  11  13  14   7  14  0.045675   0.9900    NonOverlappingTemplate
  9   4  13   9  10   8  11  13   9  14  0.554420   0.9900    NonOverlappingTemplate
  5   4  13  11   5  13  11   8  15  15  0.066882   1.0000    NonOverlappingTemplate
  5  11   9  14   9  13  14   9   8   8  0.554420   1.0000    NonOverlappingTemplate
  7  12  15  13   6  10   6   9  14   8  0.350485   1.0000    NonOverlappingTemplate
 10   6  16  10   7  14  11  10   8   8  0.474986   0.9600    NonOverlappingTemplate
 15   9  11  11   6  12   8  13   4  11  0.366918   0.9900    NonOverlappingTemplate
 12  10  12   7   8  11  12   7   7  14  0.739918   0.9900    NonOverlappingTemplate
  8  13   8  16  12   5   7  10  13   8  0.319084   0.9900    NonOverlappingTemplate
 16   5  13   8  10   6   7  11  11  13  0.275709   0.9800    NonOverlappingTemplate
  8  14  11   5  11  13   8  10  12   8  0.657933   1.0000    NonOverlappingTemplate
 10   8  14   4  13  13   9   6  13  10  0.350485   0.9700    NonOverlappingTemplate
 10  10   9  11  10  15   8   9  11   7  0.897763   0.9800    NonOverlappingTemplate
  9  16  14   5   8   8  10  11   6  13  0.262249   1.0000    NonOverlappingTemplate
  8  12   9  11  12   8   6   7  15  12  0.616305   0.9900    NonOverlappingTemplate
  9  12   8   6  11  13  12  11  10   8  0.883171   0.9800    NonOverlappingTemplate
  8  15  13  11  11  14   5   8   7   8  0.366918   0.9900    NonOverlappingTemplate
  8  12  14  10   8  12   6  10  11   9  0.834308   0.9900    OverlappingTemplate
 15  14   6   7   9   5  13  14   7  10  0.181557   0.9800    Universal
 10   8  11  10  10  10  12   9   9  11  0.998821   1.0000    ApproximateEntropy
  5   3  11   7  10   4   7   5   8   6  0.324180   1.0000    RandomExcursions
  6   7   4   6  10   8   8   5   5   7  0.804337   0.9848    RandomExcursions
  8   7   6   7   6   5   7   4   9   7  0.931952   0.9697    RandomExcursions
  9   6   8   4   5   5   7   7   5  10  0.706149   1.0000    RandomExcursions
 11   6   5   7   7   9   6   4   4   7  0.568055   0.9848    RandomExcursions
  7   4   7   7   6   7   8   7   6   7  0.985035   1.0000    RandomExcursions
  5   6  10   8   7   5   7   4   8   6  0.804337   1.0000    RandomExcursions
  6  10   7   7   7   6   7   7   7   2  0.706149   0.9848    RandomExcursions
  5   8   7   5   5  11   6   5   6   8  0.706149   1.0000    RandomExcursionsVariant
  5   9   4   5   8  11   3   7   6   8  0.378138   1.0000    RandomExcursionsVariant
  3   7   4  10  11   8   3   6   5   9  0.162606   1.0000    RandomExcursionsVariant
  2   6  10   5  11   8   9   3   6   6  0.148094   1.0000    RandomExcursionsVariant
  2   8   5   8   8   6   9   5  11   4  0.253551   1.0000    RandomExcursionsVariant
  5   4   5   9   6   9   6   8   7   7  0.834308   1.0000    RandomExcursionsVariant
  2   6   9  11   9   9   4   6   6   4  0.178278   1.0000    RandomExcursionsVariant
  3   7   7   8   7  10   6   4   7   7  0.706149   1.0000    RandomExcursionsVariant
  6   5   9   7   6   6   7   6   8   6  0.976060   0.9848    RandomExcursionsVariant
  8   5   9   6   8   9   7   7   3   4  0.637119   0.9848    RandomExcursionsVariant
  7   5   8   9   6   8  11   3   5   4  0.378138   1.0000    RandomExcursionsVariant
  7   7   7   8   6   6   5   8   5   7  0.985035   1.0000    RandomExcursionsVariant
  4  10   5   6   8   9   4  10   6   4  0.378138   1.0000    RandomExcursionsVariant
  6   3  10   9   6   7   6   9   7   3  0.437274   1.0000    RandomExcursionsVariant
  6   4  10  10   8   7   3   9   3   6  0.253551   1.0000    RandomExcursionsVariant
  6   8   5  15   4   4   5   9   4   6  0.035174   1.0000    RandomExcursionsVariant
  7   7  11   5  10   5   3   4   8   6  0.324180   1.0000    RandomExcursionsVariant
  9  10   8   3   8   8   6   4   5   5  0.468595   1.0000    RandomExcursionsVariant
 11  11   5   7   9  19  11   8   9  10  0.191687   0.9900    Serial
  9  18   9  13   9   7   9   7   8  11  0.350485   0.9900    Serial
  6  11  10  10  14  12   9  10   9   9  0.911413   0.9900    LinearComplexity
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
The minimum pass rate for each statistical test with the exception of the
random excursion (variant) test is approximately = 0.960150 for a
sample size = 100 binary sequences.
The minimum pass rate for the random excursion (variant) test
is approximately 0.953258 for a sample size = 66 binary sequences.
For further guidelines construct a probability table using the MAPLE program
provided in the addendum section of the documentation.
   - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
```

ДОДАТОК В
Список публікацій здобувача за темою дисертації

1. Бабенко В. Г. Дослідження матричних операцій криптографічного перетворення на основі арифметичних операцій за модулем. *Системи управління, навігації та зв'язку*. 2012. Вип. 4 (24). С. 85–88.

2. Бабенко В. Г. Параллельная реализация скользящего шифрования. *Системи обробки інформації*. 2013. Вип. 9 (116). С. 131–134.

3. Бабенко В. Г. Оптимизация матричных операций скользящего шифрования. *Системи озброєння і військова техніка*. 2013. № 4 (36). С. 132–135.

4. Бабенко В. Г. Складності та особливості побудови ефективних криптоалгоритмів. *Вісник Черкаського державного технологічного університету*. 2014. № 3. С. 87–91.

5. Бабенко В. Г. Застосування операцій криптографічного перетворення для синтезу криптоалгоритмів. *Сучасна спеціальна техніка*. 2014. № 3 (38). С. 49–55.

6. Рудницький В. М., Миронець І. В., Бабенко В. Г. Обґрунтування можливості розширення набору функцій перекодування інформації для захисту конфіденційних інформаційних ресурсів. *Системи управління, навігації та зв'язку*. 2010. Вип. 2 (14). С. 118–122.

7. Рудницький В. М., Миронець І. В., Бабенко В. Г. Методологія підвищення оперативності доступу до конфіденційних інформаційних ресурсів. *Системи обробки інформації*. 2010. Вип. 5 (86). С. 15–19.

8. Рудницький В. М., Миронець І. В., Бабенко В. Г. Реалізація методу підвищення оперативності доступу до конфіденційних інформаційних ресурсів. *Вісник Черкаського державного технологічного університету.* 2010. № 3. С. 60–65.

9. Рудницький В. М., Бабенко В. Г., Жиляєв Д. А. Алгебраїчна структура множини логічних операцій кодування. *Наука і техніка Повітряних Сил Збройних Сил України*. 2011. Вип. 2 (6). С. 112–114.

10. Рудницький В. М., Миронець І. В., Бабенко В. Г. Систематизація повної множини логічних функцій для криптографічного перетворення інформації. *Системи обробки інформації*. 2011. Вип. 8 (98). С. 184–188.

11. Рудницький В. М., Миронець І. В., Бабенко В. Г. Технологія побудови пристрою реалізації методу підвищення оперативності доступу до конфіденційних інформаційних ресурсів. *Збірник наукових праць Харківського університету Повітряних Сил*. 2011. Вип. 3 (29). С. 145–150.

12. Бабенко В. Г., Миронець І. В., Рудницький С. В. Декодування інформації в групі дворозрядних операцій криптографічного перетворення. *Системи управління, навігації та зв'язку*. 2011. Вип. 4 (20). С. 208–212.

13. Бабенко В. Г., Рудницький С. В., Мельник Р. П. Визначення множини трирозрядних елементарних операцій криптографічного перетворення. *Вісник інженерної академії України*. 2012. Вип. 3 (4). С. 77–79.

14. Рудницький В. М., Бабенко В. Г., Рудницький С. В. Метод синтезу матричних моделей операцій криптографічного кодування та декодування інформації. *Збірник наукових праць Харківського університету Повітряних Сил*. 2012. Вип. 4 (33). С. 198–200.

15. Рудницький В. М., Бабенко В. Г., Рудницький С. В. Метод синтезу матричних моделей операцій криптографічного перекодування інформації. *Захист інформації*. 2012. № 3 (56). С. 50–56.

16. Голуб С. В., Бабенко В. Г., Рудницький С. В. Метод синтезу операцій криптографічного перетворення на основі додавання за модулем два. *Системи обробки інформації*. 2012. Вип. 3 (101). Т. 1. С. 119–122.

17. Бабенко В. Г., Мельник Р. П., Рудницький С. В. Дослідження способів запису трьохрозрядних криптографічних операцій. *Системи управління, навігації та зв'язку.* 2012. Вип. 1 (21). Т. 2. С. 170–173.

18. Бабенко В. Г., Рудницький С. В. Синтез функцій перекодування для групи трьохрозрядних криптографічних операцій. *Системи озброєння і військова техніка*. 2012. Вип. 1 (29). С. 84–87.

19. Вдосконалення методу синтезу операцій криптографічного перетворення на основі дискретно-алгебраїчного представлення операцій / С. В. Голуб, В. Г. Бабенко, С. В. Рудницький, Р. П. Мельник. *Системи управління, навігації та зв'язку.* 2012. Вип. 2 (22). С. 163–168.

20. Бабенко В. Г., Рудницький С. В. Реалізація методу захисту інформації на основі матричних операцій криптографічного перетворення. *Системи обробки інформації*. 2012. № 9 (107). С. 130–139.

21. Бабенко В. Г., Мельник Р. П., Рудницкий С. В. Синтез операций криптографического декодирования на основе элементарных операций расширенного матричного представления. *Информационные системы и технологии: управление и безопасность:* сб. ст. I междунар. заочной науч.-практ. конф. Тольятти: ПВГУС, 2012. С. 67–77.

22. Бабенко В., Мельник О., Мельник Р. Класифікація трирозрядних елементарних функцій для криптографічного перетворення інформації. *Безпека інформації*. 2013. Т. 19. № 1. С. 56–59.

23. Бабенко В. Г., Стабецька Т. А. Побудова моделі оберненої нелінійної операції матричного криптографічного перетворення. *Системи управління, навігації та зв'язку*. 2013. Вип. 3 (27). С. 117–119.

24. Параллельная реализация нелинейного расширенного матричного криптографического преобразования / В. Г. Бабенко, С. В. Пивнева, О. Г. Мельник, Р. П. Мельник. *Вектор науки Тольяттинского государственного университета*. 2014. № 3 (29). С. 17–19.

25. Синтез модели обратной нелинейной операции расширенного матричного криптографического преобразования / В. Н. Рудницкий, С. В. Пивнева, В. Г. Бабенко и др. *Вектор науки Тольяттинского государственного университета*. 2014. № 4 (30). С. 18–21.

26. Бабенко В. Г., Мельник Р. П., Гончар С. В. Оцінка ефективності використання операцій криптографічного перетворення. *Вісник Інженерної академії України*. 2014. Вип. 2. С. 39–41.

27. Метод захисту конфіденційної інформації як складова управління інформаційною безпекою ДСНС України / Р. П. Мельник, О. Г. Мельник, С. В. Гончар, В. Г. Бабенко. *Системи обробки інформації*. 2014. Вип. 4 (120). С. 145–148.

28. Рудницкий В. Н., Козлов Е. В., Бабенко В. Г. Способ параллельной реализации операций матричного криптографического преобразования. *Вектор науки Тольяттинского государственного университета*. 2014. № 2 (28). С. 11–15.

29. Бабенко В. Г., Лада Н. В. Синтез і аналіз операцій криптографічного додавання за модулем два. *Системи обробки інформації*. 2014. Вип. 2 (118). С. 116–118.

30. Бабенко В. Г., Мельник О. Г., Стабецька Т. А. Синтез нелінійних операцій криптографічного перетворення. *Безпека інформації*. 2014. Т. 20. № 2. С. 143–147.

31. Рудницький В. М., Бабенко В. Г., Стабецька Т. А. Узагальнений метод синтезу обернених нелінійних операцій розширеного матричного криптографічного перетворення. *Системи обробки інформації*. 2014. Вип. 6 (122). С. 118–121.

32. Бабенко В. Г., Козловська С. Г. Особливості використання матричних операцій криптографічного перетворення інформації. *Системи обробки інформації*. 2015. Вип. 3 (128). С. 84–87.

33. Бабенко В. Г., Ланських Є. В., Зажома В. М. Вбудовування даних в стеганоконтейнер на основі надлишкових позиційних систем числення. *Вісник Черкаського державного технологічного університету*. 2015. № 1. С. 111–115.

34. Бабенко В. Г., Мельник Р. П., Гончар С. В. Розробка методів синтезу трирозрядних розширених матричних елементарних функцій. *Наука і техніка Повітряних Сил Збройних Сил України*. 2015. Вип. 1 (18). С. 154–156.

35. Мельник Р. П., Бабенко В. Г., Гончар С. В. Удосконалений метод синтезу розширених матричних елементарних функцій для криптоперетворення даних. *Системи озброєння і військова техніка*. 2015. Вип. 1 (41). С. 132–134.

36. Бабенко В. Г., Мельник О. Г., Нестеренко О. Б. Моделювання примітивів ковзного шифрування на основі рекурентних послідовностей. *Наука і техніка Повітряних Сил Збройних Сил України*. 2015. Вип. 3 (20). С. 129–133.

37. Бабенко В. Г., Мельник О. Г., Мельник Р. П. Мультиопераційне багаторазове ковзне шифрування. *Системи озброєння і військова техніка*. 2015. Вип. 3 (43). С. 70–72.

38. Бабенко В. Г., Зажома В. М., Нестеренко О. Б. Метод вбудовування стегоповідомлення на основі ключового елементу. *Автоматизированные системы управления и приборы автоматики.* Харьков. 2014. Вып. 168. С. 53–58.

39. Бабенко В. Г., Лада Н. В., Лада С. В. Дослідження взаємозв'язків між операціями в матричних моделях криптографічного перетворення. *Вісник Черкаського державного технологічного університету.* 2016. № 1. С. 5–11.

40. Эффективное совмещенное мультиоперандное сложение в избыточной линейной рекуррентной системе счисления третьего порядка / И. Н. Федотова-Пивень, В. Г. Бабенко, О. Б. Пивень, С. Ю. Куницкая. *Wschodnioeuropejskie Czasopismo Naukowe: East European sci. journ.* 2016. No. 11 (15). Part 2. P. 19–24. (Варшава, Польща).

41. Реалізація вершинної мінімізації булевих функцій для моделювання процесів, що не формалізуються / В. М. Рудницький, І. В. Миронець, В. Г. Бабенко та ін. *Science and Education a New Dimension*. *Natural and Ttechnical Science:* міжнар. наук. журн. 2017. Vol. 14. Iss. 132. P. 85–88. (BUDAPEST) (Будапешт, Угорщина).

42. Особенности применения операций перестановок, управляемых информацией, для криптографического преобразования / Т. В. Миронюк, И. В. Миронец, В. Г. Бабенко, С. В. Сысоенко. *Wschodnioeuropejskie Czasopismo Naukowe: East European sci. journ.* 2017. No. 11 (27). Part 1. P. 85–93. (Варшава, Польща).

43. Сисоєнко С. В., Миронець І. В., Бабенко В. Г. Побудова узагальненої математичної моделі групового матричного криптографічного перетворення. *Сучасна спеціальна техніка.* 2018. № 4. С. 96–103.

44. Миронець І. В., Бабенко В. Г., Сисоєнко С. В. Метод мінімізації булевих функцій з великою кількістю змінних на основі направленого перебору. *Щомісячний науковий журнал «Smart and Young».* 2016. № 7. С. 63–71.

45. Бабенко В. Г., Лада Н. В. Технологія дослідження операцій за модулем два. *Щомісячний науковий журнал «Smart and Young».* 2016. № 11–12. Ч. 1. С. 49–54.

46. Бабенко В. Г., Кучеренко С. Ю., Зажома В. М. Моделирование позиционных избыточных систем счисления. *Системи управління, навігації та зв'язку.* 2010. Вип. 4 (16). С. 51–54.

47. Бабенко В. Г., Кучеренко С. Ю., Зажома В. М. Синтез правил выполнения операций сложения на основе моделей позиционных систем счисления. *Системи обробки інформації.* 2010. Вип. 9 (90). С. 179–182.

48. Бабенко В. Г., Шадхін В. Ю., Шевченко О. О. Дослідження принципів організації передачі даних в TCP/IP-мережах. *Вісник Черкаського державного технологічного університету.* 2010. № 2. С. 3–6.

49. Бабенко В. Г., Шадхін В. Ю., Компанієць В. О. Оперативний розподіл навантаження на мережі передачі даних. *Вісник Хмельницького національного університету.* 2010. Вип. 3. С. 217–220.

50. Эвристические алгоритмы и распределённые вычисления в прикладных задачах (вып. 2): кол. монограф. / под ред. Б. Ф. Мельникова. Ульяновск, 2013. 202 с.

51. Наукоемкие технологии в инфокоммуникациях: обработка и защита информации: кол. монограф. / под ред. В. М. Безрука, В. В. Баранника. Харьков: Компания СМИТ, 2013. 398 с.

52. Криптографическое кодирование: методы и средства реализации: монография / В. Н. Рудницкий, С. В. Пивнева, В. Г. Бабенко и др.; Тольят. гос. ун-т. Тольятти, 2013. 196 с.

53. Криптографическое кодирование: методы и средства реализации (часть 2): монография / В. Н. Рудницкий, В. Я. Мильчевич, В. Г. Бабенко и др. Харьков: Щедрая усадьба плюс, 2014. 224 с.

54. Криптографическое кодирование: кол. монограф. / под ред. В. Н. Рудницкого, В. Я. Мильчевича. Харьков: Щедрая усадьба плюс, 2014. 240 с.

55. Рудницький В. М., Лада Н. В., Бабенко В. Г. Криптографічне кодування: синтез операцій потокового шифрування з точністю до перестановки: монографія. Харків: ДІСА ПЛЮС, 2018. 184 с.

56. Криптографічне кодування: обробка та захист інформації: кол. монографія / Бабенко В. Г., Лада Н. В. та ін.; під. ред. В. М. Рудницького. Харків: ДІСА ПЛЮС, 2018. 139 с.

57. Пристрій для виконання логічних операцій криптографічного перетворення: деклараc. пат. на корисну модель 45916 Україна, МПК H03M 13/00 / Рудницький В. М., Паціра Є. В., Миронець І. В., Бабенко В. Г. № u200907997; заявл. 29.07.2009; опубл. 25.11.2009, Бюл. № 22. 3 с.

58. Пристрій для виконання логічних операцій криптографічного перетворення: деклараc. пат. на корисну модель 45917 Україна, МПК H03M 13/00 / Рудницький В. М., Паціра Є. В., Миронець І. В., Бабенко В. Г. № u200907998; заявл. 29.07.2009; опубл. 25.11.2009, Бюл. № 22. 3 с.

59. Пристрій для виконання логічних операцій криптографічного перетворення: деклара. пат. на корисну модель 46617 Україна, МПК H03M 13/00 / Рудницький В. М., Паціра Є. В., Миронець І. В., Бабенко В. Г. № u200908000; заявл. 29.07.2009; опубл. 25.12.2009, Бюл. № 24. 3 с.

60. Пристрій для виконання логічних операцій криптографічного перетворення: деклараc. пат. на корисну модель 46618 Україна, МПК H03M 13/00 / Рудницький В. М., Паціра Є. В., Миронець І. В., Бабенко В. Г. № u200908001; заявл. 29.07.2009; опубл. 25.12.2009, Бюл. № 24. 3 с.

Відомості про апробацію результатів дисертації

1. Бабенко В. Г. Етапи реалізації технології підвищення швидкодії систем захисту інформації. *Методи та засоби кодування, захисту й ущільнення інформації:* тези доп. Третьої міжнар. наук.-практ. конф., (20–22 квіт. 2011 р.). Вінниця: ВНТУ, 2011. С. 80–81. – очна участь.
2. Бабенко В. Г. Використання матричних операцій криптографічного перетворення для ковзного шифрування. *Проблеми інформатизації:* тези доп. Першої міжнар. наук.-техн. конф., (19–20 груд. 2013 р.). Черкаси: ЧДТУ; Київ: ДУТ; Тольятті: ТДУ; Полтава: ПНТУ, 2013. С. 22. – очна участь.
3. Миронець І. В., Бабенко В. Г. Методика синтезу функцій декодування на основі спеціалізованих логічних функцій. *Проблеми інформатизації:* зб. тез доп. наук.-техн. семінару, (15–16 квіт. 2009 р.). Черкаси: ЧДТУ, 2009. Вип. 1 (3). С. 18–19. – очна участь.
4. Миронець І. В., Бабенко В. Г. Вдосконалена методика синтезу функцій декодування на основі спеціалізованих логічних функцій. *Інтегровані інтелектуальні робототехнічні комплекси:* зб. тез Другої міжнар. наук.-практ. конф., (25–28 трав. 2009 р.). Київ: НАУ, 2009. С. 228–229. – очна участь.
5. Бабенко В. Г., Рудницький С. В. Дослідження двохрозрядних операцій криптографічного перетворення. *Інтегровані комп'ютерні технології в машинобудуванні ІКТМ-2011:* тези доп. Всеукр. наук.-техн. конф. Харків: НАУ «ХАІ», 2011. Т. 3. С. 218. – заочна участь.
6. Бабенко В. Г., Рудницький С. В. Синтез функцій декодування інформації в групі трьохрозрядних криптографічних операцій перетворення. *Моделювання, ідентифікація, синтез систем керування:* зб. тез П'ятнадцятої міжнар. наук.-техн. конф., (9–16 верес. 2012 р.). Донецьк: Вид-во Ін-ту прикл. математики і механіки НАН України, 2012. С. 190–191. – заочна участь.
7. Бабенко В. Г., Рудницький С. В. Моделювання логічних функцій для систем захисту інформації. *Методи та засоби кодування, захисту й ущільнення*

інформації: тези доп. Третьої міжнар. наук.-практ. конф. Вінниця: ВНТУ, 2011. С. 82–83. – очна участь.

8. Бабенко В. Г., Рудницький С. В. Дослідження групи трьохрозрядних криптографічних операцій. *Новітні технології – для захисту повітряного простору:* тези доп. Восьмої наук. конф. Харків. ун-ту Повітр. Сил ім. І. Кожедуба, (18–19 квіт. 2012 р.). Харків: ХУПС ім. І. Кожедуба, 2012. С. 218. – заочна участь.
9. Бабенко В. Г., Лада Н. В. Дослідження множини операцій криптографічного додавання. *Інформаційні технології в освіті, науці і техніці (ІТОНТ-2014):* тези доп. ІІ Міжнар. наук.-практ. конф., (м. Черкаси, Україна, 24–26 квіт. 2014 р.). Черкаси: ЧДТУ, 2014. Т. 1. С. 135–136. – очна участь.
10. Бабенко В. Г., Стабецька Т. А. Операції матричного криптографічного декодування на основі логічних визначників. *Методи та засоби кодування, захисту й ущільнення інформації:* тези доп. Четвертої міжнар. наук.-практ. конф., (м. Вінниця, Україна, 23–25 квіт. 2013 р.). Вінниця: ТД Едельвейс і К, 2013. С. 135–137. – заочна участь.
11. Бабенко В. Г., Лада Н. В. Синтез і аналіз мікрооперацій для криптографічного перетворення. *Проблеми інформатизації:* тези доп. Другої міжнар. наук.-техн. конф., (м. Черкаси, Україна – м. Тольятті, Росія, 25–26 листоп. 2014 р.). Черкаси: ЧДТУ; Тольятті: ТДУ, 2014. С. 9–10. – очна участь.
12. Ланських Є. В., Бабенко В. Г., Зажома В. М. Алгоритми вбудовування повідомлення для LSB методу. *Інформаційні технології в освіті, науці і техніці (ІТОНТ-2014):* тези доп. ІІ Міжнар. наук.-практ. конф., (м. Черкаси, Україна, 24–26 квіт. 2014 р.). Черкаси: ЧДТУ, 2014. Т. 1. С. 141–142. – очна участь.
13. Ланських Є. В., Бабенко В. Г., Зажома В. М. Технологія застосування ключового елементу стеганоконтейнера для LSB методу. *Інтегровані інтелектуальні робототехнічні комплекси (ІІРТК-2014):* тези доп. Сьомої

міжнар. наук.-практ. конф., (19–20 трав. 2014 р.). Київ: НАУ, 2014. С. 312–313. – очна участь.

14. Ланських Є. В., Бабенко В. Г., Зажома В. М. Використання надлишковості систем числення в стеганографічних системах. *Інформаційні технології та комп'ютерна інженерія (ІТКІ-2014):* тези доп. Четвертої міжнар. наук.-практ. конф., (м. Вінниця, Україна, 27–30 трав. 2014 р.). Вінниця: ВНТУ, 2014. С. 161–162. – заочна участь.
15. Бабенко В. Г., Рудницький С. В. Способи синтезу алгоритмів на основі операцій криптографічного перетворення інформації. *Проблеми інформатизації:* тези доп. Другої міжнар. наук.-техн. конф. (м. Черкаси, Україна – м. Тольятті, Росія, 25–26 листоп. 2014 р.). Черкаси: ЧДТУ; Тольятті: ТДУ, 2014. С. 10. – очна участь.
16. Бабенко В. Г. Синтез моделей реалізації багаторазового примітиву ковзного шифрування. *Сучасні напрями розвитку інформаційно-комунікаційних технологій та засобів управління:* матеріали П'ятої міжнар. наук.-техн. конф., (23–24 квіт. 2015 р.). Полтава: ПНТУ; Баку: ВА ЗС АР; Кіровоград: КЛА НАУ; Харків: ХНДІ ТМ, 2015. С. 59. – заочна участь.
17. Гресько Є. І., Бабенко В. Г. Огляд стеганографічних методів приховування інформації. *Інформаційна безпека держави, суспільства та особистості:* зб. тез доп. Всеукр. наук.-практ. конф., (16 квіт. 2015 р.). Кіровоград: КНТУ, 2015. С. 87–89. – заочна участь.
18. Бабенко В. Г., Лада Н. В. Аналіз результатів виконання модифікованих операцій додавання за модулем два з точністю до перестановки. *The Scientific Potential of the Present:* зб. наук. праць «ЛОГОΣ». 2016. С. 108–111. – заочна участь.
19. Бабенко В. Г., Лада Н. В., Лада С. В. Взаємозв'язки між операціями в матричних моделях криптографічного перетворення. *Проблеми науково-технічного та правового забезпечення кібербезпеки у сучасному світі «ПНПЗК-2016»:* тези доп. Першої міжнар. наук.-практ. конф., (30 берез.–1 квіт. 2016 р.). Харків: Нац. техн. ун-т «ХПІ», 2016. С. 17. – заочна участь.

20. Бабенко В. Г., Лада Н. В., Лада С. В. Аналіз множини операцій, синтезованих на основі додавання за модулем два. *Методи та засоби кодування, захисту й ущільнення інформації:* тези доп. П'ятої міжнар. наук.-практ. конф., (19–21 квіт. 2016 р.). Вінниця: ВНТУ, 2016. С. 54–57. – очна участь.
21. Бабенко В. Г., Висоцький С. В. Забезпечення захисту інформації для системи моніторингу та статистики web-ресурсів. *Інформаційні технології в освіті, науці й техніці (ІТОНТ-2016):* тези доп. Третьої міжнар. наук.-практ. конф., (12–14 трав. 2016 р.). Черкаси: ЧДТУ, 2016. С. 85–86. – очна участь.
22. Бабенко В. Г., Ланських Є. В. Дослідження заміни операції для реалізації матричного криптографічного перетворення. *Інтегровані інтелектуальні робототехнічні комплекси (ІІРТК-2016):* тези доп. Дев'ятої міжнар. наук.-практ. конф., (17–18 трав. 2016 р.). Київ: НАУ, 2016. С. 246–248. – очна участь.
23. Бабенко В. Г., Стабецька Т. А. Синтез обернених операцій розширеного матричного криптографічного перетворення. *Проблеми інформатизації:* тези доп. Четвертої міжнар. наук.-техн. конф., (м. Черкаси, Україна, 3–4 листоп. 2016 р.). Черкаси: ЧДТУ; Баку: ВА ЗС АР; Бельсько-Бяла: УТіГН; Полтава: ПНТУ, 2016. С. 9. – очна участь.
24. Стабецька Т. А., Бабенко В. Г. Алгоритми побудови та застосування операцій розширеного матричного криптографічного перетворення. *Наукова думка інформаційного століття:* матеріали Міжнар. наук.-практ. конф., (м. Дніпропетровськ, Україна, 19 черв. 2017 р.). Одеса: Друкарня «Друкарик», 2017. Т. 6. С. 86–94. – заочна участь.
25. Миронюк Т. В., Бабенко В. Г. Аналіз статистичних властивостей результатів криптографічного перетворення на основі операцій перестановок, керованих інформацією. *Інноваційні тенденції сьогодення у сфері природничих, гуманітарних та точних наук:* матеріали Міжнар. наук.-практ. конф., (м. Івано-Франківськ, Україна, 17 жовт. 2017 р.). Одеса: Друкарня «Друкарик», 2017. Т. 2. С. 41–47. – заочна участь.

26. Бабенко В. Г., Лада Н. В. Потокові шифри з використанням групи модифікованих операцій криптографічного додавання за модулем два з точністю до перестановки. *Проблеми інформатизації:* тези доп. П'ятої міжнар. наук.-техн. конф., (м. Черкаси, Україна, 13–15 листоп. 2017 р.). Черкаси: ЧДТУ; Баку: ВА ЗС АР; Бельсько-Бяла: УТіГН; Полтава: ПНТУ, 2017. С. 12. – очна участь.
27. Стабецька Т. А., Бабенко В. Г. Порівняльна оцінка основних параметрів методу захисту інформації на основі операцій розширеного матричного криптографічного перетворення. *Наука у контексті сучасних глобалізаційних процесів:* зб. наук. праць «ΛΌГОΣ» з матеріалами Міжнар. наук.-практ. конф., (м. Полтава, Україна, 19 листоп. 2017 р.) / відп. за вип. М. А. Голденблат; ГО «Європейська наукова платформа». Одеса: Друкарня «Друкарик», 2017. Т. 10. С. 81–84. – заочна участь.
28. Бабенко В. Г., Нестеренко О. Б., Пустовіт М. О. Дослідження результатів багатораундового шифрування, реалізованого на основі операцій строгого стійкого кодування. *Проблеми інформатизації:* тези доп. Шостої міжнар. наук.-техн. конф., (м. Черкаси, Україна, 14–16 листоп. 2018 р.). Черкаси: ЧДТУ; Баку: ВА ЗС АР; Бельсько-Бяла: УТіГН; Полтава: ПНТУ, 2018. С. 9–10. – очна участь.
29. Сисоєнко С. В., Бабенко В. Г. Аналіз складності реалізації моделей операцій групового матричного криптографічного перетворення. *Naukowy i innowacyjny potencjał prezentacji:* kolekcja prac naukowych «ΛΌГОΣ» z materiałami Międzynar. nauk.-prakt. konf., (Opole, 18 listopada 2018 r.). Równe: Volynsky Oberegi, 2018. T. 7. S. 5–53. – заочна участь.
30. Sysoienko S., Myronets I., Babenko V. Practical implementation effectiveness of the speed increasing method of group matrix cryptographic transformation. *Second International Workshop on Computer Modeling and Proceedings of the Second International Workshop on Computer Modeling and Intelligent Systems (CMIS-2019),* (Zaporizhzhia, Ukraine, April 15–19, 2019). P. 402–412. – очна участь.