ЧЕРКАСЬКИЙ ДЕРЖАВНИЙ ТЕХНОЛОГІЧНИЙ УНІВЕРСИТЕТ
МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

Кваліфікаційна наукова
праця на правах рукопису

КОЗЛОВСЬКА Світлана Григорівна

УДК 004.421.5:004.056.55

ДИСЕРТАЦІЯ

МЕТОДИ СИНТЕЗУ ГРУП СИМЕТРИЧНИХ ОПЕРАЦІЙ ДЛЯ ПОТОКОВОГО ШИФРУВАННЯ

05.13.05 – комп'ютерні системи та компоненти
технічні науки

Подається на здобуття наукового ступеня кандидата технічних наук

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

С. Г. КОЗЛОВСЬКА

Науковий керівник Рудницький Володимир Миколайович, доктор технічних наук, професор

Черкаси – 2019

АНОТАЦІЯ

Козловська С. Г. Методи синтезу груп симетричних операцій для потокового шифрування. – Кваліфікаційна наукова праця на правах рукопису.

Дисертація на здобуття наукового ступеня кандидата технічних наук (доктора філософії) за спеціальністю 05.13.05 «Комп'ютерні системи і компоненти». – Черкаський державний технологічний університет, Черкаси, 2019.

Дисертаційну роботу присвячено підвищенню якості систем потокового шифрування конфіденційної інформації за рахунок збільшення стійкості та варіативності перетворення на основі додаткового використання груп двохоперандних двохрозрядних операцій, синтезованих на основі додавання за модулем два та чотири.

У першому розділі визначено, що використання операцій криптографічного перетворення на основі логічних функцій є одним із найперспективніших напрямів розвитку систем криптографічного захисту інформації. Розглянуто сучасний стан досліджень операцій криптографічного перетворення інформації з виокремленням особливостей застосування в потоковому та блочному шифруваннях. Наведено результати бібліографічного пошуку та огляду основних результатів досліджень, пов'язаних із синтезом та аналізом операцій криптографічного перетворення інформації. Встановлено, що двохоперандним операціям криптографічного перетворення інформації, що спеціалізовані для потокового шифрування, не приділено достатньої уваги. Множину цих операцій необхідно досліджувати й розширювати, розвивати методи їхнього синтезу, оскільки використання цих операцій забезпечує підвищення стійкості та надійності потокових шифрів. Наведено теоретичні передумови та результати проведення обчислювального експерименту, в результаті якого на основі перебору розраховано повну множину таблиць істинності симетричних двохрозрядних двохоперандних операцій криптоперетворення, а також основні результати дослідження цих операцій. Продемонстровано результати дослідження двохоперандних операцій криптоперетворення. Сформульовано мету й задачі наукового дослідження.

Другий розділ присвячено математичному моделюванню та дослідженню двохоперандних операцій криптографічного перетворення інформації на основі відомих таблиць істинності. Для забезпечення ефективності проведення досліджень проаналізовано та класифіковано таблиці істинності симетричних двохрозрядних двохоперандних операцій криптоперетворення. Кожна з досліджуваних двохоперандних операцій є операцією вибору однієї з чотирьох одноопераднних операцій перетворення першого операнда залежно від значення другого операнда, який виконує функцію команд управління. Ці операції розбито на 24-ри набори двохоперандних операцій по чотири операції в кожному наборі, до того ж, всі операції поділено на чотири математичні групи. В процесі математичного перетворення моделі операції отримано модель двохоперандної операції, яка може бути зреалізована як на апаратному, так і на програмному рівнях. Побудовано математичні моделі для всіх операцій першої математичної групи, а також перестановочні схеми побудови цих операцій. На основі аналізу отриманих результатів побудовано узагальнені перестановочні схеми для першої математичної групи двохоперандних операцій криптоперетворення. Послідовність математичних перетворень експериментальних даних, яка забезпечує отримання придатних для застосування двохоперандних операцій криптоперетворення в сукупності з перестановочними схемами візуалізації побудови операцій, за своєю природою є методом побудови та дослідження двохоперандних операцій криптоперетворення на основі результатів обчислювального експерименту. В процесі дослідження встановлено, що перестановочні схеми побудови таблиць істинності наборів двохоперандних операцій криптоперетворення першої математичної групи не перетинаються. Сукупність наборів таблиць істинності двохоперандних операцій криптоперетворення першої математичної групи створюють повну групу наборів таблиць істинності двохоперандних операцій криптоперетворення.

Третій розділ присвячено дослідженню другої математичної групи двохоперандних операцій криптоперетворення шляхом застосування методу побудови та аналізу двохоперандних операцій криптоперетворення на основі

результатів обчислювального експерименту. Досліджено всю множину операцій другої групи. В процесі аналізу перестановочних схем таблиць істинності встановлено: сукупність наборів таблиць істинності двохоперандних операцій криптоперетворення другої математичної групи створює повну групу наборів таблиць істинності двохоперандних операцій криптоперетворення; групи перестановочних схем першої та другої математичної груп досліджених операцій криптоперетворення співпадають. Виявлено, що застосування повної групи отриманих перестановочних схем забезпечить побудову повної групи наборів двохоперандних операцій криптоперетворення, невідомої групи та їхніх таблиць підстановки, якщо взяти будь-яку операцію з цієї невідомої групи.

У четвертому розділі розроблено методи синтезу груп двохоперандних операцій криптоперетворення. Після узагальнення результату дослідження моделей операцій першої групи отримано класифікацію операцій з поділом на базові операції, поєднання базових операцій з операціями перестановки та поєднання базових операцій з операціями перестановки та інверсії. Ця класифікація стала основою для розроблення методу синтезу груп двохрозрядних двохоперандних операцій для симетричного потокового шифрування, що полягає в синтезі двохоперандних операцій базової групи на основі додавання за модулем два одноопераднних операцій обробки кожного операнда; виконанні над операціями базової групи операцій перестановок; виконанні над операціями базової групи в поєднанні з операціями перестановок операцій інверсії. Оскільки основною операцією цієї групи є операція додавання за модулем два, то й групу названо симетричною групою двохоперандних двохрозрядних операцій криптографічного додавання за модулем два. За аналогією з цим методом розроблено метод синтезу симетричної групи двохоперандних двохрозрядних операцій криптографічного додавання за модулем чотири. Побудовано варіанти апаратних і програмних засобів для реалізації синтезованих операцій. Продемонстровано, що синтезовані моделі операцій та засоби їхнього застосування доцільно використати в блоці криптоперетворення під час реалізації методу підвищення стійкості та надійності потокового

шифрування. Наведені результати статистичних досліджень практичних результатів дисертаційної роботи свідчать про те, що досліджувані послідовності пройшли комплексний контроль за методикою випробувань пакетом тестів NIST_STS. Найкращі результати тестування отримано під час застосування 12-ти відомих та 48-ми синтезованих в роботі операцій криптоперетворення. Крім того, сумісне застосування операцій вп’ятеро збільшує варіативність потокового шифрування.

Наукова новизна отриманих результатів:

- вперше розроблено метод побудови та дослідження двохоперандних операцій криптоперетворення на основі результатів обчислювального експерименту шляхом формалізації, класифікації та математичного перетворення, що забезпечило встановлення нових взаємозв’язків між операндами та результатами, а також можливість застосування одноопераднних операцій в потоковому шифруванні;
- вперше розроблено методи синтезу груп симетричних двохрозрядних двохоперандних операцій потокового шифрування на основі результатів обчислювального експерименту шляхом застосування результатів реалізації розробленої технології та табличного представлення класифікації групи одноопераднних двохрозрядних операцій криптографічного перетворення, а також встановленням нових раніше невідомих взаємозв’язків між одноопераднними та двохоперандними операціями, що забезпечило синтез математичних груп симетричних двохоперандних операцій на основі додавання за модулем два та додавання за модулем чотири;
- удосконалено метод підвищення стійкості та надійності потокового шифрування на основі додаткового застосування синтезованих груп симетричних двохоперандних операцій криптографічного перетворення інформації, що забезпечило підвищення стійкості та варіативності потокового шифрування.

Практичне значення отриманих результатів. Практична цінність роботи полягає в тому, що отримані наукові результати доведено здобувачем до

конкретних інженерних методик, моделей та варіантів функціональних схем спеціалізованих дискретних пристроїв, які реалізують криптографічне перетворення інформації на основі застосування синтезованих груп операцій потокового шифрування та забезпечують підвищення варіативності й стійкості до лінійного криптоаналізу.

На підставі проведених досліджень одержано такі практичні результати: побудовано математичні моделі, алгоритми функціонування та функціональні схеми реалізації груп операцій криптографічного додавання за модулем два та модулем чотири, що дає можливість підвищувати якість систем потокового й блокового шифрувань інформації.

Реалізація. Практичну цінність роботи підтверджено актами впровадження основних результатів дисертаційного дослідження в:

– Центральному конструкторському бюро «Сокіл» Науково-виробничого комплексу «ФОТОПРИЛАД» (м. Черкаси) під час проектування спеціалізованого модуля операційної системи. Основний технічний результат – забезпечення конфіденційності та достовірності передачі команд в оптичній лінії зв'язку за допомогою виробу 1К118. Акт впровадження від 20.11.2012 р.;

– Черкаському державному технологічному університеті на кафедрі інформаційної безпеки та комп'ютерної інженерії в матеріалах лекційних курсів «Основи криптографічного захисту інформації», «Комп'ютерні методи та засоби захисту інформації». Акт впровадження від 19.02.2019 р.

Ключові слова: комп'ютерна криптографія, потокове шифрування, операції криптографічного додавання, синтез груп операцій, стійкість, варіативність.

ABSTRACT

Kozlovska S. H. Methods of synthesis of symmetric operations groups for stream encryption. – Qualification research paper printed as manuscript.

Thesis on gaining scientific degree of the Candidate of Technical Sciences (Doctor of Philosophy) / specialty 05.13.05 “Computer Systems and Components”. – Cherkasy State Technological University, Cherkasy, 2019.

The thesis is devoted to the problem of improving the quality of systems of confidential information streaming encryption due to increasing strength and variability of the transformation on the basis of the additional use of double-operand two-bit operations groups, synthesized on the basis of modulo-2 and modulo-4 addition.

The first part of the paper states that the use of cryptographic transformation operations based on logical functions is one of the most promising directions of the development of cryptographic information security systems. The present state of the research of operations of cryptographic information transformation with the singularization of application features in streaming and block encryption has been considered. The results of the bibliographic search and review of the main results of researches related to the synthesis and analysis of cryptographic information transformation operations have been presented. It has been pointed out that double-operand operations of cryptographic information transformation specialized for streaming encryption did not get enough attention. A number of these operations need to be explored and expanded, and the methods of their synthesis should be developed, since the use of these operations provides increased stability and reliability of stream ciphers. The theoretical preconditions and results of the computational experiment have been shown. As a result, a complete set of truth tables for symmetric two-bit double-operand operations of cryptographic transformation has been calculated on the basis of exhaustive search, as well as the main results of the research of these operations. The results of the investigation of double-operand operations of cryptographic transformation have been demonstrated. The purpose and tasks of the research have been formulated.

The second part of the study is devoted to mathematical modelling and investigation of double-operand operations of cryptographic information transformation based on the known truth tables. To ensure the effectiveness of the research, the truth tables of symmetric two-bit double-operand operations of cryptographic transformation have been analysed and classified. Each of the investigated double-operand operations is the operation of choosing one of the four single-operand operations of transforming the first operand depending on the value of the second operand, which performs the function of control commands. These operations have been divided into 24 sets of double-operand operations for four operations in each set; in addition, all operations have been divided into four mathematical groups. In the process of mathematical transformation of the operation model, a double-operand operation model has been obtained, which can be implemented both at hardware and at software levels. Mathematical models for all operations of the first mathematical group, as well as permutation schemes for constructing these operations, have been developed. Based on the analysis of the obtained results, generalized permutation schemes for the first mathematical group of double-operand operations of cryptographic transformation have been constructed. The sequence of mathematical transformations of experimental data, which ensures obtaining suitable operations for cryptographic transformation in combination with permutation schemes of operations construction visualization, by its nature, is a method of constructing and researching double-operand operations of cryptographic transformation based on the results of a computational experiment. In the course of the study, it has been found out that permutation schemes for constructing the truth tables of sets of double-operand operations of the cryptographic transformations of the first mathematical group do not overlap. The totality of truth tables sets for double-operand operations of the cryptographic transformation of the first mathematical group creates a complete complex of truth tables sets for double-operand operations of cryptography.

The third part of the thesis is devoted to the study of the second mathematical group of double-operand operations of cryptographic transformation using the method of constructing and analyzing double-operand operations of cryptographic

transformation based on the results of a computational experiment. The whole set of operations of the second group has been investigated. In the process of analysis of permutation schemes of the truth tables, the author has determined the following: the complex of truth tables sets for two-operand operations of the cryptographic transformation of the second mathematical group creates a complete complex of truth tables sets of double-operand operations of cryptographic transformation; groups of permutation schemes of the first and second mathematical groups of the investigated operations of cryptographic transformations coincide. It has been found out that the use of a complete group of received permutation schemes will provide the construction of a complete set of double-operand operations of cryptographic transformations, an unknown group and their substitution tables, if we take any operation from this unknown group.

In the fourth part, methods for synthesizing double-operand operations of cryptographic transformations have been developed. After summarizing the results of the study of the operations models of the first group, the classification of operations with the division into basic operations, the combination of basic operations with permutation operations and a combination of basic operations with permutations and inversions have been obtained. This classification has become the basis for developing a method for synthesizing groups of two-bit double-operand operations for symmetric streaming encryption, consisting in the synthesis of double-operand operations of the base group based on the addition of two single-operand operations of processing each operand by the modulo; execution of operations of the base group of permutation operations; execution of operations of the base group in conjunction with operations of permutations of operations of inversion. Since the main operation of this group is the operation of modulo-2 adding, then the group is called a symmetric group of double-operand two-bit operations of cryptographic addition in modulo-2. By analogy with this method, a method for synthesizing a symmetric group of double-operand two-bit operations of a cryptographic addition by modulo-4 is developed. The variants of hardware and software for the realization of synthesized operations have been constructed. It has been demonstrated that the synthesized operation models and their

means of use should be used in the cryptographic transformation unit during the implementation of the method of increasing the strength and reliability of streaming encryption. The given results of statistical researches of practical results of the thesis testify to the fact that the studied sequences passed the complex control over the testing method of the test package NIST_STS. The best test results have been obtained when applying 12 known and 48 synthesized cryptographic transformations. In addition, the combined use of operations increases the variation of streaming encryption by five times.

Research novelty of the obtained results:

- For the first time a method for constructing and researching double-operand operations of cryptographic transformation has been developed based on the results of a computational experiment by formalization, classification and mathematical transformation, which ensured the establishment of new interrelationships between operands and results, as well as the possibility of using single-operand operations in stream encryption ;
- For the first time, methods for the synthesis of groups of symmetric two-bit double-operand operations of stream encryption based on the results of a computational experiment have been developed by applying the results of the implementation of the developed technology and a table representation of the classification of a group of one-operand two-bit operations of the cryptographic transformation, as well as the establishment of new previously unknown interconnections between single-operand and double-operand operations, provided a synthesis of mathematical groups of symmetric double-operand operations on the basis of modulo-2 and modulo-4 addition;
- The method for increasing strength and reliability of streaming encryption has been improved on the basis of the additional application of synthesized groups of symmetric double-operand operations of cryptographic information transformation, which provided increased strength and variation of streaming encryption.

The practical value of the obtained results. The practical value of the study lies in the fact that the obtained research results have been developed by the applicant to the

level of engineering techniques, models and variants of functional schemes of specialized discrete devices that implement cryptographic information transformation based on the application of synthesized groups of streaming encryption operations and provide increased variability and strength to linear cryptanalysis.

Based on the research, the following practical results have been obtained: mathematical models, operational algorithms and functional schemes for the implementation of groups of cryptographic addition operations by modulo-2 and modulo-4 have been developed, which makes it possible to improve the quality of stream and block information encryption systems.

Implementation. The practical value of the paper is confirmed by the acts of implementation of the main results of the thesis at:

– Sokol Central Design Bureau of PHOTOPRYLAD Research and Production Complex (Cherkasy) when developing a specialized module of the operating system. The main technical result is to ensure the confidentiality and reliability of the transmission of commands in the optical communication line with the help of the product 1K118. Implementation Act dated 20.11.2012;

– Cherkasy State Technological University at the Department of Information Security and Computer Engineering in the materials of the lecture courses “Fundamentals of Cryptographic Information Protection”, “Computer Methods and Means of Information Protection”. Implementation Act dated 19.02.2019.

Keywords: computer cryptography, streaming encryption, cryptographic addition operations, synthesis of operation groups, strength, variability.

Список публікацій здобувача:

1. Бабенко В. Г., Козловська С. Г. Особливості використання матричних операцій криптографічного перетворення інформації. *Системи обробки інформації.* 2015. № 3 (128). С. 84–87.

2. Рудницький В. М., Лада Н. В., Козловська С. Г. Технологія побудови двохоперандних операцій криптографічного перетворення інформації за результатами моделювання. *Сучасні інформаційні системи*. 2018. Т. 2, № 4. С. 26–30.

3. Лада Н. В., Козловська С. Г. Застосування операцій криптографічного додавання за модулем два з точністю до перестановки в потокових шифрах. *Системи управління, навігації та зв'язку :* зб. наук. пр. Полтава : ПНТУ, 2018. Т. 1 (47). С. 127–130.

4. Козловська С. Г. Синтез груп двохоперандних операцій криптоперетворення на основі перестановочних схем. *Сучасна спеціальна техніка.* 2018. № 4 (55). С. 44–50.

5. Зажома В. М., Козловська С. Г. Спосіб підвищення достовірності передачі ключового елементу стегоконтейнера. *Smart and Young.* 2016. № 11-12. Частина 1. С. 42–48.

6. Криптографічне кодування: обробка та захист інформації: колективна монографія / за ред. В. М. Рудницького. Харків : ТОВ «ДІСА ПЛЮС», 2018. 139 с.

7. Козловська С. Г. Лада С. В., Аскеров Р. В. Засоби захисту програм від несанкціонованого доступу. *Проблеми інформатизації* : матеріали Першої міжнар. наук.-техн. конф.: тези доп., (Черкаси – Київ – Тольятті – Полтава, 19–20 грудня 2013 р.). Черкаси: ЧДТУ; Київ: ДУТ, Тольятті: ТДУ, Полтава: ПНТУ, 2013. С. 25.

8. Козловська С. Г. Проблеми захисту управлінської інформації. *Теоретико-методологічні і науково-практичні засади інформаційного, фінансового та облікового забезпечення розвитку економіки* : зб. тез доп. наук.-практ. конф., м. Черкаси, 21–22 лист. 2013 р. Черкаси, 2013. С. 50-51.

9. Козловська С. Г. Технічні способи запобігання просочуванню інформації. *Проблеми моделювання структури і процесів економічних систем* : зб. тез доп.

міжнар. наук.-практ. конф., м. Черкаси, 17–18 квіт. 2014 р. Черкаси, 2014. С. 93–95.

10. Козловська С. Г. Персонал підприємства як основне джерело втрати конфіденційної інформації. *Управління економіко-соціальними системами розвитку суспільства в умовах євроінтеграції* : зб. тез доп. наук.-практ. конф., м. Черкаси, 15–17 квіт. 2015 р. Черкаси, 2015. С. 79–80.

11. Козловська С. Г. Особливості криптографічного захисту інформації. *Фінансово-економічне та обліково-аналітичне забезпечення підприємницької діяльності* : зб. тез доп. Всеукр. наук.-практ. конф., м. Черкаси, 20–21 квіт. 2016 р. Черкаси, 2016. С. 360–363.

12. 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.

ЗМІСТ

ВСТУП…….. 5

РОЗДІЛ 1 СУЧАСНИЙ СТАН ТА ПЕРСПЕКТИВИ РОЗВИТКУ МЕТОДІВ СИНТЕЗУ Й АНАЛІЗУ ОПЕРАЦІЙ КРИПТОГРАФІЧНОГО ПЕРЕТВОРЕННЯ ДЛЯ ЗАХИСТУ КОНФІДЕНЦІЙНОЇ ІНФОРМАЦІЇ……..……. 11

1.1 Сучасні напрями розвитку методів криптографічного захисту інформації…….……...……...… 11

1.2 Сучасний стан досліджень операцій криптографічного перетворення інформації ……..…….. 17

1.3 Сучасний стан досліджень двохоперандних операцій криптографічного перетворення інформації …… 20

1.4 Моделювання двохоперандних операцій криптографічного перетворення інформації ……..……...…….. 23

Висновки з розділу 1……..……. 26

РОЗДІЛ 2 МОДЕЛЮВАННЯ ТА ДОСЛІДЖЕННЯ ДВОХОПЕРАНДНИХ ОПЕРАЦІЙ КРИПТОГРАФІЧНОГО ПЕРЕТВОРЕННЯ ІНФОРМАЦІЇ..... 28

2.1 Метод дослідження двохоперандних операцій криптоперетворення….. 28

2.1.1 Класифікація таблиць істинності симетричних двохрозрядних двохоперандних операцій криптоперетворення……. 28

2.1.2 Дослідження набору двохоперандних операцій криптоперетворення. 32

2.2 Дослідження першої математичної групи двохоперандних операцій криптоперетворення…… 38

2.2.1 Дослідження другого набору двохоперандних операцій криптоперетворення першої математичної групи (НДО 2)…..…… 38

2.2.2 Дослідження третього набору двохоперандних операцій криптоперетворення першої математичної групи (НДО 3)…… 43

2.2.3 Дослідження четвертого набору двохоперандних операцій криптоперетворення першої математичної групи (НДО 4)…… 47
2.2.4 Дослідження п’ятого набору двохоперандних операцій криптоперетворення першої математичної групи (НДО 5)…..…… 52
2.2.5 Дослідження шостого набору двохоперандних операцій криптоперетворення першої математичної групи (НДО 6)…… 57
2.3 Побудова узагальнюючих перестановочних схем для синтезу таблиць істинності двохоперандних операцій криптоперетворення першої математичної групи ……. 61
Висновки з розділу 2……..... 71
РОЗДІЛ 3 ДОСЛІДЖЕННЯ ДРУГОЇ МАТЕМАТИЧНОЇ ГРУПИ ДВОХОПЕРАНДНИХ ОПЕРАЦІЙ КРИПТОПЕРЕТВОРЕННЯ... 73
3.1 Дослідження першого набору двохоперандних операцій криптоперетворення другої математичної групи (НДО 7)…….. 73
3.2 Дослідження другого набору двохоперандних операцій криптоперетворення другої ї математичної групи (НДО 8)…… 77
3.3 Дослідження третього набору двохоперандних операцій криптоперетворення другої математичної групи (НДО 9)…….. 82
3.4 Дослідження четвертого набору двохоперандних операцій криптоперетворення другої математичної групи (НДО 10)…… 86
3.5 Дослідження п’ятого набору двохоперандних операцій криптоперетворення другої математичної групи (НДО 11)…… 90
3.6 Дослідження шостого набору двохоперандних операцій криптоперетворення другої математичної групи (НДО 12)…… 94
3.7 Побудова узагальнюючих перестановочних схем для синтезу таблиць істинності двохоперандних операцій криптоперетворення другої математичної групи…….. 99
Висновки з розділу 3……..…….. 107

РОЗДІЛ 4 СИНТЕЗ ГРУП ДВОХОПЕРАНДНИХ ОПЕРАЦІЙ КРИПТОПЕРЕТВОРЕННЯ ТА ОЦІНКА ЕФЕКТИВНОСТІ ЇХ ЗАСТОСУВАННЯ..... 108
4.1 Узагальнення результатів дослідження та синтез операцій криптоперетворення першої математичної групи…….……. 108
4.1.1 Узагальнення результатів дослідження операцій криптоперетворення першої математичної групи ……..……...……. 108
4.1.2 Метод синтезу операцій криптоперетворення першої математичної групи (групи двохрозрядних операцій додавання за модулем два)…… 111
4.2 Метод синтезу операцій криптоперетворення другої математичної групи…….. 118
4.3 Реалізація синтезованих двохоперандних операцій криптоперетворення……. 128
4.4 Оцінка ефективності застосування синтезованих двохоперандних операцій криптоперетворення в потокових шифрах……..... 132
Висновки з розділу 4……..…….. 137
ВИСНОВКИ……... 138
СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ…… 140
ДОДАТКИ…… 154

ВСТУП

Актуальність теми. Нині криптогрфічний захист інформації є одним із найефективніших засобів забезпечення інформаційної безпеки будь-якої держави. Проте постійний розвиток технічного прогресу вимагає невпинного створення нових та вдосконалення вже еаявних методів та засобів кроптографічного захисту. Наразі одним з шляхів досягнення цієї мети є створення нових або покращення вже розроблених алгоритмів криптографічного перетворення. Дедалі більше уваги для вирішення цієї задачі приділяють розширенню кількості операцій, придатних для прямого та оберненого криптоперетворення інформації. Для уникнення некоректності та помилок під час застосування нових операцій вони потребують детального дослідження. Саме тому синтез нових операцій криптоперетворення є актуальним.

Значний внесок у розвиток наявних та розроблення нових криптографічних методів і засобів захисту інформації зробили такі зарубіжні та вітчизняні вчені: G. Brassard, C. D. Bennett, B. Chor, W. Diffie, M. E. Hellman, N. Koblitz, J. L. Massey, U. M. Maurer, R. L. Rivest, C. E. Shannon, A. Shamir, B Schneier, А. Я. Білецький, І. Д. Горбенко, П. В. Дорошкевич, В. К. Задірака, Л. В. Ковальчук, О. Г. Корченко, Ю. В. Кузнецов, О. А. Логачов, В. А. Лужецький, А. А. Молдовян, А. М. Олексійчук, Б. Я. Рябко, В. М. Сидельніков, А. Н. Фіонов, С. О. Шестаков, В. В. Ященко та інші.

Наразі розвиток потокових шифрів пов'язаний з вирішенням задач генерації високоякісних псевдовипадкових послідовностей та побудови нових логічних операцій потокового шифрування.

Одним з перспективних напрямів розвитку потокового шифрування є застосування булевих функцій для побудови операцій криптоперетворення інформації, що підтверджується роботами О. В. Дмитришина, Л. В. Ковальчук, В. А. Лужецького, А. М. Олексійчука, О. М. Романкевича, К. Г. Самофалова.

Попри це, задачі синтезу груп симетричних двохоперандних операцій потокового шифрування не було розглянуто. Таким чином, можна стверджувати,

що тема дисертаційного дослідження «Методи синтезу груп симетричних операцій для потокового шифрування» є актуальною.

Зв'язок роботи з науковими програмами, планами, темами.

Дисертаційна робота виконана відповідно до Постанови Президії НАНУ від 25.02.2009 р. № 55 «Про основні наукові напрями та найважливіші проблеми фундаментальних досліджень у галузі природничих, технічних і гуманітарних наук на 2009 – 2013 рр.» (п. 1.2.7.1. Розробка методів та інформаційних технологій розв’язання задач комп’ютерної криптографії та стеганографії; п. 1.2.7.2. Розробка методів підвищення продуктивності систем асиметричної криптографії), Постанови Президії НАНУ від 20.12.13 №179 «Основні наукові напрями та найважливіші проблеми фундаментальних досліджень у галузі природничих, технічних і гуманітарних наук Національної академії наук України на 2014–2018 рр.», а саме – пп. 1.2.8.1. «Розробка методів та інформаційних технологій розв’язання задач комп’ютерної криптографії та стеганографії», а також Постанови КМУ від 7 вересня 2011 року №942 «Про затвердження переліку пріоритетних тематичних напрямів наукових досліджень і науково-технічних розробок на період до 2020 року», а саме – «Технології та засоби захисту інформації». Результати дисертаційної роботи включені в НДР «Метод синтезу швидкодіючих систем захисту інформації на основі спеціалізованих логічних функцій» (ДР№ 0108U000506), «Метод синтезу механізмів захисту інформації в спеціалізованих автоматизованих системах» (ДР № 0108U000508), «Синтез операцій криптографічного перетворення з заданим характеристиками» (ДР № 0116U008714), в яких автор брав участь як виконавець.

Мета і задачі дослідження. Основною метою дослідження є підвищення якості систем потокового шифрування конфіденційної інформації за рахунок збільшення стійкості та варіативності перетворення на основі додаткового використання груп двохоперандних двохрозрядних операцій, синтезованих на основі додавання за модулем два та чотири.

Для досягнення поставленої мети сформульовано та розв’язано такі задачі:

– розроблення методу побудови та дослідження двохоперандних операцій

криптоперетворення;

– розроблення методів синтезу груп симетричних двохрозрядних двохоперандних операцій потокового шифрування;

– удосконалення методу підвищення стійкості та надійності потокового шифрування та оцінка його ефективність.

Об'єкт дослідження – процеси потокового криптографічного перетворення інформації в комп’ютерних системах і мережах.

Предмет дослідження – методи та засоби синтезу груп симетричних операцій потокового шифрування на основі додавання за модулем два та модулем чотири для підвищення захищеності конфіденційної інформації.

Методи дослідження. У процесі розробки технології побудови та дослідження двохоперандних операцій криптоперетворення використовувався математичний апарат теорії інформації, теорії алгоритмів, криптографії, логіки, методів дискретної математики та комп’ютерного моделювання.

Для розроблення методів синтезу груп симетричних двохрозрядних двохоперандних операцій потокового шифрування використано: теорію алгоритмів, криптографію, методи комп’ютерного моделювання та дискретної математики.

Для вдосконалення методу підвищення стійкості й надійності потокового шифрування та оцінки його ефективності використано теорії: інформації, ймовірності, алгоритмів, криптографії із застосуванням методів дискретної математики, комп’ютерного моделювання та математичної статистики.

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

1) вперше розроблено метод побудови та дослідження двохоперандних операцій криптоперетворення на основі результатів обчислювального експерименту, шляхом формалізації, класифікації та математичного перетворення що забезпечило встановлення нових взаємозв’язків між операндами й результатами, а також можливість застосування одноопераднихоперацій у потоковому шифруванні;

2) вперше розроблено методи синтезу груп симетричних двохрозрядних двохоперандних операцій потокового шифрування на основі результатів обчислювального експерименту шляхом застосування результатів реалізації розробленого методу побудови та дослідження двохоперандних операцій, та табличного представлення класифікації групи одноопераднних двохрозрядних операцій криптографічного перетворення, а також встановлення нових раніше невідомих взаємозв'язків між одноопераднними та двохоперандними операціями, що забезпечило синтез математичних груп симетричних двохоперандних операцій на основі додавання за модулем два та додавання за модулем чотири;

3) удосконалено метод підвищення стійкості та надійності потокового шифрування на основі додаткового застосування синтезованих груп симетричних двохоперандних операцій криптографічного перетворення інформації, що забезпечило підвищення стійкості та варіативності потокового шифрування.

Практичне значення отриманих результатів. Практична цінність роботи полягає в тому що отримані наукові результати доведенні здобувачем до конкретних інженерних методик, моделей та варіантів функціональних схем спеціалізованих дискретних пристроїв, які реалізують криптографічне перетворення інформації на основі застосування синтезованих груп операцій потокового шифрування та забезпечують підвищення варіативності й стійкості до лінійного криптоаналізу.

На підставі проведених досліджень одержано такі практичні результати: побудовано математичні моделі, алгоритми функціонування та функціональні схеми реалізації груп операцій криптографічного додавання за модулем два та модулем чотири, що дало можливість підвищити якість систем потокового і блокового шифрування інформації.

Реалізація. Практична цінність роботи підтверджена актами впровадження основних результатів дисертаційного дослідження в:

–Центральному конструкторському бюро «Сокіл» Науково-виробничого комплексу «ФОТОПРИЛАД» (м. Черкаси) під час проектування спеціалізованого модуля операційної системи. Основний технічний результат – забезпечення

конфіденційності та достовірності передачі команд в оптичній лінії зв'язку за допомогою виробу 1К118. Акт впровадження від 20.11.2012 р.;

– Черкаському державному технологічному університеті на кафедрі інформаційної безпеки та комп'ютерної інженерії в матеріалах лекційних курсів «Основи криптографічного захисту інформації», «Комп'ютерні методи та засоби захисту інформації». Акт впровадження від 19.02.2019 р.

Особистий внесок здобувача. Усі нові результати дисертаційної роботи автор отримав самостійно. У опублікованих у співавторстві наукових працях з питань, що стосуються цього дослідження, автору належать: проведення аналізу та дослідження властивостей результатів шифрування фрагменту інформації, здійсненого на основі поєднання матричних операцій криптоперетворення [1], проведення побудови удосконалених моделей двохоперандних операцій криптографічного перетворення інформації [2,6], проведення оцінки результатів застосування операцій потокового шифрування за їхнього випадкового вибору на основі додаткової гамуючої послідовності [3], виконання узагальнення експериментальних досліджень результатів тестування псевдовипадкових послідовностей за різних алгоритмів і операцій реалізації [5], розгляд можливості підвищення стійкості до лінійного криптоаналізу за рахунок використання результатів попереднього перетворення в якості гамуючої послідовності для вибору операцій при захисті програм [7], проведення побудови та узагальнення перестановочнм схем операцій [12]. Результати, опубліковані в [4, 8-11], отримано одноосібно.

Апробація результатів дисертації. Результати дисертаційної роботи доповідалися й обговорювалися на Першій міжнародній науково-технічній конференції «Проблеми інформатизації» (Черкаси – Київ – Тольятті – Полтава, 2013), Науково-практичній конференції «Теоретико-методологічні і науково-практичні засади інформаційного, фінансового та облікового забезпечення розвитку економіки» (Черкаси, 2013), Міжнародній науково-практичній конференції «Проблеми моделювання структури і процесів економічних систем» (Черкаси, 2014), Науково-практичній конференції «Управління економіко-

соціальними системами розвитку суспільства в умовах євроінтеграції» (Черкаси, 2015), Всеукраїнській науково-практичній конференції «Фінансово-економічне та обліково-аналітичне забезпечення підприємницької діяльності» (Черкаси, 2016), Шостій міжнародній науково-технічній конференції «Проблеми інформатизації» (Черкаси – Баку – Бельсько-Бяла - Харків, 2018).

Публікації. Основні результати дисертаційної роботи викладено в 12-ти друкованих працях, у тому числі: 5-ти статтях у наукових журналах і збірниках наукових праць, внесених до списку українських та закордонних [1-5] фахових видань; 1 колективній монографії [6]; 6-ти тезах доповідей на міжнародних науково-технічних та науково-практичних конференціях.

Структура і обсяг дисертації. Робота складається зі вступу, чотирьох розділів, висновків, списку використаних джерел, додатків. Загальний обсяг дисертації – 173 сторінки. Основний зміст викладено на 149 сторінках, дисертація містить 23 таблиці, 57 рисунків. Список використаних джерел містить 108 найменувань. Робота містить 8 додатків.

РОЗДІЛ 1 СУЧАСНИЙ СТАН ТА ПЕРСПЕКТИВИ РОЗВИТКУ МЕТОДІВ СИНТЕЗУ Й АНАЛІЗУ ОПЕРАЦІЙ КРИПТОГРАФІЧНОГО ПЕРЕТВОРЕННЯ ДЛЯ ЗАХИСТУ КОНФІДЕНЦІЙНОЇ ІНФОРМАЦІЇ

1.1 Сучасні напрями розвитку методів криптографічного захисту інформації

В сучасному високоінформатизованому суспільстві все більш гострою стає проблема ефективного захисту інформації, як на рівні персональних даних, так і держави вцілому. Нині криптогрфічний захист інформації є одним із найефективніших засобів забезпечення інформаційної безпеки будь-якої держави. Одними з найкращих методів захисту інформації були і залишаються криптографічні методи [13]. Але для успішної протидії зловмисникам, кваліфікація і можливості яких зростають, криптографічні методи захисту конфіденційної інформації також потребують постійного вдосконалення.

Слід зазначити, що методами криптографічного захисту інформації є системи шифрування інформації, алгоритми захисту від нав’язування фальшивої інформації (MAC-коди та алгоритми електронного цифрового підпису) та криптографічні протоколи розподілу ключів, автентифікації й підтвердження факту прийому (передачі) інформації [14].

Сучасна комп’ютерна криптографія поділяється на декілька основних розділів, відповідно до яких і формуються нові криптографічні методи захисту інформації. Це симетрична криптографія, асиметрична криптографія, розділ керування ключами, еліптична, квантова, гібрідна криптографія тощо.

Симетрична криптографія [15] – один з найбільших розділів комп’ютерної криптографії, в основі якого лежить спосіб шифрування, в якому для шифрування і дешифрування застосовується один і той же криптографічний ключ, який має зберігатися в секреті обома сторонами. Криптоалгоритми симетричного шифрування виконують криптоперетворення невеликого блоку даних (1 біт або 32-128 біт).

Асиметрична криптографія [16] – розділ криптографії, в основі якого лежать алгоритми шифрування, які використовують різні ключі для шифрування та розшифрування даних. Головна перевага асиметричного шифрування полягає у відсутності потреби відправникові й одержувачеві погоджувати таємний ключ по спеціальному захищеному каналі. Процедура шифрування є необоротною навіть за відомим ключем шифрування (прочитати повідомлення можна тільки за допомогою другого ключа «дешифрування»). Недоліком асиметричних криптосистем є низька швидкість криптоперетворень, у порівнянні з симетричними криптосистемами.

Еліптична криптографія [17] – розділ криптографії, який вивчає асиметричні криптосистеми, засновані на еліптичних кривих над скінченними полями [18]. Основна перевага еліптичної криптографії полягає в тому, що насьогодні невідомо субекспоненціальні алгоритми для вирішення задачі дискретного логарифмування в групах точок еліптичних кривих [19]. Використання еліптичних кривих для створення криптосистем було незалежно запропоновано Нілом Коблицом і Віктором Міллером в 1985 р.

Варто зазначити, що українським стандартом, який описує алгоритми формування та перевірки електронного цифрового підпису є прийнятий і введений в дію наказом Державного комітету України з питань технічного регулювання та споживчої політики від 28 грудня 2002 № 31 ДСТУ 4145-2002 (повна назва: “ДСТУ 4145-2002. Інформаційні технології. Криптографічний захист інформації. Цифровий підпис, що грунтується на еліптичних кривих. Формування та перевірка”) [20].

Квантова криптографія [21-22] – розділ криптографії, що грунтується на застосуванні підходів та методів квантової механіки (зокрема, квантової передачі інформації та квантових обчислень) для безпечної передачі секретного ключа (квантовий розподіл ключа) й використання квантових комп'ютерів. Квантова криптографія вивчає методи захисту систем зв’язку й заснована на принциповій непорушності закономірностей квантової фізики, об’єкти якої забезпечують процеси безпечного передавання інформації між легітимними користувачами. В

останні роки значний інтерес посідає квантовий розподіл ключів, також виокремлюють такі напрями, як квантовий прямий безпечний зв'язок, квантове розділення секрету, квантове потокове шифрування, квантовий цифровий підпис та квантова стеганографія.

Слід зазначити, що останнім часом все більшої популярності набуває гібридна криптографія. Гібридна (або комбінована) криптосистема – це система шифрування, що поєднує переваги криптосистеми з відкритим ключем з продуктивністю симетричних криптосистем. Симетричний ключ використовується для шифрування даних, асиметричний – для шифрування самого симетричного ключа, інакше це називається числовою упаковкою [23].

Вдосконалення та створення нових методів криптографічного захисту інформації нині провадять за багатьма напрямами: збільшення довжини ключа, покращення гамуючої послідовності, збільшення спектру різноманітних операцій, що можуть бути використані при криптоперетвореннях, тощо [13].

Серед напрямків розвитку криптографії можна виокремити побудову операцій криптографічного перетворення на основі застосування логічної функції, які забезпечують побудову високошвидкісних криптографічних примітивів [13].

Особливу увагу в сучасних друкованих виданнях приділено застосовуванню матричних операцій криптографічного перетворення та криптопримітивів, побудованих на їх основі, для алгоритмів захисту інформаційних ресурсів [24–25].

Вдосконалення та розробка нових криптографічних методів повинні збільшувати стійкість, надійність та ефективність вцілому захисту інформації.

Криптографічна стійкість методів криптографічного захисту інформації визначається в широкому сенсі: здатністю криптосистеми або криптоалгоритму протистояти атакам з використанням методів криптоаналізу; у вузькому сенсі: чисельна характеристика складності взлому криптографічного алгоритму з урахуванням тих науково-технічних способів і засобів, які може використовувати криптоаналітик, а також це властивість криптографічних алгоритмів і криптографічних протоколів, що характеризує їх здатність протистояти методам

дешифрування (процес несанкціонованого відновлення оригіналу тексту повідомлення) [26].

Поняття стійкості за Шеноном поділяють на два різновиди [27]:

Теоретична стійкість – стійкість криптосистеми за наявності у криптоаналітика необмеженого часу, необмежених обчислювальних ресурсів, найкращих методів криптоаналізу.

Практична стійкість – стійкість криптосистеми на даний момент часу з урахуванням того, що криптоаналітик володіє обмеженим часом, обмеженими обчислювальними здібностями і сучасними методами криптоаналізу .

Слід зазначити, що оцінка ефективності криптографічних алгоритмів на основі нових методів повинна перевірятись за рахунок сучасних методів криптоаналізу, а саме [28-32]:

– методів «Грубої сили»;
– статистичних методів криптоаналізу;
– лінійного криптоаналізу;
– диференціального криптоаналізу;
– методу зустрічі посередині;
– SLIDE-атак;
– методу «Бумеранга» тощо.

На основі потреб протидії методам сучасного криптоаналізу, методи криптографічного захисту інформації мають передбачати як програмне, так і апаратне використання. Програмна реалізація шифрування більш дешева та практична. Водночас апаратна реалізація продуктивніша та простіша у використанні. Сучасні криптографічні системи мають задовольняти такі загальноприйняті вимоги [33-34]:

– вихідний текст із зашифрованого тексту можна відтворити лише за допомогою ключа дешифрування (набір параметрів для шифрування повідомлення);

– кількість операцій, необхідних для визначення використаного ключа шифрування за фрагментом повідомлення та відповідного йому відкритого тексту, мають бути не менше загальної кількості можливих ключів;

– кількість операцій, необхідних для розшифрування інформації шляхом перебору можливих ключів, потребує значного часу для обчислень або великих затрат на реалізацію цих обчислень, мати строгу нижню оцінку й виходити за межі можливостей сучасних комп'ютерів (із врахуванням можливості використання мережних обчислень);

– знання алгоритму шифрування не повинне впливати на надійність захисту та стійкість до зламування системи шифрування;

– незначна зміна ключа повинна призводити до значної зміни виду зашифрованого повідомлення навіть при використанні одного і того ж ключа;

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

Сучасні наукові дослідження в сфері криптографічного захисту інформації приділяють дедалі більше уваги створенню нових та вдосконаленню вже наявних алгоритмів криптографічного перетворення, а також аналізу й синтезу операцій, на основі яких будують системи криптографічного захисту інформації [35].

Зупинимося детальніше на нових методах гомоморфного шифрування інформаційних ресурсів. Під поняттям гомоморфного шифрування будемо розуміти модель шифрування, яка дозволяє виконувати певні математичні дії з зашифрованим текстом і отримувати зашифрований результат, який відповідає результату аналогічної операції, що проводиться з відкритим текстом. Сучасні гомоморфні системи шифрування поділяють на два класи: частково гомоморфні системи та повністю гомоморфні системи [36].

Вперше поняття «гомоморфне шифрування» було використане в 1978 році після розробки відомого асиметричного алгоритму RSA його авторами Рональдом Рівестом, Леонардо Адлеманом та Майклом Дертузосом, але їх перші спроби обґрунтувати необхідність та можливість практичного застосування

гомоморфного шифрування були невдалими. В 2009 році співробітником IBM Крейгом Джентрі була запропонована модель повністю гомоморфної криптографічної системи, за допомогою якої стало можливим реалізувати операції додавання та множення над зашифрованими даними без їх попереднього розшифрування [37–38].

Порівняльний аналіз та характеристика сучасних алгоритмів гомоморфного шифрування дозволяють зробити такі висновки:

– визначити, який алгоритм є найбільш ефективним та потужним практично неможливо, бо вони мають свої недоліки та переваги, тому їх пріоритет в оцінці залежить від задачі, яка має бути вирішена;

– для забезпечення криптостійкості конфіденційної інформації можливе використання асиметричних алгоритмів з відкритим ключем з метою шифрування/дешифрування інформації, генерації/перевірки ЕЦП та надійного їх зберігання в зашифрованому вигляді;

– у випадку, коли важливішим є питання швидкості обчислень, зменшення їх складності з метою економії програмно-апаратних ресурсів, пріоритетним є використання симетричних алгоритмів або використання комбінованих алгоритмів в поєднанні з функціями хешування; при цьому створюються різноманітні гібридні криптосистеми;

– у випадку, коли необхідно зберегти конфіденційність інформації, що зберігається на сервері, ця інформація потребує обробки, а її дешифрування при обробці несе загрозу для конфіденційності, тоді пріоритетним є використання моделі повного гомоморфного шифрування, що дає можливість виконання математичних операцій над зашифрованим текстом, при цьому не розшифровуючи його. Відповідно до цього, використовуючи алгоритм повного гомоморфного шифрування на сервері, конфіденційна інформація у відкритому вигляді зберігатися не буде на всіх етапах шифрування/дешифрування [39].

Одним з перспективних напрямів розвитку криптоалгоритмів є побудова принципово нових та вдосконалення наявних на основі елементарних криптографічних перетворень, які реалізуються на основі поєднання

елементарних булевих функцій. Ці перетворення отримали назву операцій криптоперетворення, а елементарні булеві функції названі елементарними функціями [40]. Проте насьогодні ці операції розроблялися орієнтовано на блочне шифрування. Спеціалізованим операціям для потокового шифрування достатньо уваги не приділялося. Враховуючи вищезазначене, актуальною постає проблема розробки методу підвищення надійності потокового шифрування на основі розширення множини функцій криптоперетворення за рахунок модифікацій операцій криптографічного додавання за модулем два.

1.2 Сучасний стан досліджень операцій криптографічного перетворення інформації

На сьогодні в науковій літературі зростає кількість публікацій, присвячених дослідженням операцій, які реалізують криптопримітиви й криптоалгоритми. Особливу увагу слід звернути на роботи зі створення нових стійких та ефективних криптографічних алгоритмів й операцій криптоперетворення інформації на основі систематичних досліджень, таких як дослідження логічних операцій криптографічного перетворення інформації, дослідження їхньої побудови або використання арифметичних операцій з різними модулями тощо [41].

Дослідження операцій матричного криптографічного перетворення та його розширення ведуть за двома основними напрямами, а саме: дослідження лінійних операцій розширеного матричного криптоперетворення та дослідження нелінійних операцій. Ці дослідження провадять майже паралельно, оскільки вони є однаково важливими для розвитку сучасної криптографічної науки.

В роботах [42-44] запропоновано використовувати для алгоритмів захисту інформації матричні операції криптографічного перетворення та криптопримітиви, побудовані на їхній основі, а для підвищення швидкості потокових криптографічних алгоритмів в [45-46] сформульовано ідею використання груп наборів операцій криптоперетворення.

В роботах [47-48] досліджено повну групу двохрозрядних операцій криптографічного перетворення інформації. Крім того, слід зазначити, що досліджувану групу операцій реалізовано за допомогою пристрою криптографічного перетворення інформації, представленого на схемотехнічному рівні в роботі [49].

В роботах [50-51] запропоновано використовувати перекодування інформації для підвищення швидкості доступу до конфіденційних інформаційних ресурсів. Таке перекодування інформації переводить її, не розкодовуючи, від закодованої двохрозрядними операціями на основі однієї псевдовипадкової послідовності в закодовану на основі іншої псевдовипадкової послідовності.

Узагальнення вищезазначених результатів дослідження лінійних операцій матричного криптоперетворення по створенню передумов підвищення швидкості та стійкості як блокових, так і потокових шифрів, представлені в роботах [52-53].

Зі свого боку, в роботах [54-55] наведено дослідження нелінійних операцій розширеного матричного криптоперетворення. Узагальнення результатів дослідження нелінійних операцій матричного криптоперетворення, а також побудова математичного апарату для них представлено в [56-57].

Як відомо, на складність реалізації операцій криптоперетворення впливають багато факторів, таких як можливість практичного використання або вплив надлишковості тощо. Дослідженню впливу деяких з цих факторів на складність реалізації операцій криптоперетворення присвячено роботи [58-59].

Окрему увагу слід звернути на дослідження операцій криптоперетворення, вибір яких залежить від ключової послідовності, а алгоритм реалізації яких та результати його виконання - від інформації, яка буде закодована, тобто на операції, які керуються як ключовою послідовністю, так і інформацією, яка закривається. Цим дослідженням присвячено роботи [60-62]. Результати застосування таких операцій криптоперетворення, які забезпечують можливість практичного використання перестановок, керованих операцією, представлено в роботах [63-64].

Ще одним перспективним напрямом досліджень операцій криптографічного перетворення інформації є дослідження, представлено в роботах [65-67], і спрямовані на встановлення нових взаємозв'язків між прямими та оберненими криптографічними операціями та впровадження ієрархічної структури групового перетворення для підвищення стійкості результатів шифрування в моделі побудови криптоперетворення на основі використання двохоперандних операцій.

На основі цих досліджень в роботах [68-70] представлено метод підвищення стійкості псевдовипадкових послідовностей, побудованих на основі застосування операцій матричного криптографічного перетворення, шляхом їх додавання за модулем, та метод підвищення швидкості реалізації групового матричного криптографічного перетворення на основі запропонованої узагальненої математичної моделі групового матричного криптографічного перетворення, за рахунок зменшення складності побудови та реалізації оберненого перетворення [68, 71]. Застосування цих методів забезпечило підвищення ймовірності вироджених результатів перетворення та зменшення математичної складності й швидкості криптографічного перетворення [72].

Крім того, слід відмітити, що синтез операцій розширеного матричного криптографічного перетворення досліджувався також з точки зору застосування довільної кількості аргументів, а саме побудови груп операцій з заданими кількостями аргументів та побудову правил синтезу операцій заданої кількості аргументів [73-74]. Основою цих досліджень було виявлення і формалізація взаємозв'язків між більшою кількістю аргументів в операції та більшою кількістю операцій на базі операцій розширеного матричного криптографічного перетворення трьох аргументів.

Виявлення і формалізація взаємозв'язків між прямими та оберненими операціями розширеного матричного криптографічного перетворення довільної кількості аргументів, на основі синтезованих невироджених операцій, наведених в [75-76], дали змогу використовувати ці операції в комп'ютерній криптографії. Зі свого боку представлений в роботах [77-78] метод реалізації операцій розширеного матричного криптоперетворення на основі застосування більшої

кількості нових синтезованих операцій розширеного матричного криптоперетворення, шляхом їх випадкового синтезу, забезпечує можливість їх застосування не лише на апаратному, але і на програмному рівнях.

У роботі К. Шенона [27] доведено, що повторне використання криптоалгоритму, який утворює математичну групу, не підвищує крипостійкість. Відповідно при побудові криптоалгоритмів для підвищення їх криптостійкості доцільно використовувати операцій криптоперетворення, які належать різним математичним групам, а при повторному застосуванні криптоалгоритму доцільно замінити хоч б одну з операцій іншою з іншої математичної групи [16]. Проте попри ці обмеження в повсякденній практиці застосовують, як правило, кілька раундів шифрування, підтвердженням цього є наявні стандарти блокового шифрування України та США. В дослідженнях операцій криптоперетворення [79-80] доведено: якщо операція забезпечує високу якість перетворення, то повторне її застосування або застосування аналогічної операції, не можуть покращити якість перетворення.

1.3 Сучасний стан досліджень двохоперандних операцій криптографічного перетворення інформації

Системи потокового криптографічного захисту інформації будують на основі операцій за модулем. В симетричних блокових шифрах широко застосовують операції множення та додавання за модулем два, чотири, шістдесят чотири і двісті п’ятдесят шість. Ці операції є двохоперандними.

Синтез двохоперандних операцій криптоперетворення може розвиватися за двома основними напрямами. Перший напрям полягає в модифікації операцій додавання за модулем на основі перестановок операндів і результатів виконання операцій. Результати цих досліджень представлено в роботах [81-82].

В роботах [83-84] запропоновано другий напрям синтезу двохоперандних операцій криптоперетворення, в основі якого лежить моделювання

двохоперандних операцій криптоперетворення на основі одноопераднних. Проте отримані результати є розрізненими і не систематизованими [85].

Встановлено, що поєднання одноопераднних операцій крипторперетворення в двохоперандні забезпечує збільшення невизначеності результатів потокового шифрування та збільшення варіативності алгоритму перетворення порівняно з операціями, синтезованими на основі додавання за модулем два з точністю до перестановки. Цей висновок ґрунтується на тому, що при поєднанні одноопераднних операцій криптоперетворення в двохоперандні отримано 96 симетричних операцій, порівняно із 12-ма операціями, побудованими на основі додавання за модулем два з точністю до перестановки [86].

Перевагою двохоперандних операцій криптоперетворення (ДОК) перед одноопераднними є їхня універсальність за рахунок можливості їхнього застосування не лише в блокових, але й в потокових шифрах [86].

Наразі все більше уваги приділяється синтезу двохоперандних операцій криптоперетворення, як за рахунок модифікації операцій додавання за модулем на основі перестановок операндів і результатів виконання операцій [87], так і за рахунок моделювання двохоперандних операцій криптоперетворення на основі одноопераднних [88].

Серед останніх досліджень і публікацій варто виокремити дослідження матричних операцій криптографічного перетворення, синтезованих на основі операції додавання за модулем [89], синтез і аналіз операцій двохоперандного криптографічного додавання за модулем два та чотири [90], які можна використовувати для здійснення криптографічного перетворення. Зокрема, в [89] синтезовано групу операцій додавання за модулем два та доведено, що вона є групою перестановок, показано її придатність для використання в алгоритмах криптографічного перетворення.

У роботі [90] синтезовано й проаналізовано модифікації базової операції криптографічного додавання за модулем два для криптографічного перетворення зі збереженням інформативності.

У роботі [91] представлено синтез двохоперандних операцій криптоперетворення для потокового шифрування на основі додавання за модулем з точністю до перестановки. Ці операції будуються на основі перестановок операндів та перестановок результатів виконання додавання за модулем.

У роботі [92] представлено результати дослідження щодо використання операцій додавання за модулем два та перестановки для реалізації матричних операцій криптоперетворення, а також виявлено, що взаємозв'язки між операціями, що застосовуються для криптографічного перетворення на основі матричних моделей, характеризуються циклічністю.

В роботі [93] на основі обчислювального експерименту по моделюванню прямих і обернених операцій криптоперетворення для використання в матричних алгоритмах проведено аналіз і дослідження взаємозв'язків між прямими та оберненими матричними моделями операцій криптоперетворення інформації, а також доведена коректність їх використання.

В роботі [94] узагальнено результати дослідження щодо виконання модифікованих операцій додавання за модулем два з точністю до перестановки, наведено методику синтезу повної групи цих операцій та технологію їх досліджень.

Дослідженню синтезу модифікованих операцій додавання за модулем два з точністю до перестановки на базі поєднання матричних криптоалгоритмів з перестановками операндів і результатів виконання операцій присвячені роботи [95-96]. Визначення і формалізація взаємозв'язків між операціями та алгоритмами для прямого і оберненого криптоперетворення забезпечило побудову симетричних та несиметричних модифікованих операцій [98].

В роботах [97-98] синтезовано та досліджено повну групу модифікованих операцій криптографічного додавання за модулем два з точністю до перестановки. Результати цих досліджень дали змогу синтезувати математичні моделі криптоперетворення та побудовати на їх основі уніфікований пристрій шифрування [35].

Водночас, слід зазначити, що застосування групи модифікованих операцій

додавання за модулем два з точністю до перестановки шляхом використання додаткової гамуючої послідовності для вибору операцій на кожному етапі шифрування підвищує стійкість та надійність потокового шифрування, а також виключає можливість витоку інформації та ускладнює злом гамуючої послідовності при однократних відмовах в системі [99]

1.4 Моделювання двохоперандних операцій криптографічного перетворення інформації

Двохоперандні операції криптографічного перетворення інформації, які розглянуто в підрозділі 1.3, відомі і достатньо досліджені.

В роботах проведена спроба встановити можливість існування інших, раніше не досліджених двохоперандних операцій криптоперетворення. Для вирішення цієї задачі було проведено обчислювальний експеримент по моделюванню двохрозрядних операцій. При проведенні експерименту було встановлено декілька обмежень: моделювалися лише симетричні операції, так як вони не потребують дослідження і побудови обернених операцій; моделювалися лише двохрозрядні двохоперандні операції, із-за практичної можливості їх дослідити в майбутньому.

Сутність експерименту полягала в повному переборі варіантів номерації двохрозрядних таблиць істинності по чотири, які забезпечують в залежності від номера пряме та обернене перетворення двох біт інформації.

В експерименті було використано всі 24 двохрозрядні одноопераднi операції наведені в табл. 1.1. Для спрощення представлення результатів експерименту номера операцій в табл. 1.1 використані для позначення послідовностей таблиць підстановки в операціях, які отримано за результатами експерименту.

Таблиця 1.1

Двохрозрядні операції матричного перетворення

Пряме перетворення	Обернене перетворення	Пряме перетворення	Обернене перетворення
$F_1^k = \begin{bmatrix} x_1 \\ x_2 \end{bmatrix} \oplus \begin{bmatrix} 0 \\ 0 \end{bmatrix}$	$F_1^d = \begin{bmatrix} x_1 \\ x_2 \end{bmatrix} \oplus \begin{bmatrix} 0 \\ 0 \end{bmatrix}$	$F_{13}^k = \begin{bmatrix} x_1 \\ x_2 \end{bmatrix} \oplus \begin{bmatrix} 1 \\ 0 \end{bmatrix}$	$F_{13}^d = \begin{bmatrix} x_1 \\ x_2 \end{bmatrix} \oplus \begin{bmatrix} 1 \\ 0 \end{bmatrix}$
$F_2^k = \begin{bmatrix} x_1 \oplus x_2 \\ x_2 \end{bmatrix} \oplus \begin{bmatrix} 0 \\ 0 \end{bmatrix}$	$F_2^d = \begin{bmatrix} x_1 \oplus x_2 \\ x_2 \end{bmatrix} \oplus \begin{bmatrix} 0 \\ 0 \end{bmatrix}$	$F_{14}^k = \begin{bmatrix} x_1 \oplus x_2 \\ x_2 \end{bmatrix} \oplus \begin{bmatrix} 1 \\ 0 \end{bmatrix}$	$F_{14}^d = \begin{bmatrix} x_1 \oplus x_2 \\ x_2 \end{bmatrix} \oplus \begin{bmatrix} 1 \\ 0 \end{bmatrix}$
$F_3^k = \begin{bmatrix} x_1 \\ x_1 \oplus x_2 \end{bmatrix} \oplus \begin{bmatrix} 0 \\ 0 \end{bmatrix}$	$F_3^d = \begin{bmatrix} x_1 \\ x_1 \oplus x_2 \end{bmatrix} \oplus \begin{bmatrix} 0 \\ 0 \end{bmatrix}$	$F_{15}^k = \begin{bmatrix} x_1 \\ x_1 \oplus x_2 \end{bmatrix} \oplus \begin{bmatrix} 1 \\ 0 \end{bmatrix}$	$F_{15}^d = \begin{bmatrix} x_1 \\ x_1 \oplus x_2 \end{bmatrix} \oplus \begin{bmatrix} 1 \\ 1 \end{bmatrix}$
$F_4^k = \begin{bmatrix} x_2 \\ x_1 \end{bmatrix} \oplus \begin{bmatrix} 0 \\ 0 \end{bmatrix}$	$F_4^d = \begin{bmatrix} x_2 \\ x_1 \end{bmatrix} \oplus \begin{bmatrix} 0 \\ 0 \end{bmatrix}$	$F_{16}^k = \begin{bmatrix} x_2 \\ x_1 \end{bmatrix} \oplus \begin{bmatrix} 1 \\ 0 \end{bmatrix}$	$F_{16}^d = \begin{bmatrix} x_2 \\ x_1 \end{bmatrix} \oplus \begin{bmatrix} 0 \\ 1 \end{bmatrix}$
$F_5^k = \begin{bmatrix} x_2 \\ x_1 \oplus x_2 \end{bmatrix} \oplus \begin{bmatrix} 0 \\ 0 \end{bmatrix}$	$F_5^d = \begin{bmatrix} x_1 \oplus x_2 \\ x_1 \end{bmatrix} \oplus \begin{bmatrix} 0 \\ 0 \end{bmatrix}$	$F_{17}^k = \begin{bmatrix} x_2 \\ x_1 \oplus x_2 \end{bmatrix} \oplus \begin{bmatrix} 1 \\ 0 \end{bmatrix}$	$F_{17}^d = \begin{bmatrix} x_1 \oplus x_2 \\ x_1 \end{bmatrix} \oplus \begin{bmatrix} 1 \\ 1 \end{bmatrix}$
$F_6^k = \begin{bmatrix} x_1 \oplus x_2 \\ x_1 \end{bmatrix} \oplus \begin{bmatrix} 0 \\ 0 \end{bmatrix}$	$F_6^d = \begin{bmatrix} x_2 \\ x_1 \oplus x_2 \end{bmatrix} \oplus \begin{bmatrix} 0 \\ 0 \end{bmatrix}$	$F_{18}^k = \begin{bmatrix} x_1 \oplus x_2 \\ x_1 \end{bmatrix} \oplus \begin{bmatrix} 1 \\ 0 \end{bmatrix}$	$F_{18}^d = \begin{bmatrix} x_2 \\ x_1 \oplus x_2 \end{bmatrix} \oplus \begin{bmatrix} 0 \\ 1 \end{bmatrix}$
$F_7^k = \begin{bmatrix} x_1 \\ x_2 \end{bmatrix} \oplus \begin{bmatrix} 0 \\ 1 \end{bmatrix}$	$F_7^d = \begin{bmatrix} x_1 \\ x_2 \end{bmatrix} \oplus \begin{bmatrix} 0 \\ 1 \end{bmatrix}$	$F_{19}^k = \begin{bmatrix} x_1 \\ x_2 \end{bmatrix} \oplus \begin{bmatrix} 1 \\ 1 \end{bmatrix}$	$F_{19}^d = \begin{bmatrix} x_1 \\ x_2 \end{bmatrix} \oplus \begin{bmatrix} 1 \\ 1 \end{bmatrix}$
$F_8^k = \begin{bmatrix} x_1 \oplus x_2 \\ x_2 \end{bmatrix} \oplus \begin{bmatrix} 0 \\ 1 \end{bmatrix}$	$F_8^d = \begin{bmatrix} x_2 \\ x_1 \oplus x_2 \end{bmatrix} \oplus \begin{bmatrix} 1 \\ 1 \end{bmatrix}$	$F_{20}^k = \begin{bmatrix} x_1 \oplus x_2 \\ x_2 \end{bmatrix} \oplus \begin{bmatrix} 1 \\ 1 \end{bmatrix}$	$F_{20}^d = \begin{bmatrix} x_1 \oplus x_2 \\ x_2 \end{bmatrix} \oplus \begin{bmatrix} 0 \\ 1 \end{bmatrix}$
$F_9^k = \begin{bmatrix} x_1 \\ x_1 \oplus x_2 \end{bmatrix} \oplus \begin{bmatrix} 0 \\ 1 \end{bmatrix}$	$F_9^d = \begin{bmatrix} x_1 \\ x_1 \oplus x_2 \end{bmatrix} \oplus \begin{bmatrix} 0 \\ 1 \end{bmatrix}$	$F_{21}^k = \begin{bmatrix} x_1 \\ x_1 \oplus x_2 \end{bmatrix} \oplus \begin{bmatrix} 1 \\ 1 \end{bmatrix}$	$F_{21}^d = \begin{bmatrix} x_1 \\ x_1 \oplus x_2 \end{bmatrix} \oplus \begin{bmatrix} 1 \\ 0 \end{bmatrix}$
$F_{10}^k = \begin{bmatrix} x_2 \\ x_1 \end{bmatrix} \oplus \begin{bmatrix} 0 \\ 1 \end{bmatrix}$	$F_{10}^d = \begin{bmatrix} x_2 \\ x_1 \end{bmatrix} \oplus \begin{bmatrix} 1 \\ 0 \end{bmatrix}$	$F_{22}^k = \begin{bmatrix} x_2 \\ x_1 \end{bmatrix} \oplus \begin{bmatrix} 1 \\ 1 \end{bmatrix}$	$F_{22}^d = \begin{bmatrix} x_2 \\ x_1 \end{bmatrix} \oplus \begin{bmatrix} 1 \\ 1 \end{bmatrix}$
$F_{11}^k = \begin{bmatrix} x_2 \\ x_1 \oplus x_2 \end{bmatrix} \oplus \begin{bmatrix} 0 \\ 1 \end{bmatrix}$	$F_{11}^d = \begin{bmatrix} x_1 \oplus x_2 \\ x_1 \end{bmatrix} \oplus \begin{bmatrix} 1 \\ 0 \end{bmatrix}$	$F_{23}^k = \begin{bmatrix} x_2 \\ x_1 \oplus x_2 \end{bmatrix} \oplus \begin{bmatrix} 1 \\ 1 \end{bmatrix}$	$F_{23}^d = \begin{bmatrix} x_1 \oplus x_2 \\ x_1 \end{bmatrix} \oplus \begin{bmatrix} 0 \\ 1 \end{bmatrix}$
$F_{12}^k = \begin{bmatrix} x_1 \oplus x_2 \\ x_1 \end{bmatrix} \oplus \begin{bmatrix} 0 \\ 1 \end{bmatrix}$	$F_{12}^d = \begin{bmatrix} x_1 \oplus x_2 \\ x_2 \end{bmatrix} \oplus \begin{bmatrix} 1 \\ 1 \end{bmatrix}$	$F_{24}^k = \begin{bmatrix} x_1 \oplus x_2 \\ x_1 \end{bmatrix} \oplus \begin{bmatrix} 1 \\ 1 \end{bmatrix}$	$F_{24}^d = \begin{bmatrix} x_2 \\ x_1 \oplus x_2 \end{bmatrix} \oplus \begin{bmatrix} 1 \\ 0 \end{bmatrix}$

В результаті проведеного експерименту отримано 96 двохрозрядних двохоперандних операцій криптографічного перетворення, які представлено в табл. 1.2. В подальших дослідженнях серед цих операцій було виділено три математичні групи перестановки [100]. Проте з’ясуванню математичної сутності операцій та розробленню методів їхнього синтезу уваги не приділяли.

Таблиця 1.2

Результати моделювання двохоперандних операцій криптографічного перетворення

Моделі двохоперандних операцій							
$O_{1,7,13,19}$	$O_{13,19,1,7}$	$O_{1,8,13,20}$	$O_{13,20,1,8}$	$O_{1,10,16,19}$	$O_{16,1,19,10}$	$O_{1,7,15,21}$	$O_{15,21,7,1}$
$O_{7,1,19,13}$	$O_{19,13,7,1}$	$O_{8,13,20,1}$	$O_{20,1,8,13}$	$O_{10,19,1,16}$	$O_{19,16,10,1}$	$O_{7,1,21,15}$	$O_{21,15,1,7}$
$O_{2,20,14,8}$	$O_{14,8,2,20}$	$O_{2,19,14,7}$	$O_{14,7,2,19}$	$O_{2,24,18,8}$	$O_{18,2,8,24}$	$O_{2,20,17,11}$	$O_{17,11,20,2}$
$O_{8,14,20,2}$	$O_{20,2,8,14}$	$O_{7,2,19,14}$	$O_{19,14,7,2}$	$O_{8,18,24,2}$	$O_{24,8,2,18}$	$O_{11,17,2,20}$	$O_{20,2,11,17}$
$O_{3,9,21,15}$	$O_{15,21,9,3}$	$O_{3,12,21,18}$	$O_{18,3,12,21}$	$O_{3,11,23,15}$	$O_{15,23,11,3}$	$O_{3,9,19,13}$	$O_{13,19,3,9}$
$O_{9,3,15,21}$	$O_{21,15,3,9}$	$O_{12,21,18,3}$	$O_{21,18,3,12}$	$O_{11,15,3,23}$	$O_{23,3,15,11}\cdot$	$O_{9,3,13,19}$	$O_{19,13,9,3}$
$O_{4,16,10,22}$	$O_{16,4,22,10}$	$O_{4,17,10,23}$	$O_{17,10,23,4}$	$O_{4,13,7,22}$	$O_{13,22,4,7}$	$O_{4,16,12,24}$	$O_{16,4,24,12}$
$O_{10,22,4,16}$	$O_{22,10,16,4}$	$O_{10,23,4,17}$	$O_{23,4,17,10}$	$O_{7,4,22,13}$	$O_{22,7,13,4}\cdot$	$O_{12,24,16,4}$	$O_{24,12,4,16}\cdot$
$O_{5,23,11,17}$	$O_{17,11,23,5}$	$O_{5,22,11,16}$	$O_{16,5,22,11}$	$O_{5,21,9,17}$	$O_{17,9,21,5}$	$O_{5,23,8,14}$	$O_{14,8,5,23}$
$O_{11,17,5,23}$	$O_{23,5,17,11}$	$O_{11,16,5,22}$	$O_{22,11,16,5}$	$O_{9,5,17,21}$	$O_{21,17,5,9}\cdot$	$O_{8,14,23,5}$	$O_{23,5,14,8}\cdot$
$O_{6,18,24,12}$	$O_{18,6,12,24}$	$O_{6,15,24,9}$	$O_{15,24,9,6}$	$O_{6,14,20,12}$	$O_{14,12,6,20}$	$O_{6,18,22,10}$	$O_{18,6,10,22}$
$O_{12,24,18,6}$	$O_{24,12,6,18}$	$O_{9,6,15,24}$	$O_{24,9,6,15}$	$O_{12,20,14,6}$	$O_{20,6,12,14}$	$O_{10,22,6,18}$	$O_{22,10,18,6}$

Одним з шляхів вирішення цих задач наразі є розширення кількості операцій, придатних для прямого та оберненого криптоперетворення інформації. Збільшення кількості операцій, придатних для криптоперетворення, їхнє застосування замість, наприклад, стандартної операції додавання за модулем, підвищує надійність та стійкість шифрування [35].

Щоб уникнути некоректності та помилок під час застосування нових операцій, їх потрібно детально досліджувати [35].

Також слід зазначити, що робота орієнтована на симетричне шифрування, так як в новітніх інформаційних системах для шифрування повідомлень, які передаються, використовуються найчастіше симетричні алгоритми шифрування, зважаючи на їх велику обчислювальну здатність (асиметричні алгоритми, здебільшого застосовують для генерації та поширення сеансових ключів) [101].

Основною метою дослідження є підвищення якості систем потокового шифрування конфіденційної інформації за рахунок збільшення стійкості та варіативності перетворення на основі додаткового використання груп двохоперандних двохрозрядних операцій, синтезованих на основі додавання за модулем два та чотири.

Для досягнення поставленої мети сформульовано і розв’язано такі задачі:

– розроблення методу побудови та дослідження двохоперандних операцій криптоперетворення;

– розроблення методів синтезу груп симетричних двохрозрядних двохоперандних операцій потокового шифрування;

– удосконалення методу підвищення стійкості та надійності потокового шифрування та оцінка його ефективності.

Висновки з розділу 1

1. Розглянуто сучасний стан та перспективи розвитку методів синтезу й аналізу операцій криптографічного перетворення для захисту конфіденційної інформації. Продемонстровано, що криптографія наразі залишається основним засобом захисту конфіденційної інформації в кіберпрсторі.

2. В процесі аналізу встановлено, що одним із перспективних напрямів розвитку систем криптографічного захисту інформації є використання операцій криптографічного перетворення на основі логічних функцій. Розглянуто сучасний стан досліджень операцій криптографічного перетворення інформації з виділенням особливостей застосування в потоковому та блочному шифруваннях. Наведено результати бібліографічного пошуку та огляду основних результатів досліджень, пов’язаних з синтезом та аналізом операцій криптографічного перетворення інформації.

3. Встановлено що двохоперандним операціям криптографічного перетворення інформації, спеціалізованим для потокового шифрування не приділялось достатньої уваги. Наведено теоретичні передумови та результати

проведення обчислювального експерименту, в результаті якого на основі перебору розраховано повну множину таблиць істинності симетричних двохрозрядних двохоперандних операцій криптоперетворення. Наведено результати дослідження цих операцій.

4. На основі проведеного аналізу сформульовано мету й задачі наукового дослідження.

РОЗДІЛ 2 МОДЕЛЮВАННЯ ТА ДОСЛІДЖЕННЯ ДВОХОПЕРАНДНИХ ОПЕРАЦІЙ КРИПТОГРАФІЧНОГО ПЕРЕТВОРЕННЯ ІНФОРМАЦІЇ

2.1 Метод дослідження двохоперандних операцій криптоперетворення

2.1.1 Класифікація таблиць істинності симетричних двохрозрядних двохоперандних операцій криптоперетворення

Операції криптографічного перетворення інформації по аналогії з командами, які реалізуються в комп'ютерних системах, класифікуються за кількістю операндів на одноопераднi, двохоперандні та багатоопераднi [10,12].

Одноопераднi операції криптографічного перетворення застосовуються в блокових шифрах. Двохоперандні операції застосовуються в блокових та потокових шифрах. Основною областю застосування багатоопераднi операцій є багатомірні примітиви блокового шифрування.

Найбільш універсальними операціями криптоперетворення, виходячи з наведеної класифікації, є двохоперандні операції, яким, на жаль, не приділено належної уваги [1].

Синтез двохоперандних операцій криптоперетворення може розвиватися за двома основними напрямами:

– модифікації операцій додавання за модулем на основі перестановок операндів і результатів виконання операцій [81-83];

– моделювання двохоперандних операцій криптоперетворення на основі одноопераднi [41-44].

Розглянемо більш детально модифікації операцій додавання за модулем два. Операцію двохрозрядного криптографічного додавання за модулем два можна представити як:

$$O_{\mathrm{mod}\,2} = \begin{vmatrix} x_{1.1} \oplus x_{2.1} \\ x_{1.2} \oplus x_{2.2} \end{vmatrix}, \qquad (2.1)$$

де $x_{i.j} \in \{0,1\}$ – операнд, $i \in \{1,2\}$ – номер операнда, $j \in \{1,2\}$ – номер розряду операнда, $\oplus$ – операція додавання за модулем два.

Виходячи з наведеної моделі (2.1), побудовано групу аналогічних операцій з точністю до перестановки [86], наведену в табл.2.1.

Таблиця 2.1

Група операцій додавання за модулем два з точністю до перестановки

$O^{\oplus}_{1.1} = \begin{vmatrix} x_{1.1} \oplus x_{2.1} \\ x_{1.2} \oplus x_{2.2} \end{vmatrix}$	$O^{\oplus}_{2.1} = \begin{vmatrix} x_{1.1} \oplus x_{2.2} \\ x_{1.2} \oplus x_{2.1} \end{vmatrix}$	$O^{\oplus}_{3.1} = \begin{vmatrix} x_{1.2} \oplus x_{2.1} \\ x_{1.1} \oplus x_{2.2} \end{vmatrix}$
$O^{\oplus}_{1.2} = \begin{vmatrix} x_{1.1} \oplus x_{2.1} \\ x_{1.2} \oplus x_{2.2} \oplus 1 \end{vmatrix}$	$O^{\oplus}_{2.2} = \begin{vmatrix} x_{1.1} \oplus x_{2.2} \\ x_{1.2} \oplus x_{2.1} \oplus 1 \end{vmatrix}$	$O^{\oplus}_{3.2} = \begin{vmatrix} x_{1.2} \oplus x_{2.1} \\ x_{1.1} \oplus x_{2.2} \oplus 1 \end{vmatrix}$
$O^{\oplus}_{1.3} = \begin{vmatrix} x_{1.1} \oplus x_{2.1} \oplus 1 \\ x_{1.2} \oplus x_{2.2} \end{vmatrix}$	$O^{\oplus}_{2.3} = \begin{vmatrix} x_{1.1} \oplus x_{2.2} \oplus 1 \\ x_{1.2} \oplus x_{2.1} \end{vmatrix}$	$O^{\oplus}_{3.3} = \begin{vmatrix} x_{1.2} \oplus x_{2.1} \oplus 1 \\ x_{1.1} \oplus x_{2.2} \end{vmatrix}$
$O^{\oplus}_{1.4} = \begin{vmatrix} x_{1.1} \oplus x_{2.1} \oplus 1 \\ x_{1.2} \oplus x_{2.2} \oplus 1 \end{vmatrix}$	$O^{\oplus}_{2.4} = \begin{vmatrix} x_{1.1} \oplus x_{2.2} \oplus 1 \\ x_{1.2} \oplus x_{2.1} \oplus 1 \end{vmatrix}$	$O^{\oplus}_{3.4} = \begin{vmatrix} x_{1.2} \oplus x_{2.1} \oplus 1 \\ x_{1.1} \oplus x_{2.2} \oplus 1 \end{vmatrix}$

В роботах [35,86] доведено, що застосування цих операцій в потокових шифрах забезпечує підвищення стійкості й надійності шифрування.

Розглянемо більш детально моделювання двохоперандних операцій криптографічного перетворення на основі одноопераднних.

Для того, щоб двохоперандна операція @, яка моделюється, могла бути використана в криптоперетвореннях, вона повинна мати такі властивості [100]: $x_1 @ x_2 = y$; $x_2 @ x_1 = y$; $x_1 @ y = x_2$; $y @ x_1 = x_2$; $x_2 @ y = x_1$; $y @ x_2 = x_1$.

Щоб операція відповідала цим властивостям, її табличне передставлення має відповідати умовам, доведеним в [102]:

1. кожен стовпець і рядок таблиці табличного представлення мають включати повну множину вхідних/вихідних значень;

2. таблиця представлення операції має бути симетрична відносно головної діагоналі, тобто має виконуватися рівність $A[i,j] = A[j,i]$.

Результати обчислювального експерименту по моделюванню двохоперандних операцій криптографічного перетворення на основі двохрозрядних операцій криптоперетворення, наведені в табл. 1.1, опубліковано в [88].

В процесі дослідження синтезованих 96 операцій, було виділено 3 математичні групи по 24 операції [88]. Останні 24 операції, які не ввійшли до виділених математичних груп, були об'єднані в 4-ту групу операцій. Результати цього дослідження наведені в табл.2.2.

Таблиця 2.2

Результати моделювання операцій над двома операндами

Група операцій 1		**Група операцій 2**		**Група операцій 3**		**Група операцій 4**	
№ НДО	**операція**	**№ НДО**	**операція**	**№ НДО**	**операція**	**№ НДО**	**операція**
1	**2**	**3**	**4**	**5**	**6**	**7**	**8**
1	$O_{1,7,13,19}$, $O_{7,1,19,13}$, $O_{13,19,1,7}$, $O_{19,13,7,1}$.	**7**	$O_{1,8,13,20}$, $O_{8,13,20,1}$, $O_{13,20,1,8}$, $O_{20,1,8,13}$.	**13**	$O_{1,10,16,19}$, $O_{10,19,1,16}$, $O_{16,1,19,10}$, $O_{19,16,10,1}$.	**19**	$O_{1,7,15,21}$, $O_{7,1,21,15}$, $O_{15,21,7,1}$, $O_{21,15,1,7}$.
2	$O_{2,20,14,8}$, $O_{8,14,20,2}$, $O_{14,8,2,20}$, $O_{20,2,8,14}$.	**8**	$O_{2,19,14,7}$, $O_{7,2,19,14}$, $O_{14,7,2,19}$, $O_{19,14,7,2}$.	**14**	$O_{2,24,18,8}$, $O_{8,18,24,2}$, $O_{18,2,8,24}$, $O_{24,8,2,18}$.	**20**	$O_{2,20,17,11}$, $O_{11,17,2,20}$, $O_{17,11,20,2}$, $O_{20,2,11,17}$
3	$O_{3,9,21,15}$, $O_{9,3,15,21}$, $O_{15,21,9,3}$, $O_{21,15,3,9}$.	**9**	$O_{3,12,21,18}$, $O_{12,21,18,3}$, $O_{18,3,12,21}$, $O_{21,18,3,12}$.	**15**	$O_{3,11,23,15}$, $O_{11,15,3,23}$, $O_{15,23,11,3}$, $O_{23,3,15,11}$.	**21**	$O_{3,9,19,13}$, $O_{9,3,13,19}$, $O_{13,19,3,9}$, $O_{19,13,9,3}$.

Продовження таблиці 2.2

1	2	3	4	5	6	7	8
4	$O_{4,16,10,22}$, $O_{10,22,4,16}$, $O_{16,4,22,10}$, $O_{22,10,16,4}$.	**10**	$O_{4,17,10,23}$, $O_{10,23,4,17}$, $O_{17,10,23,4}$, $O_{23,4,17,10}$.	**16**	$O_{4,13,7,22}$, $O_{7,4,22,13}$, $O_{13,22,4,7}$, $O_{22,7,13,4}$.	**22**	$O_{4,16,12,24}$, $O_{12,24,16,4}$, $O_{16,4,24,12}$, $O_{24,12,4,16}$.
5	$O_{5,23,11,17}$, $O_{11,17,5,23}$, $O_{17,11,23,5}$, $O_{23,5,17,11}$.	**11**	$O_{5,22,11,16}$, $O_{11,16,5,22}$, $O_{16,5,22,11}$, $O_{22,11,16,5}$.	**17**	$O_{5,21,9,17}$, $O_{9,5,17,21}$, $O_{17,9,21,5}$, $O_{21,17,5,9}$.	**23**	$O_{5,23,8,14}$, $O_{8,14,23,5}$, $O_{14,8,5,23}$, $O_{23,5,14,8}$.
6	$O_{6,18,24,12}$, $O_{12,24,18,6}$, $O_{18,6,12,24}$, $O_{24,12,6,18}$.	**12**	$O_{6,15,24,9}$, $O_{9,6,15,24}$, $O_{15,24,9,6}$, $O_{24,9,6,15}$.	**18**	$O_{6,14,20,12}$, $O_{12,20,14,6}$, $O_{14,12,6,20}$, $O_{20,6,12,14}$.	**24**	$O_{6,18,22,10}$, $O_{10,22,6,18}$, $O_{18,6,10,22}$, $O_{22,10,18,6}$.

Наведені в табл. 2.3 операції були розбиті на 24 набори двохоперандних операцій (НДО), по чотири операції в кожному наборі. Всім наборам двохоперандних операцій був присвоєний порядковий номер.

Встановлено, що поєднання одноопераднних операцій крипторперетворення в двохоперандні забезпечує збільшення невизначеності результатів потокового шифрування та збільшення варіативності алгоритму перетворення порівняно з операціями, синтезованими на основі додавання за модулем два з точністю до перестановки. Цей висновок ґрунтується на тому, що під час поєднання одноопераднних операцій крипторперетворення в двохоперандні отримано 96-ть симетричних операцій порівняно з 12-ма операціями, побудованими на основі додавання за модулем два з точністю до перестановки [1].

2.1.2 Дослідження набору двохоперандних операцій криптоперетворення

Розглянемо перший набір двохоперандних операцій, наведений в табл.2.2. Цей набір включає в себе операції: $O_{1,7,13,19}$, $O_{7,1,19,13}$, $O_{13,19,1,7}$, $O_{19,13,7,1}$. Умовно будемо вважати операцію $O_{1,7,13,19}$ основною, так як вона представлена першою в цьому наборі.

Для подальшого дослідження цього НДО розглянемо табличну форму цих операцій, наведену в табл. 2.3.

Таблиця 2.3

Перший набір двохоперандних операцій порозрядного додавання за модулем два

Операція	$O_{1,7,13,19}$				$O_{7,1,19,13}$				$O_{13,19,1,7}$				$O_{19,13,7,1}$			
Значення операндів	**0**	**1**	**2**	**3**	**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	3	2	1	0
1	1	0	3	2	0	1	2	3	3	2	1	0	2	3	0	1
2	2	3	0	1	3	2	1	0	0	1	2	3	1	0	3	2
3	3	2	1	0	2	3	0	1	1	0	3	2	0	1	2	3
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**				**0=3, 1=2, 2=1, 3=0**			

Дослідимо можливість побудови математичних моделей НДО №1, по аналогії з дослідженнями моделей модифікацій операцій з точністю до перестановки, наведеними в [35].

Математична модель основної операції першого набору двохоперандних операцій $O_{1,7,13,19}$ матиме вигляд [2]:

$$O_{1,7,13,19}=\begin{cases}\begin{bmatrix}x_1\\x_2\end{bmatrix}, \text{ якщо } k_1=0;\ k_2=0\\ \begin{bmatrix}x_1\\x_2\oplus 1\end{bmatrix}, \text{якщо } k_1=0;\ k_2=1\\ \begin{bmatrix}x_1\oplus 1\\x_2\end{bmatrix}, \text{ якщо } k_1=1;\ k_2=0\\ \begin{bmatrix}x_1\oplus 1\\x_2\oplus 1\end{bmatrix}, \text{якщо } k_1=1;\ k_2=1\end{cases}. \qquad (2.2)$$

Складність моделі двохоперандної операції (2.2) значно більша складності двохоперандних операцій, наведених в табл. 2.1.

Для встановлення сутності операції (2.2), її можна представити як:

$$O_{1,7,13,19}=\begin{cases}\begin{bmatrix}x_1\\x_2\end{bmatrix}, \text{ якщо } k_1=0;\ k_2=0\\ \begin{bmatrix}x_1\\x_2\oplus 1\end{bmatrix}, \text{якщо } k_1=0;\ k_2=1\\ \begin{bmatrix}x_1\oplus 1\\x_2\end{bmatrix}, \text{ якщо } k_1=1;\ k_2=0\\ \begin{bmatrix}x_1\oplus 1\\x_2\oplus 1\end{bmatrix}, \text{якщо } k_1=1;\ k_2=1\end{cases}=\begin{cases}\begin{bmatrix}x_1\\x_2\end{bmatrix}=\begin{bmatrix}x_1\oplus k_1\\x_2\oplus k_2\end{bmatrix}, \text{ якщо } k_1=0;\ k_2=0\\ \begin{bmatrix}x_1\\x_2\oplus 1\end{bmatrix}=\begin{bmatrix}x_1\oplus k_1\\x_2\oplus k_2\end{bmatrix}, \text{якщо } k_1=0;\ k_2=1\\ \begin{bmatrix}x_1\oplus 1\\x_2\end{bmatrix}=\begin{bmatrix}x_1\oplus k_1\\x_2\oplus k_2\end{bmatrix}, \text{ якщо } k_1=1;\ k_2=0\\ \begin{bmatrix}x_1\oplus 1\\x_2\oplus 1\end{bmatrix}=\begin{bmatrix}x_1\oplus k_1\\x_2\oplus k_2\end{bmatrix}, \text{якщо } k_1=1;\ k_2=1\end{cases}. \quad (2.3)$$

Таким чином, операцію $O_{1,7,13,19}$, представлену виразом (2.2), можна записати як:

$$O_{1,7,13,19}=\begin{cases}\begin{bmatrix}x_1\\x_2\end{bmatrix}=\begin{bmatrix}x_1\oplus k_1\\x_2\oplus k_2\end{bmatrix}, \text{ якщо } k_1=0;\ k_2=0\\ \begin{bmatrix}x_1\\x_2\oplus 1\end{bmatrix}=\begin{bmatrix}x_1\oplus k_1\\x_2\oplus k_2\end{bmatrix}, \text{якщо } k_1=0;\ k_2=1\\ \begin{bmatrix}x_1\oplus 1\\x_2\end{bmatrix}=\begin{bmatrix}x_1\oplus k_1\\x_2\oplus k_2\end{bmatrix}, \text{ якщо } k_1=1;\ k_2=0\\ \begin{bmatrix}x_1\oplus 1\\x_2\oplus 1\end{bmatrix}=\begin{bmatrix}x_1\oplus k_1\\x_2\oplus k_2\end{bmatrix}, \text{якщо } k_1=1;\ k_2=1\end{cases}=\begin{bmatrix}x_1\oplus k_1\\x_2\oplus k_2\end{bmatrix} \quad (2.4)$$

Виходячи з виразу (2.4), операцію (2.2) можна представити таким чином:

$$O_{1,7,13,19}=\begin{bmatrix}x_1\oplus k_1\\x_2\oplus k_2\end{bmatrix} \quad (2.5)$$

За аналогією з побудовою математичної моделі основної операції першого набору двохоперандних операцій $O_{1,7,13,19}$ дослідимо можливість побудови інших двохоперандних операцій цього набору.

Математична модель операції $O_{7,1,19,13}$, що є синтезованою на основі моделі основної операції $O_{1,7,13,19}$ першого набору двохоперандних операцій, представляється у вигляді:

$$O_{7,1,19,13}=\begin{cases}\begin{bmatrix}x_1\\ x_2\oplus 1\end{bmatrix}, \text{ якщо } k_1=0;\ k_2=0\\ \begin{bmatrix}x_1\\ x_2\end{bmatrix}, \text{якщо } k_1=0;\ k_2=1\\ \begin{bmatrix}x_1\oplus 1\\ x_2\oplus 1\end{bmatrix}, \text{ якщо } k_1=1;\ k_2=0\\ \begin{bmatrix}x_1\oplus 1\\ x_2\end{bmatrix}, \text{якщо } k_1=1;\ k_2=1\end{cases}. \quad (2.6)$$

Цю операцію (2.6), можна представити у вигляді, що розкриває її сутність, а саме:

$$O_{7,1,19,13}=\begin{cases}\begin{bmatrix}x_1\\ x_2\oplus 1\end{bmatrix}, \text{ якщо } k_1=0;\ k_2=0\\ \begin{bmatrix}x_1\\ x_2\end{bmatrix}, \text{якщо } k_1=0;\ k_2=1\\ \begin{bmatrix}x_1\oplus 1\\ x_2\oplus 1\end{bmatrix}, \text{ якщо } k_1=1;\ k_2=0\\ \begin{bmatrix}x_1\oplus 1\\ x_2\end{bmatrix}, \text{якщо } k_1=1;\ k_2=1\end{cases}=\begin{cases}\begin{bmatrix}x_1\\ x_2\oplus 1\end{bmatrix}=\begin{bmatrix}x_1\oplus k_1\\ x_2\oplus k_2\oplus 1\end{bmatrix}, \text{ якщо } k_1=0;\ k_2=0\\ \begin{bmatrix}x_1\\ x_2\end{bmatrix}=\begin{bmatrix}x_1\oplus k_1\\ x_2\oplus k_2\oplus 1\end{bmatrix}, \text{якщо } k_1=0;\ k_2=1\\ \begin{bmatrix}x_1\oplus 1\\ x_2\oplus 1\end{bmatrix}=\begin{bmatrix}x_1\oplus k_1\\ x_2\oplus k_2\oplus 1\end{bmatrix}, \text{ якщо } k_1=1;\ k_2=0\\ \begin{bmatrix}x_1\oplus 1\\ x_2\end{bmatrix}=\begin{bmatrix}x_1\oplus k_1\\ x_2\oplus k_2\oplus 1\end{bmatrix}, \text{якщо } k_1=1;\ k_2=1\end{cases}. \quad (2.7)$$

Отже, операцію $O_{7,1,19,13}$, представлену виразом (2.6), можна записати як:

$$O_{7,1,19,13}=\begin{cases}\begin{bmatrix}x_1\\ x_2\oplus 1\end{bmatrix}=\begin{bmatrix}x_1\oplus k_1\\ x_2\oplus k_2\oplus 1\end{bmatrix}, \text{ якщо } k_1=0;\ k_2=0\\ \begin{bmatrix}x_1\\ x_2\end{bmatrix}=\begin{bmatrix}x_1\oplus k_1\\ x_2\oplus k_2\oplus 1\end{bmatrix}, \text{якщо } k_1=0;\ k_2=1\\ \begin{bmatrix}x_1\oplus 1\\ x_2\oplus 1\end{bmatrix}=\begin{bmatrix}x_1\oplus k_1\\ x_2\oplus k_2\oplus 1\end{bmatrix}, \text{ якщо } k_1=1;\ k_2=0\\ \begin{bmatrix}x_1\oplus 1\\ x_2\end{bmatrix}=\begin{bmatrix}x_1\oplus k_1\\ x_2\oplus k_2\oplus 1\end{bmatrix}, \text{якщо } k_1=1;\ k_2=1\end{cases}=\begin{bmatrix}x_1\oplus k_1\\ x_2\oplus k_2\oplus 1\end{bmatrix}. \quad (2.8)$$

Керуючись виразом (2.8), операцію (2.6) можна представити таким чином:

$$O_{7,1,19,13}=\begin{bmatrix} x_1 \oplus k_1 \\ x_2 \oplus k_2 \oplus 1 \end{bmatrix} \tag{2.9}$$

Перестановочна схема побудови цієї операції представлена на рис.2.1.

Схематичне представлення основної операції НДО 1	Перестановочна схема	Схематичне представлення отриманої операції $O_{7,1,19,13}$
		

Рис. 2.1 Перестановочна схема для побудови операції $O_{7,1,19,13}$ на основі основної операції першого НДО $O_{1,7,13,19}$

Математична модель операції $O_{13,19,1,7}$, шо є синтезованою на основі моделі основної операції $O_{1,7,13,19}$ першого набору двохоперандних операцій, матиме вигляд:

$$O_{13,19,1,7}=\begin{cases} \begin{bmatrix} x_1 \oplus 1 \\ x_2 \end{bmatrix}, \ якщо\ k_1=0;\ k_2=0 \\ \begin{bmatrix} x_1 \oplus 1 \\ x_2 \oplus 1 \end{bmatrix}, якщо\ k_1=0;\ k_2=1 \\ \begin{bmatrix} x_1 \\ x_2 \end{bmatrix}, \ якщо\ k_1=1;\ k_2=0 \\ \begin{bmatrix} x_1 \\ x_2 \oplus 1 \end{bmatrix}, якщо\ k_1=1;\ k_2=1 \end{cases} \tag{2.10}$$

Для встановлення сутності операції $O_{13,19,1,7}$, її можна представити як:

$$O_{13,19,1,7}=\begin{cases} \begin{bmatrix} x_1 \oplus 1 \\ x_2 \end{bmatrix}, \ якщо\ k_1=0;\ k_2=0 \\ \begin{bmatrix} x_1 \oplus 1 \\ x_2 \oplus 1 \end{bmatrix}, якщо\ k_1=0;\ k_2=1 \\ \begin{bmatrix} x_1 \\ x_2 \end{bmatrix}, \ якщо\ k_1=1;\ k_2=0 \\ \begin{bmatrix} x_1 \\ x_2 \oplus 1 \end{bmatrix}, якщо\ k_1=1;\ k_2=1 \end{cases} = \begin{cases} \begin{bmatrix} x_1 \oplus 1 \\ x_2 \end{bmatrix} = \begin{bmatrix} x_1 \oplus k_1 \oplus 1 \\ x_2 \oplus k_2 \end{bmatrix}, \ якщо\ k_1=0;\ k_2=0 \\ \begin{bmatrix} x_1 \oplus 1 \\ x_2 \oplus 1 \end{bmatrix} = \begin{bmatrix} x_1 \oplus k_1 \oplus 1 \\ x_2 \oplus k_2 \end{bmatrix}, якщо\ k_1=0;\ k_2=1 \\ \begin{bmatrix} x_1 \\ x_2 \end{bmatrix} = \begin{bmatrix} x_1 \oplus k_1 \oplus 1 \\ x_2 \oplus k_2 \end{bmatrix}, \ якщо\ k_1=1;\ k_2=0 \\ \begin{bmatrix} x_1 \\ x_2 \oplus 1 \end{bmatrix} = \begin{bmatrix} x_1 \oplus k_1 \oplus 1 \\ x_2 \oplus k_2 \end{bmatrix}, якщо\ k_1=1;\ k_2=1 \end{cases} \tag{2.11}$$

Відповідно, операцію (2.10) можна записати як:

$$O_{13,19,1,7} = \begin{cases} \begin{bmatrix} x_1 \oplus 1 \\ x_2 \end{bmatrix} = \begin{bmatrix} x_1 \oplus k_1 \oplus 1 \\ x_2 \oplus k_2 \end{bmatrix}, \text{ якщо } k_1 = 0;\ k_2 = 0 \\ \begin{bmatrix} x_1 \oplus 1 \\ x_2 \oplus 1 \end{bmatrix} = \begin{bmatrix} x_1 \oplus k_1 \oplus 1 \\ x_2 \oplus k_2 \end{bmatrix}, \text{якщо } k_1 = 0;\ k_2 = 1 \\ \begin{bmatrix} x_1 \\ x_2 \end{bmatrix} = \begin{bmatrix} x_1 \oplus k_1 \oplus 1 \\ x_2 \oplus k_2 \end{bmatrix}, \text{ якщо } k_1 = 1;\ k_2 = 0 \\ \begin{bmatrix} x_1 \\ x_2 \oplus 1 \end{bmatrix} = \begin{bmatrix} x_1 \oplus k_1 \oplus 1 \\ x_2 \oplus k_2 \end{bmatrix}, \text{якщо } k_1 = 1;\ k_2 = 1 \end{cases} = \begin{bmatrix} x_1 \oplus k_1 \oplus 1 \\ x_2 \oplus k_2 \end{bmatrix} \quad (2.12)$$

Керуючись виразом (2.12), операцію (2.10) можна представити таким чином:

$$O_{13,19,1,7} = \begin{bmatrix} x_1 \oplus k_1 \oplus 1 \\ x_2 \oplus k_2 \end{bmatrix} \quad (2.13)$$

Перестановочна схема побудови цієї операції представлена на рис.2.2.

Схематичне представлення основної операції НДО 1	Перестановочна схема	Схематичне представлення отриманої операції $O_{13,19,1,7}$
1 7 13 19	1 7 13 19	13 19 1 7

Рис. 2.2 Перестановочна схема для побудови операції $O_{13,19,1,7}$ на основі основної операції першого НДО $O_{1,7,13,19}$

Математичну модель операції $O_{19,13,7,1}$, що є синтезованою на основі моделі базової операції $O_{1,7,13,19}$ першого набору двохоперандних операцій, представлено у вигляді:

$$O_{19,13,7,1}=\begin{cases}\begin{bmatrix}x_1\oplus 1\\ x_2\oplus 1\end{bmatrix}, \text{ якщо } k_1=0;\ k_2=0\\ \begin{bmatrix}x_1\oplus 1\\ x_2\end{bmatrix}, \text{якщо } k_1=0;\ k_2=1\\ \begin{bmatrix}x_1\\ x_2\oplus 1\end{bmatrix}, \text{ якщо } k_1=1;\ k_2=0\\ \begin{bmatrix}x_1\\ x_2\end{bmatrix}, \text{якщо } k_1=1;\ k_2=1\end{cases} \tag{2.14}$$

Для встановлення сутності операції (2.2), її можна представити як:

$$O_{19,13,7,1}=\begin{cases}\begin{bmatrix}x_1\oplus 1\\ x_2\oplus 1\end{bmatrix}, \text{ якщо } k_1=0;\ k_2=0\\ \begin{bmatrix}x_1\oplus 1\\ x_2\end{bmatrix}, \text{якщо } k_1=0;\ k_2=1\\ \begin{bmatrix}x_1\\ x_2\oplus 1\end{bmatrix}, \text{ якщо } k_1=1;\ k_2=0\\ \begin{bmatrix}x_1\\ x_2\end{bmatrix}, \text{якщо } k_1=1;\ k_2=1\end{cases}=\begin{cases}\begin{bmatrix}x_1\oplus 1\\ x_2\oplus 1\end{bmatrix}=\begin{bmatrix}x_1\oplus k_1\oplus 1\\ x_2\oplus k_2\oplus 1\end{bmatrix}, \text{ якщо } k_1=0;\ k_2=0\\ \begin{bmatrix}x_1\oplus 1\\ x_2\end{bmatrix}=\begin{bmatrix}x_1\oplus k_1\oplus 1\\ x_2\oplus k_2\oplus 1\end{bmatrix}, \text{якщо } k_1=0;\ k_2=1\\ \begin{bmatrix}x_1\\ x_2\oplus 1\end{bmatrix}=\begin{bmatrix}x_1\oplus k_1\oplus 1\\ x_2\oplus k_2\oplus 1\end{bmatrix}, \text{ якщо } k_1=1;\ k_2=0\\ \begin{bmatrix}x_1\\ x_2\end{bmatrix}=\begin{bmatrix}x_1\oplus k_1\oplus 1\\ x_2\oplus k_2\oplus 1\end{bmatrix}, \text{якщо } k_1=1;\ k_2=1\end{cases} \tag{2.15}$$

Таким чином, операцію $O_{19,13,7,1}$ можна записати як:

$$O_{19,13,7,1}=\begin{cases}\begin{bmatrix}x_1\oplus 1\\ x_2\oplus 1\end{bmatrix}=\begin{bmatrix}x_1\oplus k_1\oplus 1\\ x_2\oplus k_2\oplus 1\end{bmatrix}, \text{ якщо } k_1=0;\ k_2=0\\ \begin{bmatrix}x_1\oplus 1\\ x_2\end{bmatrix}=\begin{bmatrix}x_1\oplus k_1\oplus 1\\ x_2\oplus k_2\oplus 1\end{bmatrix}, \text{якщо } k_1=0;\ k_2=1\\ \begin{bmatrix}x_1\\ x_2\oplus 1\end{bmatrix}=\begin{bmatrix}x_1\oplus k_1\oplus 1\\ x_2\oplus k_2\oplus 1\end{bmatrix}, \text{ якщо } k_1=1;\ k_2=0\\ \begin{bmatrix}x_1\\ x_2\end{bmatrix}=\begin{bmatrix}x_1\oplus k_1\oplus 1\\ x_2\oplus k_2\oplus 1\end{bmatrix}, \text{якщо } k_1=1;\ k_2=1\end{cases}=\begin{bmatrix}x_1\oplus k_1\oplus 1\\ x_2\oplus k_2\oplus 1\end{bmatrix} \tag{2.16}$$

Керуючись виразом (2.16), операцію (2.14) можна представити таким чином:

$$O_{19,13,7,1}=\begin{bmatrix}x_1\oplus k_1\oplus 1\\ x_2\oplus k_2\oplus 1\end{bmatrix} \tag{2.17}$$

Перестановочна схема побудови цієї операції представлена на рис.2.3.

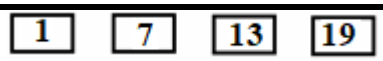
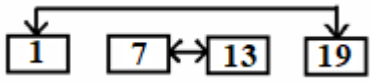
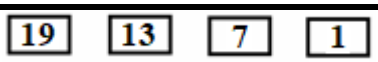
Схематичне представлення основної операції НДО 1	Перестановочна схема	Схематичне представлення отриманої операції $O_{19,13,7,1}$
		

Рис. 2.3 Перестановочна схема для побудови операції $O_{19,13,7,1}$ на основі основної операції першого НДО $O_{1,7,13,19}$

Послідовність перетворень моделі двохоперандної операції на основі поєднання одноопераднних операцій криптоперетворення при побудові узагальненої моделі двохоперандної операції меншої складності, та побудови перестановочних схем таблиці істинності для синтезу операцій з подібними властивостями можна розглядати як технологію дослідження двохоперандних операцій криптоперетворення [2].

2.2 Дослідження першої математичної групи двохоперандних операцій криптоперетворення

2.2.1 Дослідження другого набору двохоперандних операцій криптоперетворення першої математичної групи (НДО 2)

Розглянемо першу симетричну групу операцій. Ця група представлена такими наборами двохоперандних операцій як НДО 1, НДО 2, НДО 3, НДО 4, НДО 5 та НДО 6.

Розглянемо другий набір двохоперандних операцій.

Операція $O_{2,20,14,8}$ є першою в цьому наборі і умовно буде основною. На основі операції $O_{2,20,14,8}$ за рахунок перестановок будуються інші операції цього набору.

Розглянемо таблично формування операції другого набору операцій порозрядного додавання за модулем два із точністю до перестановки, що включає в себе операції: $O_{2,20,14,8}$, $O_{8,14,20,2}$, $O_{14,8,2,20}$, $O_{20,2,8,14}$.

Результати побудови даних операцій наведені в табл. 2.5.

Таблиця 2.5

Другий набір двохоперандних операцій порозрядного додавання за модулем два

Операція	$O_{2,20,14,8}$				$O_{8,14,20,2}$				$O_{14,8,2,20}$				$O_{20,2,8,14}$			
Значення операндів	**0**	**1**	**2**	**3**	**0**	**1**	**2**	**3**	**0**	**1**	**2**	**3**	**0**	**1**	**2**	**3**
0	0	3	2	1	1	2	3	0	2	1	0	3	3	0	1	2
1	3	0	1	2	2	1	0	3	1	2	3	0	0	3	2	1
2	2	1	0	3	3	0	1	2	0	3	2	1	1	2	3	0
3	1	2	3	0	0	3	2	1	3	0	1	2	2	1	0	3
Перестановка	**0=0, 1=3, 2=2, 3=1**				**0=1, 1=2, 2=3, 3=0**				**0=2, 1=1, 2=0, 3=3**				**0=3, 1=0, 2=1, 3=2**			

Розглянемо більш детально результати моделювання другого набору двохоперандних операцій, представивши їх математичними моделями.

Математична модель базової операції другого набору двохоперандних операцій $O_{2,20,14,8}$ матиме вигляд:

$$O_{2,20,14,8}=\begin{cases}\begin{bmatrix}x_1\oplus x_2\\ x_2\end{bmatrix}, \text{ якщо } k_1=0;\ k_2=0\\ \begin{bmatrix}x_1\oplus x_2\oplus 1\\ x_2\oplus 1\end{bmatrix}, \text{якщо } k_1=0;\ k_2=1\\ \begin{bmatrix}x_1\oplus x_2\oplus 1\\ x_2\end{bmatrix}, \text{ якщо } k_1=1;\ k_2=0\\ \begin{bmatrix}x_1\oplus x_2\\ x_2\oplus 1\end{bmatrix}, \text{якщо } k_1=1;\ k_2=1\end{cases}=\begin{cases}\begin{bmatrix}x_1\oplus x_2\\ x_2\end{bmatrix}=\begin{bmatrix}x_1\oplus x_2\oplus k_1\oplus k_2\\ x_2\oplus k_2\end{bmatrix}, \text{ якщо } k_1=0;\ k_2=0\\ \begin{bmatrix}x_1\oplus x_2\oplus 1\\ x_2\oplus 1\end{bmatrix}=\begin{bmatrix}x_1\oplus x_2\oplus k_1\oplus k_2\\ x_2\oplus k_2\end{bmatrix}, \text{якщо } k_1=0;\ k_2=1\\ \begin{bmatrix}x_1\oplus x_2\oplus 1\\ x_2\end{bmatrix}=\begin{bmatrix}x_1\oplus x_2\oplus k_1\oplus k_2\\ x_2\oplus k_2\end{bmatrix}, \text{ якщо } k_1=1;\ k_2=0\\ \begin{bmatrix}x_1\oplus x_2\\ x_2\oplus 1\end{bmatrix}=\begin{bmatrix}x_1\oplus x_2\oplus k_1\oplus k_2\\ x_2\oplus k_2\end{bmatrix}, \text{якщо } k_1=1;\ k_2=1\end{cases},$$

Отже, операцію $O_{2,20,14,8}$ можна записати як:

$$O_{2,20,14,8}=\begin{cases}\begin{bmatrix}x_1\oplus x_2\\ x_2\end{bmatrix}=\begin{bmatrix}x_1\oplus x_2\oplus k_1\oplus k_2\\ x_2\oplus k_2\end{bmatrix}, \text{ якщо } k_1=0;\ k_2=0\\ \begin{bmatrix}x_1\oplus x_2\oplus 1\\ x_2\oplus 1\end{bmatrix}=\begin{bmatrix}x_1\oplus x_2\oplus k_1\oplus k_2\\ x_2\oplus k_2\end{bmatrix}, \text{якщо } k_1=0;\ k_2=1\\ \begin{bmatrix}x_1\oplus x_2\oplus 1\\ x_2\end{bmatrix}=\begin{bmatrix}x_1\oplus x_2\oplus k_1\oplus k_2\\ x_2\oplus k_2\end{bmatrix}, \text{якщо } k_1=1;\ k_2=0\\ \begin{bmatrix}x_1\oplus x_2\\ x_2\oplus 1\end{bmatrix}=\begin{bmatrix}x_1\oplus x_2\oplus k_1\oplus k_2\\ x_2\oplus k_2\end{bmatrix}, \text{якщо } k_1=1;\ k_2=1\end{cases}=\begin{bmatrix}x_1\oplus x_2\oplus k_1\oplus k_2\\ x_2\oplus k_2\end{bmatrix}$$

Математичну модель операції $O_{8,14,20,2}$, що є синтезованою на основі моделі основної операції $O_{2,20,14,8}$ другого набору двохоперандних операцій, представлено у вигляді:

$$O_{8,14,20,2}=\begin{cases}\begin{bmatrix}x_1\oplus x_2\\ x_2\oplus 1\end{bmatrix}, \text{ якщо } k_1=0;\ k_2=0\\ \begin{bmatrix}x_1\oplus x_2\oplus 1\\ x_2\end{bmatrix}, \text{якщо } k_1=0;\ k_2=1\\ \begin{bmatrix}x_1\oplus x_2\oplus 1\\ x_2\oplus 1\end{bmatrix}, \text{ якщо } k_1=1;\ k_2=0\\ \begin{bmatrix}x_1\oplus x_2\\ x_2\end{bmatrix}, \text{якщо } k_1=1;\ k_2=1\end{cases}=\begin{cases}\begin{bmatrix}x_1\oplus x_2\\ x_2\oplus 1\end{bmatrix}=\begin{bmatrix}x_1\oplus x_2\oplus k_1\oplus k_2\\ x_2\oplus k_2\oplus 1\end{bmatrix}, \text{ якщо } k_1=0;\ k_2=0\\ \begin{bmatrix}x_1\oplus x_2\oplus 1\\ x_2\end{bmatrix}=\begin{bmatrix}x_1\oplus x_2\oplus k_1\oplus k_2\\ x_2\oplus k_2\oplus 1\end{bmatrix}, \text{якщо } k_1=0;\ k_2=1\\ \begin{bmatrix}x_1\oplus x_2\oplus 1\\ x_2\oplus 1\end{bmatrix}=\begin{bmatrix}x_1\oplus x_2\oplus k_1\oplus k_2\\ x_2\oplus k_2\oplus 1\end{bmatrix}, \text{ якщо } k_1=1;\ k_2=0\\ \begin{bmatrix}x_1\oplus x_2\\ x_2\end{bmatrix}=\begin{bmatrix}x_1\oplus x_2\oplus k_1\oplus k_2\\ x_2\oplus k_2\oplus 1\end{bmatrix}, \text{якщо } k_1=1;\ k_2=1\end{cases},$$

Таким чином, операцію $O_{8,14,20,2}$ можна записати як:

$$O_{8,14,20,2}=\begin{cases}\begin{bmatrix}x_1\oplus x_2\\ x_2\oplus 1\end{bmatrix}=\begin{bmatrix}x_1\oplus x_2\oplus k_1\oplus k_2\\ x_2\oplus k_2\oplus 1\end{bmatrix}, \text{ якщо } k_1=0;\ k_2=0\\ \begin{bmatrix}x_1\oplus x_2\oplus 1\\ x_2\end{bmatrix}=\begin{bmatrix}x_1\oplus x_2\oplus k_1\oplus k_2\\ x_2\oplus k_2\oplus 1\end{bmatrix}, \text{якщо } k_1=0;\ k_2=1\\ \begin{bmatrix}x_1\oplus x_2\oplus 1\\ x_2\oplus 1\end{bmatrix}=\begin{bmatrix}x_1\oplus x_2\oplus k_1\oplus k_2\\ x_2\oplus k_2\oplus 1\end{bmatrix}, \text{ якщо } k_1=1;\ k_2=0\\ \begin{bmatrix}x_1\oplus x_2\\ x_2\end{bmatrix}=\begin{bmatrix}x_1\oplus x_2\oplus k_1\oplus k_2\\ x_2\oplus k_2\oplus 1\end{bmatrix}, \text{якщо } k_1=1;\ k_2=1\end{cases}=\begin{bmatrix}x_1\oplus x_2\oplus k_1\oplus k_2\\ x_2\oplus k_2\oplus 1\end{bmatrix}$$

Перестановочна схема побудови цієї операції представлена на рис.2.4.

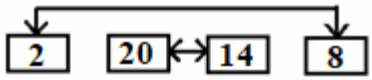
Схематичне представлення основної операції НДО 2	Перестановочна схема	Схематичне представлення отриманої операції $O_{8,14,20,2}$
		

Рис. 2.4 Перестановочна схема для побудови операції $O_{8,14,20,2}$ на основі основної операції другого НДО $O_{2,20,14,8}$

Математична модель операції $O_{14,8,2,20}$, шо є синтезованою на основі моделі операції $O_{2,20,14,8}$ другого набору двохоперандних операцій, матиме вигляд:

$$O_{14,8,2,20}=\begin{cases}\begin{bmatrix}x_1\oplus x_2\oplus 1\\ x_2\end{bmatrix}, \text{ якщо } k_1=0;\ k_2=0\\ \begin{bmatrix}x_1\oplus x_2\\ x_2\oplus 1\end{bmatrix}, \text{якщо } k_1=0;\ k_2=1\\ \begin{bmatrix}x_1\oplus x_2\\ x_2\end{bmatrix}, \text{ якщо } k_1=1;\ k_2=0\\ \begin{bmatrix}x_1\oplus x_2\oplus 1\\ x_2\oplus 1\end{bmatrix}, \text{якщо } k_1=1;\ k_2=1\end{cases}=\begin{cases}\begin{bmatrix}x_1\oplus x_2\oplus 1\\ x_2\end{bmatrix}=\begin{bmatrix}x_1\oplus x_2\oplus k_1\oplus k_2\oplus 1\\ x_2\oplus k_2\end{bmatrix}, \text{ якщо } k_1=0;\ k_2=0\\ \begin{bmatrix}x_1\oplus x_2\\ x_2\oplus 1\end{bmatrix}=\begin{bmatrix}x_1\oplus x_2\oplus k_1\oplus k_2\oplus 1\\ x_2\oplus k_2\end{bmatrix}, \text{якщо } k_1=0;\ k_2=1\\ \begin{bmatrix}x_1\oplus x_2\\ x_2\end{bmatrix}=\begin{bmatrix}x_1\oplus x_2\oplus k_1\oplus k_2\oplus 1\\ x_2\oplus k_2\end{bmatrix}, \text{ якщо } k_1=1;\ k_2=0\\ \begin{bmatrix}x_1\oplus x_2\oplus 1\\ x_2\oplus 1\end{bmatrix}=\begin{bmatrix}x_1\oplus x_2\oplus k_1\oplus k_2\oplus 1\\ x_2\oplus k_2\end{bmatrix}, \text{якщо } k_1=1;\ k_2=1\end{cases},$$

Відповідно, операцію $O_{14,8,2,20}$ можна записати як:

$$O_{14,8,2,20}=\begin{cases}\begin{bmatrix}x_1\oplus x_2\oplus 1\\ x_2\end{bmatrix}=\begin{bmatrix}x_1\oplus x_2\oplus k_1\oplus k_2\oplus 1\\ x_2\oplus k_2\end{bmatrix}, \text{ якщо } k_1=0;\ k_2=0\\ \begin{bmatrix}x_1\oplus x_2\\ x_2\oplus 1\end{bmatrix}=\begin{bmatrix}x_1\oplus x_2\oplus k_1\oplus k_2\oplus 1\\ x_2\oplus k_2\end{bmatrix}, \text{якщо } k_1=0;\ k_2=1\\ \begin{bmatrix}x_1\oplus x_2\\ x_2\end{bmatrix}=\begin{bmatrix}x_1\oplus x_2\oplus k_1\oplus k_2\oplus 1\\ x_2\oplus k_2\end{bmatrix}, \text{ якщо } k_1=1;\ k_2=0\\ \begin{bmatrix}x_1\oplus x_2\oplus 1\\ x_2\oplus 1\end{bmatrix}=\begin{bmatrix}x_1\oplus x_2\oplus k_1\oplus k_2\oplus 1\\ x_2\oplus k_2\end{bmatrix}, \text{якщо } k_1=1;\ k_2=1\end{cases}=\begin{bmatrix}x_1\oplus x_2\oplus k_1\oplus k_2\oplus 1\\ x_2\oplus k_2\end{bmatrix}$$

Перестановочна схема побудови цієї операції представлена на рис.2.5.

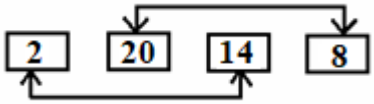
Схематичне представлення основної операції НДО 2	Перестановочна схема	Схематичне представлення отриманої операції $O_{14,8,2,20}$
		

Рис. 2.5 Перестановочна схема для побудови операції $O_{14,8,2,20}$ на основі основної операції другого НДО $O_{2,20,14,8}$

Математичну модель операції $O_{20,2,8,14}$, що є синтезованою на основі моделі основної операції $O_{2,20,14,8}$ другого набору двохоперандних операцій, представлено у вигляді:

$$O_{20,2,8,14}=\begin{cases}\begin{bmatrix}x_1\oplus x_2\oplus 1\\ x_2\oplus 1\end{bmatrix}, \text{ якщо } k_1=0;\ k_2=0\\ \begin{bmatrix}x_1\oplus x_2\\ x_2\end{bmatrix}, \text{якщо } k_1=0;\ k_2=1\\ \begin{bmatrix}x_1\oplus x_2\\ x_2\oplus 1\end{bmatrix}, \text{ якщо } k_1=1;\ k_2=0\\ \begin{bmatrix}x_1\oplus x_2\oplus 1\\ x_2\end{bmatrix}, \text{якщо } k_1=1;\ k_2=1\end{cases}=\begin{cases}\begin{bmatrix}x_1\oplus x_2\oplus 1\\ x_2\oplus 1\end{bmatrix}=\begin{bmatrix}x_1\oplus x_2\oplus k_1\oplus k_2\oplus 1\\ x_2\oplus k_2\oplus 1\end{bmatrix}, \text{ якщо } k_1=0;\ k_2=0\\ \begin{bmatrix}x_1\oplus x_2\\ x_2\end{bmatrix}=\begin{bmatrix}x_1\oplus x_2\oplus k_1\oplus k_2\oplus 1\\ x_2\oplus k_2\oplus 1\end{bmatrix}, \text{якщо } k_1=0;\ k_2=1\\ \begin{bmatrix}x_1\oplus x_2\\ x_2\oplus 1\end{bmatrix}=\begin{bmatrix}x_1\oplus x_2\oplus k_1\oplus k_2\oplus 1\\ x_2\oplus k_2\oplus 1\end{bmatrix}, \text{ якщо } k_1=1;\ k_2=0\\ \begin{bmatrix}x_1\oplus x_2\oplus 1\\ x_2\end{bmatrix}=\begin{bmatrix}x_1\oplus x_2\oplus k_1\oplus k_2\oplus 1\\ x_2\oplus k_2\oplus 1\end{bmatrix}, \text{якщо } k_1=1;\ k_2=1\end{cases}$$

Таким чином, операцію $O_{20,2,8,14}$ можна записати як:

$$O_{20,2,8,14}=\begin{cases}\begin{bmatrix}x_1\oplus x_2\oplus 1\\ x_2\oplus 1\end{bmatrix}=\begin{bmatrix}x_1\oplus x_2\oplus k_1\oplus k_2\oplus 1\\ x_2\oplus k_2\oplus 1\end{bmatrix}, \text{ якщо } k_1=0;\ k_2=0\\ \begin{bmatrix}x_1\oplus x_2\\ x_2\end{bmatrix}=\begin{bmatrix}x_1\oplus x_2\oplus k_1\oplus k_2\oplus 1\\ x_2\oplus k_2\oplus 1\end{bmatrix}, \text{якщо } k_1=0;\ k_2=1\\ \begin{bmatrix}x_1\oplus x_2\\ x_2\oplus 1\end{bmatrix}=\begin{bmatrix}x_1\oplus x_2\oplus k_1\oplus k_2\oplus 1\\ x_2\oplus k_2\oplus 1\end{bmatrix}, \text{ якщо } k_1=1;\ k_2=0\\ \begin{bmatrix}x_1\oplus x_2\oplus 1\\ x_2\end{bmatrix}=\begin{bmatrix}x_1\oplus x_2\oplus k_1\oplus k_2\oplus 1\\ x_2\oplus k_2\oplus 1\end{bmatrix}, \text{якщо } k_1=1;\ k_2=1\end{cases}=\begin{bmatrix}x_1\oplus x_2\oplus k_1\oplus k_2\oplus 1\\ x_2\oplus k_2\oplus 1\end{bmatrix}$$

Перестановочна схема побудови цієї операції представлена на рис.2.6.

Схематичне представлення основної операції НДО 2	Перестановочна схема	Схематичне представлення отриманої операції $O_{20,2,8,14}$
		

Рис. 2.6 Перестановочна схема для побудови операції $O_{20,2,8,14}$ на основі основної операції другого НДО $O_{2,20,14,8}$

Операції другого набору двохоперандних операцій порозрядного додавання за модулем два побудовано, перейдемо до дослідження третього набору двохоперандних операцій порозрядного додавання за модулем два.

2.2.2 Дослідження третього набору двохоперандних операцій криптоперетворення першої математичної групи (НДО 3)

Розглянемо третій набір двохоперандних операцій.

Операція $O_{3,9,21,15}$ є першою в цьому наборі і буде умовно основною. На основі операції $O_{3,9,21,15}$ за рахунок перестановок будуються інші операції цього набору.

Розглянемо таблично формування операції третього набору операцій порозрядного додавання за модулем два із точністю до перестановки, що включає в себе операції: $O_{3,9,21,15}$, $O_{9,3,15,21}$, $O_{15,21,9,3}$, $O_{21,15,3,9}$.

Результати побудови цих операцій наведені в табл. 2.6.

Таблиця 2.6

Третій набір двохоперандних операцій порозрядного додавання за модулем два

Операція	$O_{3,9,21,15}$				$O_{9,3,15,21}$				$O_{15,21,9,3}$				$O_{21,15,3,9}$			
Значення операндів	**0**	**1**	**2**	**3**	**0**	**1**	**2**	**3**	**0**	**1**	**2**	**3**	**0**	**1**	**2**	**3**
0	0	1	3	2	1	0	2	3	2	3	1	0	3	2	0	1
1	1	0	2	3	0	1	3	2	3	2	0	1	2	3	1	0
2	3	2	0	1	2	3	1	0	1	0	2	3	0	1	3	2
3	2	3	1	0	3	2	0	1	0	1	3	2	1	0	2	3
Перестановка	**0=0, 1=1, 2=3, 3=2**				**0=1, 1=0, 2=2, 3=3**				**0=2, 1=3, 2=1, 3=0**				**0=3, 1=2, 2=0, 3=1**			

Розглянемо більш детально результати моделювання третього набору двохоперандних операцій, представивши їх математичними моделями.

Математична модель основної операції третього набору двохоперандних операцій $O_{3,9,21,15}$ матиме вигляд:

$$O_{3,9,21,15}=\begin{cases}\begin{bmatrix}x_1\\ x_1\oplus x_2\end{bmatrix}, \text{ якщо } k_1=0;\ k_2=0\\ \begin{bmatrix}x_1\\ x_1\oplus x_2\oplus 1\end{bmatrix}, \text{якщо } k_1=0;\ k_2=1\\ \begin{bmatrix}x_1\oplus 1\\ x_1\oplus x_2\oplus 1\end{bmatrix}, \text{ якщо } k_1=1;\ k_2=0\\ \begin{bmatrix}x_1\oplus 1\\ x_1\oplus x_2\end{bmatrix}, \text{якщо } k_1=1;\ k_2=1\end{cases}=\begin{cases}\begin{bmatrix}x_1\\ x_1\oplus x_2\end{bmatrix}=\begin{bmatrix}x_1\oplus k_1\\ x_1\oplus x_2\oplus k_1\oplus k_2\end{bmatrix}, \text{ якщо } k_1=0;\ k_2=0\\ \begin{bmatrix}x_1\\ x_1\oplus x_2\oplus 1\end{bmatrix}=\begin{bmatrix}x_1\oplus k_1\\ x_1\oplus x_2\oplus k_1\oplus k_2\end{bmatrix}, \text{якщо } k_1=0;\ k_2=1\\ \begin{bmatrix}x_1\oplus 1\\ x_1\oplus x_2\oplus 1\end{bmatrix}=\begin{bmatrix}x_1\oplus k_1\\ x_1\oplus x_2\oplus k_1\oplus k_2\end{bmatrix}, \text{ якщо } k_1=1;\ k_2=0\\ \begin{bmatrix}x_1\oplus 1\\ x_1\oplus x_2\end{bmatrix}=\begin{bmatrix}x_1\oplus k_1\\ x_1\oplus x_2\oplus k_1\oplus k_2\end{bmatrix}, \text{якщо } k_1=1;\ k_2=1\end{cases}$$

Таким чином, операцію $O_{3,9,21,15}$ можна записати як:

$$O_{3,9,21,15}=\begin{cases}\begin{bmatrix}x_1\\ x_1\oplus x_2\end{bmatrix}=\begin{bmatrix}x_1\oplus k_1\\ x_1\oplus x_2\oplus k_1\oplus k_2\end{bmatrix}, \text{ якщо } k_1=0;\ k_2=0\\ \begin{bmatrix}x_1\\ x_1\oplus x_2\oplus 1\end{bmatrix}=\begin{bmatrix}x_1\oplus k_1\\ x_1\oplus x_2\oplus k_1\oplus k_2\end{bmatrix}, \text{якщо } k_1=0;\ k_2=1\\ \begin{bmatrix}x_1\oplus 1\\ x_1\oplus x_2\oplus 1\end{bmatrix}=\begin{bmatrix}x_1\oplus k_1\\ x_1\oplus x_2\oplus k_1\oplus k_2\end{bmatrix}, \text{ якщо } k_1=1;\ k_2=0\\ \begin{bmatrix}x_1\oplus 1\\ x_1\oplus x_2\end{bmatrix}=\begin{bmatrix}x_1\oplus k_1\\ x_1\oplus x_2\oplus k_1\oplus k_2\end{bmatrix}, \text{якщо } k_1=1;\ k_2=1\end{cases}=\begin{bmatrix}x_1\oplus k_1\\ x_1\oplus x_2\oplus k_1\oplus k_2\end{bmatrix}$$

Математичну модель операції $O_{9,3,15,21}$, що є синтезованою на основі моделі основної операції $O_{3,9,21,15}$ третього набору двохоперандних операцій, представлено у вигляді:

$$O_{9,3,15,21}=\begin{cases}\begin{bmatrix}x_1\\ x_1\oplus x_2\oplus 1\end{bmatrix}, \text{ якщо } k_1=0;\ k_2=0\\ \begin{bmatrix}x_1\\ x_1\oplus x_2\end{bmatrix}, \text{якщо } k_1=0;\ k_2=1\\ \begin{bmatrix}x_1\oplus 1\\ x_1\oplus x_2\end{bmatrix}, \text{ якщо } k_1=1;\ k_2=0\\ \begin{bmatrix}x_1\oplus 1\\ x_1\oplus x_2\oplus 1\end{bmatrix}, \text{якщо } k_1=1;\ k_2=1\end{cases}=\begin{cases}\begin{bmatrix}x_1\\ x_1\oplus x_2\oplus 1\end{bmatrix}=\begin{bmatrix}x_1\oplus k_1\\ x_1\oplus x_2\oplus k_1\oplus k_2\oplus 1\end{bmatrix}, \text{ якщо } k_1=0;\ k_2=0\\ \begin{bmatrix}x_1\\ x_1\oplus x_2\end{bmatrix}=\begin{bmatrix}x_1\oplus k_1\\ x_1\oplus x_2\oplus k_1\oplus k_2\oplus 1\end{bmatrix}, \text{якщо } k_1=0;\ k_2=1\\ \begin{bmatrix}x_1\oplus 1\\ x_1\oplus x_2\end{bmatrix}=\begin{bmatrix}x_1\oplus k_1\\ x_1\oplus x_2\oplus k_1\oplus k_2\oplus 1\end{bmatrix}, \text{ якщо } k_1=1;\ k_2=0\\ \begin{bmatrix}x_1\oplus 1\\ x_1\oplus x_2\oplus 1\end{bmatrix}=\begin{bmatrix}x_1\oplus k_1\\ x_1\oplus x_2\oplus k_1\oplus k_2\oplus 1\end{bmatrix}, \text{якщо } k_1=1;\ k_2=1\end{cases},$$

Відповідно, операцію $O_{9,3,15,21}$ можна записати як:

$$O_{9,3,15,21}=\begin{cases}\begin{bmatrix}x_1\\ x_1\oplus x_2\oplus 1\end{bmatrix}=\begin{bmatrix}x_1\oplus k_1\\ x_1\oplus x_2\oplus k_1\oplus k_2\oplus 1\end{bmatrix}, \text{ якщо } k_1=0;\ k_2=0\\ \begin{bmatrix}x_1\\ x_1\oplus x_2\end{bmatrix}=\begin{bmatrix}x_1\oplus k_1\\ x_1\oplus x_2\oplus k_1\oplus k_2\oplus 1\end{bmatrix}, \text{якщо } k_1=0;\ k_2=1\\ \begin{bmatrix}x_1\oplus 1\\ x_1\oplus x_2\end{bmatrix}=\begin{bmatrix}x_1\oplus k_1\\ x_1\oplus x_2\oplus k_1\oplus k_2\oplus 1\end{bmatrix}, \text{якщо } k_1=1;\ k_2=0\\ \begin{bmatrix}x_1\oplus 1\\ x_1\oplus x_2\oplus 1\end{bmatrix}=\begin{bmatrix}x_1\oplus k_1\\ x_1\oplus x_2\oplus k_1\oplus k_2\oplus 1\end{bmatrix}, \text{якщо } k_1=1;\ k_2=1\end{cases}=\begin{bmatrix}x_1\oplus k_1\\ x_1\oplus x_2\oplus k_1\oplus k_2\oplus 1\end{bmatrix}$$

Перестановочна схема побудови цієї операції представлена на рис.2.7.

Схематичне представлення основної операції НДО 3	Перестановочна схема	Схематичне представлення отриманої операції $O_{9,3,15,21}$
3 9 21 15	3 ↔ 9 21 ↔ 15	9 3 15 21

Рис. 2.7 Перестановочна схема для побудови операції $O_{9,3,15,21}$ на основі основної операції третього НДО $O_{3,9,21,15}$

Математична модель операції $O_{15,21,9,3}$, шо є синтезованою на основі моделі операції $O_{3,9,21,15}$ третього набору двохоперандних операцій, матиме вигляд:

$$O_{15,21,9,3}=\begin{cases}\begin{bmatrix}x_1\oplus 1\\ x_1\oplus x_2\end{bmatrix}, \text{ якщо } k_1=0;\ k_2=0\\ \begin{bmatrix}x_1\oplus 1\\ x_1\oplus x_2\oplus 1\end{bmatrix}, \text{якщо } k_1=0;\ k_2=1\\ \begin{bmatrix}x_1\\ x_1\oplus x_2\oplus 1\end{bmatrix}, \text{якщо } k_1=1;\ k_2=0\\ \begin{bmatrix}x_1\\ x_1\oplus x_2\end{bmatrix}, \text{якщо } k_1=1;\ k_2=1\end{cases}=\begin{cases}\begin{bmatrix}x_1\oplus 1\\ x_1\oplus x_2\end{bmatrix}=\begin{bmatrix}x_1\oplus k_1\oplus 1\\ x_1\oplus x_2\oplus k_1\oplus k_2\end{bmatrix}, \text{ якщо } k_1=0;\ k_2=0\\ \begin{bmatrix}x_1\oplus 1\\ x_1\oplus x_2\oplus 1\end{bmatrix}=\begin{bmatrix}x_1\oplus k_1\oplus 1\\ x_1\oplus x_2\oplus k_1\oplus k_2\end{bmatrix}, \text{якщо } k_1=0;\ k_2=1\\ \begin{bmatrix}x_1\\ x_1\oplus x_2\oplus 1\end{bmatrix}=\begin{bmatrix}x_1\oplus k_1\oplus 1\\ x_1\oplus x_2\oplus k_1\oplus k_2\end{bmatrix}, \text{якщо } k_1=1;\ k_2=0\\ \begin{bmatrix}x_1\\ x_1\oplus x_2\end{bmatrix}=\begin{bmatrix}x_1\oplus k_1\oplus 1\\ x_1\oplus x_2\oplus k_1\oplus k_2\end{bmatrix}, \text{якщо } k_1=1;\ k_2=1\end{cases},$$

Отже, операцію $O_{15,21,9,3}$ можна записати як:

$$O_{15,21,9,3}=\begin{cases}\begin{bmatrix}x_1\oplus 1\\ x_1\oplus x_2\end{bmatrix}=\begin{bmatrix}x_1\oplus k_1\oplus 1\\ x_1\oplus x_2\oplus k_1\oplus k_2\end{bmatrix}, \text{ якщо } k_1=0;\ k_2=0\\ \begin{bmatrix}x_1\oplus 1\\ x_1\oplus x_2\oplus 1\end{bmatrix}=\begin{bmatrix}x_1\oplus k_1\oplus 1\\ x_1\oplus x_2\oplus k_1\oplus k_2\end{bmatrix}, \text{якщо } k_1=0;\ k_2=1\\ \begin{bmatrix}x_1\\ x_1\oplus x_2\oplus 1\end{bmatrix}=\begin{bmatrix}x_1\oplus k_1\oplus 1\\ x_1\oplus x_2\oplus k_1\oplus k_2\end{bmatrix}, \text{ якщо } k_1=1;\ k_2=0\\ \begin{bmatrix}x_1\\ x_1\oplus x_2\end{bmatrix}=\begin{bmatrix}x_1\oplus k_1\oplus 1\\ x_1\oplus x_2\oplus k_1\oplus k_2\end{bmatrix}, \text{якщо } k_1=1;\ k_2=1\end{cases}=\begin{bmatrix}x_1\oplus k_1\oplus 1\\ x_1\oplus x_2\oplus k_1\oplus k_2\end{bmatrix}$$

Перестановочна схема побудови цієї операції представлена на рис.2.8.

Схематичне представлення основної операції НДО 3	Перестановочна схема	Схематичне представлення отриманої операції $O_{15,21,9,3}$
3 9 21 15	3 9 21 15	15 21 9 3

Рис. 2.8 Перестановочна схема для побудови операції $O_{15,21,9,3}$ на основі основної операції третього НДО $O_{3,9,21,15}$

Математичну модель операції $O_{21,15,3,9}$, що є синтезованою на основі моделі основної операції $O_{3,9,21,15}$ третього набору двохоперандних операцій, представлено у вигляді:

$$O_{21,15,3,9}=\begin{cases}\begin{bmatrix}x_1\oplus 1\\ x_1\oplus x_2\oplus 1\end{bmatrix}, \text{ якщо } k_1=0;\ k_2=0\\ \begin{bmatrix}x_1\oplus 1\\ x_1\oplus x_2\end{bmatrix}, \text{якщо } k_1=0;\ k_2=1\\ \begin{bmatrix}x_1\\ x_1\oplus x_2\end{bmatrix}, \text{ якщо } k_1=1;\ k_2=0\\ \begin{bmatrix}x_1\\ x_1\oplus x_2\oplus 1\end{bmatrix}, \text{якщо } k_1=1;\ k_2=1\end{cases}=\begin{cases}\begin{bmatrix}x_1\oplus 1\\ x_1\oplus x_2\oplus 1\end{bmatrix}=\begin{bmatrix}x_1\oplus k_1\oplus 1\\ x_1\oplus x_2\oplus k_1\oplus k_2\oplus 1\end{bmatrix}, \text{ якщо } k_1=0;\ k_2=0\\ \begin{bmatrix}x_1\oplus 1\\ x_1\oplus x_2\end{bmatrix}=\begin{bmatrix}x_1\oplus k_1\oplus 1\\ x_1\oplus x_2\oplus k_1\oplus k_2\oplus 1\end{bmatrix}, \text{якщо } k_1=0;\ k_2=1\\ \begin{bmatrix}x_1\\ x_1\oplus x_2\end{bmatrix}=\begin{bmatrix}x_1\oplus k_1\oplus 1\\ x_1\oplus x_2\oplus k_1\oplus k_2\oplus 1\end{bmatrix}, \text{ якщо } k_1=1;\ k_2=0\\ \begin{bmatrix}x_1\\ x_1\oplus x_2\oplus 1\end{bmatrix}=\begin{bmatrix}x_1\oplus k_1\oplus 1\\ x_1\oplus x_2\oplus k_1\oplus k_2\oplus 1\end{bmatrix}, \text{якщо } k_1=1;\ k_2=1\end{cases}$$

Таким чином, операцію $O_{21,15,3,9}$ можна записати як:

$$O_{21,15,3,9}=\begin{cases}\begin{bmatrix}x_1\oplus 1\\ x_1\oplus x_2\oplus 1\end{bmatrix}=\begin{bmatrix}x_1\oplus k_1\oplus 1\\ x_1\oplus x_2\oplus k_1\oplus k_2\oplus 1\end{bmatrix}, \text{ якщо } k_1=0;\ k_2=0\\ \begin{bmatrix}x_1\oplus 1\\ x_1\oplus x_2\end{bmatrix}=\begin{bmatrix}x_1\oplus k_1\oplus 1\\ x_1\oplus x_2\oplus k_1\oplus k_2\oplus 1\end{bmatrix}, \text{якщо } k_1=0;\ k_2=1\\ \begin{bmatrix}x_1\\ x_1\oplus x_2\end{bmatrix}=\begin{bmatrix}x_1\oplus k_1\oplus 1\\ x_1\oplus x_2\oplus k_1\oplus k_2\oplus 1\end{bmatrix}, \text{ якщо } k_1=1;\ k_2=0\\ \begin{bmatrix}x_1\\ x_1\oplus x_2\oplus 1\end{bmatrix}=\begin{bmatrix}x_1\oplus k_1\oplus 1\\ x_1\oplus x_2\oplus k_1\oplus k_2\oplus 1\end{bmatrix}, \text{якщо } k_1=1;\ k_2=1\end{cases}=\begin{bmatrix}x_1\oplus k_1\oplus 1\\ x_1\oplus x_2\oplus k_1\oplus k_2\oplus 1\end{bmatrix}$$

Перестановочна схема побудови цієї операції представлена на рис.2.9.

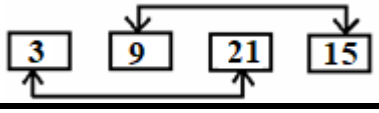
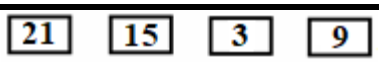
Схематичне представлення основної операції НДО 3	Перестановочна схема	Схематичне представлення отриманої операції $O_{21,15,3,9}$
		

Рис. 2.9 Перестановочна схема для побудови операції $O_{21,15,3,9}$ на основі основної операції третього НДО $O_{3,9,21,15}$

Операції трерього набору двохоперандних операцій порозрядного додавання за модулем два побудовано, перейдемо до дослідження четвертого набору двохоперандних операцій порозрядного додавання за модулем два.

2.2.3 Дослідження четвертого набору двохоперандних операцій криптоперетворення першої математичної групи (НДО 4)

Розглянемо четвертий набір двохоперандних операцій.

Операція $O_{4,16,10,22}$ є першою в цьому наборі і буде умовно основною. На основі операції $O_{4,16,10,22}$ за рахунок перестановок будуються інші операції цього набору.

Розглянемо таблично формування операції четвертого набору операцій порозрядного додавання за модулем два із точністю до перестановки, що включає в себе операції: $O_{4,16,10,22}$, $O_{10,22,4,16}$, $O_{16,4,22,10}$, $O_{22,10,16,4}$.

Результати побудови цих операцій наведені в табл. 2.7.

Таблиця 2.7

Четвертий набір двохоперандних операцій порозрядного додавання за модулем два

Операція	$O_{4,16,10,22}$				$O_{10,22,4,16}$				$O_{16,4,22,10}$				$O_{22,10,16,4}$			
Значення операндів	**0**	**1**	**2**	**3**	**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	3	1	2	0
1	2	0	3	1	3	1	2	0	0	2	1	3	1	3	0	2
2	1	3	0	2	0	2	1	3	3	1	2	0	2	0	3	1
3	3	1	2	0	2	0	3	1	1	3	0	2	0	2	1	3
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**				**0=3, 1=1, 2=2, 3=0**			

Розглянемо більш детально результати моделювання четвертого набору двохоперандних операцій, представивши їх математичними моделями.

Математична модель базової операції четвертого набору двохоперандних операцій $O_{4,16,10,22}$ матиме вигляд:

$$O_{4,16,10,22}=\begin{cases}\begin{bmatrix}x_2\\x_1\end{bmatrix}, \text{ якщо } k_1=0;\ k_2=0\\ \begin{bmatrix}x_2\oplus 1\\x_1\end{bmatrix}, \text{якщо } k_1=0;\ k_2=1\\ \begin{bmatrix}x_2\\x_1\oplus 1\end{bmatrix}, \text{ якщо } k_1=1;\ k_2=0\\ \begin{bmatrix}x_2\oplus 1\\x_1\oplus 1\end{bmatrix}, \text{якщо } k_1=1;\ k_2=1\end{cases}=\begin{cases}\begin{bmatrix}x_2\\x_1\end{bmatrix}=\begin{bmatrix}x_2\oplus k_2\\x_1\oplus k_1\end{bmatrix}, \text{ якщо } k_1=0;\ k_2=0\\ \begin{bmatrix}x_2\oplus 1\\x_1\end{bmatrix}=\begin{bmatrix}x_2\oplus k_2\\x_1\oplus k_1\end{bmatrix}, \text{якщо } k_1=0;\ k_2=1\\ \begin{bmatrix}x_2\\x_1\oplus 1\end{bmatrix}=\begin{bmatrix}x_2\oplus k_2\\x_1\oplus k_1\end{bmatrix}, \text{ якщо } k_1=1;\ k_2=0\\ \begin{bmatrix}x_2\oplus 1\\x_1\oplus 1\end{bmatrix}=\begin{bmatrix}x_2\oplus k_2\\x_1\oplus k_1\end{bmatrix}, \text{якщо } k_1=1;\ k_2=1\end{cases},$$

Отже, операцію $O_{4,16,10,22}$ можна записати як:

$$O_{4,16,10,22}=\begin{cases}\begin{bmatrix}x_2\\x_1\end{bmatrix}=\begin{bmatrix}x_2\oplus k_2\\x_1\oplus k_1\end{bmatrix},\ якщо\ k_1=0;\ k_2=0\\ \begin{bmatrix}x_2\oplus 1\\x_1\end{bmatrix}=\begin{bmatrix}x_2\oplus k_2\\x_1\oplus k_1\end{bmatrix}, якщо\ k_1=0;\ k_2=1\\ \begin{bmatrix}x_2\\x_1\oplus 1\end{bmatrix}=\begin{bmatrix}x_2\oplus k_2\\x_1\oplus k_1\end{bmatrix},\ якщо\ k_1=1;\ k_2=0\\ \begin{bmatrix}x_2\oplus 1\\x_1\oplus 1\end{bmatrix}=\begin{bmatrix}x_2\oplus k_2\\x_1\oplus k_1\end{bmatrix}, якщо\ k_1=1;\ k_2=1\end{cases}=\begin{bmatrix}x_2\oplus k_2\\x_1\oplus k_1\end{bmatrix}$$

Математичну модель операції $O_{10,22,4,16}$, що є синтезованою на основі моделі операції $O_{4,16,10,22}$ четвертого набору двохоперандних операцій, представимо у вигляді:

$$O_{10,22,4,16}=\begin{cases}\begin{bmatrix}x_2\\x_1\oplus 1\end{bmatrix},\ якщо\ k_1=0;\ k_2=0\\ \begin{bmatrix}x_2\oplus 1\\x_1\oplus 1\end{bmatrix}, якщо\ k_1=0;\ k_2=1\\ \begin{bmatrix}x_2\\x_1\end{bmatrix},\ якщо\ k_1=1;\ k_2=0\\ \begin{bmatrix}x_2\oplus 1\\x_1\end{bmatrix}, якщо\ k_1=1;\ k_2=1\end{cases}=\begin{cases}\begin{bmatrix}x_2\\x_1\oplus 1\end{bmatrix}=\begin{bmatrix}x_2\oplus k_2\\x_1\oplus k_1\oplus 1\end{bmatrix},\ якщо\ k_1=0;\ k_2=0\\ \begin{bmatrix}x_2\oplus 1\\x_1\oplus 1\end{bmatrix}=\begin{bmatrix}x_2\oplus k_2\\x_1\oplus k_1\oplus 1\end{bmatrix}, якщо\ k_1=0;\ k_2=1\\ \begin{bmatrix}x_2\\x_1\end{bmatrix}=\begin{bmatrix}x_2\oplus k_2\\x_1\oplus k_1\oplus 1\end{bmatrix},\ якщо\ k_1=1;\ k_2=0\\ \begin{bmatrix}x_2\oplus 1\\x_1\end{bmatrix}=\begin{bmatrix}x_2\oplus k_2\\x_1\oplus k_1\oplus 1\end{bmatrix}, якщо\ k_1=1;\ k_2=1\end{cases},$$

Таким чином, операцію $O_{10,22,4,16}$ можна записати як:

$$O_{10,22,4,16}=\begin{cases}\begin{bmatrix}x_2\\x_1\oplus 1\end{bmatrix}=\begin{bmatrix}x_2\oplus k_2\\x_1\oplus k_1\oplus 1\end{bmatrix},\ якщо\ k_1=0;\ k_2=0\\ \begin{bmatrix}x_2\oplus 1\\x_1\oplus 1\end{bmatrix}=\begin{bmatrix}x_2\oplus k_2\\x_1\oplus k_1\oplus 1\end{bmatrix}, якщо\ k_1=0;\ k_2=1\\ \begin{bmatrix}x_2\\x_1\end{bmatrix}=\begin{bmatrix}x_2\oplus k_2\\x_1\oplus k_1\oplus 1\end{bmatrix},\ якщо\ k_1=1;\ k_2=0\\ \begin{bmatrix}x_2\oplus 1\\x_1\end{bmatrix}=\begin{bmatrix}x_2\oplus k_2\\x_1\oplus k_1\oplus 1\end{bmatrix}, якщо\ k_1=1;\ k_2=1\end{cases}=\begin{bmatrix}x_2\oplus k_2\\x_1\oplus k_1\oplus 1\end{bmatrix}$$

Перестановочна схема побудови цієї операції представлена на рис.2.10.

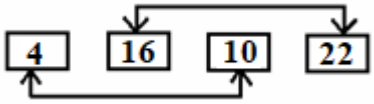
Схематичне представлення основної операції НДО 4	Перестановочна схема	Схематичне представлення отриманої операції $O_{10,22,4,16}$
		

Рис. 2.10 Перестановочна схема для побудови операції $O_{10,22,4,16}$ на основі основної операції четвертого НДО $O_{4,16,10,22}$

Математична модель операції $O_{16,4,22,10}$, щоо є синтезованою на основі моделі основної операції $O_{4,16,10,22}$ четвертого набору двохоперандних операцій, матиме вигляд:

$$O_{16,4,22,10}=\begin{cases}\begin{bmatrix}x_2\oplus 1\\ x_1\end{bmatrix}, \text{ якщо } k_1=0;\ k_2=0\\ \begin{bmatrix}x_2\\ x_1\end{bmatrix}, \text{якщо } k_1=0;\ k_2=1\\ \begin{bmatrix}x_2\oplus 1\\ x_1\oplus 1\end{bmatrix}, \text{ якщо } k_1=1;\ k_2=0\\ \begin{bmatrix}x_2\\ x_1\oplus 1\end{bmatrix}, \text{якщо } k_1=1;\ k_2=1\end{cases}=\begin{cases}\begin{bmatrix}x_2\oplus 1\\ x_1\end{bmatrix}=\begin{bmatrix}x_2\oplus k_2\oplus 1\\ x_1\oplus k_1\end{bmatrix}, \text{ якщо } k_1=0;\ k_2=0\\ \begin{bmatrix}x_2\\ x_1\end{bmatrix}=\begin{bmatrix}x_2\oplus k_2\oplus 1\\ x_1\oplus k_1\end{bmatrix}, \text{якщо } k_1=0;\ k_2=1\\ \begin{bmatrix}x_2\oplus 1\\ x_1\oplus 1\end{bmatrix}=\begin{bmatrix}x_2\oplus k_2\oplus 1\\ x_1\oplus k_1\end{bmatrix}, \text{ якщо } k_1=1;\ k_2=0\\ \begin{bmatrix}x_2\\ x_1\oplus 1\end{bmatrix}=\begin{bmatrix}x_2\oplus k_2\oplus 1\\ x_1\oplus k_1\end{bmatrix}, \text{якщо } k_1=1;\ k_2=1\end{cases}$$

Відповідно, операцію $O_{16,4,22,10}$ можна записати як:

$$O_{16,4,22,10}=\begin{cases}\begin{bmatrix}x_2\oplus 1\\ x_1\end{bmatrix}=\begin{bmatrix}x_2\oplus k_2\oplus 1\\ x_1\oplus k_1\end{bmatrix}, \text{ якщо } k_1=0;\ k_2=0\\ \begin{bmatrix}x_2\\ x_1\end{bmatrix}=\begin{bmatrix}x_2\oplus k_2\oplus 1\\ x_1\oplus k_1\end{bmatrix}, \text{якщо } k_1=0;\ k_2=1\\ \begin{bmatrix}x_2\oplus 1\\ x_1\oplus 1\end{bmatrix}=\begin{bmatrix}x_2\oplus k_2\oplus 1\\ x_1\oplus k_1\end{bmatrix}, \text{ якщо } k_1=1;\ k_2=0\\ \begin{bmatrix}x_2\\ x_1\oplus 1\end{bmatrix}=\begin{bmatrix}x_2\oplus k_2\oplus 1\\ x_1\oplus k_1\end{bmatrix}, \text{якщо } k_1=1;\ k_2=1\end{cases}=\begin{bmatrix}x_2\oplus k_2\oplus 1\\ x_1\oplus k_1\end{bmatrix}$$

Перестановочна схема побудови цієї операції представлена на рис.2.11.

Схематичне представлення основної операції НДО 4	Перестановочна схема	Схематичне представлення отриманої операції $O_{16,4,22,10}$
		

Рис. 2.11 Перестановочна схема для побудови операції $O_{16,4,22,10}$ на основі основної операції четвертого НДО $O_{4,16,10,22}$

Математичну модель операції $O_{22,10,16,4}$, що є синтезованою на основі моделі операції $O_{4,16,10,22}$ четвертого набору двохоперандних операцій, представлено у вигляді:

$$O_{22,10,16,4}=\begin{cases}\begin{bmatrix}x_2\oplus 1\\ x_1\oplus 1\end{bmatrix}, \text{ якщо } k_1=0;\ k_2=0\\ \begin{bmatrix}x_2\\ x_1\oplus 1\end{bmatrix}, \text{якщо } k_1=0;\ k_2=1\\ \begin{bmatrix}x_2\oplus 1\\ x_1\end{bmatrix}, \text{ якщо } k_1=1;\ k_2=0\\ \begin{bmatrix}x_2\\ x_1\end{bmatrix}, \text{якщо } k_1=1;\ k_2=1\end{cases}=\begin{cases}\begin{bmatrix}x_2\oplus 1\\ x_1\oplus 1\end{bmatrix}=\begin{bmatrix}x_2\oplus k_2\oplus 1\\ x_1\oplus k_1\oplus 1\end{bmatrix}, \text{ якщо } k_1=0;\ k_2=0\\ \begin{bmatrix}x_2\\ x_1\oplus 1\end{bmatrix}=\begin{bmatrix}x_2\oplus k_2\oplus 1\\ x_1\oplus k_1\oplus 1\end{bmatrix}, \text{якщо } k_1=0;\ k_2=1\\ \begin{bmatrix}x_2\oplus 1\\ x_1\end{bmatrix}=\begin{bmatrix}x_2\oplus k_2\oplus 1\\ x_1\oplus k_1\oplus 1\end{bmatrix}, \text{ якщо } k_1=1;\ k_2=0\\ \begin{bmatrix}x_2\\ x_1\end{bmatrix}=\begin{bmatrix}x_2\oplus k_2\oplus 1\\ x_1\oplus k_1\oplus 1\end{bmatrix}, \text{якщо } k_1=1;\ k_2=1\end{cases}$$

Таким чином, операцію $O_{22,10,16,4}$ можна записати як:

$$O_{22,10,16,4}=\begin{cases}\begin{bmatrix}x_2\oplus 1\\ x_1\oplus 1\end{bmatrix}=\begin{bmatrix}x_2\oplus k_2\oplus 1\\ x_1\oplus k_1\oplus 1\end{bmatrix}, \text{ якщо } k_1=0;\ k_2=0\\ \begin{bmatrix}x_2\\ x_1\oplus 1\end{bmatrix}=\begin{bmatrix}x_2\oplus k_2\oplus 1\\ x_1\oplus k_1\oplus 1\end{bmatrix}, \text{якщо } k_1=0;\ k_2=1\\ \begin{bmatrix}x_2\oplus 1\\ x_1\end{bmatrix}=\begin{bmatrix}x_2\oplus k_2\oplus 1\\ x_1\oplus k_1\oplus 1\end{bmatrix}, \text{ якщо } k_1=1;\ k_2=0\\ \begin{bmatrix}x_2\\ x_1\end{bmatrix}=\begin{bmatrix}x_2\oplus k_2\oplus 1\\ x_1\oplus k_1\oplus 1\end{bmatrix}, \text{якщо } k_1=1;\ k_2=1\end{cases}=\begin{bmatrix}x_2\oplus k_2\oplus 1\\ x_1\oplus k_1\oplus 1\end{bmatrix}$$

Перестановочна схема побудови цієї операції представлена на рис.2.12.

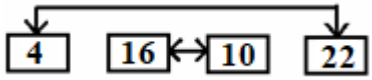
Схематичне представлення основної операції НДО 4	Перестановочна схема	Схематичне представлення отриманої операції $O_{22,10,16,4}$
		

Рис. 2.12 Перестановочна схема для побудови операції $O_{22,10,16,4}$ на основі основної операції четвертого НДО $O_{4,16,10,22}$

Операції четвертого набору двохоперандних операцій порозрядного додавання за модулем два побудовано, перейдемо до дослідження п’ятого набору двохоперандних операцій порозрядного додавання за модулем два.

2.2.4 Дослідження п’ятого набору двохоперандних операцій криптоперетворення першої математичної групи (НДО 5)

Розглянемо п’ятий набір двохоперандних операцій.

Операція $O_{5,23,11,17}$ є першою в цьому наборі і буде умовно основною. На основі операції $O_{5,23,11,17}$ за рахунок перестановок будуються інші операції цього набору.

Розглянемо таблично формування операції п’ятого набору операцій порозрядного додавання за модулем два із точністю до перестановки, що включає в себе операції: $O_{5,23,11,17}$, $O_{11,17,5,23}$, $O_{17,11,23,5}$, $O_{23,5,17,11}$.

Результати побудови цих операцій наведено в табл. 2.8.

Розглянемо більш детально результати моделювання п’ятого набору двохоперандних операцій, представивши їх математичними моделями.

Таблиця 2.8

П’ятий набір двохоперандних операцій порозрядного додавання за модулем два

Операція	$O_{5,23,11,17}$				$O_{11,17,5,23}$				$O_{17,11,23,5}$				$O_{23,5,17,11}$			
Значення операндів	**0**	**1**	**2**	**3**	**0**	**1**	**2**	**3**	**0**	**1**	**2**	**3**	**0**	**1**	**2**	**3**
0	0	3	1	2	1	2	0	3	2	1	3	0	3	0	2	1
1	3	0	2	1	2	1	3	0	1	2	0	3	0	3	1	2
2	1	2	0	3	0	3	1	2	3	0	2	1	2	1	3	0
3	2	1	3	0	3	0	2	1	0	3	1	2	1	2	0	3
Перестановка	**0=0, 1=3, 2=1, 3=2**				**0=1, 1=2, 2=0, 3=3**				**0=2, 1=1, 2=3, 3=0**				**0=3, 1=0, 2=2, 3=1**			

Математична модель основної операції п’ятого набору двохоперандних операцій $O_{5,23,11,17}$ матиме вигляд:

$$O_{5,23,11,17}=\begin{cases}\begin{bmatrix}x_2\\ x_1\oplus x_2\end{bmatrix}, \text{ якщо } k_1=0;\ k_2=0\\ \begin{bmatrix}x_2\oplus 1\\ x_1\oplus x_2\oplus 1\end{bmatrix}, \text{якщо } k_1=0;\ k_2=1\\ \begin{bmatrix}x_2\\ x_1\oplus x_2\oplus 1\end{bmatrix}, \text{ якщо } k_1=1;\ k_2=0\\ \begin{bmatrix}x_2\oplus 1\\ x_1\oplus x_2\end{bmatrix}, \text{якщо } k_1=1;\ k_2=1\end{cases}=\begin{cases}\begin{bmatrix}x_2\\ x_1\oplus x_2\end{bmatrix}=\begin{bmatrix}x_2\oplus k_2\\ x_1\oplus x_2\oplus k_1\oplus k_2\end{bmatrix}, \text{ якщо } k_1=0;\ k_2=0\\ \begin{bmatrix}x_2\oplus 1\\ x_1\oplus x_2\oplus 1\end{bmatrix}=\begin{bmatrix}x_2\oplus k_2\\ x_1\oplus x_2\oplus k_1\oplus k_2\end{bmatrix}, \text{якщо } k_1=0;\ k_2=1\\ \begin{bmatrix}x_2\\ x_1\oplus x_2\oplus 1\end{bmatrix}=\begin{bmatrix}x_2\oplus k_2\\ x_1\oplus x_2\oplus k_1\oplus k_2\end{bmatrix}, \text{ якщо } k_1=1;\ k_2=0\\ \begin{bmatrix}x_2\oplus 1\\ x_1\oplus x_2\end{bmatrix}=\begin{bmatrix}x_2\oplus k_2\\ x_1\oplus x_2\oplus k_1\oplus k_2\end{bmatrix}, \text{якщо } k_1=1;\ k_2=1\end{cases}$$

Таким чином, операцію $O_{5,23,11,17}$ можна записати як:

$$O_{5,23,11,17}=\begin{cases}\begin{bmatrix}x_2\\ x_1\oplus x_2\end{bmatrix}=\begin{bmatrix}x_2\oplus k_2\\ x_1\oplus x_2\oplus k_1\oplus k_2\end{bmatrix}, \text{ якщо } k_1=0;\ k_2=0\\ \begin{bmatrix}x_2\oplus 1\\ x_1\oplus x_2\oplus 1\end{bmatrix}=\begin{bmatrix}x_2\oplus k_2\\ x_1\oplus x_2\oplus k_1\oplus k_2\end{bmatrix}, \text{якщо } k_1=0;\ k_2=1\\ \begin{bmatrix}x_2\\ x_1\oplus x_2\oplus 1\end{bmatrix}=\begin{bmatrix}x_2\oplus k_2\\ x_1\oplus x_2\oplus k_1\oplus k_2\end{bmatrix}, \text{ якщо } k_1=1;\ k_2=0\\ \begin{bmatrix}x_2\oplus 1\\ x_1\oplus x_2\end{bmatrix}=\begin{bmatrix}x_2\oplus k_2\\ x_1\oplus x_2\oplus k_1\oplus k_2\end{bmatrix}, \text{якщо } k_1=1;\ k_2=1\end{cases}=\begin{bmatrix}x_2\oplus k_2\\ x_1\oplus x_2\oplus k_1\oplus k_2\end{bmatrix}$$

Математичну модель операції $O_{11,17,5,23}$, що є синтезованою на основі моделі операції $O_{5,23,11,17}$ п'ятого набору двохоперандних операцій, представлено у вигляді:

$$O_{11,17,5,23}=\begin{cases}\begin{bmatrix}x_2\\ x_1\oplus x_2\oplus 1\end{bmatrix}, \text{ якщо } k_1=0;\ k_2=0\\ \begin{bmatrix}x_2\oplus 1\\ x_1\oplus x_2\end{bmatrix}, \text{якщо } k_1=0;\ k_2=1\\ \begin{bmatrix}x_2\\ x_1\oplus x_2\end{bmatrix}, \text{ якщо } k_1=1;\ k_2=0\\ \begin{bmatrix}x_2\oplus 1\\ x_1\oplus x_2\oplus 1\end{bmatrix}, \text{якщо } k_1=1;\ k_2=1\end{cases}=\begin{cases}\begin{bmatrix}x_2\\ x_1\oplus x_2\oplus 1\end{bmatrix}=\begin{bmatrix}x_2\oplus k_2\\ x_1\oplus x_2\oplus k_1\oplus k_2\oplus 1\end{bmatrix}, \text{ якщо } k_1=0;\ k_2=0\\ \begin{bmatrix}x_2\oplus 1\\ x_1\oplus x_2\end{bmatrix}=\begin{bmatrix}x_2\oplus k_2\\ x_1\oplus x_2\oplus k_1\oplus k_2\oplus 1\end{bmatrix}, \text{якщо } k_1=0;\ k_2=1\\ \begin{bmatrix}x_2\\ x_1\oplus x_2\end{bmatrix}=\begin{bmatrix}x_2\oplus k_2\\ x_1\oplus x_2\oplus k_1\oplus k_2\oplus 1\end{bmatrix}, \text{ якщо } k_1=1;\ k_2=0\\ \begin{bmatrix}x_2\oplus 1\\ x_1\oplus x_2\oplus 1\end{bmatrix}=\begin{bmatrix}x_2\oplus k_2\\ x_1\oplus x_2\oplus k_1\oplus k_2\oplus 1\end{bmatrix}, \text{якщо } k_1=1;\ k_2=1\end{cases}$$

Отже, операцію $O_{11,17,5,23}$ можна записати як:

$$O_{11,17,5,23}=\begin{cases}\begin{bmatrix}x_2\\ x_1\oplus x_2\oplus 1\end{bmatrix}=\begin{bmatrix}x_2\oplus k_2\\ x_1\oplus x_2\oplus k_1\oplus k_2\oplus 1\end{bmatrix}, \text{ якщо } k_1=0;\ k_2=0\\ \begin{bmatrix}x_2\oplus 1\\ x_1\oplus x_2\end{bmatrix}=\begin{bmatrix}x_2\oplus k_2\\ x_1\oplus x_2\oplus k_1\oplus k_2\oplus 1\end{bmatrix}, \text{якщо } k_1=0;\ k_2=1\\ \begin{bmatrix}x_2\\ x_1\oplus x_2\end{bmatrix}=\begin{bmatrix}x_2\oplus k_2\\ x_1\oplus x_2\oplus k_1\oplus k_2\oplus 1\end{bmatrix}, \text{ якщо } k_1=1;\ k_2=0\\ \begin{bmatrix}x_2\oplus 1\\ x_1\oplus x_2\oplus 1\end{bmatrix}=\begin{bmatrix}x_2\oplus k_2\\ x_1\oplus x_2\oplus k_1\oplus k_2\oplus 1\end{bmatrix}, \text{якщо } k_1=1;\ k_2=1\end{cases}=\begin{bmatrix}x_2\oplus k_2\\ x_1\oplus x_2\oplus k_1\oplus k_2\oplus 1\end{bmatrix}$$

Перестановочна схема побудови цієї операції представлена на рис.2.13.

Схематичне представлення основної операції НДО 5	Перестановочна схема	Схематичне представлення отриманої операції $O_{11,17,5,23}$
5 23 11 17	5 23 11 17	11 17 5 23

Рис. 2.13 Перестановочна схема для побудови операції $O_{11,17,5,23}$ на основі основної операції п'ятого НДО $O_{5,23,11,17}$

Математична модель операції $O_{17,11,23,5}$, що є синтезованою на основі моделі операції $O_{5,23,11,17}$ п'ятого набору двохоперандних операцій, матиме вигляд:

$$O_{17,11,23,5}=\begin{cases}\begin{bmatrix}x_2\oplus 1\\ x_1\oplus x_2\end{bmatrix}, & якщо\ k_1=0;\ k_2=0\\ \begin{bmatrix}x_2\\ x_1\oplus x_2\oplus 1\end{bmatrix}, & якщо\ k_1=0;\ k_2=1\\ \begin{bmatrix}x_2\oplus 1\\ x_1\oplus x_2\oplus 1\end{bmatrix}, & якщо\ k_1=1;\ k_2=0\\ \begin{bmatrix}x_2\\ x_1\oplus x_2\end{bmatrix}, & якщо\ k_1=1;\ k_2=1\end{cases}=\begin{cases}\begin{bmatrix}x_2\oplus 1\\ x_1\oplus x_2\end{bmatrix}=\begin{bmatrix}x_2\oplus k_2\oplus 1\\ x_1\oplus x_2\oplus k_1\oplus k_2\end{bmatrix}, & якщо\ k_1=0;\ k_2=0\\ \begin{bmatrix}x_2\\ x_1\oplus x_2\oplus 1\end{bmatrix}=\begin{bmatrix}x_2\oplus k_2\oplus 1\\ x_1\oplus x_2\oplus k_1\oplus k_2\end{bmatrix}, & якщо\ k_1=0;\ k_2=1\\ \begin{bmatrix}x_2\oplus 1\\ x_1\oplus x_2\oplus 1\end{bmatrix}=\begin{bmatrix}x_2\oplus k_2\oplus 1\\ x_1\oplus x_2\oplus k_1\oplus k_2\end{bmatrix}, & якщо\ k_1=1;\ k_2=0\\ \begin{bmatrix}x_2\\ x_1\oplus x_2\end{bmatrix}=\begin{bmatrix}x_2\oplus k_2\oplus 1\\ x_1\oplus x_2\oplus k_1\oplus k_2\end{bmatrix}, & якщо\ k_1=1;\ k_2=1\end{cases}$$

Відповідно, операцію $O_{17,11,23,5}$ можна записати як:

$$O_{17,11,23,5}=\begin{cases}\begin{bmatrix}x_2\oplus 1\\ x_1\oplus x_2\end{bmatrix}=\begin{bmatrix}x_2\oplus k_2\oplus 1\\ x_1\oplus x_2\oplus k_1\oplus k_2\end{bmatrix}, & якщо\ k_1=0;\ k_2=0\\ \begin{bmatrix}x_2\\ x_1\oplus x_2\oplus 1\end{bmatrix}=\begin{bmatrix}x_2\oplus k_2\oplus 1\\ x_1\oplus x_2\oplus k_1\oplus k_2\end{bmatrix}, & якщо\ k_1=0;\ k_2=1\\ \begin{bmatrix}x_2\oplus 1\\ x_1\oplus x_2\oplus 1\end{bmatrix}=\begin{bmatrix}x_2\oplus k_2\oplus 1\\ x_1\oplus x_2\oplus k_1\oplus k_2\end{bmatrix}, & якщо\ k_1=1;\ k_2=0\\ \begin{bmatrix}x_2\\ x_1\oplus x_2\end{bmatrix}=\begin{bmatrix}x_2\oplus k_2\oplus 1\\ x_1\oplus x_2\oplus k_1\oplus k_2\end{bmatrix}, & якщо\ k_1=1;\ k_2=1\end{cases}=\begin{bmatrix}x_2\oplus k_2\oplus 1\\ x_1\oplus x_2\oplus k_1\oplus k_2\end{bmatrix}$$

Перестановочна схема побудови цієї операції представлена на рис.2.14.

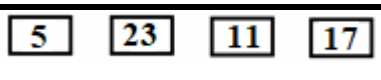
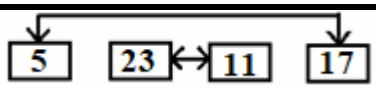
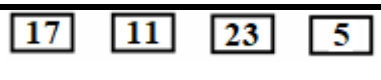
Схематичне представлення основної операції НДО 5	Перестановочна схема	Схематичне представлення отриманої операції $O_{17,11,23,5}$
		

Рис. 2.14 Перестановочна схема для побудови операції $O_{17,11,23,5}$ на основі основної операції п'ятого НДО $O_{5,23,11,17}$

Математичну модель операції $O_{23,5,17,11}$, що є синтезованою на основі моделі основної операції $O_{5,23,11,17}$ п'ятого набору двохоперандних операцій, представлено у вигляді:

$$O_{23,5,17,11}=\begin{cases}\begin{bmatrix}x_2\oplus 1\\ x_1\oplus x_2\oplus 1\end{bmatrix}, \text{ якщо } k_1=0;\ k_2=0\\ \begin{bmatrix}x_2\\ x_1\oplus x_2\end{bmatrix}, \text{якщо } k_1=0;\ k_2=1\\ \begin{bmatrix}x_2\oplus 1\\ x_1\oplus x_2\end{bmatrix}, \text{ якщо } k_1=1;\ k_2=0\\ \begin{bmatrix}x_2\\ x_1\oplus x_2\oplus 1\end{bmatrix}, \text{якщо } k_1=1;\ k_2=1\end{cases}=\begin{cases}\begin{bmatrix}x_2\oplus 1\\ x_1\oplus x_2\oplus 1\end{bmatrix}=\begin{bmatrix}x_2\oplus k_2\oplus 1\\ x_1\oplus x_2\oplus k_1\oplus k_2\oplus 1\end{bmatrix}, \text{ якщо } k_1=0;\ k_2=0\\ \begin{bmatrix}x_2\\ x_1\oplus x_2\end{bmatrix}=\begin{bmatrix}x_2\oplus k_2\oplus 1\\ x_1\oplus x_2\oplus k_1\oplus k_2\oplus 1\end{bmatrix}, \text{якщо } k_1=0;\ k_2=1\\ \begin{bmatrix}x_2\oplus 1\\ x_1\oplus x_2\end{bmatrix}=\begin{bmatrix}x_2\oplus k_2\oplus 1\\ x_1\oplus x_2\oplus k_1\oplus k_2\oplus 1\end{bmatrix}, \text{ якщо } k_1=1;\ k_2=0\\ \begin{bmatrix}x_2\\ x_1\oplus x_2\oplus 1\end{bmatrix}=\begin{bmatrix}x_2\oplus k_2\oplus 1\\ x_1\oplus x_2\oplus k_1\oplus k_2\oplus 1\end{bmatrix}, \text{якщо } k_1=1;\ k_2=1\end{cases}$$

Таким чином, операцію $O_{23,5,17,11}$ можна записати як:

$$O_{23,5,17,11}=\begin{cases}\begin{bmatrix}x_2\oplus 1\\ x_1\oplus x_2\oplus 1\end{bmatrix}=\begin{bmatrix}x_2\oplus k_2\oplus 1\\ x_1\oplus x_2\oplus k_1\oplus k_2\oplus 1\end{bmatrix}, \text{ якщо } k_1=0;\ k_2=0\\ \begin{bmatrix}x_2\\ x_1\oplus x_2\end{bmatrix}=\begin{bmatrix}x_2\oplus k_2\oplus 1\\ x_1\oplus x_2\oplus k_1\oplus k_2\oplus 1\end{bmatrix}, \text{якщо } k_1=0;\ k_2=1\\ \begin{bmatrix}x_2\oplus 1\\ x_1\oplus x_2\end{bmatrix}=\begin{bmatrix}x_2\oplus k_2\oplus 1\\ x_1\oplus x_2\oplus k_1\oplus k_2\oplus 1\end{bmatrix}, \text{ якщо } k_1=1;\ k_2=0\\ \begin{bmatrix}x_2\\ x_1\oplus x_2\oplus 1\end{bmatrix}=\begin{bmatrix}x_2\oplus k_2\oplus 1\\ x_1\oplus x_2\oplus k_1\oplus k_2\oplus 1\end{bmatrix}, \text{якщо } k_1=1;\ k_2=1\end{cases}=\begin{bmatrix}x_2\oplus k_2\oplus 1\\ x_1\oplus x_2\oplus k_1\oplus k_2\oplus 1\end{bmatrix}$$

Перестановочна схема побудови цієї операції представлена на рис.2.15.

Схематичне представлення основної операції НДО 5	Перестановочна схема	Схематичне представлення отриманої операції $O_{23,5,17,11}$
5 23 11 17	5 ↔ 23 11 ↔ 17	23 5 17 11

Рис. 2.15 Перестановочна схема для побудови операції $O_{23,5,17,11}$ на основі основної операції п'ятого НДО $O_{5,23,11,17}$

Операції п’ятого набору двохоперандних операцій порозрядного додавання за модулем два побудовано, перейдемо до дослідження шостого набору двохоперандних операцій порозрядного додавання за модулем два.

2.2.5 Дослідження шостого набору двохоперандних операцій криптоперетворення першої математичної групи (НДО 6)

Розглянемо шостий набір двохоперандних операцій.

Операція $O_{6,18,24,12}$ є першою в цьому наборі і буде умовно основною. На основі цієї операції $O_{6,18,24,12}$ за рахунок перестановок будуються інші операції цього набору.

Розглянемо таблично формування операції двадцять шостого набору операцій порозрядного додавання за модулем два із точністю до перестановки, що включає в себе операції: $O_{6,18,24,12}$, $O_{12,24,18,6}$, $O_{18,6,12,24}$, $O_{24,12,6,18}$.

Результати побудови цих операцій наведені в табл. 2.9.

Таблиця 2.9

Шостий набір двохоперандних операцій порозрядного додавання за модулем два

Операція	$O_{6,18,24,12}$				$O_{12,24,18,6}$				$O_{18,6,12,24}$				$O_{24,12,6,18}$			
Значення операндів	**0**	**1**	**2**	**3**	**0**	**1**	**2**	**3**	**0**	**1**	**2**	**3**	**0**	**1**	**2**	**3**
0	0	2	3	1	1	3	2	0	2	0	1	3	3	1	0	2
1	2	0	1	3	3	1	0	2	0	2	3	1	1	3	2	0
2	3	1	0	2	2	0	1	3	1	3	2	0	0	2	3	1
3	1	3	2	0	0	2	3	1	3	1	0	2	2	0	1	3
Перестановка	**0=0, 1=2, 2=3, 3=1**				**0=1, 1=3, 2=2, 3=0**				**0=2, 1=0, 2=1, 3=3**				**0=3, 1=1, 2=0, 3=2**			

Розглянемо більш детально результати моделювання шостого набору двохоперандних операцій, представивши їх математичними моделями.

Математична модель основної операції шостого набору двохоперандних операцій $O_{6,18,24,12}$ матиме вигляд:

$$O_{6,18,24,12}=\begin{cases}\begin{bmatrix}x_1\oplus x_2\\ x_1\end{bmatrix}, \text{ якщо } k_1=0;\ k_2=0\\ \begin{bmatrix}x_1\oplus x_2\oplus 1\\ x_1\end{bmatrix}, \text{якщо } k_1=0;\ k_2=1\\ \begin{bmatrix}x_1\oplus x_2\oplus 1\\ x_1\oplus 1\end{bmatrix}, \text{ якщо } k_1=1;\ k_2=0\\ \begin{bmatrix}x_1\oplus x_2\\ x_1\oplus 1\end{bmatrix}, \text{якщо } k_1=1;\ k_2=1\end{cases}=\begin{cases}\begin{bmatrix}x_1\oplus x_2\\ x_1\end{bmatrix}=\begin{bmatrix}x_1\oplus x_2\oplus k_1\oplus k_2\\ x_1\oplus k_1\end{bmatrix}, \text{ якщо } k_1=0;\ k_2=0\\ \begin{bmatrix}x_1\oplus x_2\oplus 1\\ x_1\end{bmatrix}=\begin{bmatrix}x_1\oplus x_2\oplus k_1\oplus k_2\\ x_1\oplus k_1\end{bmatrix}, \text{якщо } k_1=0;\ k_2=1\\ \begin{bmatrix}x_1\oplus x_2\oplus 1\\ x_1\oplus 1\end{bmatrix}=\begin{bmatrix}x_1\oplus x_2\oplus k_1\oplus k_2\\ x_1\oplus k_1\end{bmatrix}, \text{ якщо } k_1=1;\ k_2=0\\ \begin{bmatrix}x_1\oplus x_2\\ x_1\oplus 1\end{bmatrix}=\begin{bmatrix}x_1\oplus x_2\oplus k_1\oplus k_2\\ x_1\oplus k_1\end{bmatrix}, \text{якщо } k_1=1;\ k_2=1\end{cases}$$

Відповідно, операцію $O_{6,18,24,12}$ можна записати як:

$$O_{6,18,24,12}=\begin{cases}\begin{bmatrix}x_1\oplus x_2\\ x_1\end{bmatrix}=\begin{bmatrix}x_1\oplus x_2\oplus k_1\oplus k_2\\ x_1\oplus k_1\end{bmatrix}, \text{ якщо } k_1=0;\ k_2=0\\ \begin{bmatrix}x_1\oplus x_2\oplus 1\\ x_1\end{bmatrix}=\begin{bmatrix}x_1\oplus x_2\oplus k_1\oplus k_2\\ x_1\oplus k_1\end{bmatrix}, \text{якщо } k_1=0;\ k_2=1\\ \begin{bmatrix}x_1\oplus x_2\oplus 1\\ x_1\oplus 1\end{bmatrix}=\begin{bmatrix}x_1\oplus x_2\oplus k_1\oplus k_2\\ x_1\oplus k_1\end{bmatrix}, \text{ якщо } k_1=1;\ k_2=0\\ \begin{bmatrix}x_1\oplus x_2\\ x_1\oplus 1\end{bmatrix}=\begin{bmatrix}x_1\oplus x_2\oplus k_1\oplus k_2\\ x_1\oplus k_1\end{bmatrix}, \text{якщо } k_1=1;\ k_2=1\end{cases}=\begin{bmatrix}x_1\oplus x_2\oplus k_1\oplus k_2\\ x_1\oplus k_1\end{bmatrix}$$

Математичну модель операції $O_{12,24,18,6}$, що є синтезованою на основі моделі операції $O_{6,18,24,12}$ шостого набору двохоперандних операцій, представлено у вигляді:

$$O_{12,24,18,6}=\begin{cases}\begin{bmatrix}x_1\oplus x_2\\ x_1\oplus 1\end{bmatrix}, \text{ якщо } k_1=0;\ k_2=0\\ \begin{bmatrix}x_1\oplus x_2\oplus 1\\ x_1\oplus 1\end{bmatrix}, \text{якщо } k_1=0;\ k_2=1\\ \begin{bmatrix}x_1\oplus x_2\oplus 1\\ x_1\end{bmatrix}, \text{ якщо } k_1=1;\ k_2=0\\ \begin{bmatrix}x_1\oplus x_2\\ x_1\end{bmatrix}, \text{якщо } k_1=1;\ k_2=1\end{cases}=\begin{cases}\begin{bmatrix}x_1\oplus x_2\\ x_1\oplus 1\end{bmatrix}=\begin{bmatrix}x_1\oplus x_2\oplus k_1\oplus k_2\\ x_1\oplus k_1\oplus 1\end{bmatrix}, \text{ якщо } k_1=0;\ k_2=0\\ \begin{bmatrix}x_1\oplus x_2\oplus 1\\ x_1\oplus 1\end{bmatrix}=\begin{bmatrix}x_1\oplus x_2\oplus k_1\oplus k_2\\ x_1\oplus k_1\oplus 1\end{bmatrix}, \text{якщо } k_1=0;\ k_2=1\\ \begin{bmatrix}x_1\oplus x_2\oplus 1\\ x_1\end{bmatrix}=\begin{bmatrix}x_1\oplus x_2\oplus k_1\oplus k_2\\ x_1\oplus k_1\oplus 1\end{bmatrix}, \text{ якщо } k_1=1;\ k_2=0\\ \begin{bmatrix}x_1\oplus x_2\\ x_1\end{bmatrix}=\begin{bmatrix}x_1\oplus x_2\oplus k_1\oplus k_2\\ x_1\oplus k_1\oplus 1\end{bmatrix}, \text{якщо } k_1=1;\ k_2=1\end{cases}$$

Таким чином, операцію $O_{12,24,18,6}$ можна записати як:

$$O_{12,24,18,6}=\begin{cases}\begin{bmatrix}x_1\oplus x_2\\ x_1\oplus 1\end{bmatrix}=\begin{bmatrix}x_1\oplus x_2\oplus k_1\oplus k_2\\ x_1\oplus k_1\oplus 1\end{bmatrix}, \text{ якщо } k_1=0;\ k_2=0\\ \begin{bmatrix}x_1\oplus x_2\oplus 1\\ x_1\oplus 1\end{bmatrix}=\begin{bmatrix}x_1\oplus x_2\oplus k_1\oplus k_2\\ x_1\oplus k_1\oplus 1\end{bmatrix}, \text{якщо } k_1=0;\ k_2=1\\ \begin{bmatrix}x_1\oplus x_2\oplus 1\\ x_1\end{bmatrix}=\begin{bmatrix}x_1\oplus x_2\oplus k_1\oplus k_2\\ x_1\oplus k_1\oplus 1\end{bmatrix}, \text{ якщо } k_1=1;\ k_2=0\\ \begin{bmatrix}x_1\oplus x_2\\ x_1\end{bmatrix}=\begin{bmatrix}x_1\oplus x_2\oplus k_1\oplus k_2\\ x_1\oplus k_1\oplus 1\end{bmatrix}, \text{якщо } k_1=1;\ k_2=1\end{cases}=\begin{bmatrix}x_1\oplus x_2\oplus k_1\oplus k_2\\ x_1\oplus k_1\oplus 1\end{bmatrix}$$

Перестановочна схема побудови цієї операції представлена на рис.2.16.

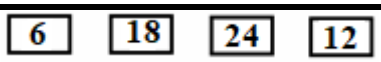
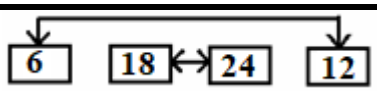
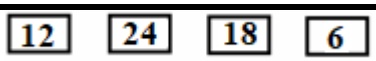
Схематичне представлення основної операції НДО 6	Перестановочна схема	Схематичне представлення отриманої внаслідок перестановки операції $O_{12,24,18,6}$
		

Рис. 2.16 Перестановочна схема для побудови операції $O_{12,24,18,6}$ на основі основної операції шостого НДО $O_{6,18,24,12}$

Математична модель операції $O_{18,6,12,24}$, що є синтезованою на основі моделі операції $O_{6,18,24,12}$ шостого набору двохоперандних операцій, матиме вигляд:

$$O_{18,6,12,24}=\begin{cases}\begin{bmatrix}x_1\oplus x_2\oplus 1\\ x_1\end{bmatrix}, \text{ якщо } k_1=0;\ k_2=0\\ \begin{bmatrix}x_1\oplus x_2\\ x_1\end{bmatrix}, \text{якщо } k_1=0;\ k_2=1\\ \begin{bmatrix}x_1\oplus x_2\\ x_1\oplus 1\end{bmatrix}, \text{ якщо } k_1=1;\ k_2=0\\ \begin{bmatrix}x_1\oplus x_2\oplus 1\\ x_1\oplus 1\end{bmatrix}, \text{якщо } k_1=1;\ k_2=1\end{cases}=\begin{cases}\begin{bmatrix}x_1\oplus x_2\oplus 1\\ x_1\end{bmatrix}=\begin{bmatrix}x_1\oplus x_2\oplus k_1\oplus k_2\oplus 1\\ x_1\oplus k_1\end{bmatrix}, \text{ якщо } k_1=0;\ k_2=0\\ \begin{bmatrix}x_1\oplus x_2\\ x_1\end{bmatrix}=\begin{bmatrix}x_1\oplus x_2\oplus k_1\oplus k_2\oplus 1\\ x_1\oplus k_1\end{bmatrix}, \text{якщо } k_1=0;\ k_2=1\\ \begin{bmatrix}x_1\oplus x_2\\ x_1\oplus 1\end{bmatrix}=\begin{bmatrix}x_1\oplus x_2\oplus k_1\oplus k_2\oplus 1\\ x_1\oplus k_1\end{bmatrix}, \text{ якщо } k_1=1;\ k_2=0\\ \begin{bmatrix}x_1\oplus x_2\oplus 1\\ x_1\oplus 1\end{bmatrix}=\begin{bmatrix}x_1\oplus x_2\oplus k_1\oplus k_2\oplus 1\\ x_1\oplus k_1\end{bmatrix}, \text{якщо } k_1=1;\ k_2=1\end{cases}$$

Таким чином, операцію $O_{18,6,12,24}$ можна записати як:

$$O_{18,6,12,24}=\begin{cases}\begin{bmatrix}x_1\oplus x_2\oplus 1\\ x_1\end{bmatrix}=\begin{bmatrix}x_1\oplus x_2\oplus k_1\oplus k_2\oplus 1\\ x_1\oplus k_1\end{bmatrix}, \text{ якщо } k_1=0;\ k_2=0\\ \begin{bmatrix}x_1\oplus x_2\\ x_1\end{bmatrix}=\begin{bmatrix}x_1\oplus x_2\oplus k_1\oplus k_2\oplus 1\\ x_1\oplus k_1\end{bmatrix}, \text{якщо } k_1=0;\ k_2=1\\ \begin{bmatrix}x_1\oplus x_2\\ x_1\oplus 1\end{bmatrix}=\begin{bmatrix}x_1\oplus x_2\oplus k_1\oplus k_2\oplus 1\\ x_1\oplus k_1\end{bmatrix}, \text{ якщо } k_1=1;\ k_2=0\\ \begin{bmatrix}x_1\oplus x_2\oplus 1\\ x_1\oplus 1\end{bmatrix}=\begin{bmatrix}x_1\oplus x_2\oplus k_1\oplus k_2\oplus 1\\ x_1\oplus k_1\end{bmatrix}, \text{якщо } k_1=1;\ k_2=1\end{cases}=\begin{bmatrix}x_1\oplus x_2\oplus k_1\oplus k_2\oplus 1\\ x_1\oplus k_1\end{bmatrix}$$

Перестановочна схема побудови цієї операції представлена на рис.2.17.

Схематичне представлення основної операції НДО 6	Перестановочна схема	Схематичне представлення отриманої операції $O_{18,6,12,24}$
6 18 24 12	6 ↔ 18 24 ↔ 12	18 6 12 24

Рис. 2.17 Перестановочна схема для побудови операції $O_{18,6,12,24}$ на основі основної операції шостого НДО $O_{6,18,24,12}$

Математичну модель операції $O_{24,12,6,18}$, що є синтезованою на основі моделі операції $O_{6,18,24,12}$ шостого набору двохоперандних операцій, представлено у вигляді:

$$O_{24,12,6,18}=\begin{cases}\begin{bmatrix}x_1\oplus x_2\oplus 1\\ x_1\oplus 1\end{bmatrix}, \text{ якщо } k_1=0;\ k_2=0\\ \begin{bmatrix}x_1\oplus x_2\\ x_1\oplus 1\end{bmatrix}, \text{якщо } k_1=0;\ k_2=1\\ \begin{bmatrix}x_1\oplus x_2\\ x_1\end{bmatrix}, \text{ якщо } k_1=1;\ k_2=0\\ \begin{bmatrix}x_1\oplus x_2\oplus 1\\ x_1\end{bmatrix}, \text{якщо } k_1=1;\ k_2=1\end{cases}=\begin{cases}\begin{bmatrix}x_1\oplus x_2\oplus 1\\ x_1\oplus 1\end{bmatrix}=\begin{bmatrix}x_1\oplus x_2\oplus k_1\oplus k_2\oplus 1\\ x_1\oplus k_1\oplus 1\end{bmatrix}, \text{ якщо } k_1=0;\ k_2=0\\ \begin{bmatrix}x_1\oplus x_2\\ x_1\oplus 1\end{bmatrix}=\begin{bmatrix}x_1\oplus x_2\oplus k_1\oplus k_2\oplus 1\\ x_1\oplus k_1\oplus 1\end{bmatrix}, \text{якщо } k_1=0;\ k_2=1\\ \begin{bmatrix}x_1\oplus x_2\\ x_1\end{bmatrix}=\begin{bmatrix}x_1\oplus x_2\oplus k_1\oplus k_2\oplus 1\\ x_1\oplus k_1\oplus 1\end{bmatrix}, \text{ якщо } k_1=1;\ k_2=0\\ \begin{bmatrix}x_1\oplus x_2\oplus 1\\ x_1\end{bmatrix}=\begin{bmatrix}x_1\oplus x_2\oplus k_1\oplus k_2\oplus 1\\ x_1\oplus k_1\oplus 1\end{bmatrix}, \text{якщо } k_1=1;\ k_2=1\end{cases}$$

Отже, операцію $O_{24,12,6,18}$ можна записати як:

$$O_{24,12,6,18} = \begin{cases} \begin{bmatrix} x_1 \oplus x_2 \oplus 1 \\ x_1 \oplus 1 \end{bmatrix} = \begin{bmatrix} x_1 \oplus x_2 \oplus k_1 \oplus k_2 \oplus 1 \\ x_1 \oplus k_1 \oplus 1 \end{bmatrix}, \text{ якщо } k_1 = 0; k_2 = 0 \\ \begin{bmatrix} x_1 \oplus x_2 \\ x_1 \oplus 1 \end{bmatrix} = \begin{bmatrix} x_1 \oplus x_2 \oplus k_1 \oplus k_2 \oplus 1 \\ x_1 \oplus k_1 \oplus 1 \end{bmatrix}, \text{якщо } k_1 = 0; k_2 = 1 \\ \begin{bmatrix} x_1 \oplus x_2 \\ x_1 \end{bmatrix} = \begin{bmatrix} x_1 \oplus x_2 \oplus k_1 \oplus k_2 \oplus 1 \\ x_1 \oplus k_1 \oplus 1 \end{bmatrix}, \text{ якщо } k_1 = 1; k_2 = 0 \\ \begin{bmatrix} x_1 \oplus x_2 \oplus 1 \\ x_1 \end{bmatrix} = \begin{bmatrix} x_1 \oplus x_2 \oplus k_1 \oplus k_2 \oplus 1 \\ x_1 \oplus k_1 \oplus 1 \end{bmatrix}, \text{якщо } k_1 = 1; k_2 = 1 \end{cases} = \begin{bmatrix} x_1 \oplus x_2 \oplus k_1 \oplus k_2 \oplus 1 \\ x_1 \oplus k_1 \oplus 1 \end{bmatrix}$$

Перестановочна схема побудови цієї операції представлена на рис.2.18.

Схематичне представлення основної операції НДО 6	Перестановочна схема	Схематичне представлення отриманої операції $O_{24,12,6,18}$
6 18 24 12	6 18 24 12	24 12 6 18

Рис. 2.18 Перестановочна схема для побудови операції $O_{24,12,6,18}$ на основі основної операції шостого НДО $O_{6,18,24,12}$

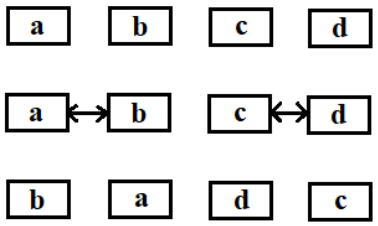
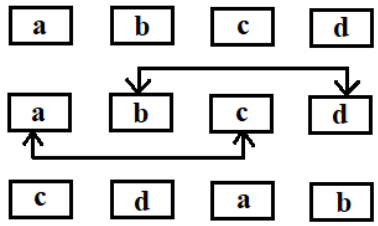
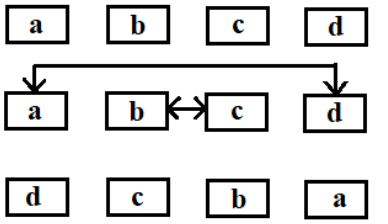
Операції шостого набору двохоперандних операцій порозрядного додавання за модулем два побудовано. Проведемо узагальнинння отриманих результатів на прикладі перестановочних схем.

2.3 Побудова узагальнюючих перестановочних схем для синтезу таблиць істинності двохоперандних операцій криптоперетворення першої математичної групи

В процесі дослідження, встановлено, що всі операції кожного НДО першої математичної групи двохоперандних операцій криптоперетворення (НДО 1-6) можуть бути отримані на основі узагальнюючих перестановочних схем, наведених в табл. 2.10 [12].

Таблиця 2.10

Узагальнюючі перестановочні схеми для першої математичної групи двохоперандних операцій криптоперетворення

№ перестановочної схеми		Перестановочна схема
1	НДО 1 $O_{1,7,13,19} \leftrightarrow O_{7,1,19,13}$; НДО 2 $O_{2,20,14,8} \leftrightarrow O_{20,2,8,14}$ НДО 3 $O_{3,9,21,15} \leftrightarrow O_{9,3,15,21}$; НДО 4 $O_{4,16,10,22} \leftrightarrow O_{16,4,22,10}$ НДО 5 $O_{5,23,11,17} \leftrightarrow O_{23,5,17,11}$; НДО 6 $O_{6,18,24,12} \leftrightarrow O_{18,6,12,24}$	
2	НДО 1 $O_{1,7,13,19} \leftrightarrow O_{13,19,1,7}$; НДО 2 $O_{2,20,14,8} \leftrightarrow O_{14,8,2,20}$; НДО 3 $O_{3,9,21,15} \leftrightarrow O_{21,15,3,9}$; НДО 4 $O_{4,16,10,22} \leftrightarrow O_{10,22,4,16}$; НДО 5 $O_{5,23,11,17} \leftrightarrow O_{11,17,5,23}$; НДО 6 $O_{6,18,24,12} \leftrightarrow O_{24,12,6,18}$	
3	НДО1 $O_{1,7,13,19} \leftrightarrow O_{19,13,7,1}$; НДО 2 $O_{2,20,14,8} \leftrightarrow O_{8,14,20,2}$; НДО 3 $O_{3,9,21,15} \leftrightarrow O_{15,21,9,3}$; НДО 4 $O_{4,16,10,22} \leftrightarrow O_{22,10,16,4}$; НДО 5 $O_{5,23,11,17} \leftrightarrow O_{17,11,23,5}$; НДО 6 $O_{6,18,24,12} \leftrightarrow O_{12,24,18,6}$	

Якщо представити значення операндів в таблиці істинності схематично таким чином:

a - нульового значення операнда;

b - перше значення операнда;

c - друге значення операнда;

d - третє значення операнда,

тоді маємо наступне.

Перша узагальнювальна перестановочна схема є одночасною перестановкою в таблиці істинності значення операнда *a* на значення операнда *b* та значення операнда *c* на значення операнда *d*.

Друга узагальнювальна перестановочна схема передбачає перестановку в таблиці істинності значення операнда *a* на значення операнда *c* та значення операнда *b* на значення операнда *d*.

Третя узагальнююча перестановочна схема містить перестановку в таблиці істинності значення операнда *a* на значення операнда *d* та одночасну перестановку значення операнда *b* на значення операнда *c*.

Таким чином, таблиці істинності першої математичної групи двохоперандних операцій криптоперетворення по кожному з шести НДО можуть бути побудовані на основі основної операції відповідного набору та трьох узагальнюючих перестановочних схем.

Відповідно перший рядок в узагальнюючій перестановочній схемі – це схематичне значення операндів основної операції НДО в таблиці істинності, другий рядок візуалізація перестановки, а третій рядок – схематичне значення операндів отриманої операції НДО.

Але, варто зазначити, що використання узагальнюючих перестановочних схем для першої математичної групи двохоперандних операцій криптоперетворення дають змогу отримати всі операції кожного НДО лише в межах цього НДО. Узагальнюючі перестановочні схеми для першої математичної групи двохоперандних операцій криптоперетворення не дають можливості знайти всі операції цієї групи на основі однієї операції цієї групи.

При подальшому дослідженні цього питання за допомогою аналізу таблиць істинності операцій першої математичної групи двохоперандних операцій криптоперетворення були знайдені перестановочні схеми для побудови таблиць істинності всіх операцій цієї групи на основі однієї базової операції (в нашому випадку першої операції НДО 1 $O_{1,7,13,19}$) [4].

Розглянемо перестановочні схеми для побудови таблиць істинності операцій на основі базової операції першої математичної групи окремо по кожному НДО.

Розглянемо перший набір двохоперандних операцій.

Слід зазначити, що побудова таблиць істинності операцій НДО 1 відбувається за рахунок попарної перестановки в кожному стовпці таблиці істинності. Крім того, перестановки в стовпцях по кожній операції є однаковими.

Перестановочні схеми для побудови таблиць істинності операцій НДО 1 на основі базової операції першої математичної групи представлені на рис. 2.19.

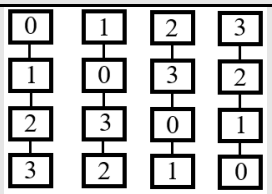
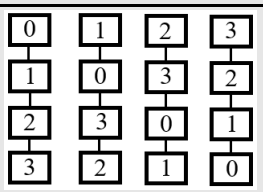
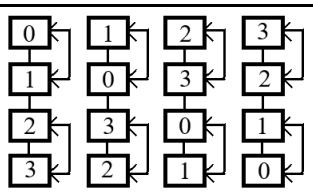
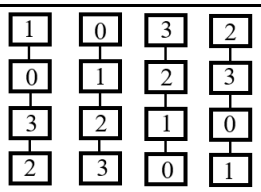
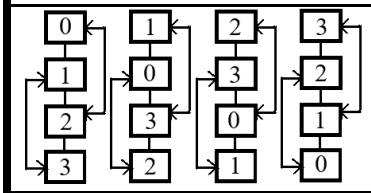
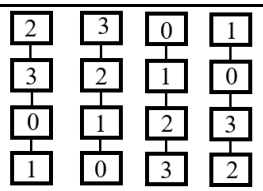
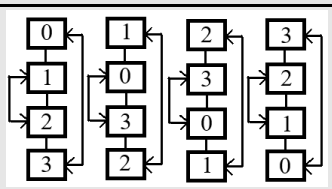
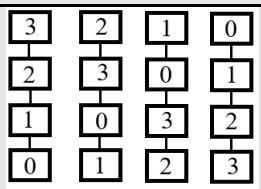
Схематичне представлення реалізації перестановочної схеми таблиці істинності базової операції		Схематичне представлення перестановочної схеми таблиці істинності базової операції	
перестановочна схема	Результат перестановки	перестановочна схема	Результат перестановки
$O_{1,7,13,19}$	$O_{1,7,13,19}$	$O_{1,7,13,19}$	$O_{7,1,19,13}$
			
$O_{1,7,13,19}$	$O_{13,19,1,7}$	$O_{1,7,13,19}$	$O_{19,13,7,1}$
			

Рис. 2.19 Перестановочні схеми для побудови таблиць істинності операцій НДО 1 на основі базової операції першої математичної групи

Отже, відповідно рисунку 2.19, маємо такі результати:

– для реалізації перестановочної схеми таблиці істинності базової операції в операцію $O_{7,1,19,13}$ необхідна попарна перестановка елементів $0 \leftrightarrow 1$, а також $2 \leftrightarrow 3$;

– для реалізації перестановочної схеми таблиці істинності базової операції в операцію $O_{13,19,1,7}$ необхідна попарна перестановка елементів $0 \leftrightarrow 2$, а також $1 \leftrightarrow 3$;

– для реалізації перестановочної схеми таблиці істинності базової операції в операцію $O_{19,13,7,1}$ необхідна попарна перестановка елементів $0 \leftrightarrow 3$, а також $1 \leftrightarrow 2$.

Розглянемо другий набір двохоперандних операцій.

В результаті дослідження було встановлено, що побудова таблиць істинності операцій НДО 2 відбувається за рахунок одинарної перестановки в кожному стовпці таблиці істинності або циклічної поелементної перестановки всіх чотирьох елементів кожного стовпчики таблиці істинності. Крім того, перестановки в стовпцях по кожній операції не є однаковими, вони мають по два подібних варіанти, що чергуються між собою.

Результати побудови перестановочних схеми для побудови таблиць істинності операцій НДО 2 на основі базової операції першої математичної групи представлені на рисунку 2.20 [4].

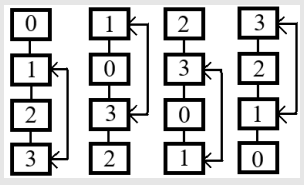
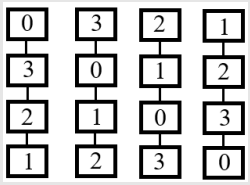
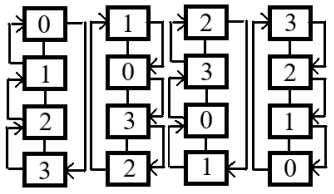
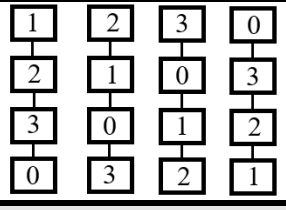
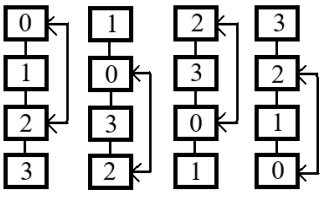
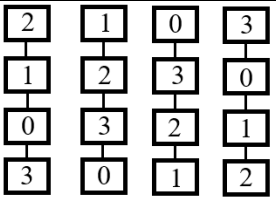
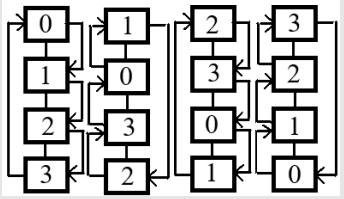
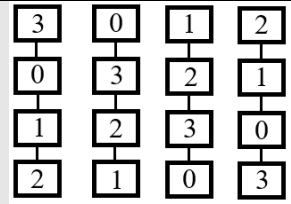
Схематичне представлення перестановочної схеми таблиці істинності базової операції	Схематичне представлення таблиці істинності отриманої операції	Схематичне представлення перестановочної схеми таблиці істинності базової операції	Схематичне представлення таблиці істинності отриманої операції
$O_{1,7,13,19}$	$O_{2,20,14,8}$	$O_{1,7,13,19}$	$O_{8,14,20,2}$
			
$O_{1,7,13,19}$	$O_{14,8,2,20}$	$O_{1,7,13,19}$	$O_{20,2,8,14}$
			

Рис. 2.20 Перестановочні схеми для побудови таблиць істинності операцій НДО 2 на основі базової операції першої математичної групи

Згідно даних, наведених на рисунку 2.20, маємо наступне:

– для реалізації перестановочної схеми таблиці істинності базової операції в операцію $O_{2,20,14,8}$ необхідна одинарна перестановка елементів $1 \leftrightarrow 3$;

– для реалізації перестановочної схеми таблиці істинності базової операції в операцію $O_{8,14,20,2}$ необхідна циклічна перестановка чотирьох елементів $0 \to 3 \to 2 \to 1 \to 0$;

– для реалізації перестановочної схеми таблиці істинності базової операції в операцію $O_{14,8,2,20}$ необхідна одинарна перестановка елементів $0 \leftrightarrow 2$;

– для реалізації перестановочної схеми таблиці істинності базової операції в операцію $O_{20,2,8,14}$ необхідна циклічна перестановка чотирьох елементів $0 \to 1 \to 2 \to 3 \to 0$.

Розглянемо третій набір двохоперандних операцій.

Результати побудови перестановочних схеми для побудови таблиць істинності операцій НДО 3 на основі базової операції першої математичної групи представлені на рисунку 2.21 [4].

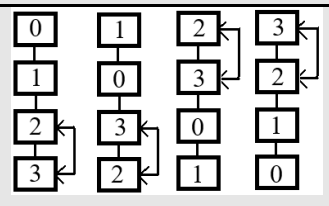
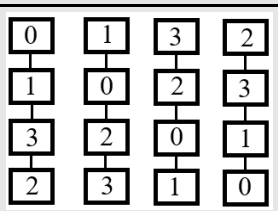
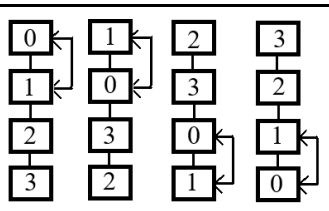
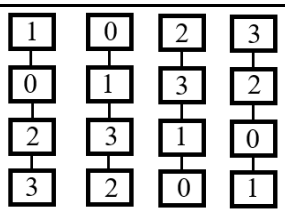
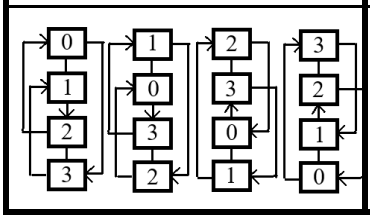
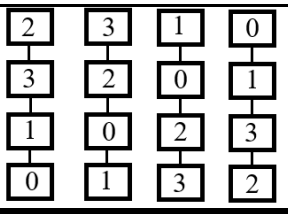
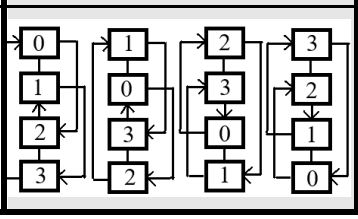
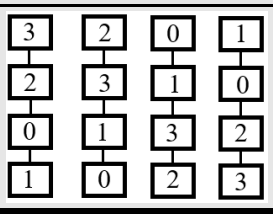
Схематичне представлення перестановочної схеми таблиці істинності базової операції	Схематичне представлення таблиці істинності отриманої операції	Схематичне представлення перестановочної схеми таблиці істинності базової операції	Схематичне представлення таблиці істинності отриманої операції
$O_{1,7,13,19}$	$O_{3,9,21,15}$	$O_{1,7,13,19}$	$O_{9,3,15,21}$
			
$O_{1,7,13,19}$	$O_{15,21,9,3}$	$O_{1,7,13,19}$	$O_{21,15,3,9}$
			

Рис. 2.21 Перестановочні схеми для побудови таблиць істинності операцій НДО 3 на основі базової операції першої математичної групи

Таким чином, відповідно до рисунка 2.21, маємо такі результати:

– для реалізації перестановочної схеми таблиці істинності базової операції в операцію $O_{3,9,21,15}$ необхідна одинарна перестановка елементів $2 \leftrightarrow 3$;

– для реалізації перестановочної схеми таблиці істинності базової операції в операцію $O_{9,3,15,21}$ необхідна одинарна перестановка елементів $0 \leftrightarrow 1$;

– для реалізації перестановочної схеми таблиці істинності базової операції в операцію $O_{15,21,9,3}$ необхідна циклічна перестановка чотирьох елементів $0 \to 3 \to 1 \to 2 \to 0$;

– для реалізації перестановочної схеми таблиці істинності базової операції в операцію $O_{21,15,3,9}$ необхідна циклічна перестановка чотирьох елементів $0 \to 2 \to 1 \to 3 \to 0$.

Розглянемо четвертий набір двохоперандних операцій.

Перестановочні схеми для побудови таблиць істинності операцій НДО 4 на основі базової операції першої математичної групи представлені на рисунку 2.22.

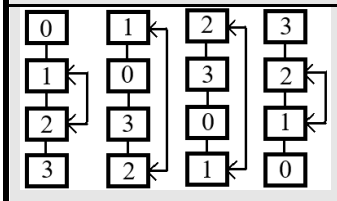
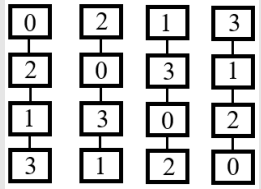
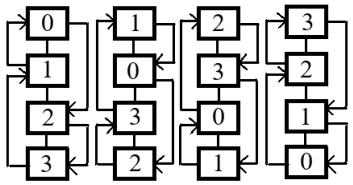
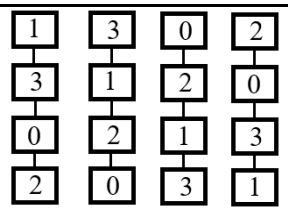
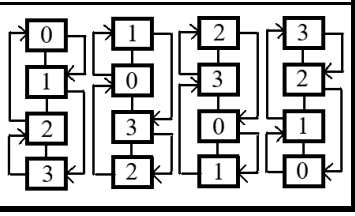
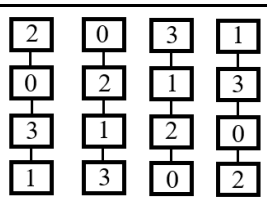
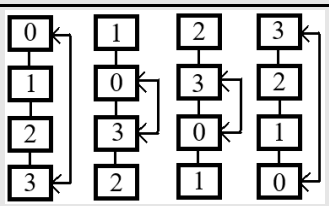
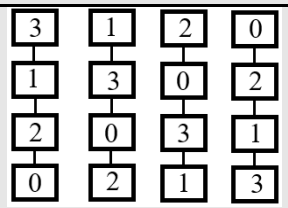
Схематичне представлення перестановочної схеми таблиці істинності базової операції	Схематичне представлення таблиці істинності отриманої операції	Схематичне представлення перестановочної схеми таблиці істинності базової операції	Схематичне представлення таблиці істинності отриманої операції
$O_{1,7,13,19}$	$O_{4,16,10,22}$	$O_{1,7,13,19}$	$O_{10,22,4,16}$
			
$O_{1,7,13,19}$	$O_{16,4,22,10}$	$O_{1,7,13,19}$	$O_{22,10,16,4}$
			

Рис. 2.22 Перестановочні схеми для побудови таблиць істинності операцій НДО 4 на основі базової операції першої математичної групи

Отже, на рисунку 2.22 представлені такі результати [4]:

– для реалізації перестановочної схеми таблиці істинності базової операції в операцію $O_{4,16,10,22}$ необхідна одинарна перестановка елементів $1 \leftrightarrow 2$;

– для реалізації перестановочної схеми таблиці істинності базової операції в операцію $O_{10,22,4,16}$ необхідна циклічна перестановка чотирьох елементів $0 \to 2 \to 3 \to 1 \to 0$;

– для реалізації перестановочної схеми таблиці істинності базової операції в операцію $O_{16,4,22,10}$ необхідна циклічна перестановка чотирьох елементів $0 \to 1 \to 3 \to 2 \to 0$;

– для реалізації перестановочної схеми таблиці істинності базової операції в операцію $O_{22,10,16,4}$ необхідна одинарна перестановка елементів $0 \leftrightarrow 3$.

Розглянемо п’ятий набір двохоперандних операцій.

Перестановочні схеми для побудови таблиць істинності операцій НДО 5 на основі базової операції першої математичної групи представлені на рисунку 2.23.

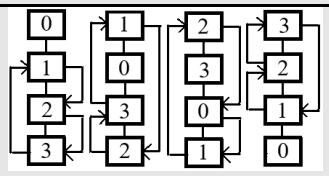
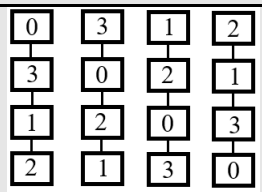
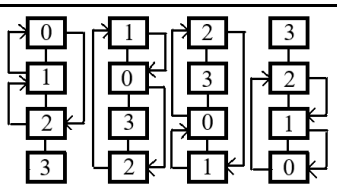
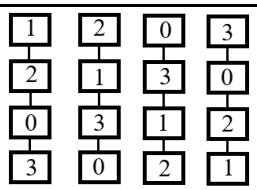
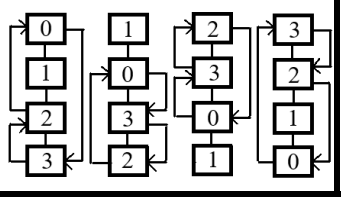
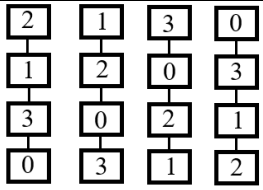
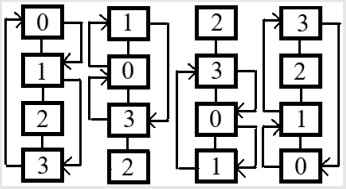
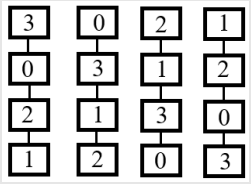
Схематичне представлення перестановочної схеми таблиці істинності базової операції	Схематичне представлення таблиці істинності отриманої операції	Схематичне представлення перестановочної схеми таблиці істинності базової операції	Схематичне представлення таблиці істинності отриманої операції
$O_{1,7,13,19}$	$O_{5,23,11,17}$	$O_{1,7,13,19}$	$O_{11,17,5,23}$
			
$O_{1,7,13,19}$	$O_{17,11,23,5}$	$O_{1,7,13,19}$	$O_{23,5,17,11}$
			

Рис. 2.23 Перестановочні схеми для побудови таблиць істинності операцій НДО 5 на основі базової операції першої математичної групи

Відповідно до рисунка 2.23, маємо такі результати:

– для реалізації перестановочної схеми таблиці істинності базової операції в операцію $O_{5,23,11,17}$ необхідна циклічна перестановка трьох елементів $1 \to 2 \to 3 \to 1$ (елемент 0 залишається без змін);

– для реалізації перестановочної схеми таблиці істинності базової операції в операцію $O_{11,17,5,23}$ необхідна циклічна перестановка трьох елементів $0 \to 2 \to 1 \to 0$ (елемент 3 залишається без змін);

– для реалізації перестановочної схеми таблиці істинності базової операції в операцію $O_{17,11,23,5}$ необхідна циклічна перестановка трьох елементів $0 \to 3 \to 2 \to 0$ (елемент 1 залишається без змін);

– для реалізації перестановочної схеми таблиці істинності базової операції в операцію $O_{23,5,17,11}$ необхідна циклічна перестановка трьох елементів $0 \to 1 \to 3 \to 0$ (елемент 2 залишається без змін);

Розглянемо шостий набір двохоперандних операцій.

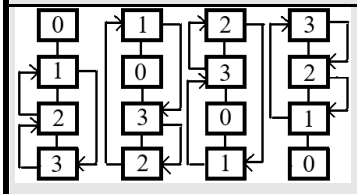
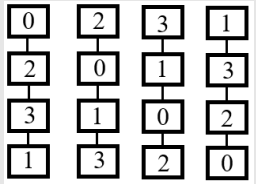
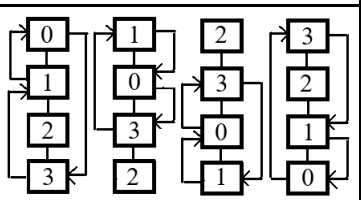
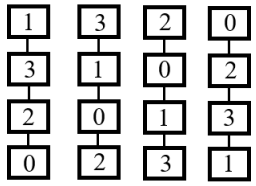
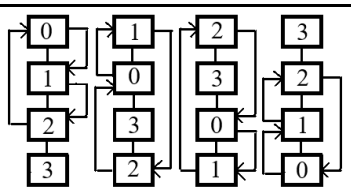
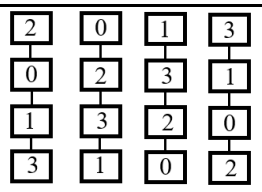
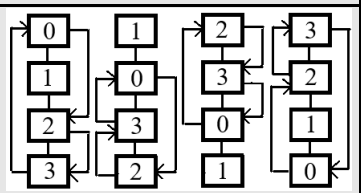
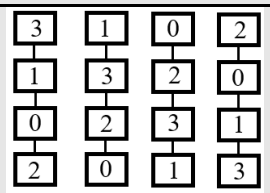
Схематичне представлення перестановочної схеми таблиці істинності базової операції	Схематичне представлення таблиці істинності отриманої операції	Схематичне представлення перестановочної схеми таблиці істинності базової операції	Схематичне представлення таблиці істинності отриманої операції
$O_{1,7,13,19}$	$O_{6,18,24,12}$	$O_{1,7,13,19}$	$O_{12,24,18,6}$
			
$O_{1,7,13,19}$	$O_{18,6,12,24}$	$O_{1,7,13,19}$	$O_{24,12,6,18}$
			

Рис. 2.24 Перестановочні схеми для побудови таблиць істинності операцій НДО 6 на основі базової операції першої математичної групи

Результати побудови перестановочних схеми для побудови таблиць істинності операцій НДО 6 на основі базової операції першої математичної групи представлені на рисунку 2.24 [4].

Таким чином, згідно з рисунком 2.24 маємо такі результати:

– для реалізації перестановочної схеми таблиці істинності базової операції в операцію $O_{6,18,24,12}$ необхідна циклічна перестановка трьох елементів $1 \to 3 \to 2 \to 1$ (елемент 0 залишається без змін);

– для реалізації перестановочної схеми таблиці істинності базової операції в операцію $O_{12,24,18,6}$ необхідна циклічна перестановка трьох елементів $0 \to 3 \to 1 \to 0$ (елемент 2 залишається без змін);

– для реалізації перестановочної схеми таблиці істинності базової операції в операцію $O_{18,6,12,24}$ необхідна циклічна перестановка трьох елементів $0 \to 1 \to 2 \to 0$ (елемент 3 залишається без змін);

– для реалізації перестановочної схеми таблиці істинності базової операції в операцію $O_{24,12,6,18}$ необхідна циклічна перестановка трьох елементів $0 \to 2 \to 3 \to 0$ (елемент 1 залишається без змін).

Узагальнимо отримані результати.

- В процесі дослідження було встановлено, що перестановочні схеми побудови таблиць істинності наборів двохоперандних операцій криптоперетворення першої математичної групи не перетинаються.
- Сукупність наборів таблиць істинності двохоперандних операцій криптоперетворення першої математичної групи створюють повну групу наборів таблиць істинності двохоперандних операцій криптоперетворення.
- Застосування цієї групи перестановочних схем забезпечує побудову повної групи операцій криптоперетворення на основі будь-якої з операцій цієї групи.
- Застосування цієї групи перестановочних схем забезпечує побудову повної групи таблиць підстановок.

Отримані результати дозволяють зробити припущення, що застосування побудованої групи перестановочних схем забезпечить побудову повної групи наборів двохоперандних операцій криптоперетворення невідомої групи, якщо взяти будь-яку операцію з цієї невідомої групи.

Висновки з розділу 2

1. Для забезпечення ефективності проведення досліджень проаналізовано та класифіковано напрями дослідження і синтезу двохоперандних операцій криптоперетворення. Встановлено, що поєднання одноопераднних операцій крипторперетворення в двохоперандні забезпечує збільшення невизначеності результатів потокового шифрування та збільшення варіативності алгоритму перетворення, порівняно з операціями, синтезованими на основі додавання за модулем два з точністю до перестановки. Встановлено, що складність моделей двохоперандних операцій, синтезованих на основі поєднання одноопераднних, значно більша складності двохоперандних перестановочних операцій.

2. Для зменшення складності моделей двохоперандних операцій, синтезованих на основі поєднання одноопераднних операцій, запропоновано технологію дослідження двохоперандних операцій криптоперетворення, яка включає в себе послідовність перетворень поєднаних одноопераднних операцій, для отримання узагальненої моделі меншої складності та побудову перестановочних схем таблиці істинності для синтезу операцій з подібними властивостями.

3. Застосування запропонованої технології дослідження двохоперандних операцій криптоперетворення стосовно першої групи операцій, синтезованих на основі обчислювального експерименту, дозволило побудувати першу групу узагальнених моделей симетричних двохоперандних операцій криптографічного перетворення інформації, придатних для застосування при побудові блокових і потокових шифрів.

4. Встановлені перестановочні схеми побудови таблиць істинності наборів двохоперандних операцій криптоперетворення першої групи не перетинаються і створюють повну групу наборів таблиць істинності двохоперандних операцій криптоперетворення. Застосування цієї групи перестановочних схем забезпечує побудову повної групи операцій криптоперетворення на основі будь-якої з операцій цієї групи, а також забезпечує побудову повної групи таблиць підстановок.

5. Зроблено припущення, що застосування побудованої групи перестановочних схем забезпечить побудову повної групи наборів двохоперандних операцій криптоперетворення невідомої групи, якщо взяти будь-яку операцію з невідомої групи.

Матеріали розділу опубліковано в [1, 2, 4, 10, 12].

РОЗДІЛ 3 ДОСЛІДЖЕННЯ ДРУГОЇ МАТЕМАТИЧНОЇ ГРУПИ ДВОХОПЕРАНДНИХ ОПЕРАЦІЙ КРИПТОПЕРЕТВОРЕННЯ

3.1 Дослідження першого набору двохоперандних операцій криптоперетворення другої математичної групи (НДО 7)

Розглянемо другу симетричну групу двохоперандних операцій криптоперетворення. Ця група представлена такими наборами операцій як НДО 7, НДО 8, НДО 9, НДО 10, НДО 11 та НДО 12.

Розглянемо сьомий набір двохоперандних операцій.

Операція $O_{1,8,13,20}$ є першою в цьому наборі й умовно буде основною. На основі цієї операції $O_{1,8,13,20}$ за рахунок перестановок будуються інші операції цього набору [2].

Розглянемо таблично формування операції сьомого набору операцій порозрядного додавання за модулем два із точністю до перестановки, що включає в себе операції: $O_{1,8,13,20}$, $O_{8,13,20,1}$, $O_{13,20,1,8}$, $O_{20,1,8,13}$.

Результати побудови цих операцій наведено в табл. 3.1.

Таблиця 3.1

Сьомий набір двохоперандних операцій порозрядного додавання за модулем два

Операція	$O_{1,8,13,20}$				$O_{8,13,20,1}$				$O_{13,20,1,8}$				$O_{20,1,8,13}$			
Значення операндів	**0**	**1**	**2**	**3**	**0**	**1**	**2**	**3**	**0**	**1**	**2**	**3**	**0**	**1**	**2**	**3**
0	**0**	**1**	**2**	**3**	**1**	**2**	**3**	**0**	**2**	**3**	**0**	**1**	**3**	**0**	**1**	**2**
1	**1**	**2**	**3**	**0**	**2**	**3**	**0**	**1**	**3**	**0**	**1**	**2**	**0**	**1**	**2**	**3**
2	**2**	**3**	**0**	**1**	**3**	**0**	**1**	**2**	**0**	**1**	**2**	**3**	**1**	**2**	**3**	**0**
3	**3**	**0**	**1**	**2**	**0**	**1**	**2**	**3**	**1**	**2**	**3**	**0**	**2**	**3**	**0**	**1**
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**				**0=3, 1=2, 2=1, 3=0**			

Розглянемо більш детально результати моделювання сьомого набору двохоперандних операцій, представивши їх математичними моделями [6].

Математична модель основної операції сьомого набору двохоперандних операцій $O_{1,8,13,20}$ матиме вигляд:

$$O_{1,8,13,20}=\begin{cases}\begin{bmatrix}x_1\\x_2\end{bmatrix}, \textit{якщо } k_1=0;\ k_2=0\\ \begin{bmatrix}x_1\oplus x_2\\x_2\oplus 1\end{bmatrix}, \textit{якщо } k_1=0;\ k_2=1\\ \begin{bmatrix}x_1\oplus 1\\x_2\end{bmatrix}, \textit{якщо } k_1=1;\ k_2=0\\ \begin{bmatrix}x_1\oplus x_2\oplus 1\\x_2\oplus 1\end{bmatrix}, \textit{якщо } k_1=1;\ k_2=1\end{cases}=\begin{cases}\begin{bmatrix}x_1\\x_2\end{bmatrix}=\begin{bmatrix}x_1\oplus x_2\cdot k_2\oplus k_1\\x_2\oplus k_2\end{bmatrix}, \textit{якщо } k_1=0;\ k_2=0\\ \begin{bmatrix}x_1\oplus x_2\\x_2\oplus 1\end{bmatrix}=\begin{bmatrix}x_1\oplus x_2\cdot k_2\oplus k_1\\x_2\oplus k_2\end{bmatrix}, \textit{якщо } k_1=0;\ k_2=1\\ \begin{bmatrix}x_1\oplus 1\\x_2\end{bmatrix}=\begin{bmatrix}x_1\oplus x_2\cdot k_2\oplus k_1\\x_2\oplus k_2\end{bmatrix}, \textit{якщо } k_1=1;\ k_2=0\\ \begin{bmatrix}x_1\oplus x_2\oplus 1\\x_2\oplus 1\end{bmatrix}=\begin{bmatrix}x_1\oplus x_2\cdot k_2\oplus k_1\\x_2\oplus k_2\end{bmatrix}, \textit{якщо } k_1=1;\ k_2=1\end{cases}$$

Таким чином, операцію $O_{1,8,13,20}$ можна записати як:

$$O_{1,8,13,20}=\begin{cases}\begin{bmatrix}x_1\\x_2\end{bmatrix}=\begin{bmatrix}x_1\oplus x_2\cdot k_2\oplus k_1\\x_2\oplus k_2\end{bmatrix}, \textit{якщо } k_1=0;\ k_2=0\\ \begin{bmatrix}x_1\oplus x_2\\x_2\oplus 1\end{bmatrix}=\begin{bmatrix}x_1\oplus x_2\cdot k_2\oplus k_1\\x_2\oplus k_2\end{bmatrix}, \textit{якщо } k_1=0;\ k_2=1\\ \begin{bmatrix}x_1\oplus 1\\x_2\end{bmatrix}=\begin{bmatrix}x_1\oplus x_2\cdot k_2\oplus k_1\\x_2\oplus k_2\end{bmatrix}, \textit{якщо } k_1=1;\ k_2=0\\ \begin{bmatrix}x_1\oplus x_2\oplus 1\\x_2\oplus 1\end{bmatrix}=\begin{bmatrix}x_1\oplus x_2\cdot k_2\oplus k_1\\x_2\oplus k_2\end{bmatrix}, \textit{якщо } k_1=1;\ k_2=1\end{cases}=\begin{bmatrix}x_1\oplus x_2\cdot k_2\oplus k_1\\x_2\oplus k_2\end{bmatrix}$$

Математичну модель операції $O_{8,13,20,1}$, що є синтезованою на основі моделі операції $O_{1,8,13,20}$ сьомого НДО, представлено у вигляді:

$$O_{8,13,20,1}=\begin{cases}\begin{bmatrix}x_1\oplus x_2\\x_2\oplus 1\end{bmatrix}, \textit{якщо } k_1=0;\ k_2=0\\ \begin{bmatrix}x_1\oplus 1\\x_2\end{bmatrix}, \textit{якщо } k_1=0;\ k_2=1\\ \begin{bmatrix}x_1\oplus x_2\oplus 1\\x_2\oplus 1\end{bmatrix}, \textit{якщо } k_1=1;\ k_2=0\\ \begin{bmatrix}x_1\\x_2\end{bmatrix}, \textit{якщо } k_1=1;\ k_2=1\end{cases}=\begin{cases}\begin{bmatrix}x_1\oplus x_2\\x_2\oplus 1\end{bmatrix}=\begin{bmatrix}x_1\oplus x_2\oplus x_2\cdot k_2\oplus k_1\\x_2\oplus k_2\oplus 1\end{bmatrix}, \textit{якщо } k_1=0;\ k_2=0\\ \begin{bmatrix}x_1\oplus 1\\x_2\end{bmatrix}=\begin{bmatrix}x_1\oplus x_2\oplus x_2\cdot k_2\oplus k_1\\x_2\oplus k_2\oplus 1\end{bmatrix}, \textit{якщо } k_1=0;\ k_2=1\\ \begin{bmatrix}x_1\oplus x_2\oplus 1\\x_2\oplus 1\end{bmatrix}=\begin{bmatrix}x_1\oplus x_2\oplus x_2\cdot k_2\oplus k_1\\x_2\oplus k_2\oplus 1\end{bmatrix}, \textit{якщо } k_1=1;\ k_2=0\\ \begin{bmatrix}x_1\\x_2\end{bmatrix}=\begin{bmatrix}x_1\oplus x_2\oplus x_2\cdot k_2\oplus k_1\\x_2\oplus k_2\oplus 1\end{bmatrix}, \textit{якщо } k_1=1;\ k_2=1\end{cases}$$

Отже, операцію $O_{8,13,20,1}$ можна записати як:

$$O_{8,13,20,1}=\begin{cases}\begin{bmatrix}x_1\oplus x_2\\ x_2\oplus 1\end{bmatrix}=\begin{bmatrix}x_1\oplus x_2\oplus x_2\cdot k_2\oplus k_1\\ x_2\oplus k_2\oplus 1\end{bmatrix}, \text{ якщо } k_1=0;\ k_2=0\\ \begin{bmatrix}x_1\oplus 1\\ x_2\end{bmatrix}=\begin{bmatrix}x_1\oplus x_2\oplus x_2\cdot k_2\oplus k_1\\ x_2\oplus k_2\oplus 1\end{bmatrix}, \text{ якщо } k_1=0;\ k_2=1\\ \begin{bmatrix}x_1\oplus x_2\oplus 1\\ x_2\oplus 1\end{bmatrix}=\begin{bmatrix}x_1\oplus x_2\oplus x_2\cdot k_2\oplus k_1\\ x_2\oplus k_2\oplus 1\end{bmatrix}, \text{ якщо } k_1=1;\ k_2=0\\ \begin{bmatrix}x_1\\ x_2\end{bmatrix}=\begin{bmatrix}x_1\oplus x_2\oplus x_2\cdot k_2\oplus k_1\\ x_2\oplus k_2\oplus 1\end{bmatrix}, \text{ якщо } k_1=1;\ k_2=1\end{cases}=\begin{bmatrix}x_1\oplus x_2\cdot\bar{k}_2\oplus k_1\oplus k_2\\ x_2\oplus k_2\oplus 1\end{bmatrix}$$

Перестановочна схема побудови цієї операції представлена на рис. 3.1.

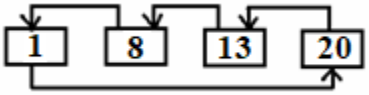
Схематичне представлення основної операції НДО 7	Перестановочна схема	Схематичне представлення отриманої операції $O_{8,13,20,1}$
1 8 13 20		8 13 20 1

Рис. 3.1 Перестановочна схема для побудови операції $O_{8,13,20,1}$ на основі основної операції сьомого НДО $O_{1,8,13,20}$

Математична модель операції $O_{13,20,1,8}$, що є синтезованою на основі моделі основної операції $O_{1,8,13,20}$ сьомого НДО, матиме вигляд:

$$O_{13,20,1,8}=\begin{cases}\begin{bmatrix}x_1\oplus 1\\ x_2\end{bmatrix}, \text{ якщо } k_1=0;\ k_2=0\\ \begin{bmatrix}x_1\oplus x_2\oplus 1\\ x_2\oplus 1\end{bmatrix}, \text{ якщо } k_1=0;\ k_2=1\\ \begin{bmatrix}x_1\\ x_2\end{bmatrix}, \text{ якщо } k_1=1;\ k_2=0\\ \begin{bmatrix}x_1\oplus x_2\\ x_2\oplus 1\end{bmatrix}, \text{ якщо } k_1=1;\ k_2=1\end{cases}=\begin{cases}\begin{bmatrix}x_1\oplus 1\\ x_2\end{bmatrix}=\begin{bmatrix}x_1\oplus x_2\cdot k_2\oplus k_1\oplus 1\\ x_2\oplus k_2\end{bmatrix}, \text{ якщо } k_1=0;\ k_2=0\\ \begin{bmatrix}x_1\oplus x_2\oplus 1\\ x_2\oplus 1\end{bmatrix}=\begin{bmatrix}x_1\oplus x_2\cdot k_2\oplus k_1\oplus 1\\ x_2\oplus k_2\end{bmatrix}, \text{ якщо } k_1=0;\ k_2=1\\ \begin{bmatrix}x_1\\ x_2\end{bmatrix}=\begin{bmatrix}x_1\oplus x_2\cdot k_2\oplus k_1\oplus 1\\ x_2\oplus k_2\end{bmatrix}, \text{ якщо } k_1=1;\ k_2=0\\ \begin{bmatrix}x_1\oplus x_2\\ x_2\oplus 1\end{bmatrix}=\begin{bmatrix}x_1\oplus x_2\cdot k_2\oplus k_1\oplus 1\\ x_2\oplus k_2\end{bmatrix}, \text{ якщо } k_1=1;\ k_2=1\end{cases}$$

Відповідно, операцію $O_{13,20,1,8}$ можна записати як:

$$O_{13,20,1,8}=\begin{cases}\begin{bmatrix}x_1\oplus 1\\ x_2\end{bmatrix}=\begin{bmatrix}x_1\oplus x_2\cdot k_2\oplus k_1\oplus 1\\ x_2\oplus k_2\end{bmatrix}, \text{ якщо } k_1=0;\ k_2=0\\ \begin{bmatrix}x_1\oplus x_2\oplus 1\\ x_2\oplus 1\end{bmatrix}=\begin{bmatrix}x_1\oplus x_2\cdot k_2\oplus k_1\oplus 1\\ x_2\oplus k_2\end{bmatrix}, \text{ якщо } k_1=0;\ k_2=1\\ \begin{bmatrix}x_1\\ x_2\end{bmatrix}=\begin{bmatrix}x_1\oplus x_2\cdot k_2\oplus k_1\oplus 1\\ x_2\oplus k_2\end{bmatrix}, \text{ якщо } k_1=1;\ k_2=0\\ \begin{bmatrix}x_1\oplus x_2\\ x_2\oplus 1\end{bmatrix}=\begin{bmatrix}x_1\oplus x_2\cdot k_2\oplus k_1\oplus 1\\ x_2\oplus k_2\end{bmatrix}, \text{ якщо } k_1=1;\ k_2=1\end{cases}=\begin{bmatrix}x_1\oplus x_2\cdot k_2\oplus k_1\oplus 1\\ x_2\oplus k_2\end{bmatrix}$$

Перестановочна схема побудови цієї операції представлена на рис. 3.2.

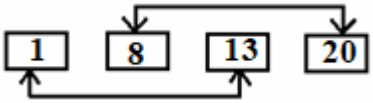
Схематичне представлення основної операції НДО 7	Перестановочна схема	Схематичне представлення отриманої операції $O_{13,20,1,8}$
		

Рис. 3.2 Перестановочна схема для побудови операції $O_{13,20,1,8}$ на основі основної операції сьомого НДО $O_{1,8,13,20}$

Математичну модель операції $O_{20,1,8,13}$, що є синтезованою на основі моделі операції $O_{1,8,13,20}$ сьомого набору двохоперандних операцій, представимо у вигляді [6]:

$$O_{20,1,8,13}=\begin{cases}\begin{bmatrix}x_1\oplus x_2\oplus 1\\ x_2\oplus 1\end{bmatrix}, \text{ якщо } k_1=0;\ k_2=0\\ \begin{bmatrix}x_1\\ x_2\end{bmatrix}, \text{ якщо } k_1=0;\ k_2=1\\ \begin{bmatrix}x_1\oplus x_2\\ x_2\oplus 1\end{bmatrix}, \text{ якщо } k_1=1;\ k_2=0\\ \begin{bmatrix}x_1\oplus 1\\ x_2\end{bmatrix}, \text{ якщо } k_1=1;\ k_2=1\end{cases}=\begin{cases}\begin{bmatrix}x_1\oplus x_2\oplus 1\\ x_2\oplus 1\end{bmatrix}=\begin{bmatrix}x_1\oplus x_2\oplus x_2\cdot k_2\oplus k_1\oplus k_2\oplus 1\\ x_2\oplus k_2\oplus 1\end{bmatrix}, \text{ якщо } k_1=0;\ k_2=0\\ \begin{bmatrix}x_1\\ x_2\end{bmatrix}=\begin{bmatrix}x_1\oplus x_2\oplus x_2\cdot k_2\oplus k_1\oplus k_2\oplus 1\\ x_2\oplus k_2\oplus 1\end{bmatrix}, \text{ якщо } k_1=0;\ k_2=1\\ \begin{bmatrix}x_1\oplus x_2\\ x_2\oplus 1\end{bmatrix}=\begin{bmatrix}x_1\oplus x_2\oplus x_2\cdot k_2\oplus k_1\oplus k_2\oplus 1\\ x_2\oplus k_2\oplus 1\end{bmatrix}, \text{ якщо } k_1=1;\ k_2=0\\ \begin{bmatrix}x_1\oplus 1\\ x_2\end{bmatrix}=\begin{bmatrix}x_1\oplus x_2\oplus x_2\cdot k_2\oplus k_1\oplus k_2\oplus 1\\ x_2\oplus k_2\oplus 1\end{bmatrix}, \text{ якщо } k_1=1;\ k_2=1\end{cases}$$

Таким чином, операцію $O_{20,1,8,13}$ можна записати як [2]:

$$O_{20,1,8,13}=\begin{cases}\begin{bmatrix}x_1\oplus x_2\oplus 1\\ x_2\oplus 1\end{bmatrix}=\begin{bmatrix}x_1\oplus x_2\oplus x_2\cdot k_2\oplus k_1\oplus k_2\oplus 1\\ x_2\oplus k_2\oplus 1\end{bmatrix}, \text{ якщо } k_1=0;\ k_2=0\\ \begin{bmatrix}x_1\\ x_2\end{bmatrix}=\begin{bmatrix}x_1\oplus x_2\oplus x_2\cdot k_2\oplus k_1\oplus k_2\oplus 1\\ x_2\oplus k_2\oplus 1\end{bmatrix}, \text{ якщо } k_1=0;\ k_2=1\\ \begin{bmatrix}x_1\oplus x_2\\ x_2\oplus 1\end{bmatrix}=\begin{bmatrix}x_1\oplus x_2\oplus x_2\cdot k_2\oplus k_1\oplus k_2\oplus 1\\ x_2\oplus k_2\oplus 1\end{bmatrix}, \text{ якщо } k_1=1;\ k_2=0\\ \begin{bmatrix}x_1\oplus 1\\ x_2\end{bmatrix}=\begin{bmatrix}x_1\oplus x_2\oplus x_2\cdot k_2\oplus k_1\oplus k_2\oplus 1\\ x_2\oplus k_2\oplus 1\end{bmatrix}, \text{ якщо } k_1=1;\ k_2=1\end{cases}=\begin{bmatrix}x_1\oplus x_2\cdot\bar{k}_2\oplus k_1\oplus k_2\oplus 1\\ x_2\oplus k_2\oplus 1\end{bmatrix}$$

Перестановочна схема для побудови операції $O_{20,1,8,13}$ на основі основної операції сьомого НДО $O_{1,8,13,20}$ наведена на рис. 3.3

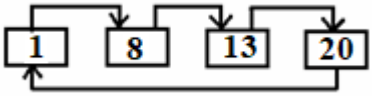
Схематичне представлення основної операції НДО 7	Перестановочна схема	Схематичне представлення отриманої операції $O_{20,1,8,13}$
		

Рис. 3.3 Перестановочна схема для побудови операції $O_{20,1,8,13}$ на основі основної операції сьомого НДО $O_{1,8,13,20}$

3.2 Дослідження другого набору двохоперандних операцій криптоперетворення другої математичної групи (НДО 8)

Розглянемо восьмий набір двохоперандних операцій.

Операція $O_{2,19,14,7}$ є першою в цьому наборі і умовно буде основною. На основі операції $O_{2,19,14,7}$ за рахунок перестановок будуються інші операції цього набору [2].

Розглянемо таблично формування операції восьмого набору операцій порозрядного додавання за модулем два із точністю до перестановки, що включає в себе операції: $O_{2,19,14,7}$, $O_{7,2,19,14}$, $O_{14,7,2,19}$, $O_{19,14,7,2}$.

Результати побудови цих операцій наведено в табл. 3.2.

Таблиця 3.2

Восьмий набір двохоперандних операцій порозрядного додавання за модулем два

Операція	$O_{2,19,14,7}$				$O_{7,2,19,14}$				$O_{14,7,2,19}$				$O_{19,14,7,2}$			
Значення операндів	**0**	**1**	**2**	**3**	**0**	**1**	**2**	**3**	**0**	**1**	**2**	**3**	**0**	**1**	**2**	**3**
0	0	3	2	1	1	0	3	2	2	1	0	3	3	2	1	0
1	3	2	1	0	0	3	2	1	1	0	3	2	2	1	0	3
2	2	1	0	3	3	2	1	0	0	3	2	1	1	0	3	2
3	1	0	3	2	2	1	0	3	3	2	1	0	0	3	2	1
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**				**0=3, 1=2, 2=1, 3=0**			

Розглянемо більш детально результати моделювання восьмого набору двохоперандних операцій, представивши їх математичними моделями [6].

Математична модель основної операції восьмого набору двохоперандних операцій $O_{2,19,14,7}$ матиме вигляд:

$$O_{2,19,14,7}=\begin{cases}\begin{bmatrix}x_1\oplus x_2\\ x_2\end{bmatrix}, \text{ якщо } k_1=0;\ k_2=0\\ \begin{bmatrix}x_1\oplus 1\\ x_2\oplus 1\end{bmatrix}, \text{якщо } k_1=0;\ k_2=1\\ \begin{bmatrix}x_1\oplus x_2\oplus 1\\ x_2\end{bmatrix}, \text{ якщо } k_1=1;\ k_2=0\\ \begin{bmatrix}x_1\\ x_2\oplus 1\end{bmatrix}, \text{якщо } k_1=1;\ k_2=1\end{cases}=\begin{cases}\begin{bmatrix}x_1\oplus x_2\\ x_2\end{bmatrix}=\begin{bmatrix}x_1\oplus x_2\oplus k_1\oplus k_2\\ x_2\oplus k_2\end{bmatrix}, \text{ якщо } k_1=0;\ k_2=0\\ \begin{bmatrix}x_1\oplus x_2\oplus 1\\ x_2\oplus 1\end{bmatrix}=\begin{bmatrix}x_1\oplus x_2\oplus k_1\oplus k_2\\ x_2\oplus k_2\end{bmatrix}, \text{якщо } k_1=0;\ k_2=1\\ \begin{bmatrix}x_1\oplus x_2\oplus 1\\ x_2\end{bmatrix}=\begin{bmatrix}x_1\oplus x_2\oplus k_1\oplus k_2\\ x_2\oplus k_2\end{bmatrix}, \text{ якщо } k_1=1;\ k_2=0\\ \begin{bmatrix}x_1\oplus x_2\\ x_2\oplus 1\end{bmatrix}=\begin{bmatrix}x_1\oplus x_2\oplus k_1\oplus k_2\\ x_2\oplus k_2\end{bmatrix}, \text{якщо } k_1=1;\ k_2=1\end{cases}$$

Отже, операцію $O_{2,19,14,7}$ можна записати як:

$$O_{2,19,14,7}=\begin{cases}\begin{bmatrix}x_1\oplus x_2\\ x_2\end{bmatrix}=\begin{bmatrix}x_1\oplus x_2\oplus x_2\cdot k_2\oplus k_1\oplus k_2\\ x_2\oplus k_2\end{bmatrix}, \text{ якщо } k_1=0;\ k_2=0\\ \begin{bmatrix}x_1\oplus 1\\ x_2\oplus 1\end{bmatrix}=\begin{bmatrix}x_1\oplus x_2\oplus x_2\cdot k_2\oplus k_1\oplus k_2\\ x_2\oplus k_2\end{bmatrix}, \text{якщо } k_1=0;\ k_2=1\\ \begin{bmatrix}x_1\oplus x_2\oplus 1\\ x_2\end{bmatrix}=\begin{bmatrix}x_1\oplus x_2\oplus x_2\cdot k_2\oplus k_1\oplus k_2\\ x_2\oplus k_2\end{bmatrix}, \text{ якщо } k_1=1;\ k_2=0\\ \begin{bmatrix}x_1\\ x_2\oplus 1\end{bmatrix}=\begin{bmatrix}x_1\oplus x_2\oplus x_2\cdot k_2\oplus k_1\oplus k_2\\ x_2\oplus k_2\end{bmatrix}, \text{якщо } k_1=1;\ k_2=1\end{cases}=\begin{bmatrix}x_1\oplus x_2\cdot\bar{k}_2\oplus k_1\oplus k_2\\ x_2\oplus k_2\end{bmatrix}$$

Математичну модель операції $O_{7,2,19,14}$, що є синтезованою на основі моделі операції $O_{2,19,14,7}$ восьмого НДО, представимо у вигляді:

$$O_{7,2,19,14}=\begin{cases}\begin{bmatrix}x_1\\ x_2\oplus 1\end{bmatrix}, \text{ якщо } k_1=0;\ k_2=0\\ \begin{bmatrix}x_1\oplus x_2\\ x_2\end{bmatrix}, \text{якщо } k_1=0;\ k_2=1\\ \begin{bmatrix}x_1\oplus 1\\ x_2\oplus 1\end{bmatrix}, \text{ якщо } k_1=1;\ k_2=0\\ \begin{bmatrix}x_1\oplus x_2\oplus 1\\ x_2\end{bmatrix}, \text{якщо } k_1=1;\ k_2=1\end{cases}=\begin{cases}\begin{bmatrix}x_1\\ x_2\oplus 1\end{bmatrix}=\begin{bmatrix}x_1\oplus x_2\cdot k_2\oplus k_1\\ x_2\oplus k_2\oplus 1\end{bmatrix}, \text{ якщо } k_1=0;\ k_2=0\\ \begin{bmatrix}x_1\oplus x_2\\ x_2\end{bmatrix}=\begin{bmatrix}x_1\oplus x_2\cdot k_2\oplus k_1\\ x_2\oplus k_2\oplus 1\end{bmatrix}, \text{якщо } k_1=0;\ k_2=1\\ \begin{bmatrix}x_1\oplus 1\\ x_2\oplus 1\end{bmatrix}=\begin{bmatrix}x_1\oplus x_2\cdot k_2\oplus k_1\\ x_2\oplus k_2\oplus 1\end{bmatrix}, \text{ якщо } k_1=1;\ k_2=0\\ \begin{bmatrix}x_1\oplus x_2\oplus 1\\ x_2\end{bmatrix}=\begin{bmatrix}x_1\oplus x_2\cdot k_2\oplus k_1\\ x_2\oplus k_2\oplus 1\end{bmatrix}, \text{якщо } k_1=1;\ k_2=1\end{cases}$$

Таким чином, операцію $O_{7,2,19,14}$ можна записати як:

$$O_{7,2,19,14}=\begin{cases}\begin{bmatrix}x_1\\ x_2\oplus 1\end{bmatrix}=\begin{bmatrix}x_1\oplus x_2\cdot k_2\oplus k_1\\ x_2\oplus k_2\oplus 1\end{bmatrix}, \text{ якщо } k_1=0;\ k_2=0\\ \begin{bmatrix}x_1\oplus x_2\\ x_2\end{bmatrix}=\begin{bmatrix}x_1\oplus x_2\cdot k_2\oplus k_1\\ x_2\oplus k_2\oplus 1\end{bmatrix}, \text{якщо } k_1=0;\ k_2=1\\ \begin{bmatrix}x_1\oplus 1\\ x_2\oplus 1\end{bmatrix}=\begin{bmatrix}x_1\oplus x_2\cdot k_2\oplus k_1\\ x_2\oplus k_2\oplus 1\end{bmatrix}, \text{ якщо } k_1=1;\ k_2=0\\ \begin{bmatrix}x_1\oplus x_2\oplus 1\\ x_2\end{bmatrix}=\begin{bmatrix}x_1\oplus x_2\cdot k_2\oplus k_1\\ x_2\oplus k_2\oplus 1\end{bmatrix}, \text{якщо } k_1=1;\ k_2=1\end{cases}=\begin{bmatrix}x_1\oplus x_2\cdot k_2\oplus k_1\\ x_2\oplus k_2\oplus 1\end{bmatrix}$$

Перестановочна схема побудови цієї операції представлена на рис. 3.4.

Схематичне представлення основної операції НДО 8	Перестановочна схема	Схематичне представлення отриманої операції $O_{7,2,19,14}$
2 19 14 7	2 19 14 7	7 2 19 14

Рис. 3.4 Перестановочна схема для побудови операції $O_{7,2,19,14}$ на основі основної операції восьмого НДО $O_{2,19,14,7}$

Математична модель операції $O_{14,7,2,19}$, що є синтезованою на основі моделі основної операції $O_{2,19,14,7}$ восьмого набору двохоперандних операцій, матиме вигляд:

$$O_{14,7,2,19}=\begin{cases}\begin{bmatrix}x_1\oplus x_2\oplus 1\\ x_2\end{bmatrix}, \text{ якщо } k_1=0;\ k_2=0\\ \begin{bmatrix}x_1\\ x_2\oplus 1\end{bmatrix}, \text{якщо } k_1=0;\ k_2=1\\ \begin{bmatrix}x_1\oplus x_2\\ x_2\end{bmatrix}, \text{ якщо } k_1=1;\ k_2=0\\ \begin{bmatrix}x_1\oplus 1\\ x_2\oplus 1\end{bmatrix}, \text{якщо } k_1=1;\ k_2=1\end{cases}=\begin{cases}\begin{bmatrix}x_1\oplus x_2\oplus 1\\ x_2\end{bmatrix}=\begin{bmatrix}x_1\oplus x_2\oplus x_2\cdot k_2\oplus k_1\oplus k_2\oplus 1\\ x_2\oplus k_2\end{bmatrix}, \text{ якщо } k_1=0;\ k_2=0\\ \begin{bmatrix}x_1\\ x_2\oplus 1\end{bmatrix}=\begin{bmatrix}x_1\oplus x_2\oplus x_2\cdot k_2\oplus k_1\oplus k_2\oplus 1\\ x_2\oplus k_2\end{bmatrix}, \text{якщо } k_1=0;\ k_2=1\\ \begin{bmatrix}x_1\oplus x_2\\ x_2\end{bmatrix}=\begin{bmatrix}x_1\oplus x_2\oplus x_2\cdot k_2\oplus k_1\oplus k_2\oplus 1\\ x_2\oplus k_2\end{bmatrix}, \text{ якщо } k_1=1;\ k_2=0\\ \begin{bmatrix}x_1\oplus 1\\ x_2\oplus 1\end{bmatrix}=\begin{bmatrix}x_1\oplus x_2\oplus x_2\cdot k_2\oplus k_1\oplus k_2\oplus 1\\ x_2\oplus k_2\end{bmatrix}, \text{якщо } k_1=1;\ k_2=1\end{cases}$$

Відповідно, операцію $O_{14,7,2,19}$ можна записати як:

$$O_{14,7,2,19}=\begin{cases}\begin{bmatrix}x_1\oplus x_2\oplus 1\\ x_2\end{bmatrix}=\begin{bmatrix}x_1\oplus x_2\oplus x_2\cdot k_2\oplus k_1\oplus k_2\oplus 1\\ x_2\oplus k_2\end{bmatrix}, \text{ якщо } k_1=0;\ k_2=0\\ \begin{bmatrix}x_1\\ x_2\oplus 1\end{bmatrix}=\begin{bmatrix}x_1\oplus x_2\oplus x_2\cdot k_2\oplus k_1\oplus k_2\oplus 1\\ x_2\oplus k_2\end{bmatrix}, \text{якщо } k_1=0;\ k_2=1\\ \begin{bmatrix}x_1\oplus x_2\\ x_2\end{bmatrix}=\begin{bmatrix}x_1\oplus x_2\oplus x_2\cdot k_2\oplus k_1\oplus k_2\oplus 1\\ x_2\oplus k_2\end{bmatrix}, \text{ якщо } k_1=1;\ k_2=0\\ \begin{bmatrix}x_1\oplus 1\\ x_2\oplus 1\end{bmatrix}=\begin{bmatrix}x_1\oplus x_2\oplus x_2\cdot k_2\oplus k_1\oplus k_2\oplus 1\\ x_2\oplus k_2\end{bmatrix}, \text{якщо } k_1=1;\ k_2=1\end{cases}=\begin{bmatrix}x_1\oplus x_2\cdot\bar{k}_2\oplus k_1\oplus k_2\oplus 1\\ x_2\oplus k_2\end{bmatrix}$$

Перестановочна схема побудови цієї операції представлена на рис. 3.5.

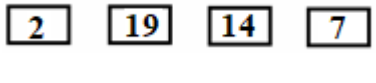
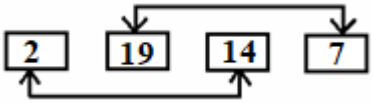
Схематичне представлення основної операції НДО 8	Перестановочна схема	Схематичне представлення отриманої операції $O_{14,7,2,19}$
		

Рис. 3.5 Перестановочна схема для побудови операції $O_{14,7,2,19}$ на основі основної операції восьмого НДО $O_{2,19,14,7}$

Математичну модель операції $O_{19,14,7,2}$, що є синтезованою на основі моделі операції $O_{2,20,14,8}$ восьмого набору двохоперандних операцій, представлено у вигляді:

$$O_{19,14,7,2}=\begin{cases}\begin{bmatrix}x_1\oplus 1\\ x_2\oplus 1\end{bmatrix}, \text{ якщо } k_1=0;\ k_2=0\\ \begin{bmatrix}x_1\oplus x_2\oplus 1\\ x_2\end{bmatrix}, \text{якщо } k_1=0;\ k_2=1\\ \begin{bmatrix}x_1\\ x_2\oplus 1\end{bmatrix}, \text{ якщо } k_1=1;\ k_2=0\\ \begin{bmatrix}x_1\oplus x_2\\ x_2\end{bmatrix}, \text{якщо } k_1=1;\ k_2=1\end{cases}=\begin{cases}\begin{bmatrix}x_1\oplus 1\\ x_2\oplus 1\end{bmatrix}=\begin{bmatrix}x_1\oplus x_2\cdot k_2\oplus k_1\oplus 1\\ x_2\oplus k_2\oplus 1\end{bmatrix}, \text{ якщо } k_1=0;\ k_2=0\\ \begin{bmatrix}x_1\oplus x_2\oplus 1\\ x_2\end{bmatrix}=\begin{bmatrix}x_1\oplus x_2\cdot k_2\oplus k_1\oplus 1\\ x_2\oplus k_2\oplus 1\end{bmatrix}, \text{якщо } k_1=0;\ k_2=1\\ \begin{bmatrix}x_1\\ x_2\oplus 1\end{bmatrix}=\begin{bmatrix}x_1\oplus x_2\cdot k_2\oplus k_1\oplus 1\\ x_2\oplus k_2\oplus 1\end{bmatrix}, \text{ якщо } k_1=1;\ k_2=0\\ \begin{bmatrix}x_1\oplus x_2\\ x_2\end{bmatrix}=\begin{bmatrix}x_1\oplus x_2\cdot k_2\oplus k_1\oplus 1\\ x_2\oplus k_2\oplus 1\end{bmatrix}, \text{якщо } k_1=1;\ k_2=1\end{cases}$$

Таким чином, операцію $O_{19,14,7,2}$ можна записати як:

$$O_{19,14,7,2}=\begin{cases}\begin{bmatrix}x_1\oplus 1\\ x_2\oplus 1\end{bmatrix}=\begin{bmatrix}x_1\oplus x_2\cdot k_2\oplus k_1\oplus 1\\ x_2\oplus k_2\oplus 1\end{bmatrix}, \text{ якщо } k_1=0;\ k_2=0\\ \begin{bmatrix}x_1\oplus x_2\oplus 1\\ x_2\end{bmatrix}=\begin{bmatrix}x_1\oplus x_2\cdot k_2\oplus k_1\oplus 1\\ x_2\oplus k_2\oplus 1\end{bmatrix}, \text{якщо } k_1=0;\ k_2=1\\ \begin{bmatrix}x_1\\ x_2\oplus 1\end{bmatrix}=\begin{bmatrix}x_1\oplus x_2\cdot k_2\oplus k_1\oplus 1\\ x_2\oplus k_2\oplus 1\end{bmatrix}, \text{ якщо } k_1=1;\ k_2=0\\ \begin{bmatrix}x_1\oplus x_2\\ x_2\end{bmatrix}=\begin{bmatrix}x_1\oplus x_2\cdot k_2\oplus k_1\oplus 1\\ x_2\oplus k_2\oplus 1\end{bmatrix}, \text{якщо } k_1=1;\ k_2=1\end{cases}=\begin{bmatrix}x_1\oplus x_2\cdot k_2\oplus k_1\oplus 1\\ x_2\oplus k_2\oplus 1\end{bmatrix}$$

Перестановочна схема побудови цієї операції представлена на рис. 3.6.

Схематичне представлення основної операції НДО 8	Перестановочна схема	Схематичне представлення отриманої операції $O_{19,14,7,2}$
2 19 14 7	2 19 14 7	19 14 7 2

Рис. 3.6 Перестановочна схема для побудови операції $O_{20,2,8,14}$ на основі основної операції восьмого НДО $O_{19,14,7,2}$

3.3 Дослідження третього набору двохоперандних операцій криптоперетворення другої математичної групи (НДО 9)

Розглянемо дев'ятий набір двохоперандних операцій.

Операція $O_{3,12,21,18}$ є першою в цьому наборі і буде умовно основною. На основі цієї операції $O_{3,12,21,18}$ за рахунок перестановок будуються інші операції цього набору [2].

Розглянемо таблично формування операції дев'ятого набору операцій порозрядного додавання за модулем два із точністю до перестановки, що включає в себе операції: $O_{3,12,21,18}$, $O_{12,21,18,3}$, $O_{18,3,12,21}$, $O_{21,18,3,12}$.

Результати побудови цих операцій наведені в табл. 3.3.

Таблиця 3.3

Дев'ятий набір двохоперандних операцій порозрядного додавання за модулем два

Операція	$O_{3,12,21,18}$				$O_{12,21,18,3}$				$O_{18,3,12,21}$				$O_{21,18,3,12}$			
Значення операндів	**0**	**1**	**2**	**3**	**0**	**1**	**2**	**3**	**0**	**1**	**2**	**3**	**0**	**1**	**2**	**3**
0	0	1	3	2	1	3	2	0	2	3	1	3	3	2	0	1
1	1	3	2	0	3	2	0	1	0	2	3	2	2	0	1	3
2	3	2	0	1	2	0	1	3	1	0	2	0	0	1	3	2
3	2	0	1	3	0	1	3	2	3	1	0	1	1	3	2	0
Перестановка	**0=0, 1=1, 2=3, 3=2**				**0=1, 1=0, 2=2, 3=3**				**0=2, 1=3, 2=1, 3=0**				**0=3, 1=2, 2=0, 3=1**			

Розглянемо більш детально результати моделювання дев'ятого набору двохоперандних операцій, представивши їх математичними моделями [6].

Математична модель основної операції дев'ятого набору матричних операцій $O_{3,12,21,18}$ матиме вигляд:

$$O_{3,12,21,18}=\begin{cases}\begin{bmatrix}x_1\\ x_1\oplus x_2\end{bmatrix}, \text{ якщо } k_1=0;\ k_2=0\\ \begin{bmatrix}x_1\oplus x_2\\ x_1\oplus 1\end{bmatrix}, \text{ якщо } k_1=0;\ k_2=1\\ \begin{bmatrix}x_1\oplus 1\\ x_1\oplus x_2\oplus 1\end{bmatrix}, \text{ якщо } k_1=1;\ k_2=0\\ \begin{bmatrix}x_1\oplus x_2\oplus 1\\ x_1\end{bmatrix}, \text{ якщо } k_1=1;\ k_2=1\end{cases}=\begin{cases}\begin{bmatrix}x_1\\ x_1\oplus x_2\end{bmatrix}=\begin{bmatrix}x_1\oplus x_2\cdot k_2\oplus k_1\\ x_1\oplus x_2\oplus x_2\cdot k_2\oplus k_1\oplus k_2\end{bmatrix}, \text{ якщо } k_1=0;\ k_2=0\\ \begin{bmatrix}x_1\oplus x_2\\ x_1\oplus 1\end{bmatrix}=\begin{bmatrix}x_1\oplus x_2\cdot k_2\oplus k_1\\ x_1\oplus x_2\oplus x_2\cdot k_2\oplus k_1\oplus k_2\end{bmatrix}, \text{ якщо } k_1=0;\ k_2=1\\ \begin{bmatrix}x_1\oplus 1\\ x_1\oplus x_2\oplus 1\end{bmatrix}=\begin{bmatrix}x_1\oplus x_2\cdot k_2\oplus k_1\\ x_1\oplus x_2\oplus x_2\cdot k_2\oplus k_1\oplus k_2\end{bmatrix}, \text{ якщо } k_1=1;\ k_2=0\\ \begin{bmatrix}x_1\oplus x_2\oplus 1\\ x_1\end{bmatrix}=\begin{bmatrix}x_1\oplus x_2\cdot k_2\oplus k_1\\ x_1\oplus x_2\oplus x_2\cdot k_2\oplus k_1\oplus k_2\end{bmatrix}, \text{ якщо } k_1=1;\ k_2=1\end{cases}$$

Таким чином, операцію $O_{3,12,21,18}$ можна записати як:

$$O_{3,12,21,18}=\begin{cases}\begin{bmatrix}x_1\\ x_1\oplus x_2\end{bmatrix}=\begin{bmatrix}x_1\oplus x_2\cdot k_2\oplus k_1\\ x_1\oplus x_2\oplus x_2\cdot k_2\oplus k_1\oplus k_2\end{bmatrix}, \text{ якщо } k_1=0;\ k_2=0\\ \begin{bmatrix}x_1\oplus x_2\\ x_1\oplus 1\end{bmatrix}=\begin{bmatrix}x_1\oplus x_2\cdot k_2\oplus k_1\\ x_1\oplus x_2\oplus x_2\cdot k_2\oplus k_1\oplus k_2\end{bmatrix}, \text{ якщо } k_1=0;\ k_2=1\\ \begin{bmatrix}x_1\oplus 1\\ x_1\oplus x_2\oplus 1\end{bmatrix}=\begin{bmatrix}x_1\oplus x_2\cdot k_2\oplus k_1\\ x_1\oplus x_2\oplus x_2\cdot k_2\oplus k_1\oplus k_2\end{bmatrix}, \text{ якщо } k_1=1;\ k_2=0\\ \begin{bmatrix}x_1\oplus x_2\oplus 1\\ x_1\end{bmatrix}=\begin{bmatrix}x_1\oplus x_2\cdot k_2\oplus k_1\\ x_1\oplus x_2\oplus x_2\cdot k_2\oplus k_1\oplus k_2\end{bmatrix}, \text{ якщо } k_1=1;\ k_2=1\end{cases}=\begin{bmatrix}x_1\oplus x_2\cdot k_2\oplus k_1\\ x_1\oplus x_2\cdot\bar{k}_2\oplus k_1\oplus k_2\end{bmatrix}$$

Математичну модель операції $O_{12,21,18,3}$, що є синтезованою на основі моделі операції $O_{3,12,21,18}$ дев'ятого набору двохоперандних операцій, представимо у вигляді:

$$O_{12,21,18,3}=\begin{cases}\begin{bmatrix}x_1\oplus x_2\\ x_1\oplus 1\end{bmatrix}, \text{ якщо } k_1=0;\ k_2=0\\ \begin{bmatrix}x_1\oplus 1\\ x_1\oplus x_2\oplus 1\end{bmatrix}, \text{ якщо } k_1=0;\ k_2=1\\ \begin{bmatrix}x_1\oplus x_2\oplus 1\\ x_1\end{bmatrix}, \text{ якщо } k_1=1;\ k_2=0\\ \begin{bmatrix}x_1\\ x_1\oplus x_2\end{bmatrix}, \text{ якщо } k_1=1;\ k_2=1\end{cases}=\begin{cases}\begin{bmatrix}x_1\oplus x_2\\ x_1\oplus 1\end{bmatrix}=\begin{bmatrix}x_1\oplus x_2\cdot\bar{k}_2\oplus k_1\oplus k_2\\ x_1\oplus x_2\cdot k_2\oplus k_1\oplus 1\end{bmatrix}, \text{ якщо } k_1=0;\ k_2=0\\ \begin{bmatrix}x_1\oplus 1\\ x_1\oplus x_2\oplus 1\end{bmatrix}=\begin{bmatrix}x_1\oplus x_2\cdot\bar{k}_2\oplus k_1\oplus k_2\\ x_1\oplus x_2\cdot k_2\oplus k_1\oplus 1\end{bmatrix}, \text{ якщо } k_1=0;\ k_2=1\\ \begin{bmatrix}x_1\oplus x_2\oplus 1\\ x_1\end{bmatrix}=\begin{bmatrix}x_1\oplus x_2\cdot\bar{k}_2\oplus k_1\oplus k_2\\ x_1\oplus x_2\cdot k_2\oplus k_1\oplus 1\end{bmatrix}, \text{ якщо } k_1=1;\ k_2=0\\ \begin{bmatrix}x_1\\ x_1\oplus x_2\end{bmatrix}=\begin{bmatrix}x_1\oplus x_2\cdot\bar{k}_2\oplus k_1\oplus k_2\\ x_1\oplus x_2\cdot k_2\oplus k_1\oplus 1\end{bmatrix}, \text{ якщо } k_1=1;\ k_2=1\end{cases}$$

Відповідно, операцію $O_{12,21,18,3}$ можна записати як:

$$O_{12,21,18,3}=\begin{cases}\begin{bmatrix}x_1\oplus x_2\\ x_1\oplus 1\end{bmatrix}=\begin{bmatrix}x_1\oplus x_2\cdot\bar{k}_2\oplus k_1\oplus k_2\\ x_1\oplus x_2\cdot k_2\oplus k_1\oplus 1\end{bmatrix}, \text{ якщо } k_1=0;\ k_2=0\\ \begin{bmatrix}x_1\oplus 1\\ x_1\oplus x_2\oplus 1\end{bmatrix}=\begin{bmatrix}x_1\oplus x_2\cdot\bar{k}_2\oplus k_1\oplus k_2\\ x_1\oplus x_2\cdot k_2\oplus k_1\oplus 1\end{bmatrix}, \text{ якщо } k_1=0;\ k_2=1\\ \begin{bmatrix}x_1\oplus x_2\oplus 1\\ x_1\end{bmatrix}=\begin{bmatrix}x_1\oplus x_2\cdot\bar{k}_2\oplus k_1\oplus k_2\\ x_1\oplus x_2\cdot k_2\oplus k_1\oplus 1\end{bmatrix}, \text{ якщо } k_1=1;\ k_2=0\\ \begin{bmatrix}x_1\\ x_1\oplus x_2\end{bmatrix}=\begin{bmatrix}x_1\oplus x_2\cdot\bar{k}_2\oplus k_1\oplus k_2\\ x_1\oplus x_2\cdot k_2\oplus k_1\oplus 1\end{bmatrix}, \text{ якщо } k_1=1;\ k_2=1\end{cases}=\begin{bmatrix}x_1\oplus x_2\cdot\bar{k}_2\oplus k_1\oplus k_2\\ x_1\oplus x_2\cdot k_2\oplus k_1\oplus 1\end{bmatrix}$$

Схематичне представлення основної операції НДО 9	Перестановочна схема	Схематичне представлення отриманої операції $O_{12,21,18,3}$
3 12 21 18	3 12 21 18	12 21 18 3

Рис. 3.7 Перестановочна схема для побудови операції $O_{12,21,18,3}$ на основі основної операції дев'ятого НДО $O_{3,12,21,18}$

Математична модель операції $O_{18,3,12,21}$, матиме вигляд:

$$O_{18,3,12,21}=\begin{cases}\begin{bmatrix}x_1\oplus x_2\oplus 1\\ x_1\end{bmatrix}, \text{ якщо } k_1=0;\ k_2=0\\ \begin{bmatrix}x_1\\ x_1\oplus x_2\end{bmatrix}, \text{ якщо } k_1=0;\ k_2=1\\ \begin{bmatrix}x_1\oplus x_2\\ x_1\oplus 1\end{bmatrix}, \text{ якщо } k_1=1;\ k_2=0\\ \begin{bmatrix}x_1\oplus 1\\ x_1\oplus x_2\oplus 1\end{bmatrix}, \text{ якщо } k_1=1;\ k_2=1\end{cases}=\begin{cases}\begin{bmatrix}x_1\oplus x_2\oplus 1\\ x_1\end{bmatrix}=\begin{bmatrix}x_1\oplus x_2\cdot\bar{k}_2\oplus k_1\oplus k_2\oplus 1\\ x_1\oplus x_2\cdot k_2\oplus k_1\end{bmatrix}, \text{ якщо } k_1=0;\ k_2=0\\ \begin{bmatrix}x_1\\ x_1\oplus x_2\end{bmatrix}=\begin{bmatrix}x_1\oplus x_2\cdot\bar{k}_2\oplus k_1\oplus k_2\oplus 1\\ x_1\oplus x_2\cdot k_2\oplus k_1\end{bmatrix}, \text{ якщо } k_1=0;\ k_2=1\\ \begin{bmatrix}x_1\oplus x_2\\ x_1\oplus 1\end{bmatrix}=\begin{bmatrix}x_1\oplus x_2\cdot\bar{k}_2\oplus k_1\oplus k_2\oplus 1\\ x_1\oplus x_2\cdot k_2\oplus k_1\end{bmatrix}, \text{ якщо } k_1=1;\ k_2=0\\ \begin{bmatrix}x_1\oplus 1\\ x_1\oplus x_2\oplus 1\end{bmatrix}=\begin{bmatrix}x_1\oplus x_2\cdot\bar{k}_2\oplus k_1\oplus k_2\oplus 1\\ x_1\oplus x_2\cdot k_2\oplus k_1\end{bmatrix}, \text{ якщо } k_1=1;\ k_2=1\end{cases}$$

Отже, операцію $O_{18,3,12,21}$ можна записати як:

$$O_{18,3,12,21}=\begin{cases}\begin{bmatrix}x_1\oplus x_2\oplus 1\\ x_1\end{bmatrix}=\begin{bmatrix}x_1\oplus x_2\cdot\bar{k}_2\oplus k_1\oplus k_2\oplus 1\\ x_1\oplus x_2\cdot k_2\oplus k_1\end{bmatrix}, \text{ якщо } k_1=0;\ k_2=0\\ \begin{bmatrix}x_1\\ x_1\oplus x_2\end{bmatrix}=\begin{bmatrix}x_1\oplus x_2\cdot\bar{k}_2\oplus k_1\oplus k_2\oplus 1\\ x_1\oplus x_2\cdot k_2\oplus k_1\end{bmatrix}, \text{ якщо } k_1=0;\ k_2=1\\ \begin{bmatrix}x_1\oplus x_2\\ x_1\oplus 1\end{bmatrix}=\begin{bmatrix}x_1\oplus x_2\cdot\bar{k}_2\oplus k_1\oplus k_2\oplus 1\\ x_1\oplus x_2\cdot k_2\oplus k_1\end{bmatrix}, \text{ якщо } k_1=1;\ k_2=0\\ \begin{bmatrix}x_1\oplus 1\\ x_1\oplus x_2\oplus 1\end{bmatrix}=\begin{bmatrix}x_1\oplus x_2\cdot\bar{k}_2\oplus k_1\oplus k_2\oplus 1\\ x_1\oplus x_2\cdot k_2\oplus k_1\end{bmatrix}, \text{ якщо } k_1=1;\ k_2=1\end{cases}=\begin{bmatrix}x_1\oplus x_2\cdot\bar{k}_2\oplus k_1\oplus k_2\oplus 1\\ x_1\oplus x_2\cdot k_2\oplus k_1\end{bmatrix}$$

Перестановочна схема побудови цієї операції представлена на рис. 3.8.

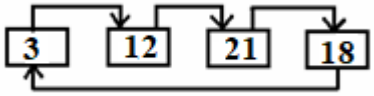
Схематичне представлення основної операції НДО 9	Перестановочна схема	Схематичне представлення отриманої операції $O_{18,3,12,21}$
		

Рис. 3.8 Перестановочна схема для побудови операції $O_{18,3,12,21}$ на основі основної операції дев'ятого НДО $O_{3,12,21,18}$

Математичну модель операції $O_{21,18,3,12}$, що є синтезованою на основі моделі основної операції $O_{3,12,21,18}$ дев'ятого набору двохоперандних операцій, представимо у вигляді:

$$O_{21,18,3,12}=\begin{cases}\begin{bmatrix}x_1\oplus 1\\ x_1\oplus x_2\oplus 1\end{bmatrix}, & якщо\ k_1=0;\ k_2=0\\ \begin{bmatrix}x_1\oplus x_2\oplus 1\\ x_1\end{bmatrix}, & якщо\ k_1=0;\ k_2=1\\ \begin{bmatrix}x_1\\ x_1\oplus x_2\end{bmatrix}, & якщо\ k_1=1;\ k_2=0\\ \begin{bmatrix}x_1\oplus x_2\\ x_1\oplus 1\end{bmatrix}, & якщо\ k_1=1;\ k_2=1\end{cases}=\begin{cases}\begin{bmatrix}x_1\oplus 1\\ x_1\oplus x_2\oplus 1\end{bmatrix}=\begin{bmatrix}x_1\oplus x_2\cdot k_2\oplus k_1\oplus 1\\ x_1\oplus x_2\cdot\bar{k}_2\oplus k_1\oplus k_2\oplus 1\end{bmatrix}, & якщо\ k_1=0;\ k_2=0\\ \begin{bmatrix}x_1\oplus x_2\oplus 1\\ x_1\end{bmatrix}=\begin{bmatrix}x_1\oplus x_2\cdot k_2\oplus k_1\oplus 1\\ x_1\oplus x_2\cdot\bar{k}_2\oplus k_1\oplus k_2\oplus 1\end{bmatrix}, & якщо\ k_1=0;\ k_2=1\\ \begin{bmatrix}x_1\\ x_1\oplus x_2\end{bmatrix}=\begin{bmatrix}x_1\oplus x_2\cdot k_2\oplus k_1\oplus 1\\ x_1\oplus x_2\cdot\bar{k}_2\oplus k_1\oplus k_2\oplus 1\end{bmatrix}, & якщо\ k_1=1;\ k_2=0\\ \begin{bmatrix}x_1\oplus x_2\\ x_1\oplus 1\end{bmatrix}=\begin{bmatrix}x_1\oplus x_2\cdot k_2\oplus k_1\oplus 1\\ x_1\oplus x_2\cdot\bar{k}_2\oplus k_1\oplus k_2\oplus 1\end{bmatrix}, & якщо\ k_1=1;\ k_2=1\end{cases}$$

Таким чином, операцію $O_{21,18,3,12}$ можна записати як:

$$O_{21,18,3,12}=\begin{cases}\begin{bmatrix}x_1\oplus 1\\ x_1\oplus x_2\oplus 1\end{bmatrix}=\begin{bmatrix}x_1\oplus x_2\cdot k_2\oplus k_1\oplus 1\\ x_1\oplus x_2\cdot\bar{k}_2\oplus k_1\oplus k_2\oplus 1\end{bmatrix}, & якщо\ k_1=0;\ k_2=0\\ \begin{bmatrix}x_1\oplus x_2\oplus 1\\ x_1\end{bmatrix}=\begin{bmatrix}x_1\oplus x_2\cdot k_2\oplus k_1\oplus 1\\ x_1\oplus x_2\cdot\bar{k}_2\oplus k_1\oplus k_2\oplus 1\end{bmatrix}, & якщо\ k_1=0;\ k_2=1\\ \begin{bmatrix}x_1\\ x_1\oplus x_2\end{bmatrix}=\begin{bmatrix}x_1\oplus x_2\cdot k_2\oplus k_1\oplus 1\\ x_1\oplus x_2\cdot\bar{k}_2\oplus k_1\oplus k_2\oplus 1\end{bmatrix}, & якщо\ k_1=1;\ k_2=0\\ \begin{bmatrix}x_1\oplus x_2\\ x_1\oplus 1\end{bmatrix}=\begin{bmatrix}x_1\oplus x_2\cdot k_2\oplus k_1\oplus 1\\ x_1\oplus x_2\cdot\bar{k}_2\oplus k_1\oplus k_2\oplus 1\end{bmatrix}, & якщо\ k_1=1;\ k_2=1\end{cases}=\begin{bmatrix}x_1\oplus x_2\cdot k_2\oplus k_1\oplus 1\\ x_1\oplus x_2\cdot\bar{k}_2\oplus k_1\oplus k_2\oplus 1\end{bmatrix}$$

Перестановочна схема побудови цієї операції представлена на рис. 3.9.

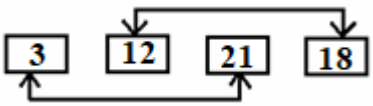
Схематичне представлення основної операції НДО 9	Перестановочна схема	Схематичне представлення отриманої операції $O_{21,18,3,12}$
		

Рис. 3.9 Перестановочна схема для побудови операції $O_{21,18,3,12}$ на основі основної операції дев'ятого НДО $O_{3,12,21,18}$

3.4 Дослідження четвертого набору двохоперандних операцій криптоперетворення другої математичної групи (НДО 10)

Розглянемо десятий набір двохоперандних операцій.

Операція $O_{4,17,10,23}$ є першою в цьому наборі і буде умовно основною. На основі цієї операції $O_{4,17,10,23}$ за рахунок перестановок будуються інші операції цього набору.

Розглянемо таблично формування операції десятого набору операцій порозрядного додавання за модулем два із точністю до перестановки, що включає в себе операції: $O_{4,17,10,23}$, $O_{10,23,4,17}$, $O_{17,10,23,4}$, $O_{23,4,17,10}$ [2].

Результати побудови цих операцій наведено в табл. 3.4.

Таблиця 3.4

Десятий набір двохоперандних операцій порозрядного додавання за модулем два

Операція	$O_{4,17,10,23}$				$O_{10,23,4,17}$				$O_{17,10,23,4}$				$O_{23,4,17,10}$			
Значення операндів	**0**	**1**	**2**	**3**	**0**	**1**	**2**	**3**	**0**	**1**	**2**	**3**	**0**	**1**	**2**	**3**
0	**0**	**2**	**1**	**3**	**1**	**3**	**0**	**2**	**2**	**1**	**3**	**0**	**3**	**0**	**2**	**1**
1	**2**	**1**	**3**	**0**	**3**	**0**	**2**	**1**	**1**	**3**	**0**	**2**	**0**	**2**	**1**	**3**
2	**1**	**3**	**0**	**2**	**0**	**2**	**1**	**3**	**3**	**0**	**2**	**1**	**2**	**1**	**3**	**0**
3	**3**	**0**	**2**	**1**	**2**	**1**	**3**	**0**	**0**	**2**	**1**	**3**	**1**	**3**	**0**	**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**				**0=3, 1=2, 2=1, 3=0**			

Розглянемо більш детально результати моделювання десятого набору двохоперандних операцій, представивши їх математичними моделями [6].

Математична модель основної операції десятого набору двохоперандних операцій $O_{4,17,10,23}$ матиме вигляд:

$$O_{4,17,10,23}=\begin{cases}\begin{bmatrix}x_2\\x_1\end{bmatrix}, \text{ якщо } k_1=0;\ k_2=0\\ \begin{bmatrix}x_2\oplus 1\\x_1\oplus x_2\end{bmatrix}, \text{якщо } k_1=0;\ k_2=1\\ \begin{bmatrix}x_2\\x_1\oplus 1\end{bmatrix}, \text{ якщо } k_1=1;\ k_2=0\\ \begin{bmatrix}x_2\oplus 1\\x_1\oplus x_2\oplus 1\end{bmatrix}, \text{якщо } k_1=1;\ k_2=1\end{cases}=\begin{cases}\begin{bmatrix}x_2\\x_1\end{bmatrix}=\begin{bmatrix}x_2\oplus k_2\\x_1\oplus x_2\cdot k_2\oplus k_1\end{bmatrix}, \text{ якщо } k_1=0;\ k_2=0\\ \begin{bmatrix}x_2\oplus 1\\x_1\oplus x_2\end{bmatrix}=\begin{bmatrix}x_2\oplus k_2\\x_1\oplus x_2\cdot k_2\oplus k_1\end{bmatrix}, \text{якщо } k_1=0;\ k_2=1\\ \begin{bmatrix}x_2\\x_1\oplus 1\end{bmatrix}=\begin{bmatrix}x_2\oplus k_2\\x_1\oplus x_2\cdot k_2\oplus k_1\end{bmatrix}, \text{ якщо } k_1=1;\ k_2=0\\ \begin{bmatrix}x_2\oplus 1\\x_1\oplus x_2\oplus 1\end{bmatrix}=\begin{bmatrix}x_2\oplus k_2\\x_1\oplus x_2\cdot k_2\oplus k_1\end{bmatrix}, \text{якщо } k_1=1;\ k_2=1\end{cases}$$

Отже, операцію $O_{4,17,10,23}$ можна записати як:

$$O_{4,17,10,23}=\begin{cases}\begin{bmatrix}x_2\\x_1\end{bmatrix}=\begin{bmatrix}x_2\oplus k_2\\x_1\oplus x_2\cdot k_2\oplus k_1\end{bmatrix}, \text{ якщо } k_1=0;\ k_2=0\\ \begin{bmatrix}x_2\oplus 1\\x_1\oplus x_2\end{bmatrix}=\begin{bmatrix}x_2\oplus k_2\\x_1\oplus x_2\cdot k_2\oplus k_1\end{bmatrix}, \text{якщо } k_1=0;\ k_2=1\\ \begin{bmatrix}x_2\\x_1\oplus 1\end{bmatrix}=\begin{bmatrix}x_2\oplus k_2\\x_1\oplus x_2\cdot k_2\oplus k_1\end{bmatrix}, \text{ якщо } k_1=1;\ k_2=0\\ \begin{bmatrix}x_2\oplus 1\\x_1\oplus x_2\oplus 1\end{bmatrix}=\begin{bmatrix}x_2\oplus k_2\\x_1\oplus x_2\cdot k_2\oplus k_1\end{bmatrix}, \text{якщо } k_1=1;\ k_2=1\end{cases}=\begin{bmatrix}x_2\oplus k_2\\x_1\oplus x_2\cdot k_2\oplus k_1\end{bmatrix}$$

Математичну модель операції $O_{10,23,4,17}$, що є синтезованою на основі моделі операції $O_{4,17,10,23}$ десятого НДО, представимо у вигляді:

$$O_{10,23,4,17}=\begin{cases}\begin{bmatrix}x_2\\x_1\oplus 1\end{bmatrix}, \text{ якщо } k_1=0;\ k_2=0\\ \begin{bmatrix}x_2\oplus 1\\x_1\oplus x_2\oplus 1\end{bmatrix}, \text{якщо } k_1=0;\ k_2=1\\ \begin{bmatrix}x_2\\x_1\end{bmatrix}, \text{ якщо } k_1=1;\ k_2=0\\ \begin{bmatrix}x_2\oplus 1\\x_1\oplus x_2\end{bmatrix}, \text{якщо } k_1=1;\ k_2=1\end{cases}=\begin{cases}\begin{bmatrix}x_2\\x_1\oplus 1\end{bmatrix}=\begin{bmatrix}x_2\oplus k_2\\x_1\oplus x_2\cdot k_2\oplus k_1\oplus 1\end{bmatrix}, \text{ якщо } k_1=0;\ k_2=0\\ \begin{bmatrix}x_2\oplus 1\\x_1\oplus x_2\oplus 1\end{bmatrix}=\begin{bmatrix}x_2\oplus k_2\\x_1\oplus x_2\cdot k_2\oplus k_1\oplus 1\end{bmatrix}, \text{якщо } k_1=0;\ k_2=1\\ \begin{bmatrix}x_2\\x_1\end{bmatrix}=\begin{bmatrix}x_2\oplus k_2\\x_1\oplus x_2\cdot k_2\oplus k_1\oplus 1\end{bmatrix}, \text{ якщо } k_1=1;\ k_2=0\\ \begin{bmatrix}x_2\oplus 1\\x_1\oplus x_2\end{bmatrix}=\begin{bmatrix}x_2\oplus k_2\\x_1\oplus x_2\cdot k_2\oplus k_1\oplus 1\end{bmatrix}, \text{якщо } k_1=1;\ k_2=1\end{cases}$$

Таким чином, операцію $O_{10,23,4,17}$ можна записати як:

$$O_{10,23,4,17}=\begin{cases}\begin{bmatrix}x_2\\ x_1\oplus 1\end{bmatrix}=\begin{bmatrix}x_2\oplus k_2\\ x_1\oplus x_2\cdot k_2\oplus k_1\oplus 1\end{bmatrix}, \text{ якщо } k_1=0;\ k_2=0\\ \begin{bmatrix}x_2\oplus 1\\ x_1\oplus x_2\oplus 1\end{bmatrix}=\begin{bmatrix}x_2\oplus k_2\\ x_1\oplus x_2\cdot k_2\oplus k_1\oplus 1\end{bmatrix}, \text{якщо } k_1=0;\ k_2=1\\ \begin{bmatrix}x_2\\ x_1\end{bmatrix}=\begin{bmatrix}x_2\oplus k_2\\ x_1\oplus x_2\cdot k_2\oplus k_1\oplus 1\end{bmatrix}, \text{ якщо } k_1=1;\ k_2=0\\ \begin{bmatrix}x_2\oplus 1\\ x_1\oplus x_2\end{bmatrix}=\begin{bmatrix}x_2\oplus k_2\\ x_1\oplus x_2\cdot k_2\oplus k_1\oplus 1\end{bmatrix}, \text{якщо } k_1=1;\ k_2=1\end{cases}=\begin{bmatrix}x_2\oplus k_2\\ x_1\oplus x_2\cdot k_2\oplus k_1\oplus 1\end{bmatrix}$$

Перестановочна схема побудови цієї операції представлена на рис. 3.10.

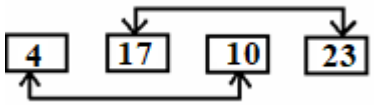
Схематичне представлення основної операції НДО 10	Перестановочна схема	Схематичне представлення отриманої операції $O_{10,23,4,17}$
		

Рис. 3.10 Перестановочна схема для побудови операції $O_{10,23,4,17}$ на основі основної операції десятого НДО $O_{4,17,10,23}$

Математична модель операції $O_{17,10,23,4}$, шо є синтезованою на основі моделі основної операції $O_{4,17,10,23}$ десятого НДО, матиме вигляд:

$$O_{17,10,23,4}=\begin{cases}\begin{bmatrix}x_2\oplus 1\\ x_1\oplus x_2\end{bmatrix}, \text{ якщо } k_1=0;\ k_2=0\\ \begin{bmatrix}x_2\\ x_1\oplus 1\end{bmatrix}, \text{якщо } k_1=0;\ k_2=1\\ \begin{bmatrix}x_2\oplus 1\\ x_1\oplus x_2\oplus 1\end{bmatrix}, \text{ якщо } k_1=1;\ k_2=0\\ \begin{bmatrix}x_2\\ x_1\end{bmatrix}, \text{якщо } k_1=1;\ k_2=1\end{cases}=\begin{cases}\begin{bmatrix}x_2\oplus 1\\ x_1\oplus x_2\end{bmatrix}=\begin{bmatrix}x_2\oplus k_2\oplus 1\\ x_1\oplus x_2\cdot\bar{k}_2\oplus k_1\oplus k_2\end{bmatrix}, \text{ якщо } k_1=0;\ k_2=0\\ \begin{bmatrix}x_2\\ x_1\oplus 1\end{bmatrix}=\begin{bmatrix}x_2\oplus k_2\oplus 1\\ x_1\oplus x_2\cdot\bar{k}_2\oplus k_1\oplus k_2\end{bmatrix}, \text{якщо } k_1=0;\ k_2=1\\ \begin{bmatrix}x_2\oplus 1\\ x_1\oplus x_2\oplus 1\end{bmatrix}=\begin{bmatrix}x_2\oplus k_2\oplus 1\\ x_1\oplus x_2\cdot\bar{k}_2\oplus k_1\oplus k_2\end{bmatrix}, \text{ якщо } k_1=1;\ k_2=0\\ \begin{bmatrix}x_2\\ x_1\end{bmatrix}=\begin{bmatrix}x_2\oplus k_2\oplus 1\\ x_1\oplus x_2\cdot\bar{k}_2\oplus k_1\oplus k_2\end{bmatrix}, \text{якщо } k_1=1;\ k_2=1\end{cases}$$

Відповідно, операцію $O_{17,10,23,4}$ можна записати як:

$$O_{17,10,23,4}=\begin{cases}\begin{bmatrix}x_2\oplus 1\\ x_1\oplus x_2\end{bmatrix}=\begin{bmatrix}x_2\oplus k_2\oplus 1\\ x_1\oplus x_2\cdot\bar{k}_2\oplus k_1\oplus k_2\end{bmatrix}, \text{ якщо } k_1=0;\ k_2=0\\ \begin{bmatrix}x_2\\ x_1\oplus 1\end{bmatrix}=\begin{bmatrix}x_2\oplus k_2\oplus 1\\ x_1\oplus x_2\cdot\bar{k}_2\oplus k_1\oplus k_2\end{bmatrix}, \text{якщо } k_1=0;\ k_2=1\\ \begin{bmatrix}x_2\oplus 1\\ x_1\oplus x_2\oplus 1\end{bmatrix}=\begin{bmatrix}x_2\oplus k_2\oplus 1\\ x_1\oplus x_2\cdot\bar{k}_2\oplus k_1\oplus k_2\end{bmatrix}, \text{якщо } k_1=1;\ k_2=0\\ \begin{bmatrix}x_2\\ x_1\end{bmatrix}=\begin{bmatrix}x_2\oplus k_2\oplus 1\\ x_1\oplus x_2\cdot\bar{k}_2\oplus k_1\oplus k_2\end{bmatrix}, \text{якщо } k_1=1;\ k_2=1\end{cases}=\begin{bmatrix}x_2\oplus k_2\oplus 1\\ x_1\oplus x_2\cdot\bar{k}_2\oplus k_1\oplus k_2\end{bmatrix}$$

Перестановочна схема побудови цієї операції представлена на рис. 3.11.

Схематичне представлення основної операції НДО 10	Перестановочна схема	Схематичне представлення отриманої операції $O_{17,10,23,4}$
4 17 10 23	4 17 10 23	17 10 23 4

Рис. 3.11 Перестановочна схема для побудови операції $O_{17,10,23,4}$ на основі основної операції десятого НДО $O_{4,17,10,23}$

Математичну модель операції $O_{23,4,17,10}$, що є синтезованою на основі моделі основної операції $O_{4,17,10,23}$ десятого набору двохоперандних операцій, представлено у вигляді [6]:

$$O_{23,4,17,10}=\begin{cases}\begin{bmatrix}x_2\oplus 1\\ x_1\oplus x_2\oplus 1\end{bmatrix}, \text{ якщо } k_1=0;\ k_2=0\\ \begin{bmatrix}x_2\\ x_1\end{bmatrix}, \text{якщо } k_1=0;\ k_2=1\\ \begin{bmatrix}x_2\oplus 1\\ x_1\oplus x_2\end{bmatrix}, \text{якщо } k_1=1;\ k_2=0\\ \begin{bmatrix}x_2\\ x_1\oplus 1\end{bmatrix}, \text{якщо } k_1=1;\ k_2=1\end{cases}=\begin{cases}\begin{bmatrix}x_2\oplus 1\\ x_1\oplus x_2\oplus 1\end{bmatrix}=\begin{bmatrix}x_2\oplus k_2\oplus 1\\ x_1\oplus x_2\cdot\bar{k}_2\oplus k_1\oplus k_2\oplus 1\end{bmatrix}, \text{ якщо } k_1=0;\ k_2=0\\ \begin{bmatrix}x_2\\ x_1\end{bmatrix}=\begin{bmatrix}x_2\oplus k_2\oplus 1\\ x_1\oplus x_2\cdot\bar{k}_2\oplus k_1\oplus k_2\oplus 1\end{bmatrix}, \text{якщо } k_1=0;\ k_2=1\\ \begin{bmatrix}x_2\oplus 1\\ x_1\oplus x_2\end{bmatrix}=\begin{bmatrix}x_2\oplus k_2\oplus 1\\ x_1\oplus x_2\cdot\bar{k}_2\oplus k_1\oplus k_2\oplus 1\end{bmatrix}, \text{якщо } k_1=1;\ k_2=0\\ \begin{bmatrix}x_2\\ x_1\oplus 1\end{bmatrix}=\begin{bmatrix}x_2\oplus k_2\oplus 1\\ x_1\oplus x_2\cdot\bar{k}_2\oplus k_1\oplus k_2\oplus 1\end{bmatrix}, \text{якщо } k_1=1;\ k_2=1\end{cases}$$

Таким чином, операцію $O_{23,4,17,10}$ можна записати як:

$$O_{23,4,17,10}=\begin{cases}\begin{bmatrix}x_2\oplus 1\\ x_1\oplus x_2\oplus 1\end{bmatrix}=\begin{bmatrix}x_2\oplus k_2\oplus 1\\ x_1\oplus x_2\cdot\bar{k}_2\oplus k_1\oplus k_2\oplus 1\end{bmatrix}, \text{ якщо } k_1=0;\ k_2=0\\ \begin{bmatrix}x_2\\ x_1\end{bmatrix}=\begin{bmatrix}x_2\oplus k_2\oplus 1\\ x_1\oplus x_2\cdot\bar{k}_2\oplus k_1\oplus k_2\oplus 1\end{bmatrix}, \text{якщо } k_1=0;\ k_2=1\\ \begin{bmatrix}x_2\oplus 1\\ x_1\oplus x_2\end{bmatrix}=\begin{bmatrix}x_2\oplus k_2\oplus 1\\ x_1\oplus x_2\cdot\bar{k}_2\oplus k_1\oplus k_2\oplus 1\end{bmatrix}, \text{якщо } k_1=1;\ k_2=0\\ \begin{bmatrix}x_2\\ x_1\oplus 1\end{bmatrix}=\begin{bmatrix}x_2\oplus k_2\oplus 1\\ x_1\oplus x_2\cdot\bar{k}_2\oplus k_1\oplus k_2\oplus 1\end{bmatrix}, \text{якщо } k_1=1;\ k_2=1\end{cases}=\begin{bmatrix}x_2\oplus k_2\oplus 1\\ x_1\oplus x_2\cdot\bar{k}_2\oplus k_1\oplus k_2\oplus 1\end{bmatrix}$$

Перестановочна схема побудови цієї операції представлена на рис. 3.12.

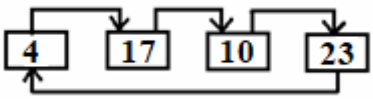
Схематичне представлення основної операції НДО 10	Перестановочна схема	Схематичне представлення отриманої операції $O_{23,4,17,10}$
		

Рис. 3.12 Перестановочна схема для побудови операції $O_{23,4,17,10}$ на основі основної операції десятого НДО $O_{4,17,10,23}$

3.5 Дослідження п’ятого набору двохоперандних операцій криптоперетворення другої математичної групи (НДО 11)

Розглянемо одинадцятий набір двохоперандних операцій.

Операція $O_{5,22,11,16}$ є першою в цьому наборі і буде умовно основною. На основі базової операції $O_{5,22,11,16}$ за рахунок перестановок будуються інші операції цього набору [2].

Розглянемо таблично формування операції одинадцятого набору операцій порозрядного додавання за модулем два із точністю до перестановки, що включає в себе операції: $O_{5,22,11,16}$, $O_{11,16,5,22}$, $O_{16,5,22,11}$, $O_{22,11,16,5}$.

Результати побудови цих операцій наведено в табл. 3.5.

Таблиця 3.5

Одинадцятий набір двохоперандних операцій порозрядного додавання за модулем два

Операція	$O_{5,22,11,16}$				$O_{11,16,5,22}$				$O_{16,5,22,11}$				$O_{22,11,16,5}$			
Значення операндів	**0**	**1**	**2**	**3**	**0**	**1**	**2**	**3**	**0**	**1**	**2**	**3**	**0**	**1**	**2**	**3**
0	**0**	**3**	**1**	**2**	**1**	**2**	**0**	**3**	**2**	**0**	**3**	**1**	**3**	**1**	**2**	**0**
1	**3**	**1**	**2**	**0**	**2**	**0**	**3**	**1**	**0**	**3**	**1**	**2**	**1**	**2**	**0**	**3**
2	**1**	**2**	**0**	**3**	**0**	**3**	**1**	**2**	**3**	**1**	**2**	**0**	**2**	**0**	**3**	**1**
3	**2**	**0**	**3**	**1**	**3**	**1**	**2**	**0**	**1**	**2**	**0**	**3**	**0**	**3**	**1**	**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**				**0=3, 1=2, 2=1, 3=0**			

Розглянемо більш детально результати моделювання одинадцятого набору двохоперандних операцій, представивши їх математичними моделями.

Математична модель основної операції одинадцятого набору двохоперандних операцій $O_{5,22,11,16}$ матиме вигляд:

$$O_{5,22,11,16}=\begin{cases}\begin{bmatrix}x_2\\ x_1\oplus x_2\end{bmatrix}, \text{ якщо } k_1=0;\ k_2=0\\ \begin{bmatrix}x_2\oplus 1\\ x_1\oplus 1\end{bmatrix}, \text{ якщо } k_1=0;\ k_2=1\\ \begin{bmatrix}x_2\\ x_1\oplus x_2\oplus 1\end{bmatrix}, \text{ якщо } k_1=1;\ k_2=0\\ \begin{bmatrix}x_2\oplus 1\\ x_1\end{bmatrix}, \text{ якщо } k_1=1;\ k_2=1\end{cases}=\begin{cases}\begin{bmatrix}x_2\\ x_1\oplus x_2\end{bmatrix}=\begin{bmatrix}x_2\oplus k_2\\ x_1\oplus x_2\cdot\bar{k}_2\oplus k_1\oplus k_2\end{bmatrix}, \text{ якщо } k_1=0;\ k_2=0\\ \begin{bmatrix}x_2\oplus 1\\ x_1\oplus 1\end{bmatrix}=\begin{bmatrix}x_2\oplus k_2\\ x_1\oplus x_2\cdot\bar{k}_2\oplus k_1\oplus k_2\end{bmatrix}, \text{ якщо } k_1=0;\ k_2=1\\ \begin{bmatrix}x_2\\ x_1\oplus x_2\oplus 1\end{bmatrix}=\begin{bmatrix}x_2\oplus k_2\\ x_1\oplus x_2\cdot\bar{k}_2\oplus k_1\oplus k_2\end{bmatrix}, \text{ якщо } k_1=1;\ k_2=0\\ \begin{bmatrix}x_2\oplus 1\\ x_1\end{bmatrix}=\begin{bmatrix}x_2\oplus k_2\\ x_1\oplus x_2\cdot\bar{k}_2\oplus k_1\oplus k_2\end{bmatrix}, \text{ якщо } k_1=1;\ k_2=1\end{cases}$$

Таким чином, операцію $O_{5,22,11,16}$ можна записати як:

$$O_{5,22,11,16}=\begin{cases}\begin{bmatrix}x_2\\ x_1\oplus x_2\end{bmatrix}=\begin{bmatrix}x_2\oplus k_2\\ x_1\oplus x_2\cdot\bar{k}_2\oplus k_1\oplus k_2\end{bmatrix}, \text{ якщо } k_1=0;\ k_2=0\\ \begin{bmatrix}x_2\oplus 1\\ x_1\oplus 1\end{bmatrix}=\begin{bmatrix}x_2\oplus k_2\\ x_1\oplus x_2\cdot\bar{k}_2\oplus k_1\oplus k_2\end{bmatrix}, \text{ якщо } k_1=0;\ k_2=1\\ \begin{bmatrix}x_2\\ x_1\oplus x_2\oplus 1\end{bmatrix}=\begin{bmatrix}x_2\oplus k_2\\ x_1\oplus x_2\cdot\bar{k}_2\oplus k_1\oplus k_2\end{bmatrix}, \text{ якщо } k_1=1;\ k_2=0\\ \begin{bmatrix}x_2\oplus 1\\ x_1\end{bmatrix}=\begin{bmatrix}x_2\oplus k_2\\ x_1\oplus x_2\cdot\bar{k}_2\oplus k_1\oplus k_2\end{bmatrix}, \text{ якщо } k_1=1;\ k_2=1\end{cases}=\begin{bmatrix}x_2\oplus k_2\\ x_1\oplus x_2\cdot\bar{k}_2\oplus k_1\oplus k_2\end{bmatrix}$$

Математичну модель операції $O_{11,16,5,22}$, що є синтезованою на основі моделі операції $O_{5,22,11,16}$ одинадцятого НДО, представимо у вигляді:

$$O_{11,16,5,22}=\begin{cases}\begin{bmatrix}x_2\\ x_1\oplus x_2\oplus 1\end{bmatrix}, \text{ якщо } k_1=0;\ k_2=0\\ \begin{bmatrix}x_2\oplus 1\\ x_1\end{bmatrix}, \text{ якщо } k_1=0;\ k_2=1\\ \begin{bmatrix}x_2\\ x_1\oplus x_2\end{bmatrix}, \text{ якщо } k_1=1;\ k_2=0\\ \begin{bmatrix}x_2\oplus 1\\ x_1\oplus 1\end{bmatrix}, \text{ якщо } k_1=1;\ k_2=1\end{cases}=\begin{cases}\begin{bmatrix}x_2\\ x_1\oplus x_2\oplus 1\end{bmatrix}=\begin{bmatrix}x_2\oplus k_2\\ x_1\oplus x_2\cdot\bar{k}_2\oplus k_1\oplus k_2\oplus 1\end{bmatrix}, \text{ якщо } k_1=0;\ k_2=0\\ \begin{bmatrix}x_2\oplus 1\\ x_1\end{bmatrix}=\begin{bmatrix}x_2\oplus k_2\\ x_1\oplus x_2\cdot\bar{k}_2\oplus k_1\oplus k_2\oplus 1\end{bmatrix}, \text{ якщо } k_1=0;\ k_2=1\\ \begin{bmatrix}x_2\\ x_1\oplus x_2\end{bmatrix}=\begin{bmatrix}x_2\oplus k_2\\ x_1\oplus x_2\cdot\bar{k}_2\oplus k_1\oplus k_2\oplus 1\end{bmatrix}, \text{ якщо } k_1=1;\ k_2=0\\ \begin{bmatrix}x_2\oplus 1\\ x_1\oplus 1\end{bmatrix}=\begin{bmatrix}x_2\oplus k_2\\ x_1\oplus x_2\cdot\bar{k}_2\oplus k_1\oplus k_2\oplus 1\end{bmatrix}, \text{ якщо } k_1=1;\ k_2=1\end{cases}$$

Отже, операцію $O_{11,16,5,22}$ можна записати як [2]:

$$O_{11,16,5,22}=\begin{cases}\begin{bmatrix}x_2\\ x_1\oplus x_2\oplus 1\end{bmatrix}=\begin{bmatrix}x_2\oplus k_2\\ x_1\oplus x_2\cdot\bar{k}_2\oplus k_1\oplus k_2\oplus 1\end{bmatrix}, \text{ якщо } k_1=0;\ k_2=0\\ \begin{bmatrix}x_2\oplus 1\\ x_1\end{bmatrix}=\begin{bmatrix}x_2\oplus k_2\\ x_1\oplus x_2\cdot\bar{k}_2\oplus k_1\oplus k_2\oplus 1\end{bmatrix}, \text{ якщо } k_1=0;\ k_2=1\\ \begin{bmatrix}x_2\\ x_1\oplus x_2\end{bmatrix}=\begin{bmatrix}x_2\oplus k_2\\ x_1\oplus x_2\cdot\bar{k}_2\oplus k_1\oplus k_2\oplus 1\end{bmatrix}, \text{ якщо } k_1=1;\ k_2=0\\ \begin{bmatrix}x_2\oplus 1\\ x_1\oplus 1\end{bmatrix}=\begin{bmatrix}x_2\oplus k_2\\ x_1\oplus x_2\cdot\bar{k}_2\oplus k_1\oplus k_2\oplus 1\end{bmatrix}, \text{ якщо } k_1=1;\ k_2=1\end{cases}=\begin{bmatrix}x_2\oplus k_2\\ x_1\oplus x_2\cdot\bar{k}_2\oplus k_1\oplus k_2\oplus 1\end{bmatrix}$$

Перестановочна схема побудови цієї операції представлена на рис. 3.13.

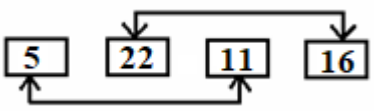
Схематичне представлення основної операції НДО 11	Перестановочна схема	Схематичне представлення отриманої операції $O_{11,16,5,22}$
		

Рис. 3.13 Перестановочна схема для побудови операції $O_{11,16,5,22}$ на основі основної операції одинадцятого НДО $O_{5,22,11,16}$

Математична модель операції $O_{16,5,22,11}$, що є синтезованою на основі моделі основної операції $O_{5,22,11,16}$ одинадцятого набору двохоперандних операцій, матиме вигляд:

$$O_{16,5,22,11}=\begin{cases}\begin{bmatrix}x_2\oplus 1\\ x_1\end{bmatrix}, \textit{якщо } k_1=0;\ k_2=0\\ \begin{bmatrix}x_2\\ x_1\oplus x_2\end{bmatrix}, \textit{якщо } k_1=0;\ k_2=1\\ \begin{bmatrix}x_2\oplus 1\\ x_1\oplus 1\end{bmatrix}, \textit{якщо } k_1=1;\ k_2=0\\ \begin{bmatrix}x_2\\ x_1\oplus x_2\oplus 1\end{bmatrix}, \textit{якщо } k_1=1;\ k_2=1\end{cases}=\begin{cases}\begin{bmatrix}x_2\oplus 1\\ x_1\end{bmatrix}=\begin{bmatrix}x_2\oplus k_2\oplus 1\\ x_1\oplus x_2\cdot k_2\oplus k_1\end{bmatrix}, \textit{якщо } k_1=0;\ k_2=0\\ \begin{bmatrix}x_2\\ x_1\oplus x_2\end{bmatrix}=\begin{bmatrix}x_2\oplus k_2\oplus 1\\ x_1\oplus x_2\cdot k_2\oplus k_1\end{bmatrix}, \textit{якщо } k_1=0;\ k_2=1\\ \begin{bmatrix}x_2\oplus 1\\ x_1\oplus 1\end{bmatrix}=\begin{bmatrix}x_2\oplus k_2\oplus 1\\ x_1\oplus x_2\cdot k_2\oplus k_1\end{bmatrix}, \textit{якщо } k_1=1;\ k_2=0\\ \begin{bmatrix}x_2\\ x_1\oplus x_2\oplus 1\end{bmatrix}=\begin{bmatrix}x_2\oplus k_2\oplus 1\\ x_1\oplus x_2\cdot k_2\oplus k_1\end{bmatrix}, \textit{якщо } k_1=1;\ k_2=1\end{cases}$$

Відповідно, операцію $O_{16,5,22,11}$ можна записати як:

$$O_{16,5,22,11}=\begin{cases}\begin{bmatrix}x_2\oplus 1\\ x_1\end{bmatrix}=\begin{bmatrix}x_2\oplus k_2\oplus 1\\ x_1\oplus x_2\cdot k_2\oplus k_1\end{bmatrix}, \textit{якщо } k_1=0;\ k_2=0\\ \begin{bmatrix}x_2\\ x_1\oplus x_2\end{bmatrix}=\begin{bmatrix}x_2\oplus k_2\oplus 1\\ x_1\oplus x_2\cdot k_2\oplus k_1\end{bmatrix}, \textit{якщо } k_1=0;\ k_2=1\\ \begin{bmatrix}x_2\oplus 1\\ x_1\oplus 1\end{bmatrix}=\begin{bmatrix}x_2\oplus k_2\oplus 1\\ x_1\oplus x_2\cdot k_2\oplus k_1\end{bmatrix}, \textit{якщо } k_1=1;\ k_2=0\\ \begin{bmatrix}x_2\\ x_1\oplus x_2\oplus 1\end{bmatrix}=\begin{bmatrix}x_2\oplus k_2\oplus 1\\ x_1\oplus x_2\cdot k_2\oplus k_1\end{bmatrix}, \textit{якщо } k_1=1;\ k_2=1\end{cases}=\begin{bmatrix}x_2\oplus k_2\oplus 1\\ x_1\oplus x_2\cdot k_2\oplus k_1\end{bmatrix}$$

Перестановочна схема побудови цієї операції представлена на рис. 3.14.

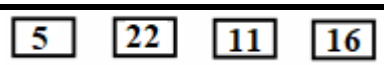
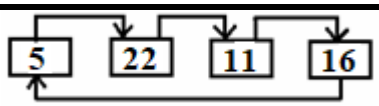
Схематичне представлення основної операції НДО 11	Перестановочна схема	Схематичне представлення отриманої операції $O_{16,5,22,11}$
		

Рис. 3.14 Перестановочна схема для побудови операції $O_{16,5,22,11}$ на основі основної операції одинадцятого НДО $O_{5,22,11,16}$

Математичну модель операції $O_{22,11,16,5}$, що є синтезованою на основі моделі основної операції $O_{5,22,11,16}$ одинадцятого набору двохоперандних операцій, представимо у вигляді [6]:

$$O_{22,11,16,5}=\begin{cases}\begin{bmatrix}x_2\oplus 1\\ x_1\oplus 1\end{bmatrix}, \text{ якщо } k_1=0;\ k_2=0\\ \begin{bmatrix}x_2\\ x_1\oplus x_2\oplus 1\end{bmatrix}, \text{ якщо } k_1=0;\ k_2=1\\ \begin{bmatrix}x_2\oplus 1\\ x_1\end{bmatrix}, \text{ якщо } k_1=1;\ k_2=0\\ \begin{bmatrix}x_2\\ x_1\oplus x_2\end{bmatrix}, \text{ якщо } k_1=1;\ k_2=1\end{cases}=\begin{cases}\begin{bmatrix}x_2\oplus 1\\ x_1\oplus 1\end{bmatrix}=\begin{bmatrix}x_2\oplus k_2\oplus 1\\ x_1\oplus x_2\cdot k_2\oplus k_1\oplus 1\end{bmatrix}, \text{ якщо } k_1=0;\ k_2=0\\ \begin{bmatrix}x_2\\ x_1\oplus x_2\oplus 1\end{bmatrix}=\begin{bmatrix}x_2\oplus k_2\oplus 1\\ x_1\oplus x_2\cdot k_2\oplus k_1\oplus 1\end{bmatrix}, \text{ якщо } k_1=0;\ k_2=1\\ \begin{bmatrix}x_2\oplus 1\\ x_1\end{bmatrix}=\begin{bmatrix}x_2\oplus k_2\oplus 1\\ x_1\oplus x_2\cdot k_2\oplus k_1\oplus 1\end{bmatrix}, \text{ якщо } k_1=1;\ k_2=0\\ \begin{bmatrix}x_2\\ x_1\oplus x_2\end{bmatrix}=\begin{bmatrix}x_2\oplus k_2\oplus 1\\ x_1\oplus x_2\cdot k_2\oplus k_1\oplus 1\end{bmatrix}, \text{ якщо } k_1=1;\ k_2=1\end{cases}$$

Таким чином, операцію $O_{22,11,16,5}$ можна записати як:

$$O_{22,11,16,5}=\begin{cases}\begin{bmatrix}x_2\oplus 1\\ x_1\oplus 1\end{bmatrix}=\begin{bmatrix}x_2\oplus k_2\oplus 1\\ x_1\oplus x_2\cdot k_2\oplus k_1\oplus 1\end{bmatrix}, \text{ якщо } k_1=0;\ k_2=0\\ \begin{bmatrix}x_2\\ x_1\oplus x_2\oplus 1\end{bmatrix}=\begin{bmatrix}x_2\oplus k_2\oplus 1\\ x_1\oplus x_2\cdot k_2\oplus k_1\oplus 1\end{bmatrix}, \text{ якщо } k_1=0;\ k_2=1\\ \begin{bmatrix}x_2\oplus 1\\ x_1\end{bmatrix}=\begin{bmatrix}x_2\oplus k_2\oplus 1\\ x_1\oplus x_2\cdot k_2\oplus k_1\oplus 1\end{bmatrix}, \text{ якщо } k_1=1;\ k_2=0\\ \begin{bmatrix}x_2\\ x_1\oplus x_2\end{bmatrix}=\begin{bmatrix}x_2\oplus k_2\oplus 1\\ x_1\oplus x_2\cdot k_2\oplus k_1\oplus 1\end{bmatrix}, \text{ якщо } k_1=1;\ k_2=1\end{cases}=\begin{bmatrix}x_2\oplus k_2\oplus 1\\ x_1\oplus x_2\cdot k_2\oplus k_1\oplus 1\end{bmatrix}$$

Перестановочна схема побудови цієї операції представлена на рис. 3.15.

Схематичне представлення основної операції НДО 11	Перестановочна схема	Схематичне представлення отриманої операції $O_{22,11,16,5}$
5 22 11 16	5 22 11 16	22 11 16 5

Рис. 3.15 Перестановочна схема для побудови операції $O_{22,11,16,5}$ на основі основної операції одинадцятого НДО $O_{5,22,11,16}$

3.6 Дослідження шостого набору двохоперандних операцій криптоперетворення другої математичної групи (НДО 12)

Розглянемо дванадцятий набір двохоперандних операцій.

Операція $O_{6,15,24,9}$ є першою в цьому наборі і буде умовно основною. На основі операції $O_{6,15,24,9}$ за рахунок перестановок будуються інші операції цього набору.

Розглянемо таблично формування операції дванадцятого набору операцій порозрядного додавання за модулем два із точністю до перестановки, що включає в себе операції: $O_{6,15,24,9}$, $O_{9,6,15,24}$, $O_{15,24,9,6}$, $O_{24,9,6,15}$ [2].

Результати побудови цих операцій наведено в табл. 3.6.

Таблиця 3.6

Дванадцятий набір двохоперандних операцій порозрядного додавання за модулем два

Операція	$O_{6,15,24,9}$				$O_{9,6,15,24}$				$O_{15,24,9,6}$				$O_{24,9,6,15}$			
Значення операндів	**0**	**1**	**2**	**3**	**0**	**1**	**2**	**3**	**0**	**1**	**2**	**3**	**0**	**1**	**2**	**3**
0	**0**	**2**	**3**	**1**	**1**	**0**	**2**	**3**	**2**	**3**	**1**	**0**	**3**	**1**	**0**	**2**
1	**2**	**3**	**1**	**0**	**0**	**2**	**3**	**1**	**3**	**1**	**0**	**2**	**1**	**0**	**2**	**3**
2	**3**	**1**	**0**	**2**	**2**	**3**	**1**	**0**	**1**	**0**	**2**	**3**	**0**	**2**	**3**	**1**
3	**1**	**0**	**2**	**3**	**3**	**1**	**0**	**2**	**0**	**2**	**3**	**1**	**2**	**3**	**1**	**0**
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**				**0=3, 1=2, 2=1, 3=0**			

Розглянемо більш детально результати моделювання дванадцятого набору двохоперандних операцій, представивши їх математичними моделями.

Математична модель основної операції дванадцятого набору двохоперандних операцій $O_{6,15,24,9}$ матиме вигляд:

$$O_{6,15,24,9}=\begin{cases}\begin{bmatrix}x_1\oplus x_2\\ x_1\end{bmatrix}, \text{ якщо } k_1=0;\ k_2=0\\ \begin{bmatrix}x_1\oplus 1\\ x_1\oplus x_2\end{bmatrix}, \text{ якщо } k_1=0;\ k_2=1\\ \begin{bmatrix}x_1\oplus x_2\oplus 1\\ x_1\oplus 1\end{bmatrix}, \text{ якщо } k_1=1;\ k_2=0\\ \begin{bmatrix}x_1\\ x_1\oplus x_2\oplus 1\end{bmatrix}, \text{ якщо } k_1=1;\ k_2=1\end{cases}=\begin{cases}\begin{bmatrix}x_1\oplus x_2\\ x_1\end{bmatrix}=\begin{bmatrix}x_1\oplus x_2\cdot\bar{k}_2\oplus k_1\oplus k_2\\ x_1\oplus x_2\cdot k_2\oplus k_1\end{bmatrix}, \text{ якщо } k_1=0;\ k_2=0\\ \begin{bmatrix}x_1\oplus 1\\ x_1\oplus x_2\end{bmatrix}=\begin{bmatrix}x_1\oplus x_2\cdot\bar{k}_2\oplus k_1\oplus k_2\\ x_1\oplus x_2\cdot k_2\oplus k_1\end{bmatrix}, \text{ якщо } k_1=0;\ k_2=1\\ \begin{bmatrix}x_1\oplus x_2\oplus 1\\ x_1\oplus 1\end{bmatrix}=\begin{bmatrix}x_1\oplus x_2\cdot\bar{k}_2\oplus k_1\oplus k_2\\ x_1\oplus x_2\cdot k_2\oplus k_1\end{bmatrix}, \text{ якщо } k_1=1;\ k_2=0\\ \begin{bmatrix}x_1\\ x_1\oplus x_2\oplus 1\end{bmatrix}=\begin{bmatrix}x_1\oplus x_2\cdot\bar{k}_2\oplus k_1\oplus k_2\\ x_1\oplus x_2\cdot k_2\oplus k_1\end{bmatrix}, \text{ якщо } k_1=1;\ k_2=1\end{cases}$$

Відповідно, операцію $O_{6,15,24,9}$ можна записати як:

$$O_{6,15,24,9}=\begin{cases}\begin{bmatrix}x_1\oplus x_2\\ x_1\end{bmatrix}=\begin{bmatrix}x_1\oplus x_2\cdot\bar{k}_2\oplus k_1\oplus k_2\\ x_1\oplus x_2\cdot k_2\oplus k_1\end{bmatrix}, \text{ якщо } k_1=0;\ k_2=0\\ \begin{bmatrix}x_1\oplus 1\\ x_1\oplus x_2\end{bmatrix}=\begin{bmatrix}x_1\oplus x_2\cdot\bar{k}_2\oplus k_1\oplus k_2\\ x_1\oplus x_2\cdot k_2\oplus k_1\end{bmatrix}, \text{ якщо } k_1=0;\ k_2=1\\ \begin{bmatrix}x_1\oplus x_2\oplus 1\\ x_1\oplus 1\end{bmatrix}=\begin{bmatrix}x_1\oplus x_2\cdot\bar{k}_2\oplus k_1\oplus k_2\\ x_1\oplus x_2\cdot k_2\oplus k_1\end{bmatrix}, \text{ якщо } k_1=1;\ k_2=0\\ \begin{bmatrix}x_1\\ x_1\oplus x_2\oplus 1\end{bmatrix}=\begin{bmatrix}x_1\oplus x_2\cdot\bar{k}_2\oplus k_1\oplus k_2\\ x_1\oplus x_2\cdot k_2\oplus k_1\end{bmatrix}, \text{ якщо } k_1=1;\ k_2=1\end{cases}=\begin{bmatrix}x_1\oplus x_2\cdot\bar{k}_2\oplus k_1\oplus k_2\\ x_1\oplus x_2\cdot k_2\oplus k_1\end{bmatrix}$$

Математичну модель операції $O_{9,6,15,24}$, що є синтезованою на основі моделі операції $O_{6,15,24,9}$ дванадцятого НДО, представлено у вигляді:

$$O_{9,6,15,24}=\begin{cases}\begin{bmatrix}x_1\\ x_1\oplus x_2\oplus 1\end{bmatrix}, \text{ якщо } k_1=0;\ k_2=0\\ \begin{bmatrix}x_1\oplus x_2\\ x_1\end{bmatrix}, \text{ якщо } k_1=0;\ k_2=1\\ \begin{bmatrix}x_1\oplus 1\\ x_1\oplus x_2\end{bmatrix}, \text{ якщо } k_1=1;\ k_2=0\\ \begin{bmatrix}x_1\oplus x_2\oplus 1\\ x_1\oplus 1\end{bmatrix}, \text{ якщо } k_1=1;\ k_2=1\end{cases}=\begin{cases}\begin{bmatrix}x_1\\ x_1\oplus x_2\oplus 1\end{bmatrix}=\begin{bmatrix}x_1\oplus x_2\cdot k_2\oplus k_1\\ x_1\oplus x_2\cdot\bar{k}_2\oplus k_1\oplus k_2\oplus 1\end{bmatrix}, \text{ якщо } k_1=0;\ k_2=0\\ \begin{bmatrix}x_1\oplus x_2\\ x_1\end{bmatrix}=\begin{bmatrix}x_1\oplus x_2\cdot k_2\oplus k_1\\ x_1\oplus x_2\cdot\bar{k}_2\oplus k_1\oplus k_2\oplus 1\end{bmatrix}, \text{ якщо } k_1=0;\ k_2=1\\ \begin{bmatrix}x_1\oplus 1\\ x_1\oplus x_2\end{bmatrix}=\begin{bmatrix}x_1\oplus x_2\cdot k_2\oplus k_1\\ x_1\oplus x_2\cdot\bar{k}_2\oplus k_1\oplus k_2\oplus 1\end{bmatrix}, \text{ якщо } k_1=1;\ k_2=0\\ \begin{bmatrix}x_1\oplus x_2\oplus 1\\ x_1\oplus 1\end{bmatrix}=\begin{bmatrix}x_1\oplus x_2\cdot k_2\oplus k_1\\ x_1\oplus x_2\cdot\bar{k}_2\oplus k_1\oplus k_2\oplus 1\end{bmatrix}, \text{ якщо } k_1=1;\ k_2=1\end{cases}$$

Таким чином, операцію $O_{9,6,15,24}$ можна записати як:

$$O_{9,6,15,24}=\begin{cases}\begin{bmatrix}x_1\\ x_1\oplus x_2\oplus 1\end{bmatrix}=\begin{bmatrix}x_1\oplus x_2\cdot k_2\oplus k_1\\ x_1\oplus x_2\cdot\bar{k}_2\oplus k_1\oplus k_2\oplus 1\end{bmatrix}, \text{ якщо } k_1=0;\ k_2=0\\ \begin{bmatrix}x_1\oplus x_2\\ x_1\end{bmatrix}=\begin{bmatrix}x_1\oplus x_2\cdot k_2\oplus k_1\\ x_1\oplus x_2\cdot\bar{k}_2\oplus k_1\oplus k_2\oplus 1\end{bmatrix}, \text{ якщо } k_1=0;\ k_2=1\\ \begin{bmatrix}x_1\oplus 1\\ x_1\oplus x_2\end{bmatrix}=\begin{bmatrix}x_1\oplus x_2\cdot k_2\oplus k_1\\ x_1\oplus x_2\cdot\bar{k}_2\oplus k_1\oplus k_2\oplus 1\end{bmatrix}, \text{ якщо } k_1=1;\ k_2=0\\ \begin{bmatrix}x_1\oplus x_2\oplus 1\\ x_1\oplus 1\end{bmatrix}=\begin{bmatrix}x_1\oplus x_2\cdot k_2\oplus k_1\\ x_1\oplus x_2\cdot\bar{k}_2\oplus k_1\oplus k_2\oplus 1\end{bmatrix}, \text{ якщо } k_1=1;\ k_2=1\end{cases}=\begin{bmatrix}x_1\oplus x_2\cdot k_2\oplus k_1\\ x_1\oplus x_2\cdot\bar{k}_2\oplus k_1\oplus k_2\oplus 1\end{bmatrix}$$

Перестановочна схема побудови цієї операції представлена на рис. 3.16.

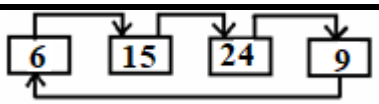
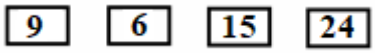
Схематичне представлення основної операції НДО 12	Перестановочна схема	Схематичне представлення отриманої операції $O_{9,6,15,24}$
		

Рис. 3.16 Перестановочна схема для побудови операції $O_{9,6,15,24}$ на основі основної операції дванадцятого НДО $O_{6,15,24,9}$

Математична модель операції $O_{15,24,9,6}$, що є синтезованою на основі моделі основної операції $O_{6,15,24,9}$ дванадцятого НДО, матиме вигляд [6]:

$$O_{15,24,9,6}=\begin{cases}\begin{bmatrix}x_1\oplus 1\\ x_1\oplus x_2\end{bmatrix}, \text{ якщо } k_1=0;\ k_2=0\\ \begin{bmatrix}x_1\oplus x_2\oplus 1\\ x_1\oplus 1\end{bmatrix}, \text{ якщо } k_1=0;\ k_2=1\\ \begin{bmatrix}x_1\\ x_1\oplus x_2\oplus 1\end{bmatrix}, \text{ якщо } k_1=1;\ k_2=0\\ \begin{bmatrix}x_1\oplus x_2\\ x_1\end{bmatrix}, \text{ якщо } k_1=1;\ k_2=1\end{cases}=\begin{cases}\begin{bmatrix}x_1\oplus 1\\ x_1\oplus x_2\end{bmatrix}=\begin{bmatrix}x_1\oplus x_2\cdot k_2\oplus k_1\oplus 1\\ x_1\oplus x_2\cdot \bar{k}_2\oplus k_1\oplus k_2\end{bmatrix}, \text{ якщо } k_1=0;\ k_2=0\\ \begin{bmatrix}x_1\oplus x_2\oplus 1\\ x_1\oplus 1\end{bmatrix}=\begin{bmatrix}x_1\oplus x_2\cdot k_2\oplus k_1\oplus 1\\ x_1\oplus x_2\cdot \bar{k}_2\oplus k_1\oplus k_2\end{bmatrix}, \text{ якщо } k_1=0;\ k_2=1\\ \begin{bmatrix}x_1\\ x_1\oplus x_2\oplus 1\end{bmatrix}=\begin{bmatrix}x_1\oplus x_2\cdot k_2\oplus k_1\oplus 1\\ x_1\oplus x_2\cdot \bar{k}_2\oplus k_1\oplus k_2\end{bmatrix}, \text{ якщо } k_1=1;\ k_2=0\\ \begin{bmatrix}x_1\oplus x_2\\ x_1\end{bmatrix}=\begin{bmatrix}x_1\oplus x_2\cdot k_2\oplus k_1\oplus 1\\ x_1\oplus x_2\cdot \bar{k}_2\oplus k_1\oplus k_2\end{bmatrix}, \text{ якщо } k_1=1;\ k_2=1\end{cases}$$

Таким чином, операцію $O_{15,24,9,6}$ можна записати як:

$$O_{15,24,9,6}=\begin{cases}\begin{bmatrix}x_1\oplus 1\\ x_1\oplus x_2\end{bmatrix}=\begin{bmatrix}x_1\oplus x_2\cdot k_2\oplus k_1\oplus 1\\ x_1\oplus x_2\cdot \bar{k}_2\oplus k_1\oplus k_2\end{bmatrix}, \text{ якщо } k_1=0;\ k_2=0\\ \begin{bmatrix}x_1\oplus x_2\oplus 1\\ x_1\oplus 1\end{bmatrix}=\begin{bmatrix}x_1\oplus x_2\cdot k_2\oplus k_1\oplus 1\\ x_1\oplus x_2\cdot \bar{k}_2\oplus k_1\oplus k_2\end{bmatrix}, \text{ якщо } k_1=0;\ k_2=1\\ \begin{bmatrix}x_1\\ x_1\oplus x_2\oplus 1\end{bmatrix}=\begin{bmatrix}x_1\oplus x_2\cdot k_2\oplus k_1\oplus 1\\ x_1\oplus x_2\cdot \bar{k}_2\oplus k_1\oplus k_2\end{bmatrix}, \text{ якщо } k_1=1;\ k_2=0\\ \begin{bmatrix}x_1\oplus x_2\\ x_1\end{bmatrix}=\begin{bmatrix}x_1\oplus x_2\cdot k_2\oplus k_1\oplus 1\\ x_1\oplus x_2\cdot \bar{k}_2\oplus k_1\oplus k_2\end{bmatrix}, \text{ якщо } k_1=1;\ k_2=1\end{cases}=\begin{bmatrix}x_1\oplus x_2\oplus k_1\oplus k_2\oplus 1\\ x_1\oplus k_1\end{bmatrix}$$

Перестановочна схема побудови цієї операції представлена на рис. 3.17.

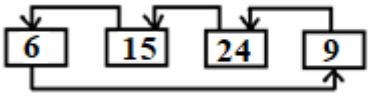
Схематичне представлення основної операції НДО 12	Перестановочна схема	Схематичне представлення отриманої операції $O_{15,24,9,6}$
		

Рис. 3.17 Перестановочна схема для побудови операції $O_{15,24,9,6}$ на основі основної операції дванадцятого НДО $O_{6,15,24,9}$

Математичну модель операції $O_{24,9,6,15}$, що є синтезованою на основі моделі операції $O_{6,15,24,9}$ дванадцятого набору двохоперандних операцій, представлено у вигляді:

$$O_{24,9,6,15}=\begin{cases}\begin{bmatrix}x_1\oplus x_2\oplus 1\\ x_1\oplus 1\end{bmatrix}, \textit{якщо } k_1=0;\ k_2=0\\ \begin{bmatrix}x_1\\ x_1\oplus x_2\oplus 1\end{bmatrix}, \textit{якщо } k_1=0;\ k_2=1\\ \begin{bmatrix}x_1\oplus x_2\\ x_1\end{bmatrix}, \textit{якщо } k_1=1;\ k_2=0\\ \begin{bmatrix}x_1\oplus 1\\ x_1\oplus x_2\end{bmatrix}, \textit{якщо } k_1=1;\ k_2=1\end{cases}=\begin{cases}\begin{bmatrix}x_1\oplus x_2\oplus 1\\ x_1\oplus 1\end{bmatrix}=\begin{bmatrix}x_1\oplus x_2\cdot\bar{k}_2\oplus k_1\oplus k_2\oplus 1\\ x_1\oplus x_2\cdot k_2\oplus k_1\oplus 1\end{bmatrix}, \textit{якщо } k_1=0;\ k_2=0\\ \begin{bmatrix}x_1\\ x_1\oplus x_2\oplus 1\end{bmatrix}=\begin{bmatrix}x_1\oplus x_2\cdot\bar{k}_2\oplus k_1\oplus k_2\oplus 1\\ x_1\oplus x_2\cdot k_2\oplus k_1\oplus 1\end{bmatrix}, \textit{якщо } k_1=0;\ k_2=1\\ \begin{bmatrix}x_1\oplus x_2\\ x_1\end{bmatrix}=\begin{bmatrix}x_1\oplus x_2\cdot\bar{k}_2\oplus k_1\oplus k_2\oplus 1\\ x_1\oplus x_2\cdot k_2\oplus k_1\oplus 1\end{bmatrix}, \textit{якщо } k_1=1;\ k_2=0\\ \begin{bmatrix}x_1\oplus 1\\ x_1\oplus x_2\end{bmatrix}=\begin{bmatrix}x_1\oplus x_2\cdot\bar{k}_2\oplus k_1\oplus k_2\oplus 1\\ x_1\oplus x_2\cdot k_2\oplus k_1\oplus 1\end{bmatrix}, \textit{якщо } k_1=1;\ k_2=1\end{cases}$$

Отже, операцію $O_{24,9,6,15}$ можна записати як:

$$O_{24,9,6,15}=\begin{cases}\begin{bmatrix}x_1\oplus x_2\oplus 1\\ x_1\oplus 1\end{bmatrix}=\begin{bmatrix}x_1\oplus x_2\cdot\bar{k}_2\oplus k_1\oplus k_2\oplus 1\\ x_1\oplus x_2\cdot k_2\oplus k_1\oplus 1\end{bmatrix}, \textit{якщо } k_1=0;\ k_2=0\\ \begin{bmatrix}x_1\\ x_1\oplus x_2\oplus 1\end{bmatrix}=\begin{bmatrix}x_1\oplus x_2\cdot\bar{k}_2\oplus k_1\oplus k_2\oplus 1\\ x_1\oplus x_2\cdot k_2\oplus k_1\oplus 1\end{bmatrix}, \textit{якщо } k_1=0;\ k_2=1\\ \begin{bmatrix}x_1\oplus x_2\\ x_1\end{bmatrix}=\begin{bmatrix}x_1\oplus x_2\cdot\bar{k}_2\oplus k_1\oplus k_2\oplus 1\\ x_1\oplus x_2\cdot k_2\oplus k_1\oplus 1\end{bmatrix}, \textit{якщо } k_1=1;\ k_2=0\\ \begin{bmatrix}x_1\oplus 1\\ x_1\oplus x_2\end{bmatrix}=\begin{bmatrix}x_1\oplus x_2\cdot\bar{k}_2\oplus k_1\oplus k_2\oplus 1\\ x_1\oplus x_2\cdot k_2\oplus k_1\oplus 1\end{bmatrix}, \textit{якщо } k_1=1;\ k_2=1\end{cases}=\begin{bmatrix}x_1\oplus x_2\cdot\bar{k}_2\oplus k_1\oplus k_2\oplus 1\\ x_1\oplus x_2\cdot k_2\oplus k_1\oplus 1\end{bmatrix}$$

Перестановочна схема побудови цієї операції представлена на рис. 3.18.

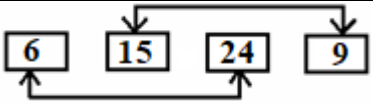
Схематичне представлення основної операції НДО 12	Перестановочна схема	Схематичне представлення отриманої операції $O_{24,9,6,15}$
		

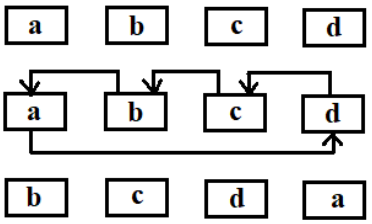
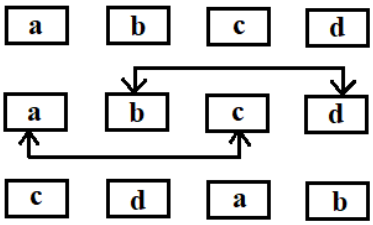
Рис. 3.18 Перестановочна схема для побудови операції $O_{24,9,6,15}$ на основі основної операції дванадцятого НДО $O_{6,15,24,9}$

3.7 Побудова узагальнюючих перестановочних схем для синтезу таблиць істинності двохоперандних операцій криптоперетворення другої математичної групи

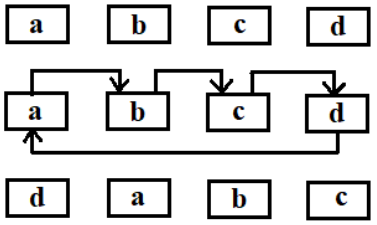
В процесі дослідження, було встановлено, що всі операції кожного НДО другої математичної групи двохоперандних операцій криптоперетворення (НДО 7-12) можуть бути отримані на основі узагальнюючих перестановочних схем, наведених в табл. 3.7 [4].

Таблиця 3.7

Узагальнюючі перестановочні схеми для другої математичної групи двохоперандних операцій криптоперетворення

№ перестановочної схеми		Перестановочна схема
1	НДО 7 $O_{1,8,13,20} \leftrightarrow O_{8,13,20,1}$; НДО 8 $O_{2,19,14,7} \leftrightarrow O_{20,2,8,14}$ НДО 9 $O_{3,12,21,18} \leftrightarrow O_{12,21,18,3}$; НДО 10 $O_{4,17,10,23} \leftrightarrow O_{17,10,23,4}$ НДО 11 $O_{5,22,11,16} \leftrightarrow O_{22,11,16,5}$; НДО 12 $O_{6,15,24,9} \leftrightarrow O_{15,24,9,6}$	
2	НДО 7 $O_{1,8,13,20} \leftrightarrow O_{13,20,1,8}$; НДО 8 $O_{2,19,14,7} \leftrightarrow O_{14,7,2,19}$; НДО 9 $O_{3,12,21,18} \leftrightarrow O_{21,18,3,12}$; НДО 10 $O_{4,17,10,23} \leftrightarrow O_{10,23,4,17}$; НДО 11 $O_{5,22,11,16} \leftrightarrow O_{11,16,5,22}$; НДО 12 $O_{6,15,24,9} \leftrightarrow O_{24,9,6,15}$	

Продовження таблиці 3.7

3	НДО 7 $O_{1,8,13,20} \leftrightarrow O_{20,1,8,13}$; НДО 8 $O_{2,19,14,7} \leftrightarrow O_{7,2,19,14}$; НДО 9 $O_{3,12,21,18} \leftrightarrow O_{18,3,12,21}$; НДО 10 $O_{4,17,10,23} \leftrightarrow O_{23,4,17,10}$; НДО 11 $O_{5,22,11,16} \leftrightarrow O_{16,5,22,11}$; НДО 12 $O_{6,15,24,9} \leftrightarrow O_{9,6,15,24}$	

Розглянемо сьомий набір двохоперандних операцій.

Перестановочні схеми для побудови таблиць істинності операцій НДО 7 на основі базової операції другої математичної групи представлені на рисунку 3.19.

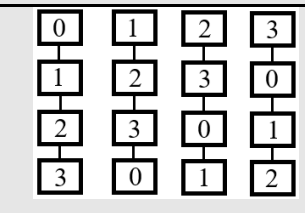
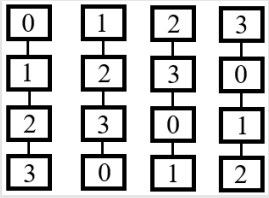
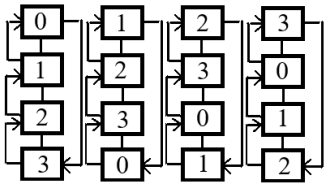
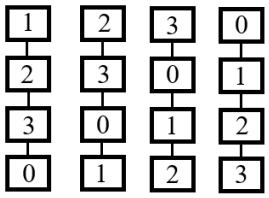
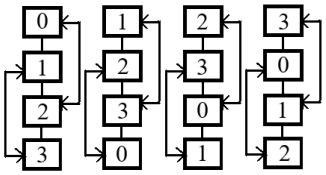
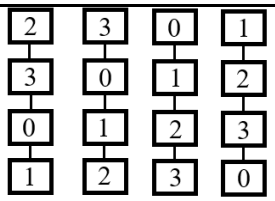
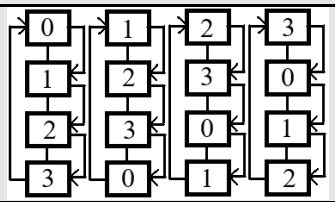
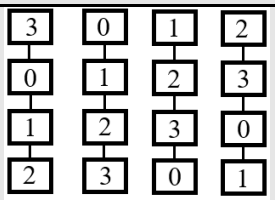
Схематичне представлення реалізації перестановочної схеми таблиці істинності базової операції		Схематичне представлення перестановочної схеми таблиці істинності базової операції	
перестановочна схема	Результат перестановки	перестановочна схема	Результат перестановки
$O_{1,8,13,20}$	$O_{1,8,13,20}$	$O_{1,8,13,20}$	$O_{8,13,20,1}$
			
$O_{1,8,13,20}$	$O_{13,20,1,8}$	$O_{1,8,13,20}$	$O_{20,1,8,13}$
			

Рис. 3.19 Перестановочні схеми для побудови таблиць істинності операцій НДО 7 на основі базової операції другої математичної групи

Таким чином, відповідно до рисунка 3.19, маємо такі результати:

– для реалізації перестановочної схеми таблиці істинності базової операції в операцію $O_{8,13,20,1}$ необхідна циклічна перестановка чотирьох елементів $0 \to 3 \to 2 \to 1 \to 0$;

– для реалізації перестановочної схеми таблиці істинності базової операції в операцію $O_{13,20,1,8}$ необхідна попарна перестановка елементів $0 \leftrightarrow 2$, а також $1 \leftrightarrow 3$;

– для реалізації перестановочної схеми таблиці істинності базової операції в операцію $O_{20,1,8,13}$ необхідна циклічна перестановка чотирьох елементів $0 \to 1 \to 2 \to 3 \to 0$.

Розглянемо восьмий набір двохоперандних операцій.

Результати побудови перестановочних схеми для побудови таблиць істинності операцій НДО 8 на основі базової операції другої математичної групи представлено на рисунку 3.20 [4].

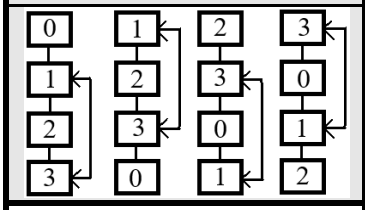
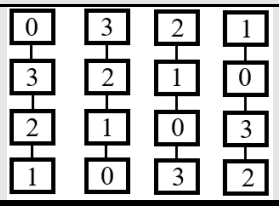
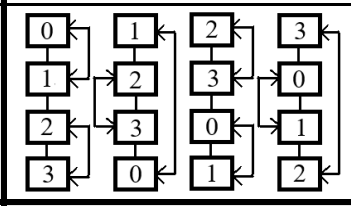
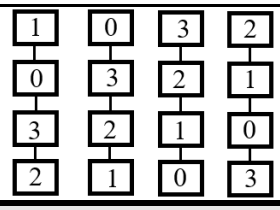
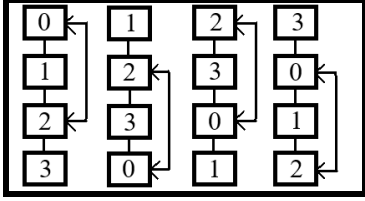
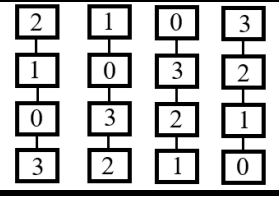
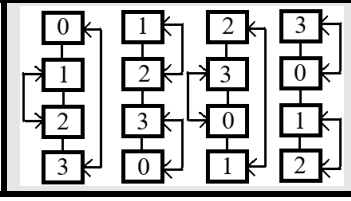
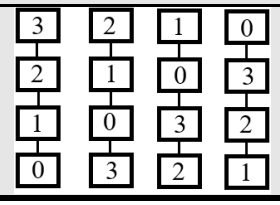
Схематичне представлення перестановочної схеми таблиці істинності базової операції	Схематичне представлення таблиці істинності отриманої операції	Схематичне представлення перестановочної схеми таблиці істинності базової операції	Схематичне представлення таблиці істинності отриманої операції
$O_{1,8,13,20}$	$O_{2,19,14,7}$	$O_{1,8,13,20}$	$O_{7,2,19,14}$
			
$O_{1,8,13,20}$	$O_{14,7,2,19}$	$O_{1,8,13,20}$	$O_{19,14,7,2}$
			

Рис. 3.20 Перестановочні схеми для побудови таблиць істинності операцій НДО 8 на основі базової операції другої математичної групи

Таким чином, згідно з рисунком 3.20 маємо такі результати:

– для реалізації перестановочної схеми таблиці істинності базової операції в операцію $O_{2,19,14,7}$ необхідна одинарна перестановка елементів $1 \leftrightarrow 3$;

– для реалізації перестановочної схеми таблиці істинності базової операції в операцію $O_{7,2,19,14}$ необхідна попарна перестановка елементів $0 \leftrightarrow 1$, а також $2 \leftrightarrow 3$;

– для реалізації перестановочної схеми таблиці істинності базової операції в операцію $O_{14,7,2,19}$ необхідна одинарна перестановка елементів $0 \leftrightarrow 2$;

– для реалізації перестановочної схеми таблиці істинності базової операції в операцію $O_{19,14,7,2}$ необхідна попарна перестановка елементів $0 \leftrightarrow 3$, а також $1 \leftrightarrow 2$.

Розглянемо дев'ятий набір двохоперандних операцій.

Перестановочні схеми для побудови таблиць істинності операцій НДО 9 на основі базової операції другої математичної групи представлені на рисунку 3.21.

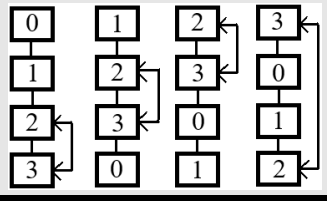
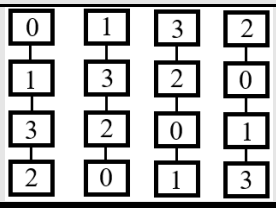
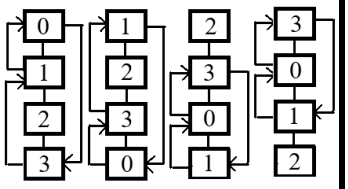
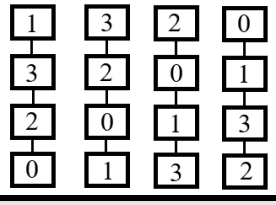
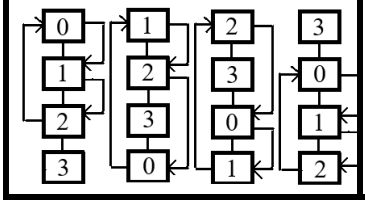
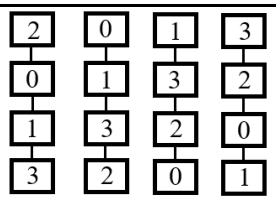
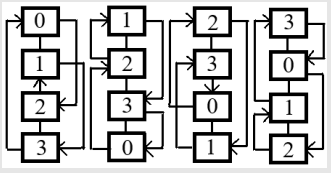
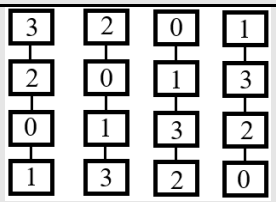
Схематичне представлення перестановочної схеми таблиці істинності базової операції	Схематичне представлення таблиці істинності отриманої операції	Схематичне представлення перестановочної схеми таблиці істинності базової операції	Схематичне представлення таблиці істинності отриманої операції
$O_{1,8,13,20}$	$O_{3,12,21,18}$	$O_{1,8,13,20}$	$O_{12,21,18,3}$
			
$O_{1,8,13,20}$	$O_{18,3,12,21}$	$O_{1,8,13,20}$	$O_{21,18,3,12}$
			

Рис. 3.21 Перестановочні схеми для побудови таблиць істинності операцій НДО 9 на основі базової операції другої математичної групи

Згідно даних, наведених на рисунку 3.21, маємо наступне :

– для реалізації перестановочної схеми таблиці істинності базової операції в операцію $O_{3,12,21,18}$ необхідна одинарна перестановка елементів $2 \leftrightarrow 3$;

– для реалізації перестановочної схеми таблиці істинності базової операції в операцію $O_{12,21,18,3}$ необхідна циклічна перестановка трьох елементів $0 \to 3 \to 1 \to 0$ (елемент 2 залишається без змін);

– для реалізації перестановочної схеми таблиці істинності базової операції в операцію $O_{18,3,12,21}$ необхідна циклічна перестановка трьох елементів $0 \to 1 \to 2 \to 0$ (елемент 3 залишається без змін);

– для реалізації перестановочної схеми таблиці істинності базової операції в операцію $O_{21,18,3,12}$ необхідна циклічна перестановка чотирьох елементів $0 \to 2 \to 1 \to 3 \to 0$.

Розглянемо десятий набір двохоперандних операцій.

Результати побудови перестановочних схеми для побудови таблиць істинності операцій НДО 10 на основі базової операції другої математичної групи представлено на рисунку 3.22 [4].

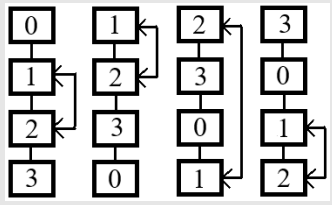
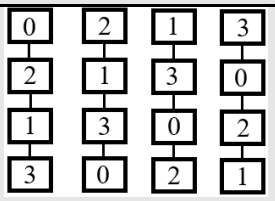
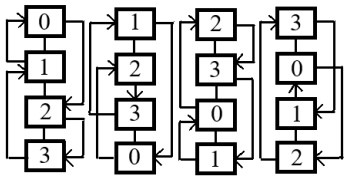
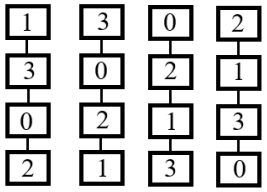
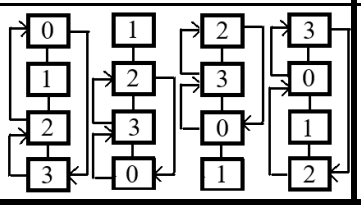
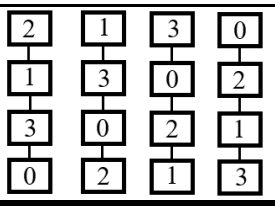
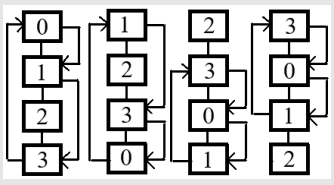
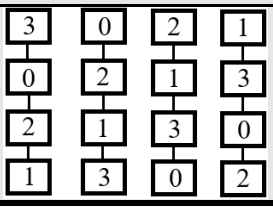
Схематичне представлення перестановочної схеми таблиці істинності базової операції	Схематичне представлення таблиці істинності отриманої операції	Схематичне представлення перестановочної схеми таблиці істинності базової операції	Схематичне представлення таблиці істинності отриманої операції
$O_{1,8,13,20}$	$O_{4,17,10,23}$	$O_{1,8,13,20}$ м	$O_{10,23,4,17}$
			
$O_{1,8,13,20}$	$O_{17,10,23,4}$	$O_{1,8,13,20}$	$O_{23,4,17,10}$
			

Рис. 3.22 Перестановочні схеми для побудови таблиць істинності операцій НДО 10 на основі базової операції другої математичної групи

Отже, відповідно до рисунку 3.22, маємо такі результати:

– для реалізації перестановочної схеми таблиці істинності базової операції в операцію $O_{4,17,10,23}$ необхідна одинарна перестановка елементів $1 \leftrightarrow 2$;

– для реалізації перестановочної схеми таблиці істинності базової операції в операцію $O_{10,23,4,17}$ необхідна циклічна перестановка чотирьох елементів $0 \to 2 \to 3 \to 1 \to 0$;

– для реалізації перестановочної схеми таблиці істинності базової операції в операцію $O_{17,10,23,4}$ необхідна циклічна перестановка трьох елементів $0 \to 3 \to 2 \to 0$ (елемент 1 залишається без змін);

– для реалізації перестановочної схеми таблиці істинності базової операції в операцію $O_{23,4,17,10}$ необхідна циклічна перестановка трьох елементів $0 \to 1 \to 3 \to 0$ (елемент 2 залишається без змін).

Розглянемо одинадцятий набір двохоперандних операцій.

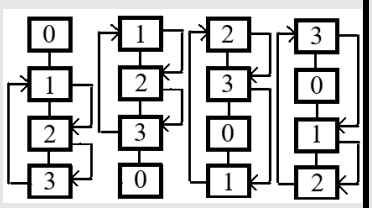
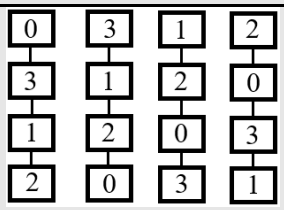
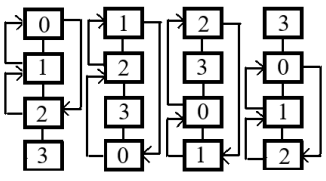
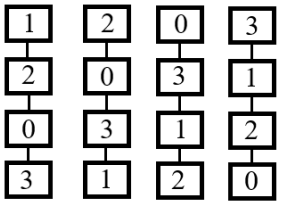
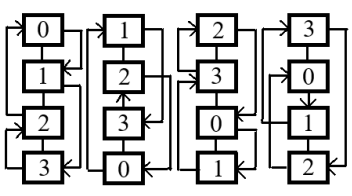
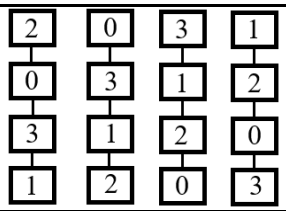
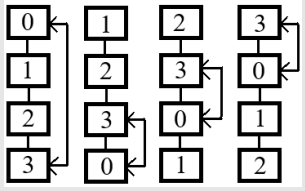
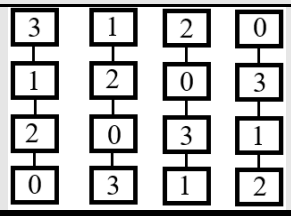
Схематичне представлення перестановочної схеми таблиці істинності базової операції	Схематичне представлення таблиці істинності отриманої операції	Схематичне представлення перестановочної схеми таблиці істинності базової операції	Схематичне представлення таблиці істинності отриманої операції
$O_{1,8,13,20}$	$O_{5,22,11,16}$	$O_{1,8,13,20}$	$O_{11,16,5,22}$
			
$O_{1,8,13,20}$	$O_{16,5,22,11}$	$O_{1,8,13,20}$	$O_{22,11,16,5}$
			

Рис. 3.23 Перестановочні схеми для побудови таблиць істинності операцій НДО 11 на основі базової операції другої математичної групи

Перестановочні схеми для побудови таблиць істинності операцій НДО 11 на основі базової операції другої математичної групи представлено на рисунку 3.23 [4].

Таким чином, відповідно до рисунка 3.23, маємо такі результати:

– для реалізації перестановочної схеми таблиці істинності базової операції в операцію $O_{5,22,11,16}$ необхідна циклічна перестановка трьох елементів $1 \to 2 \to 3 \to 1$ (елемент 0 залишається без змін);

– для реалізації перестановочної схеми таблиці істинності базової операції в операцію $O_{11,16,5,22}$ необхідна циклічна перестановка трьох елементів $0 \to 2 \to 1 \to 0$ (елемент 3 залишається без змін);

– для реалізації перестановочної схеми таблиці істинності базової операції в операцію $O_{16,5,22,11}$ необхідна циклічна перестановка чотирьох елементів $0 \to 1 \to 3 \to 2 \to 0$;

– для реалізації перестановочної схеми таблиці істинності базової операції в операцію $O_{22,11,16,5}$ необхідна одинарна перестановка елементів $0 \leftrightarrow 3$.

Розглянемо дванадцятий набір двохоперандних операцій.

Результати побудови перестановочних схем для побудови таблиць істинності операцій НДО 12 на основі базової операції другої математичної групи представлено на рисунку 3.24.

Отже, на рисунку 3.24 представлено такі результати:

– для реалізації перестановочної схеми таблиці істинності базової операції в операцію $O_{6,15,24,9}$ необхідна циклічна перестановка трьох елементів $1 \to 3 \to 2 \to 1$ (елемент 0 залишається без змін);

– для реалізації перестановочної схеми таблиці істинності базової операції в операцію $O_{9,6,15,24}$ необхідна одинарна перестановка елементів $0 \leftrightarrow 1$;

– для реалізації перестановочної схеми таблиці істинності базової операції в операцію $O_{15,24,9,6}$ необхідна циклічна перестановка чотирьох елементів $0 \to 3 \to 1 \to 2 \to 0$;

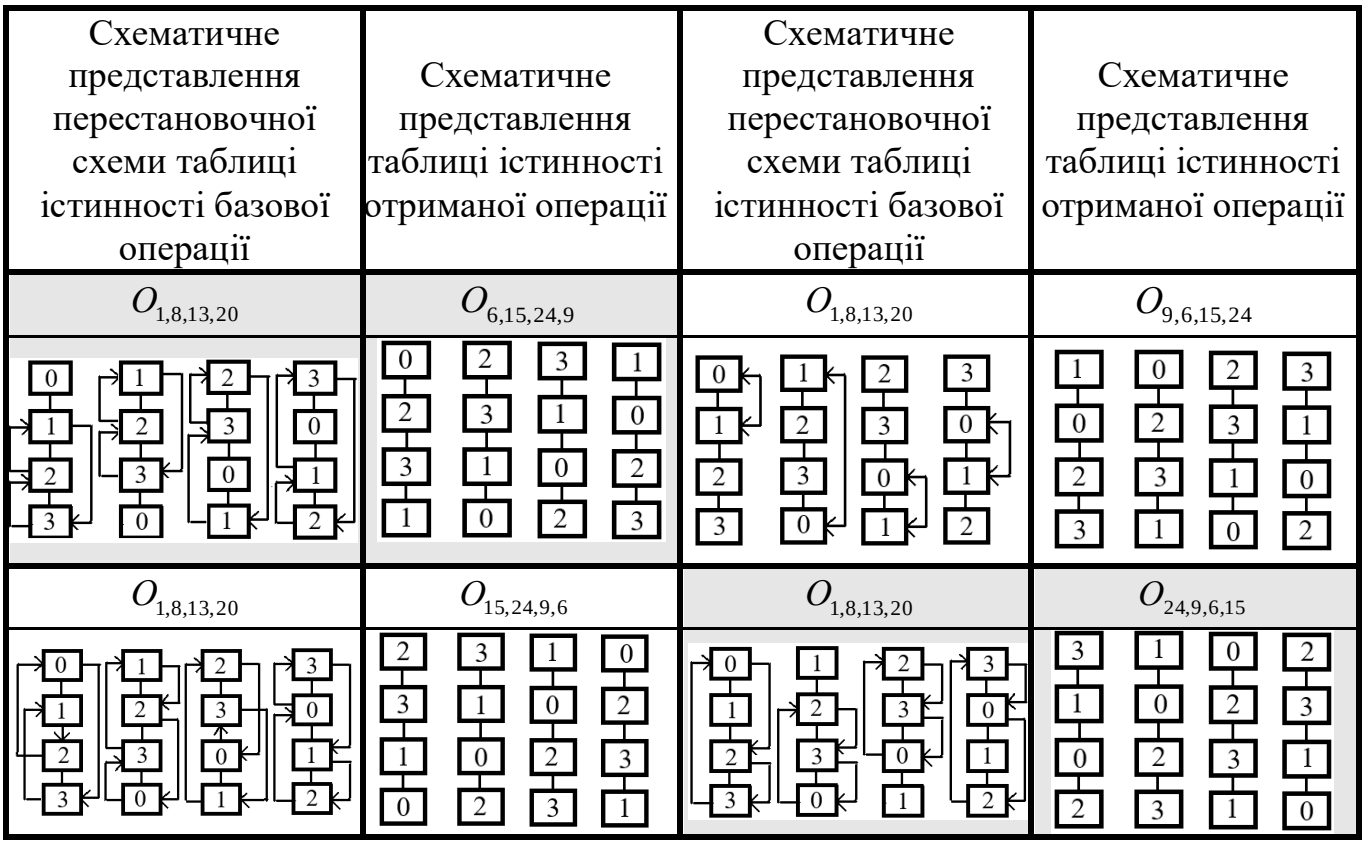


Рис. 3.24 Перестановочні схеми для побудови таблиць істинності операцій НДО 12 на основі базової операції другої математичної групи

– для реалізації перестановочної схеми таблиці істинності базової операції в операцію $O_{24,9,6,15}$ необхідна циклічна перестановка трьох елементів $0 \to 2 \to 3 \to 0$ (елемент 1 залишається без змін).

У ході дослідження перестановочних схем таблиць істинності встановлено наступне:

- Сукупність наборів таблиць істинності двохоперандних операцій криптоперетворення другої математичної групи створюють повну групу наборів таблиць істинності двохоперандних операцій криптоперетворення.
- Встановлено, що групи перестановочних схем першої та другої математичних груп досліджених операцій криптоперетворення співпадають.
- Отримало підтвердження припущення, що застосування повної групи перестановочних схем забезпечить побудову повної групи наборів двохоперандних операцій криптоперетворення невідомої групи, та їх таблиць підстановки, якщо взяти будь яку операцію з цієї невідомої групи.

Висновки з розділу 3

1. Виконано математичне моделювання та дослідження двохоперандних операцій криптографічного перетворення інформації другої математичної групи на основі відомих таблиць істинності, за результатами яких отримано нові, раніше не відомі симетричні двохоперандні двохрозрядні операції придатні для реалізації в потоковому шифруванні.

2. Для візуалізації і встановлення варіативності зміни взаємозв'язків між даними і результатами виконання операції побудовано перестановочні схеми та узагальнено перестановочні схеми побудови операцій. Слід відмітити, що узагальнені перестановочні схеми побудови операцій першої та другої груп операцій відрізняються.

3. Встановлено перестановочні схеми побудови таблиць істинності наборів двохоперандних операцій криптоперетворення другої групи операцій. В процесі дослідження перестановочних схем таблиць істинності першої та другої групп двохоперандних операцій криптоперетворення встановлено наступне:

- сукупність наборів таблиць істинності двохоперандних операцій криптоперетворення другої математичної групи створюють повну групу наборів таблиць істинності двохоперандних операцій криптоперетворення.
- встановлено, що групи перестановочних схем першої та другої математичної групи досліджених операцій криптоперетворення співпадають.

4. Отримало підтвердження припущення, що застосування повної групи перестановочних схем забезпечить побудову повної групи наборів двохоперандних операцій криптоперетворення невідомої групи та їх таблиць підстановки, якщо взяти будь-яку операцію з цієї невідомої групи.

5. Результати розділу опубліковано в [2, 4, 6].

РОЗДІЛ 4 СИНТЕЗ ГРУП ДВОХОПЕРАНДНИХ ОПЕРАЦІЙ КРИПТОПЕРЕТВОРЕННЯ ТА ОЦІНКА ЕФЕКТИВНОСТІ ЇХ ЗАСТОСУВАННЯ

4.1 Узагальнення результатів дослідження та синтез операцій криптоперетворення першої математичної групи

4.1.1 Узагальнення результатів дослідження операцій криптоперетворення першої математичної групи

Одноопераднді операції криптографічного перетворення інформації поділяються на базові операції, операції перестановок, які накладаються на базові операції та операції інверсії, які накладаються на базові операції та операції перестановок [11, 103]. Представимо відповідно до цієї класифікації одноопераднді двохрозрядні операції криптографічного перетворення інформації, які наведено в [104]. Результати класифікації цих операцій наведено в табл. 4.1.

Вибір розрядності операцій, які було класифіковано, проводився, виходячи з розрядності двохоперандних операцій, які синтезуються в цій роботі, а також виходячи з потужності груп операцій. Математичні групи синтезованих операцій включають по 24 операції, і класифікована група операцій також включає 24 операції.

Можна припустити, що за аналогією до одноопераднних операцій двохоперандні операції також можна класифікувати на базові операції, операції перестановок та операції інверсії.

Дослідимо можливість класифікації математичних моделей двохоперандних двохрозрядних операцій криптографічного перетворення інформації, отриманих в розділі 2. Рузультати класифікації першої симетричної групи двохоперандних двохрозрядних операцій криптографічного перетворення інформації наведено в табл. 4.2.

Таблиця 4.1

Класифікація одноопераднних двохрозрядних операцій криптографічного перетворення інформації

Класифікатор операцій	**Операції інверсії**			
	$\begin{bmatrix}0\\0\end{bmatrix}$	$\begin{bmatrix}0\\1\end{bmatrix}$	$\begin{bmatrix}1\\0\end{bmatrix}$	$\begin{bmatrix}1\\1\end{bmatrix}$
Базові операції	$F_{3,5}=\begin{bmatrix}x_1\\x_2\end{bmatrix}$	$F_{3,10}=\begin{bmatrix}x_1\\x_2\oplus 1\end{bmatrix}$	$F_{12,5}=\begin{bmatrix}x_1\oplus 1\\x_2\end{bmatrix}$	$F_{12,10}=\begin{bmatrix}x_1\oplus 1\\x_2\oplus 1\end{bmatrix}$
	$F_{6,5}=\begin{bmatrix}x_1\oplus x_2\\x_2\end{bmatrix}$	$F_{6,10}=\begin{bmatrix}x_1\oplus x_2\\x_2\oplus 1\end{bmatrix}$	$F_{9,5}=\begin{bmatrix}x_1\oplus x_2\oplus 1\\x_2\end{bmatrix}$	$F_{9,10}=\begin{bmatrix}x_1\oplus x_2\oplus 1\\x_2\oplus 1\end{bmatrix}$
	$F_{3,6}=\begin{bmatrix}x_1\\x_1\oplus x_2\end{bmatrix}$	$F_{3,9}=\begin{bmatrix}x_1\\x_1\oplus x_2\oplus 1\end{bmatrix}$	$F_{12,6}=\begin{bmatrix}x_1\oplus 1\\x_1\oplus x_2\end{bmatrix}$	$F_{12,9}=\begin{bmatrix}x_1\oplus 1\\x_1\oplus x_2\oplus 1\end{bmatrix}$
Операції перестановок	$F_{5,3}=\begin{bmatrix}x_2\\x_1\end{bmatrix}$	$F_{5,12}=\begin{bmatrix}x_2\\x_1\oplus 1\end{bmatrix}$	$F_{10,3}=\begin{bmatrix}x_2\oplus 1\\x_1\end{bmatrix}$	$F_{10,12}=\begin{bmatrix}x_2\oplus 1\\x_1\oplus 1\end{bmatrix}$
	$F_{5,6}=\begin{bmatrix}x_2\\x_1\oplus x_2\end{bmatrix}$	$F_{5,9}=\begin{bmatrix}x_2\\x_1\oplus x_2\oplus 1\end{bmatrix}$	$F_{10,6}=\begin{bmatrix}x_2\oplus 1\\x_1\oplus x_2\end{bmatrix}$	$F_{10,9}=\begin{bmatrix}x_2\oplus 1\\x_1\oplus x_2\oplus 1\end{bmatrix}$
	$F_{6,3}=\begin{bmatrix}x_1\oplus x_2\\x_1\end{bmatrix}$	$F_{6,12}=\begin{bmatrix}x_1\oplus x_2\\x_1\oplus 1\end{bmatrix}$	$F_{9,3}=\begin{bmatrix}x_1\oplus x_2\oplus 1\\x_1\end{bmatrix}$	$F_{9,12}=\begin{bmatrix}x_1\oplus x_2\oplus 1\\x_1\oplus 1\end{bmatrix}$

Таблиця 4.2

Класифікація першої симетричної групи двохоперандних двохрозрядних операцій криптографічного додавання (групи двохрозрядних операцій додавання за модулем два)

Класифікатор операцій	**Операції інверсії**			
	$\begin{bmatrix}0\\0\end{bmatrix}$	$\begin{bmatrix}0\\1\end{bmatrix}$	$\begin{bmatrix}1\\0\end{bmatrix}$	$\begin{bmatrix}1\\1\end{bmatrix}$
Базові операції	$O_{1,7,13,19}=\begin{bmatrix}x_1\oplus k_1\\x_2\oplus k_2\end{bmatrix}$	$O_{7,1,19,13}=\begin{bmatrix}x_1\oplus k_1\\x_2\oplus k_2\oplus 1\end{bmatrix}$	$O_{13,19,1,7}=\begin{bmatrix}x_1\oplus k_1\oplus 1\\x_2\oplus k_2\end{bmatrix}$	$O_{19,13,7,1}=\begin{bmatrix}x_1\oplus k_1\oplus 1\\x_2\oplus k_2\oplus 1\end{bmatrix}$
	$O_{2,20,14,8}=\begin{bmatrix}x_1\oplus x_2\oplus k_1\oplus k_2\\x_2\oplus k_2\end{bmatrix}$	$O_{8,14,20,2}=\begin{bmatrix}x_1\oplus x_2\oplus k_1\oplus k_2\\x_2\oplus k_2\oplus 1\end{bmatrix}$	$O_{14,8,2,20}=\begin{bmatrix}x_1\oplus x_2\oplus k_1\oplus k_2\oplus 1\\x_2\oplus k_2\end{bmatrix}$	$O_{20,2,8,14}=\begin{bmatrix}x_1\oplus x_2\oplus k_1\oplus k_2\oplus 1\\x_2\oplus k_2\oplus 1\end{bmatrix}$
	$O_{3,9,21,15}=\begin{bmatrix}x_1\oplus k_1\\x_1\oplus x_2\oplus k_1\oplus k_2\end{bmatrix}$	$O_{9,3,15,21}=\begin{bmatrix}x_1\oplus k_1\\x_1\oplus x_2\oplus k_1\oplus k_2\oplus 1\end{bmatrix}$	$O_{15,21,9,3}=\begin{bmatrix}x_1\oplus k_1\oplus 1\\x_1\oplus x_2\oplus k_1\oplus k_2\end{bmatrix}$	$O_{21,15,3,9}=\begin{bmatrix}x_1\oplus k_1\oplus 1\\x_1\oplus x_2\oplus k_1\oplus k_2\oplus 1\end{bmatrix}$
Операції перестановок	$O_{4,16,10,22}=\begin{bmatrix}x_2\oplus k_2\\x_1\oplus k_1\end{bmatrix}$	$O_{10,22,4,16}=\begin{bmatrix}x_2\oplus k_2\\x_1\oplus k_1\oplus 1\end{bmatrix}$	$O_{16,4,22,10}=\begin{bmatrix}x_2\oplus k_2\oplus 1\\x_1\oplus k_1\end{bmatrix}$	$O_{22,10,16,4}=\begin{bmatrix}x_2\oplus k_2\oplus 1\\x_1\oplus k_1\oplus 1\end{bmatrix}$
	$O_{5,23,11,17}=\begin{bmatrix}x_2\oplus k_2\\x_1\oplus x_2\oplus k_1\oplus k_2\end{bmatrix}$	$O_{11,17,5,23}=\begin{bmatrix}x_2\oplus k_2\\x_1\oplus x_2\oplus k_1\oplus k_2\oplus 1\end{bmatrix}$	$O_{17,11,23,5}=\begin{bmatrix}x_2\oplus k_2\oplus 1\\x_1\oplus x_2\oplus k_1\oplus k_2\end{bmatrix}$	$O_{23,5,17,11}=\begin{bmatrix}x_2\oplus k_2\oplus 1\\x_1\oplus x_2\oplus k_1\oplus k_2\oplus 1\end{bmatrix}$
	$O_{6,18,24,12}=\begin{bmatrix}x_1\oplus x_2\oplus k_1\oplus k_2\\x_1\oplus k_1\end{bmatrix}$	$O_{12,24,18,6}=\begin{bmatrix}x_1\oplus x_2\oplus k_1\oplus k_2\\x_1\oplus k_1\oplus 1\end{bmatrix}$	$O_{18,6,12,24}=\begin{bmatrix}x_1\oplus x_2\oplus k_1\oplus k_2\oplus 1\\x_1\oplus k_1\end{bmatrix}$	$O_{24,12,6,18}=\begin{bmatrix}x_1\oplus x_2\oplus k_1\oplus k_2\oplus 1\\x_1\oplus k_1\oplus 1\end{bmatrix}$

Перша класифікована базова операція є двохрозрядною операцією додавання по модулю два [35], і тому першу математичну групу операцій, синтезованих в р. 2 будемо називати групою двохрозрядних операцій додавання за модулем два.

4.1.2 Метод синтезу операцій криптоперетворення першої математичної групи (групи двохрозрядних операцій додавання за модулем два)

Методи синтезу одноопераднних двохрозрядних операцій криптоперетворення відомі [105]. Розробимо метод синтезу групи двохрозрядних операцій додавання за модулем два на основі відомих одноопераднних двохрозрядних операцій. Для розробки методу синтезу проведемо порівняльне дослідження табл.4.1 і табл. 4.2.

Розглянемо перші рядки таблиць, слід відмітити, що перший рядок табл. 4.2 відображає операції НДО 1.

Під час порівняльного аналізу отримано взаємозв'язки між моделями, які можна формалізувати таким чином.

Якщо $F_{3,5}^{1}=\begin{bmatrix} x_1 \\ x_2 \end{bmatrix}$ - операція перетворення першого операнда, а $F_{3,5}^{2}=\begin{bmatrix} k_1 \\ k_2 \end{bmatrix}$ – операція перетворення другого операнда, тоді $F_{3,5}^{1}\oplus F_{3,5}^{2}=\begin{bmatrix} x_1 \\ x_2 \end{bmatrix}\oplus\begin{bmatrix} k_1 \\ k_2 \end{bmatrix}=\begin{bmatrix} x_1\oplus k_1 \\ x_2\oplus k_2 \end{bmatrix}=O_{1,7,13,19}$.

Якщо $F_{3,10}^{1}=\begin{bmatrix} x_1 \\ x_2\oplus 1 \end{bmatrix}$ - операція перетворення першого операнда, а $F_{3,5}^{2}=\begin{bmatrix} k_1 \\ k_2 \end{bmatrix}$ – операція перетворення другого операнда, тоді $F_{3,10}^{1}\oplus F_{3,5}^{2}=\begin{bmatrix} x_1 \\ x_2\oplus 1 \end{bmatrix}\oplus\begin{bmatrix} k_1 \\ k_2 \end{bmatrix}=\begin{bmatrix} x_1\oplus k_1 \\ x_2\oplus k_2\oplus 1 \end{bmatrix}=O_{7,1,19,13}$.

Якщо $F^1_{12,5}=\begin{bmatrix} x_1 \oplus 1 \\ x_2 \end{bmatrix}$ – операція перетворення першого операнда, а $F^2_{3,5}=\begin{bmatrix} k_1 \\ k_2 \end{bmatrix}$ – операція перетворення другого операнда, тоді $F^1_{12,5} \oplus F^2_{3,5}=\begin{bmatrix} x_1 \oplus 1 \\ x_2 \end{bmatrix} \oplus \begin{bmatrix} k_1 \\ k_2 \end{bmatrix} = \begin{bmatrix} x_1 \oplus k_1 \oplus 1 \\ x_2 \oplus k_2 \end{bmatrix} = O_{13,19,1,7}$

Якщо $F^1_{12,10}=\begin{bmatrix} x_1 \oplus 1 \\ x_2 \oplus 1 \end{bmatrix}$ - операція перетворення першого операнда, а $F^2_{3,5}=\begin{bmatrix} k_1 \\ k_2 \end{bmatrix}$ – операція перетворення другого операнда, тоді $F^1_{12,10} \oplus F^2_{3,5}=\begin{bmatrix} x_1 \oplus 1 \\ x_2 \oplus 1 \end{bmatrix} \oplus \begin{bmatrix} k_1 \\ k_2 \end{bmatrix} = \begin{bmatrix} x_1 \oplus k_1 \oplus 1 \\ x_2 \oplus k_2 \oplus 1 \end{bmatrix} = O_{19,13,7,1}$.

На основі наведених формалізованих перетворень можна константувати наступне: двохрозрядні операції НДО 1 можна отримати шляхом додавання по модулю два до одноопераднних операцій криптоперетворення першого операнда, наведених в групі 1 одноопераднної операції обробки другого операнда $F^2_{3,5}=\begin{bmatrix} k_1 \\ k_2 \end{bmatrix}$. В результаті додавання будуть отримані моделі двохрозрядних операцій додавання

Наведемо формалізовані взаємозв’язки, які отримано при дослідженні операцій в других рядках табл. 4.1 та табл. 4.2 (НДО 2).

Якщо $F^1_{6,5}=\begin{bmatrix} x_1 \oplus x_2 \\ x_2 \end{bmatrix}$ – операція перетворення першого операнда, а $F^2_{6,5}=\begin{bmatrix} k_1 \oplus k_2 \\ k_2 \end{bmatrix}$ – операція перетворення другого операнда, тоді $F^1_{6,5} \oplus F^2_{6,5}=\begin{bmatrix} x_1 \oplus x_2 \\ x_2 \end{bmatrix} \oplus \begin{bmatrix} k_1 \oplus k_2 \\ k_2 \end{bmatrix} = \begin{bmatrix} x_1 \oplus x_2 \oplus k_1 \oplus k_2 \\ x_2 \oplus k_2 \end{bmatrix} = O_{2,20,14,8}$.

Якщо $F^1_{6,10}=\begin{bmatrix} x_1 \oplus x_2 \\ x_2 \oplus 1 \end{bmatrix}$ – операція перетворення першого операнда, а $F^2_{6,5}=\begin{bmatrix} k_1 \oplus k_2 \\ k_2 \end{bmatrix}$ – операція перетворення другого операнда, тоді $F^1_{6,10} \oplus F^2_{6,5}=\begin{bmatrix} x_1 \oplus x_2 \\ x_2 \oplus 1 \end{bmatrix} \oplus \begin{bmatrix} k_1 \oplus k_2 \\ k_2 \end{bmatrix} = \begin{bmatrix} x_1 \oplus x_2 \oplus k_1 \oplus k_2 \\ x_2 \oplus k_2 \oplus 1 \end{bmatrix} = O_{8,14,20,2}$.

Якщо $F_{9,5}^{1}=\begin{bmatrix} x_1 \oplus x_2 \oplus 1 \\ x_2 \end{bmatrix}$ – операція перетворення першого операнда, а $F_{6,5}^{2}=\begin{bmatrix} k_1 \oplus k_2 \\ k_2 \end{bmatrix}$ – операція перетворення другого операнда, тоді $F_{9,5}^{1} \oplus F_{6,5}^{2}=\begin{bmatrix} x_1 \oplus x_2 \oplus 1 \\ x_2 \end{bmatrix} \oplus \begin{bmatrix} k_1 \oplus k_2 \\ k_2 \end{bmatrix} = \begin{bmatrix} x_1 \oplus x_2 \oplus k_1 \oplus k_2 \oplus 1 \\ x_2 \oplus k_2 \end{bmatrix} = O_{14,8,2,20}$.

Якщо $F_{9,10}^{1}=\begin{bmatrix} x_1 \oplus x_2 \oplus 1 \\ x_2 \oplus 1 \end{bmatrix}$ – операція перетворення першого операнда, а $F_{6,5}^{2}=\begin{bmatrix} k_1 \oplus k_2 \\ k_2 \end{bmatrix}$ – операція перетворення другого операнда, тоді $F_{9,10}^{1} \oplus F_{6,5}^{2}=\begin{bmatrix} x_1 \oplus x_2 \oplus 1 \\ x_2 \oplus 1 \end{bmatrix} \oplus \begin{bmatrix} k_1 \oplus k_2 \\ k_2 \end{bmatrix} = \begin{bmatrix} x_1 \oplus x_2 \oplus k_1 \oplus k_2 \oplus 1 \\ x_2 \oplus k_2 \oplus 1 \end{bmatrix} = O_{20,2,8,14}$.

В результаті дослідження встановлено, що двохрозрядні операції НДО 2 можна отримати шляхом додавання по модулю два до одноопераднних операцій криптоперетворення першого операнда, наведених в групі 1 одноопераднної операції обробки другого операнда $F_{6,5}^{2}=\begin{bmatrix} k_1 \oplus k_2 \\ k_2 \end{bmatrix}$.

Дослідимо взаємозв’язки між третіми рядками табл. 4.1 і табл. 4.2 та формалізуємо, які отримані результати.

Якщо $F_{3,6}^{1}=\begin{bmatrix} x_1 \\ x_1 \oplus x_2 \end{bmatrix}$ – операція перетворення першого операнда, а $F_{3,6}^{2}=\begin{bmatrix} k_1 \\ k_1 \oplus k_2 \end{bmatrix}$ – операція перетворення другого операнда, тоді $F_{3,6}^{1} \oplus F_{3,6}^{2}=\begin{bmatrix} x_1 \\ x_1 \oplus x_2 \end{bmatrix} \oplus \begin{bmatrix} k_1 \\ k_1 \oplus k_2 \end{bmatrix} = \begin{bmatrix} x_1 \oplus k_1 \\ x_1 \oplus x_2 \oplus k_1 \oplus k_2 \end{bmatrix} = O_{3,9,21,15}$.

Якщо $F_{3,9}^{1}=\begin{bmatrix} x_1 \\ x_1 \oplus x_2 \oplus 1 \end{bmatrix}$ – операція перетворення першого операнда, а $F_{3,6}^{2}=\begin{bmatrix} k_1 \\ k_1 \oplus k_2 \end{bmatrix}$ – операція перетворення другого операнда, тоді $F_{3,9}^{1} \oplus F_{3,6}^{2}=\begin{bmatrix} x_1 \\ x_1 \oplus x_2 \oplus 1 \end{bmatrix} \oplus \begin{bmatrix} k_1 \\ k_1 \oplus k_2 \end{bmatrix} = \begin{bmatrix} x_1 \oplus k_1 \\ x_1 \oplus x_2 \oplus k_1 \oplus k_2 \oplus 1 \end{bmatrix} = O_{9,3,15,21}$.

Якщо $F_{12,6}^{1}=\begin{bmatrix} x_1 \oplus 1 \\ x_1 \oplus x_2 \end{bmatrix}$ – операція перетворення першого операнда, а $F_{3,6}^{2}=\begin{bmatrix} k_1 \\ k_1 \oplus k_2 \end{bmatrix}$ – операція перетворення другого операнда, тоді $F_{12,6}^{1} \oplus F_{3,6}^{2}=\begin{bmatrix} x_1 \oplus 1 \\ x_1 \oplus x_2 \end{bmatrix} \oplus \begin{bmatrix} k_1 \\ k_1 \oplus k_2 \end{bmatrix}=\begin{bmatrix} x_1 \oplus k_1 \oplus 1 \\ x_1 \oplus x_2 \oplus k_1 \oplus k_2 \end{bmatrix}=O_{15,21,9,3}$.

Якщо $F_{12,9}^{1}=\begin{bmatrix} x_1 \oplus 1 \\ x_1 \oplus x_2 \oplus 1 \end{bmatrix}$ – операція перетворення першого операнда, а $F_{3,6}^{2}=\begin{bmatrix} k_1 \\ k_1 \oplus k_2 \end{bmatrix}$ – операція перетворення другого операнда, тоді $F_{12,9}^{1} \oplus F_{3,6}^{2}=\begin{bmatrix} x_1 \oplus 1 \\ x_1 \oplus x_2 \oplus 1 \end{bmatrix} \oplus \begin{bmatrix} k_1 \\ k_1 \oplus k_2 \end{bmatrix}=\begin{bmatrix} x_1 \oplus k_1 \oplus 1 \\ x_1 \oplus x_2 \oplus k_1 \oplus k_2 \oplus 1 \end{bmatrix}=O_{21,15,3,9}$.

Встановлено, що операції НДО 3 можна отримати шляхом додавання по модулю два до одноопераднних операцій криптоперетворення першого операнда, одноопераднної операції обробки другого операнда $F_{3,6}^{2}=\begin{bmatrix} k_1 \\ k_1 \oplus k_2 \end{bmatrix}$.

Формалізуємо взаємозв'язки між четвертими рядками табл. 4.1 та табл. 4.2 (НДО 4).

Якщо $F_{5,3}^{1}=\begin{bmatrix} x_2 \\ x_1 \end{bmatrix}$ – операція перетворення першого операнда, а $F_{5,3}^{2}=\begin{bmatrix} k_2 \\ k_1 \end{bmatrix}$ – операція перетворення другого операнда, тоді $F_{5,3}^{1} \oplus F_{5,3}^{2}=\begin{bmatrix} x_2 \\ x_1 \end{bmatrix} \oplus \begin{bmatrix} k_2 \\ k_1 \end{bmatrix}=\begin{bmatrix} x_2 \oplus k_2 \\ x_1 \oplus k_1 \end{bmatrix}=O_{4,16,10,22}$.

Якщо $F_{5,12}^{1}=\begin{bmatrix} x_2 \\ x_1 \oplus 1 \end{bmatrix}$ – операція перетворення першого операнда, а $F_{5,3}^{2}=\begin{bmatrix} k_2 \\ k_1 \end{bmatrix}$ – операція перетворення другого операнда, тоді $F_{5,12}^{1} \oplus F_{5,3}^{2}=\begin{bmatrix} x_2 \\ x_1 \oplus 1 \end{bmatrix} \oplus \begin{bmatrix} k_2 \\ k_1 \end{bmatrix}=\begin{bmatrix} x_2 \oplus k_2 \\ x_1 \oplus k_1 \oplus 1 \end{bmatrix}=O_{10,22,4,16}$.

Якщо $F^1_{10,3}=\begin{bmatrix} x_2 \oplus 1 \\ x_1 \end{bmatrix}$ – операція перетворення першого операнда, а $F^2_{5,3}=\begin{bmatrix} k_2 \\ k_1 \end{bmatrix}$ – операція перетворення другого операнда, тоді $F^1_{10,3} \oplus F^2_{5,3}=\begin{bmatrix} x_2 \oplus 1 \\ x_1 \end{bmatrix} \oplus \begin{bmatrix} k_2 \\ k_1 \end{bmatrix} = \begin{bmatrix} x_2 \oplus k_2 \oplus 1 \\ x_1 \oplus k_1 \end{bmatrix} = O_{16,4,22,10}$.

Якщо $F^1_{10,12}=\begin{bmatrix} x_2 \oplus 1 \\ x_1 \oplus 1 \end{bmatrix}$ – операція перетворення першого операнда, а $F^2_{5,3}=\begin{bmatrix} k_2 \\ k_1 \end{bmatrix}$ – операція перетворення другого операнда, тоді $F^1_{10,12} \oplus F^2_{5,3}=\begin{bmatrix} x_2 \oplus 1 \\ x_1 \oplus 1 \end{bmatrix} \oplus \begin{bmatrix} k_2 \\ k_1 \end{bmatrix} = \begin{bmatrix} x_2 \oplus k_2 \oplus 1 \\ x_1 \oplus k_1 \oplus 1 \end{bmatrix} = O_{22,10,16,4}$.

Встановлено, що двохрозрядні операції, які входять до НДО 4, можна отримати шляхом додавання по модулю два до одноопераднних операцій криптоперетворення першого операнда, наведених у четвертому рядку табл. 4.1, одноопераднної операції обробки другого операнда $F^2_{5,3}=\begin{bmatrix} k_2 \\ k_1 \end{bmatrix}$.

Дослідимо взаємозв’язки необхідні для синтезу НДО 5.

Якщо $F^1_{5,6}=\begin{bmatrix} x_2 \\ x_1 \oplus x_2 \end{bmatrix}$ – операція перетворення першого операнда, а $F^2_{5,6}=\begin{bmatrix} k_2 \\ k_1 \oplus k_2 \end{bmatrix}$ – операція перетворення другого операнда, тоді $F^1_{5,6} \oplus F^2_{5,6}=\begin{bmatrix} x_2 \\ x_1 \oplus x_2 \end{bmatrix} \oplus \begin{bmatrix} k_2 \\ k_1 \oplus k_2 \end{bmatrix} = \begin{bmatrix} x_2 \oplus k_2 \\ x_1 \oplus x_2 \oplus k_1 \oplus k_2 \end{bmatrix} = O_{5,23,11,17}$.

Якщо $F^1_{5,9}=\begin{bmatrix} x_2 \\ x_1 \oplus x_2 \oplus 1 \end{bmatrix}$ – операція перетворення першого операнда, а $F^2_{5,6}=\begin{bmatrix} k_2 \\ k_1 \oplus k_2 \end{bmatrix}$ – операція перетворення другого операнда, тоді $F^1_{5,9} \oplus F^2_{5,6}=\begin{bmatrix} x_2 \\ x_1 \oplus x_2 \oplus 1 \end{bmatrix} \oplus \begin{bmatrix} k_2 \\ k_1 \oplus k_2 \end{bmatrix} = \begin{bmatrix} x_2 \oplus k_2 \\ x_1 \oplus x_2 \oplus k_1 \oplus k_2 \oplus 1 \end{bmatrix} = O_{11,17,5,23}$.

Якщо $F_{10,6}^{1}=\begin{bmatrix} x_2 \oplus 1 \\ x_1 \oplus x_2 \end{bmatrix}$ – операція перетворення першого операнда, а $F_{5,6}^{2}=\begin{bmatrix} k_2 \\ k_1 \oplus k_2 \end{bmatrix}$ – операція перетворення другого операнда, тоді $F_{10,6}^{1} \oplus F_{5,6}^{2}=\begin{bmatrix} x_2 \oplus 1 \\ x_1 \oplus x_2 \end{bmatrix} \oplus \begin{bmatrix} k_2 \\ k_1 \oplus k_2 \end{bmatrix}=\begin{bmatrix} x_2 \oplus k_2 \oplus 1 \\ x_1 \oplus x_2 \oplus k_1 \oplus k_2 \end{bmatrix}=O_{17,11,23,5}$.

Якщо $F_{10,9}^{1}=\begin{bmatrix} x_2 \oplus 1 \\ x_1 \oplus x_2 \oplus 1 \end{bmatrix}$ – операція перетворення першого операнда, а $F_{5,6}^{2}=\begin{bmatrix} k_2 \\ k_1 \oplus k_2 \end{bmatrix}$ – операція перетворення другого операнда, тоді $F_{10,9}^{1} \oplus F_{5,6}^{2}=\begin{bmatrix} x_2 \oplus 1 \\ x_1 \oplus x_2 \oplus 1 \end{bmatrix} \oplus \begin{bmatrix} k_2 \\ k_1 \oplus k_2 \end{bmatrix}=\begin{bmatrix} x_2 \oplus k_2 \oplus 1 \\ x_1 \oplus x_2 \oplus k_1 \oplus k_2 \oplus 1 \end{bmatrix}=O_{23,5,17,11}$.

Операції НДО 5 можна отримати шляхом додавання по модулю два до одноопераднних операцій криптоперетворення, наведених в п’ятому рядку табл. 4.1 одноопераднної операції обробки другого операнда $F_{5,6}^{2}=\begin{bmatrix} k_2 \\ k_1 \oplus k_2 \end{bmatrix}$.

Взаємозв’язки для отримання операцій НДО 6 такі:

Якщо $F_{6,3}^{1}=\begin{bmatrix} x_1 \oplus x_2 \\ x_1 \end{bmatrix}$ – операція перетворення першого операнда, а $F_{6,3}^{2}=\begin{bmatrix} k_1 \oplus k_2 \\ k_1 \end{bmatrix}$ – операція перетворення другого операнда, тоді $F_{6,3}^{1} \oplus F_{6,3}^{2}=\begin{bmatrix} x_1 \oplus x_2 \\ x_1 \end{bmatrix} \oplus \begin{bmatrix} k_1 \oplus k_2 \\ k_1 \end{bmatrix}=\begin{bmatrix} x_1 \oplus x_2 \oplus k_1 \oplus k_2 \\ x_1 \oplus k_1 \end{bmatrix}=O_{6,18,24,12}$.

Якщо $F_{6,12}^{1}=\begin{bmatrix} x_1 \oplus x_2 \\ x_1 \oplus 1 \end{bmatrix}$ – операція перетворення першого операнда, а $F_{6,3}^{2}=\begin{bmatrix} k_1 \oplus k_2 \\ k_1 \end{bmatrix}$ – операція перетворення другого операнда, тоді $F_{6,12}^{1} \oplus F_{6,3}^{2}=\begin{bmatrix} x_1 \oplus x_2 \\ x_1 \oplus 1 \end{bmatrix} \oplus \begin{bmatrix} k_1 \oplus k_2 \\ k_1 \end{bmatrix}=\begin{bmatrix} x_1 \oplus x_2 \oplus k_1 \oplus k_2 \\ x_1 \oplus k_1 \oplus 1 \end{bmatrix}=O_{12,24,18,6}$.

Якщо $F_{9,3}^{1}=\begin{bmatrix} x_1 \oplus x_2 \oplus 1 \\ x_1 \end{bmatrix}$ – операція перетворення першого операнда, а $F_{6,3}^{2}=\begin{bmatrix} k_1 \oplus k_2 \\ k_1 \end{bmatrix}$ – операція перетворення другого операнда, тоді $F_{9,3}^{1} \oplus F_{6,3}^{2}=\begin{bmatrix} x_1 \oplus x_2 \oplus 1 \\ x_1 \end{bmatrix} \oplus \begin{bmatrix} k_1 \oplus k_2 \\ k_1 \end{bmatrix} = \begin{bmatrix} x_1 \oplus x_2 \oplus k_1 \oplus k_2 \oplus 1 \\ x_1 \oplus k_1 \end{bmatrix} = O_{18,6,12,24}$.

Якщо $F_{9,12}^{1}=\begin{bmatrix} x_1 \oplus x_2 \oplus 1 \\ x_1 \oplus 1 \end{bmatrix}$ – операція перетворення першого операнда, а $F_{6,3}^{2}=\begin{bmatrix} k_1 \oplus k_2 \\ k_1 \end{bmatrix}$ – операція перетворення другого операнда, тоді $F_{9,12}^{1} \oplus F_{6,3}^{2}=\begin{bmatrix} x_1 \oplus x_2 \oplus 1 \\ x_1 \oplus 1 \end{bmatrix} \oplus \begin{bmatrix} k_1 \oplus k_2 \\ k_1 \end{bmatrix} = \begin{bmatrix} x_2 \oplus k_2 \oplus 1 \\ x_1 \oplus x_2 \oplus k_1 \oplus k_2 \oplus 1 \end{bmatrix} = O_{23,5,17,11}$.

Операції НДО 6 математично синтезуються шляхом додавання по модулю два до одноопераднних операцій крипто перетворення, наведених в табл. 4.1 одноопераднної операції обробки другого операнда $F_{6,3}^{2}=\begin{bmatrix} k_1 \oplus k_2 \\ k_1 \end{bmatrix}$.

В результаті проведеного дослідження встановлено, що група двохрозрядних операцій додавання за модулем два включає в себе базову групу двохрозрядних операцій додавання за модулем два, групу операцій перестановок та групу операцій інверсії. На основі цього узагальнимо результати дослідження:

– синтез двохоперандних двохрозрядних операцій базової групи на основі поєднання по модулю два двох однакових одноопераднних операцій базової групи для обробки двох різних операндів;

– розширення двохоперандних двохрозрядних операцій базової групи на основі перестановок до групи базових операцій та операцій перестановок;

- розширення групи двохоперандних двохрозрядних операцій базової групи і операцій перестановок на основі операцій інверсії до групи двохрозрядних операцій додавання за модулем два.

Отримані узагальнені результати дозволили розробити метод синтезу груп двохрозрядних двохоперандних операцій для симетричного потокового шифрування, який полягає в наступному:

- синтез двохоперандних операцій базової групи на основі додавання за модулем два одноопераднних операцій обробки кожного операнда. Виконується перетворення на основі моделі $F = \begin{bmatrix} k_1 \\ k_2 \end{bmatrix}$. На основі цього, перетворення операцій базової групи будуть представлені:

$$O_{1,7,13,19} = F^1_{3,5} \oplus F^2_{3,5} = \begin{bmatrix} x_1 \\ x_2 \end{bmatrix} \oplus \begin{bmatrix} k_1 \\ k_2 \end{bmatrix} = \begin{bmatrix} x_1 \oplus k_1 \\ x_2 \oplus k_2 \end{bmatrix}$$

$$O_{2,20,14,8} = F^1_{6,5} \oplus F^2_{6,5} = \begin{bmatrix} x_1 \oplus x_2 \\ x_2 \end{bmatrix} \oplus \begin{bmatrix} k_1 \oplus k_2 \\ k_2 \end{bmatrix} = \begin{bmatrix} x_1 \oplus x_2 \oplus k_1 \oplus k_2 \\ x_2 \oplus k_2 \end{bmatrix}$$

$$O_{3,9,21,15} = F^1_{3,6} \oplus F^2_{3,6} = \begin{bmatrix} x_1 \\ x_1 \oplus x_2 \end{bmatrix} \oplus \begin{bmatrix} k_1 \\ k_1 \oplus k_2 \end{bmatrix} = \begin{bmatrix} x_1 \oplus k_1 \\ x_1 \oplus x_2 \oplus k_1 \oplus k_2 \end{bmatrix}$$

- виконання над операціями базової групи операцій перестановок;
- виконання над операціями базової групи в поєднанні з операціями перестановок операцій інверсії.

Так як основною операцією цієї групи є операція додавання за модулем два, то і група була названа симетричною групою двохоперандних двохрозрядних операцій криптографічного додавання за модулем два.

Застосування цього методу дозволяє синтезувати всі двохрозрядні операції додавання за модулем два на основі застосування трьох базових одноопераднних двохрозрядних опрерацій додавання за модулем два.

4.2 Метод синтезу операцій криптоперетворення другої математичної групи

Для подальшого дослідження розглянемо можливість класифікації математичних моделей двохоперандних двохрозрядних операцій криптографічного перетворення інформації, отриманих в розділі 3. Рузультати класифікації другої симетричної групи двохоперандних

двохрозрядних операцій криптографічного перетворення інформації наведено в табл. 4.3.

Як бачимо з табл. 4.3, перша класифікована базова операція є двохрозрядною операцією додавання по модулю чотири [105]. Тому, аналогічно до першої математичної групи операцій, синтезованих в розд. 2, другу математичну групу операцій, синтезованих в розд. 3, будемо називати групою двохрозрядних операцій додавання за модулем чотири.

Встановимо аналогічні взаємозв'язки для операцій другої математичної групи, а якщо вони не співпадуть з уже відомими, то по аналогії розробимо метод синтезу двохрозрядних операцій другої групи. Проведемо порівняльне дослідження табл. 4.1 й табл. 4.3.

Розглянемо перший рядок табл. 4.3. Під час проведеного дослідження отримано взаємозв'язки між моделями, які можна формалізувати таким чином.

Якщо $F_{3,5}^{1}=\begin{bmatrix} x_1 \\ x_2 \end{bmatrix}$ – операція перетворення першого операнда, а $F_{пк}^{2.1}=\begin{bmatrix} k_1 \oplus x_2 \cdot k_2 \\ k_2 \end{bmatrix}$ – операція перетворення другого операнда, тоді $F_{3,5}^{1} \oplus F_{пк}^{2.1}=\begin{bmatrix} x_1 \\ x_2 \end{bmatrix} \oplus \begin{bmatrix} k_1 \oplus x_2 \cdot k_2 \\ k_2 \end{bmatrix}=\begin{bmatrix} x_1 \oplus x_2 \cdot k_2 \oplus k_1 \\ x_2 \oplus k_2 \end{bmatrix}=O_{1,8,13,20}$.

Якщо $F_{3,10}=\begin{bmatrix} x_1 \\ x_2 \oplus 1 \end{bmatrix}$ – операція перетворення першого операнда, а $F_{пк}^{2.1}=\begin{bmatrix} k_1 \oplus x_2 \cdot k_2 \\ k_2 \end{bmatrix}$ – операція перетворення другого операнда, тоді $F_{3,10}^{1} \oplus F_{пк}^{2.1}=\begin{bmatrix} x_1 \\ x_2 \oplus 1 \end{bmatrix} \oplus \begin{bmatrix} k_1 \oplus x_2 \cdot k_2 \\ k_2 \end{bmatrix}=\begin{bmatrix} x_1 \oplus x_2 \cdot k_2 \oplus k_1 \\ x_2 \oplus k_2 \oplus 1 \end{bmatrix}=O_{7,2,19,14}$.

Таблиця 4.3

Класифікація другої симетричної групи двохоперандних двохрозрядних операцій криптографічного додавання (групи двохрозрядних операцій додавання за модулем чотири)

Класифікатор операцій	**Операції інверсії**			
	$\begin{bmatrix}0\\0\end{bmatrix}$	$\begin{bmatrix}0\\1\end{bmatrix}$	$\begin{bmatrix}1\\0\end{bmatrix}$	$\begin{bmatrix}1\\1\end{bmatrix}$
Базові операції	$O_{1,8,13,20}=\begin{bmatrix}x_1\oplus x_2\cdot k_2\oplus k_1\\ x_2\oplus k_2\end{bmatrix}$	$O_{7,2,19,14}=\begin{bmatrix}x_1\oplus x_2\cdot k_2\oplus k_1\\ x_2\oplus k_2\oplus 1\end{bmatrix}$	$O_{13,20,1,8}=\begin{bmatrix}x_1\oplus x_2\cdot k_2\oplus k_1\oplus 1\\ x_2\oplus k_2\end{bmatrix}$	$O_{19,14,7,2}=\begin{bmatrix}x_1\oplus x_2\cdot k_2\oplus k_1\oplus 1\\ x_2\oplus k_2\oplus 1\end{bmatrix}$
	$O_{2,19,14,7}=\begin{bmatrix}x_1\oplus x_2\cdot\bar{k}_2\oplus k_1\oplus k_2\\ x_2\oplus k_2\end{bmatrix}$	$O_{8,13,20,1}=\begin{bmatrix}x_1\oplus x_2\cdot\bar{k}_2\oplus k_1\oplus k_2\\ x_2\oplus k_2\oplus 1\end{bmatrix}$	$O_{14,7,2,19}=\begin{bmatrix}x_1\oplus x_2\cdot\bar{k}_2\oplus k_1\oplus k_2\oplus 1\\ x_2\oplus k_2\end{bmatrix}$	$O_{20,1,8,13}=\begin{bmatrix}x_1\oplus x_2\cdot\bar{k}_2\oplus k_1\oplus k_2\oplus 1\\ x_2\oplus k_2\oplus 1\end{bmatrix}$
	$O_{3,12,21,18}=\begin{bmatrix}x_1\oplus x_2\cdot k_2\oplus k_1\\ x_1\oplus x_2\cdot\bar{k}_2\oplus k_1\oplus k_2\end{bmatrix}$	$O_{9,6,15,24}=\begin{bmatrix}x_1\oplus x_2\cdot k_2\oplus k_1\\ x_1\oplus x_2\cdot\bar{k}_2\oplus k_1\oplus k_2\oplus 1\end{bmatrix}$	$O_{15,24,9,6}=\begin{bmatrix}x_1\oplus x_2\cdot k_2\oplus k_1\oplus 1\\ x_1\oplus x_2\cdot\bar{k}_2\oplus k_1\oplus k_2\end{bmatrix}$	$O_{21,18,3,12}=\begin{bmatrix}x_1\oplus x_2\cdot k_2\oplus k_1\oplus 1\\ x_1\oplus x_2\cdot\bar{k}_2\oplus k_1\oplus k_2\oplus 1\end{bmatrix}$
Операції перестановок	$O_{4,17,10,23}=\begin{bmatrix}x_2\oplus k_2\\ x_1\oplus x_2\cdot k_2\oplus k_1\end{bmatrix}$	$O_{10,23,4,17}=\begin{bmatrix}x_2\oplus k_2\\ x_1\oplus x_2\cdot k_2\oplus k_1\oplus 1\end{bmatrix}$	$O_{17,10,23,4}=\begin{bmatrix}x_2\oplus k_2\oplus 1\\ x_1\oplus x_2\cdot\bar{k}_2\oplus k_1\oplus k_2\end{bmatrix}$	$O_{23,4,17,10}=\begin{bmatrix}x_2\oplus k_2\oplus 1\\ x_1\oplus x_2\cdot\bar{k}_2\oplus k_1\oplus k_2\oplus 1\end{bmatrix}$.
	$O_{5,22,11,16}=\begin{bmatrix}x_2\oplus k_2\\ x_1\oplus x_2\cdot\bar{k}_2\oplus k_1\oplus k_2\end{bmatrix}$	$O_{11,16,5,22}=\begin{bmatrix}x_2\oplus k_2\\ x_1\oplus x_2\cdot\bar{k}_2\oplus k_1\oplus k_2\oplus 1\end{bmatrix}$	$O_{16,5,22,11}=\begin{bmatrix}x_2\oplus k_2\oplus 1\\ x_1\oplus x_2\cdot k_2\oplus k_1\end{bmatrix}$	$O_{22,11,16,5}=\begin{bmatrix}x_2\oplus k_2\oplus 1\\ x_1\oplus x_2\cdot k_2\oplus k_1\oplus 1\end{bmatrix}$
	$O_{6,15,24,9}=\begin{bmatrix}x_1\oplus x_2\cdot\bar{k}_2\oplus k_1\oplus k_2\\ x_1\oplus x_2\cdot k_2\oplus k_1\end{bmatrix}$	$O_{12,21,18,3}=\begin{bmatrix}x_1\oplus x_2\cdot\bar{k}_2\oplus k_1\oplus k_2\\ x_1\oplus x_2\cdot k_2\oplus k_1\oplus 1\end{bmatrix}$	$O_{18,3,12,21}=\begin{bmatrix}x_1\oplus x_2\cdot\bar{k}_2\oplus k_1\oplus k_2\oplus 1\\ x_1\oplus x_2\cdot k_2\oplus k_1\end{bmatrix}$	$O_{24,9,6,15}=\begin{bmatrix}x_1\oplus x_2\cdot\bar{k}_2\oplus k_1\oplus k_2\oplus 1\\ x_1\oplus x_2\cdot k_2\oplus k_1\oplus 1\end{bmatrix}$

Якщо $F_{12,5}=\begin{bmatrix} x_1 \oplus 1 \\ x_2 \end{bmatrix}$ – операція перетворення першого операнда, а $F_{пк}^{2.1}=\begin{bmatrix} k_1 \oplus x_2 \cdot k_2 \\ k_2 \end{bmatrix}$ – операція перетворення другого операнда, тоді

$$F_{12,5}^{1} \oplus F_{пк}^{2.1}=\begin{bmatrix} x_1 \oplus 1 \\ x_2 \end{bmatrix} \oplus \begin{bmatrix} k_1 \oplus x_2 \cdot k_2 \\ k_2 \end{bmatrix} = \begin{bmatrix} x_1 \oplus x_2 \cdot k_2 \oplus k_1 \oplus 1 \\ x_2 \oplus k_2 \end{bmatrix} = O_{13,20,1,8}$$

Якщо $F_{12,10}=\begin{bmatrix} x_1 \oplus 1 \\ x_2 \oplus 1 \end{bmatrix}$ – операція перетворення першого операнда, а $F_{пк}^{2.1}=\begin{bmatrix} k_1 \oplus x_2 \cdot k_2 \\ k_2 \end{bmatrix}$ – операція перетворення другого операнда, тоді

$$F_{12,10}^{1} \oplus F_{пк}^{2.1}=\begin{bmatrix} x_1 \oplus 1 \\ x_2 \oplus 1 \end{bmatrix} \oplus \begin{bmatrix} k_1 \oplus x_2 \cdot k_2 \\ k_2 \end{bmatrix} = \begin{bmatrix} x_1 \oplus x_2 \cdot k_2 \oplus k_1 \oplus 1 \\ x_2 \oplus k_2 \oplus 1 \end{bmatrix} = O_{19,14,7,2}.$$

На основі наведених формалізованих перетворень можна константувати наступне: перший рядок табл. 4.3 можна отримати шляхом додавання по модулю два одноопераднної операції обробки другого операнда $F_{пк}^{2.1}=\begin{bmatrix} k_1 \oplus x_2 \cdot k_2 \\ k_2 \end{bmatrix}$.

Дослідимо другий рядок табл. 4.3.

Якщо $F_{6,5}^{1}=\begin{bmatrix} x_1 \oplus x_2 \\ x_2 \end{bmatrix}$ – операція перетворення першого операнда, а $F_{пк}^{2.2}=\begin{bmatrix} x_2 \cdot k_2 \oplus k_1 \oplus k_2 \\ k_2 \end{bmatrix}$ – операція перетворення другого операнда, тоді

$$F_{6,5}^{1} \oplus F_{пк}^{2.2}=\begin{bmatrix} x_1 \oplus x_2 \\ x_2 \end{bmatrix} \oplus \begin{bmatrix} x_2 \cdot k_2 \oplus k_1 \oplus k_2 \\ k_2 \end{bmatrix} = \begin{bmatrix} x_1 \oplus x_2 \cdot \bar{k}_2 \oplus k_1 \oplus k_2 \\ x_2 \oplus k_2 \end{bmatrix}.$$

Так як

$$F_{6,5}^{1} \oplus F_{пк}^{2.2}=\begin{bmatrix} x_1 \oplus x_2 \oplus x_2 \cdot k_2 \oplus k_1 \oplus k_2 \\ x_2 \oplus k_2 \end{bmatrix} = \begin{bmatrix} x_1 \oplus x_2 \cdot (1 \oplus k_2) \oplus k_1 \oplus k_2 \\ x_2 \oplus k_2 \end{bmatrix} = \begin{bmatrix} x_1 \oplus x_2 \cdot \bar{k}_2 \oplus k_1 \oplus k_2 \\ x_2 \oplus k_2 \end{bmatrix} = O_{2,19,14,7}$$

Якщо $F_{6,10}^{1}=\begin{bmatrix} x_1 \oplus x_2 \\ x_2 \oplus 1 \end{bmatrix}$ – операція перетворення першого операнда, а $F_{пк}^{2.2}=\begin{bmatrix} x_2 \cdot k_2 \oplus k_1 \oplus k_2 \\ k_2 \end{bmatrix}$ – операція перетворення другого операнда, тоді

$$F_{6,10}^{1} \oplus F_{пк}^{2.2}=\begin{bmatrix} x_1 \oplus x_2 \\ x_2 \oplus 1 \end{bmatrix} \oplus \begin{bmatrix} x_2 \cdot k_2 \oplus k_1 \oplus k_2 \\ k_2 \end{bmatrix} = \begin{bmatrix} x_1 \oplus x_2 \oplus x_2 \cdot k_2 \oplus k_1 \oplus k_2 \\ x_2 \oplus k_2 \oplus 1 \end{bmatrix}.$$

Так як

$$F^{1}_{6,10} \oplus F^{2.2}_{пк} = \begin{bmatrix} x_1 \oplus x_2 \oplus x_2 \cdot k_2 \oplus k_1 \oplus k_2 \\ x_2 \oplus k_2 \oplus 1 \end{bmatrix} = \begin{bmatrix} x_1 \oplus x_2 \cdot \bar{k}_2 \oplus k_1 \oplus k_2 \\ x_2 \oplus k_2 \oplus 1 \end{bmatrix} = O_{8,13,20,1}.$$

Якщо $F^{1}_{9,5} = \begin{bmatrix} x_1 \oplus x_2 \oplus 1 \\ x_2 \end{bmatrix}$ – операція перетворення першого операнда, а $F^{2.2}_{пк} = \begin{bmatrix} x_2 \cdot k_2 \oplus k_1 \oplus k_2 \\ k_2 \end{bmatrix}$ – операція перетворення другого операнда, тоді

$$F^{1}_{9,5} \oplus F^{2.2}_{пк} = \begin{bmatrix} x_1 \oplus x_2 \oplus 1 \\ x_2 \end{bmatrix} \oplus \begin{bmatrix} x_2 \cdot k_2 \oplus k_1 \oplus k_2 \\ k_2 \end{bmatrix} = \begin{bmatrix} x_1 \oplus x_2 \oplus x_2 \cdot k_2 \oplus k_1 \oplus k_2 \oplus 1 \\ x_2 \oplus k_2 \end{bmatrix}.$$

Так як

$$F^{1}_{9,5} \oplus F^{2.2}_{пк} = \begin{bmatrix} x_1 \oplus x_2 \oplus x_2 \cdot k_2 \oplus k_1 \oplus k_2 \oplus 1 \\ x_2 \oplus k_2 \end{bmatrix} = \begin{bmatrix} x_1 \oplus x_2 \cdot \bar{k}_2 \oplus k_1 \oplus k_2 \oplus 1 \\ x_2 \oplus k_2 \end{bmatrix} = O_{14,7,2,19}.$$

Якщо $F^{1}_{9,10} = \begin{bmatrix} x_1 \oplus x_2 \oplus 1 \\ x_2 \oplus 1 \end{bmatrix}$ – операція перетворення першого операнда, а $F^{2.2}_{пк} = \begin{bmatrix} x_2 \cdot k_2 \oplus k_1 \oplus k_2 \\ k_2 \end{bmatrix}$ – операція перетворення другого операнда, тоді

$$F^{1}_{9,10} \oplus F^{2.2}_{пк} = \begin{bmatrix} x_1 \oplus x_2 \oplus 1 \\ x_2 \oplus 1 \end{bmatrix} \oplus \begin{bmatrix} x_2 \cdot k_2 \oplus k_1 \oplus k_2 \\ k_2 \end{bmatrix} = \begin{bmatrix} x_1 \oplus x_2 \oplus x_2 \cdot k_2 \oplus k_1 \oplus k_2 \oplus 1 \\ x_2 \oplus k_2 \oplus 1 \end{bmatrix}.$$

Так як

$$F^{1}_{9,10} \oplus F^{2.2}_{пк} = \begin{bmatrix} x_1 \oplus x_2 \oplus x_2 \cdot k_2 \oplus k_1 \oplus k_2 \oplus 1 \\ x_2 \oplus k_2 \oplus 1 \end{bmatrix} = \begin{bmatrix} x_1 \oplus x_2 \cdot \bar{k}_2 \oplus k_1 \oplus k_2 \oplus 1 \\ x_2 \oplus k_2 \oplus 1 \end{bmatrix} = O_{20,1,8,13}$$

В результаті дослідження встановлено, що другий рядок табл. 4.3 можна отримати шляхом додавання по модулю два до кожної операції операцію обробки другого операнда $F^{2.2}_{пк} = \begin{bmatrix} x_2 \cdot k_2 \oplus k_1 \oplus k_2 \\ k_2 \end{bmatrix}$.

Наведемо формалізовані взаємозв’язки, які отримано при дослідженні третього рядка табл. 4.3.

Якщо $F^{1}_{3,6} = \begin{bmatrix} x_1 \\ x_1 \oplus x_2 \end{bmatrix}$ – операція перетворення першого операнда, а $F^{2.3}_{пк} = \begin{bmatrix} x_2 \cdot k_2 \oplus k_1 \\ x_2 \cdot k_2 \oplus k_1 \oplus k_2 \end{bmatrix}$ – операція перетворення другого операнда, тоді

$$F^{1}_{3,6} \oplus F^{2.3}_{пк} = \begin{bmatrix} x_1 \\ x_1 \oplus x_2 \end{bmatrix} \oplus \begin{bmatrix} x_2 \cdot k_2 \oplus k_1 \\ x_2 \cdot k_2 \oplus k_1 \oplus k_2 \end{bmatrix} = \begin{bmatrix} x_1 \oplus x_2 \cdot k_2 \oplus k_1 \\ x_1 \oplus x_2 \oplus x_2 \cdot k_2 \oplus k_1 \oplus k_2 \end{bmatrix}.$$

Так як

$$F^{1}_{3,6} \oplus F^{2.3}_{пк} = \begin{bmatrix} x_1 \oplus x_2 \cdot k_2 \oplus k_1 \\ x_1 \oplus x_2 \oplus x_2 \cdot k_2 \oplus k_1 \oplus k_2 \end{bmatrix} = \begin{bmatrix} x_1 \oplus x_2 \cdot k_2 \oplus k_1 \\ x_1 \oplus x_2 \cdot \bar{k}_2 \oplus k_1 \oplus k_2 \end{bmatrix} = O_{3,12,21,18}$$

Якщо $F^{1}_{3,9} = \begin{bmatrix} x_1 \\ x_1 \oplus x_2 \oplus 1 \end{bmatrix}$ – операція перетворення першого операнда, а $F^{2.3}_{пк} = \begin{bmatrix} x_2 \cdot k_2 \oplus k_1 \\ x_2 \cdot k_2 \oplus k_1 \oplus k_2 \end{bmatrix}$ – операція перетворення другого операнда, тоді

$$F^{1}_{3,9} \oplus F^{2.3}_{пк} = \begin{bmatrix} x_1 \\ x_1 \oplus x_2 \oplus 1 \end{bmatrix} \oplus \begin{bmatrix} x_2 \cdot k_2 \oplus k_1 \\ x_2 \cdot k_2 \oplus k_1 \oplus k_2 \end{bmatrix} = \begin{bmatrix} x_1 \oplus x_2 \cdot k_2 \oplus k_1 \\ x_1 \oplus x_2 \oplus x_2 \cdot k_2 \oplus k_1 \oplus k_2 \oplus 1 \end{bmatrix}.$$

Так як

$$F^{1}_{3,9} \oplus F^{2.3}_{пк} = \begin{bmatrix} x_1 \oplus x_2 \cdot k_2 \oplus k_1 \\ x_1 \oplus x_2 \oplus x_2 \cdot k_2 \oplus k_1 \oplus k_2 \oplus 1 \end{bmatrix} = \begin{bmatrix} x_1 \oplus x_2 \cdot k_2 \oplus k_1 \\ x_1 \oplus x_2 \cdot \bar{k}_2 \oplus k_1 \oplus k_2 \oplus 1 \end{bmatrix} = O_{9,6,15,24}$$

Якщо $F^{1}_{12,6} = \begin{bmatrix} x_1 \oplus 1 \\ x_1 \oplus x_2 \end{bmatrix}$ – операція перетворення першого операнда, а $F^{2.3}_{пк} = \begin{bmatrix} x_2 \cdot k_2 \oplus k_1 \\ x_2 \cdot k_2 \oplus k_1 \oplus k_2 \end{bmatrix}$ – операція перетворення другого операнда, тоді

$$F^{1}_{12,6} \oplus F^{2.3}_{пк} = \begin{bmatrix} x_1 \oplus 1 \\ x_1 \oplus x_2 \end{bmatrix} \oplus \begin{bmatrix} x_2 \cdot k_2 \oplus k_1 \\ x_2 \cdot k_2 \oplus k_1 \oplus k_2 \end{bmatrix} = \begin{bmatrix} x_1 \oplus x_2 \cdot k_2 \oplus k_1 \oplus 1 \\ x_1 \oplus x_2 \oplus x_2 \cdot k_2 \oplus k_1 \oplus k_2 \end{bmatrix}.$$

Так як

$$F^{1}_{12,6} \oplus F^{2.3}_{пк} = \begin{bmatrix} x_1 \oplus x_2 \cdot k_2 \oplus k_1 \oplus 1 \\ x_1 \oplus x_2 \oplus x_2 \cdot k_2 \oplus k_1 \oplus k_2 \end{bmatrix} = \begin{bmatrix} x_1 \oplus x_2 \cdot k_2 \oplus k_1 \oplus 1 \\ x_1 \oplus x_2 \cdot \bar{k}_2 \oplus k_1 \oplus k_2 \end{bmatrix} = O_{15,24,9,6}$$

Якщо $F^{1}_{12,9} = \begin{bmatrix} x_1 \oplus 1 \\ x_1 \oplus x_2 \oplus 1 \end{bmatrix}$ – операція перетворення першого операнда, а $F^{2.3}_{пк} = \begin{bmatrix} x_2 \cdot k_2 \oplus k_1 \\ x_2 \cdot k_2 \oplus k_1 \oplus k_2 \end{bmatrix}$ – операція перетворення другого операнда, тоді

$$F^{1}_{12,9} \oplus F^{2.3}_{пк} = \begin{bmatrix} x_1 \oplus 1 \\ x_1 \oplus x_2 \oplus 1 \end{bmatrix} \oplus \begin{bmatrix} x_2 \cdot k_2 \oplus k_1 \\ x_2 \cdot k_2 \oplus k_1 \oplus k_2 \end{bmatrix} = \begin{bmatrix} x_1 \oplus x_2 \cdot k_2 \oplus k_1 \oplus 1 \\ x_1 \oplus x_2 \oplus x_2 \cdot k_2 \oplus k_1 \oplus k_2 \oplus 1 \end{bmatrix}.$$

Так як

$$F^{1}_{12,9} \oplus F^{2.3}_{пк} = \begin{bmatrix} x_1 \oplus x_2 \cdot k_2 \oplus k_1 \oplus 1 \\ x_1 \oplus x_2 \oplus x_2 \cdot k_2 \oplus k_1 \oplus k_2 \oplus 1 \end{bmatrix} = \begin{bmatrix} x_1 \oplus x_2 \cdot k_2 \oplus k_1 \oplus 1 \\ x_1 \oplus x_2 \cdot \bar{k}_2 \oplus k_1 \oplus k_2 \oplus 1 \end{bmatrix} = O_{21,18,3,12}$$

Операції третього рядка табл. 4.3 синтезуються шляхом додавання за модулем два до кожної операції рядка з табл. 4.1 операції $F_{пк}^{2.3} = \begin{bmatrix} x_2 \cdot k_2 \oplus k_1 \\ x_2 \cdot k_2 \oplus k_1 \oplus k_2 \end{bmatrix}$.

Формалізуємо взаємозв'язки, які отримано при дослідженні четвертого рядка табл. 4.3.

Якщо $F_{5,3}^{1} = \begin{bmatrix} x_2 \\ x_1 \end{bmatrix}$ – операція перетворення першого операнда, а $F_{пк}^{2.4} = \begin{bmatrix} k_2 \\ k_1 \oplus x_2 \cdot k_2 \end{bmatrix}$ – операція перетворення другого операнда, тоді $F_{5,3}^{1} \oplus F_{пк}^{2.4} = \begin{bmatrix} x_2 \\ x_1 \end{bmatrix} \oplus \begin{bmatrix} k_2 \\ k_1 \oplus x_2 \cdot k_2 \end{bmatrix} = \begin{bmatrix} x_2 \oplus k_2 \\ x_1 \oplus x_2 \cdot k_2 \oplus k_1 \end{bmatrix} = O_{4,17,10,23}$.

Якщо $F_{5,12}^{1} = \begin{bmatrix} x_2 \\ x_1 \oplus 1 \end{bmatrix}$ – операція перетворення першого операнда, а $F_{пк}^{2.4} = \begin{bmatrix} k_2 \\ k_1 \oplus x_2 \cdot k_2 \end{bmatrix}$ – операція перетворення другого операнда, тоді $F_{5,12}^{1} \oplus F_{пк}^{2.4} = \begin{bmatrix} x_2 \\ x_1 \oplus 1 \end{bmatrix} \oplus \begin{bmatrix} k_2 \\ k_1 \oplus x_2 \cdot k_2 \end{bmatrix} = \begin{bmatrix} x_2 \oplus k_2 \\ x_1 \oplus x_2 \cdot k_2 \oplus k_1 \oplus 1 \end{bmatrix} = O_{10,23,4,17}$.

Якщо $F_{10,3}^{1} = \begin{bmatrix} x_2 \oplus 1 \\ x_1 \end{bmatrix}$ – операція перетворення першого операнда, а $F_{пк}^{2.4} = \begin{bmatrix} k_2 \\ k_1 \oplus x_2 \cdot k_2 \end{bmatrix}$ – операція перетворення другого операнда, тоді $F_{10,3}^{1} \oplus F_{пк}^{2.4} = \begin{bmatrix} x_2 \oplus 1 \\ x_1 \end{bmatrix} \oplus \begin{bmatrix} k_2 \\ k_1 \oplus x_2 \cdot k_2 \end{bmatrix} = \begin{bmatrix} x_2 \oplus k_2 \oplus 1 \\ x_1 \oplus x_2 \cdot \bar{k}_2 \oplus k_1 \oplus k_2 \end{bmatrix} = O_{17,10,23,4}$.

Якщо $F_{10,12}^{1} = \begin{bmatrix} x_2 \oplus 1 \\ x_1 \oplus 1 \end{bmatrix}$ – операція перетворення першого операнда, а $F_{пк}^{2.4} = \begin{bmatrix} k_2 \\ k_1 \oplus x_2 \cdot k_2 \end{bmatrix}$ – операція перетворення другого операнда, тоді $F_{10,12}^{1} \oplus F_{пк}^{2.4} = \begin{bmatrix} x_2 \oplus 1 \\ x_1 \oplus 1 \end{bmatrix} \oplus \begin{bmatrix} k_2 \\ k_1 \oplus x_2 \cdot k_2 \end{bmatrix} = \begin{bmatrix} x_2 \oplus k_2 \oplus 1 \\ x_1 \oplus x_2 \cdot \bar{k}_2 \oplus k_1 \oplus k_2 \oplus 1 \end{bmatrix} = O_{23,4,17,10}$.

Четвертий рядок табл. 4.3 синтезуються шляхом додавання за модулем два до кожної операції рядка з табл. 4.1 операції $F_{пк}^{2.4}=\begin{bmatrix} k_2 \\ k_1 \oplus x_2 \cdot k_2 \end{bmatrix}$.

Дослідимо п’ятий рядок табл. 4.3.

Якщо $F_{5,6}^{1}=\begin{bmatrix} x_2 \\ x_1 \oplus x_2 \end{bmatrix}$ – операція перетворення першого операнда, а $F_{пк}^{2.5}=\begin{bmatrix} k_2 \\ x_2 \cdot k_2 \oplus k_1 \oplus k_2 \end{bmatrix}$ – операція перетворення другого операнда, тоді

$$F_{5,6}^{1} \oplus F_{пк}^{2.5}=\begin{bmatrix} x_2 \\ x_1 \oplus x_2 \end{bmatrix} \oplus \begin{bmatrix} k_2 \\ x_2 \cdot k_2 \oplus k_1 \oplus k_2 \end{bmatrix}=\begin{bmatrix} x_2 \oplus k_2 \\ x_1 \oplus x_2 \oplus x_2 \cdot k_2 \oplus k_1 \oplus k_2 \end{bmatrix}.$$

Так як

$$F_{5,6}^{1} \oplus F_{пк}^{2.5}=\begin{bmatrix} x_2 \oplus k_2 \\ x_1 \oplus x_2 \oplus x_2 \cdot k_2 \oplus k_1 \oplus k_2 \end{bmatrix}=\begin{bmatrix} x_2 \oplus k_2 \\ x_1 \oplus x_2 \cdot \bar{k}_2 \oplus k_1 \oplus k_2 \end{bmatrix}=O_{5,22,11,16}.$$

Якщо $F_{5,9}^{1}=\begin{bmatrix} x_2 \\ x_1 \oplus x_2 \oplus 1 \end{bmatrix}$ – операція перетворення першого операнда, а $F_{пк}^{2.5}=\begin{bmatrix} k_2 \\ x_2 \cdot k_2 \oplus k_1 \oplus k_2 \end{bmatrix}$ – операція перетворення другого операнда, тоді

$$F_{5,9}^{1} \oplus F_{пк}^{2.5}=\begin{bmatrix} x_2 \\ x_1 \oplus x_2 \oplus 1 \end{bmatrix} \oplus \begin{bmatrix} k_2 \\ x_2 \cdot k_2 \oplus k_1 \oplus k_2 \end{bmatrix}=\begin{bmatrix} x_2 \oplus k_2 \\ x_1 \oplus x_2 \oplus x_2 \cdot k_2 \oplus k_1 \oplus k_2 \oplus 1 \end{bmatrix}.$$

Так як

$$F_{5,9}^{1} \oplus F_{пк}^{2.5}=\begin{bmatrix} x_2 \oplus k_2 \\ x_1 \oplus x_2 \oplus x_2 \cdot k_2 \oplus k_1 \oplus k_2 \oplus 1 \end{bmatrix}=\begin{bmatrix} x_2 \oplus k_2 \\ x_1 \oplus x_2 \cdot \bar{k}_2 \oplus k_1 \oplus k_2 \oplus 1 \end{bmatrix}=O_{11,16,5,22}.$$

Якщо $F_{10,6}^{1}=\begin{bmatrix} x_2 \oplus 1 \\ x_1 \oplus x_2 \end{bmatrix}$ – операція перетворення першого операнда, а $F_{пк}^{2.5}=\begin{bmatrix} k_2 \\ x_2 \cdot k_2 \oplus k_1 \oplus k_2 \end{bmatrix}$ – операція перетворення другого операнда, тоді

$$F_{10,6}^{1} \oplus F_{пк}^{2.5}=\begin{bmatrix} x_2 \oplus 1 \\ x_1 \oplus x_2 \end{bmatrix} \oplus \begin{bmatrix} k_2 \\ x_2 \cdot k_2 \oplus k_1 \oplus k_2 \end{bmatrix}=\begin{bmatrix} x_2 \oplus k_2 \oplus 1 \\ x_1 \oplus x_2 \oplus x_2 \cdot k_2 \oplus k_1 \oplus k_2 \end{bmatrix}.$$

Так як

$$F_{10,6}^{1} \oplus F_{пк}^{2.5}=\begin{bmatrix} x_2 \oplus k_2 \oplus 1 \\ x_1 \oplus x_2 \oplus x_2 \cdot k_2 \oplus k_1 \oplus k_2 \end{bmatrix}=\begin{bmatrix} x_2 \oplus k_2 \oplus 1 \\ x_1 \oplus x_2 \cdot k_2 \oplus k_1 \end{bmatrix}=O_{16,5,22,11}.$$

Якщо $F^{1}_{10,9}=\begin{bmatrix} x_2 \oplus 1 \\ x_1 \oplus x_2 \oplus 1 \end{bmatrix}$ – операція перетворення першого операнда, а $F^{2.5}_{пк}=\begin{bmatrix} k_2 \\ x_2 \cdot k_2 \oplus k_1 \oplus k_2 \end{bmatrix}$ – операція перетворення другого операнда, тоді

$$F^{1}_{10,9} \oplus F^{2.5}_{пк}=\begin{bmatrix} x_2 \oplus 1 \\ x_1 \oplus x_2 \oplus 1 \end{bmatrix} \oplus \begin{bmatrix} k_2 \\ x_2 \cdot k_2 \oplus k_1 \oplus k_2 \end{bmatrix}=\begin{bmatrix} x_2 \oplus k_2 \oplus 1 \\ x_1 \oplus x_2 \oplus x_2 \cdot k_2 \oplus k_1 \oplus k_2 \oplus 1 \end{bmatrix}.$$

Так як

$$F^{1}_{10,9} \oplus F^{2.5}_{пк}=\begin{bmatrix} x_2 \oplus k_2 \oplus 1 \\ x_1 \oplus x_2 \oplus x_2 \cdot k_2 \oplus k_1 \oplus k_2 \oplus 1 \end{bmatrix}=\begin{bmatrix} x_2 \oplus k_2 \oplus 1 \\ x_1 \oplus x_2 \cdot k_2 \oplus k_1 \oplus 1 \end{bmatrix}=O_{22,11,16,5}.$$

Додавши по модулю два до операцій крипто перетворення, наведених в табл. 4.1, одноопернадну операцію $F^{2.5}_{пк}=\begin{bmatrix} k_2 \\ x_2 \cdot k_2 \oplus k_1 \oplus k_2 \end{bmatrix}$, отримаємо операції п’ятого рядка табл. 4.3.

По аналогії дослідимо синтез операцій шостого рядка табл. 4.3.

Якщо $F^{1}_{6,3}=\begin{bmatrix} x_1 \oplus x_2 \\ x_1 \end{bmatrix}$ – операція перетворення першого операнда, а $F^{2.6}_{пк}=\begin{bmatrix} x_2 \cdot k_2 \oplus k_1 \oplus k_2 \\ x_2 \cdot k_2 \oplus k_1 \end{bmatrix}$ – операція перетворення другого операнда, тоді

$$F^{1}_{6,3} \oplus F^{2.6}_{пк}=\begin{bmatrix} x_1 \oplus x_2 \\ x_1 \end{bmatrix} \oplus \begin{bmatrix} x_2 \cdot k_2 \oplus k_1 \oplus k_2 \\ x_2 \cdot k_2 \oplus k_1 \end{bmatrix}=\begin{bmatrix} x_1 \oplus x_2 \oplus x_2 \cdot k_2 \oplus k_1 \oplus k_2 \\ x_1 \oplus x_2 \cdot k_2 \oplus k_1 \end{bmatrix}.$$

Так як

$$F^{1}_{6,3} \oplus F^{2.6}_{пк}=\begin{bmatrix} x_1 \oplus x_2 \oplus x_2 \cdot k_2 \oplus k_1 \oplus k_2 \\ x_1 \oplus x_2 \cdot k_2 \oplus k_1 \end{bmatrix}=\begin{bmatrix} x_1 \oplus x_2 \cdot \bar{k}_2 \oplus k_1 \oplus k_2 \\ x_1 \oplus x_2 \cdot k_2 \oplus k_1 \end{bmatrix}=O_{6,15,24,9}.$$

Якщо $F^{1}_{6,12}=\begin{bmatrix} x_1 \oplus x_2 \\ x_1 \oplus 1 \end{bmatrix}$ – операція перетворення першого операнда, а $F^{2.6}_{пк}=\begin{bmatrix} x_2 \cdot k_2 \oplus k_1 \oplus k_2 \\ x_2 \cdot k_2 \oplus k_1 \end{bmatrix}$ – операція перетворення другого операнда, тоді

$$F^{1}_{6,12} \oplus F^{2.6}_{пк}=\begin{bmatrix} x_1 \oplus x_2 \\ x_1 \oplus 1 \end{bmatrix} \oplus \begin{bmatrix} x_2 \cdot k_2 \oplus k_1 \oplus k_2 \\ x_2 \cdot k_2 \oplus k_1 \end{bmatrix}=\begin{bmatrix} x_1 \oplus x_2 \oplus x_2 \cdot k_2 \oplus k_1 \oplus k_2 \\ x_1 \oplus x_2 \cdot k_2 \oplus k_1 \oplus 1 \end{bmatrix}.$$

Так як

$$F^{1}_{6,12} \oplus F^{2.6}_{пк}=\begin{bmatrix} x_1 \oplus x_2 \oplus x_2 \cdot k_2 \oplus k_1 \oplus k_2 \\ x_1 \oplus x_2 \cdot k_2 \oplus k_1 \oplus 1 \end{bmatrix}=\begin{bmatrix} x_1 \oplus x_2 \cdot \bar{k}_2 \oplus k_1 \oplus k_2 \\ x_1 \oplus x_2 \cdot k_2 \oplus k_1 \oplus 1 \end{bmatrix}=O_{12,21,18,3}.$$

Якщо $F^{1}_{9,3}=\begin{bmatrix} x_1 \oplus x_2 \oplus 1 \\ x_1 \end{bmatrix}$ – операція перетворення першого операнда, а $F^{2.6}_{пк}=\begin{bmatrix} x_2 \cdot k_2 \oplus k_1 \oplus k_2 \\ x_2 \cdot k_2 \oplus k_1 \end{bmatrix}$ – операція перетворення другого операнда, тоді

$$F^{1}_{9,3} \oplus F^{2.6}_{пк}=\begin{bmatrix} x_1 \oplus x_2 \oplus 1 \\ x_1 \end{bmatrix} \oplus \begin{bmatrix} x_2 \cdot k_2 \oplus k_1 \oplus k_2 \\ x_2 \cdot k_2 \oplus k_1 \end{bmatrix} = \begin{bmatrix} x_1 \oplus x_2 \oplus x_2 \cdot k_2 \oplus k_1 \oplus k_2 \oplus 1 \\ x_1 \oplus x_2 \cdot k_2 \oplus k_1 \end{bmatrix}.$$

Так як

$$F^{1}_{9,3} \oplus F^{2.6}_{пк}=\begin{bmatrix} x_1 \oplus x_2 \oplus x_2 \cdot k_2 \oplus k_1 \oplus k_2 \oplus 1 \\ x_1 \oplus x_2 \cdot k_2 \oplus k_1 \end{bmatrix} = \begin{bmatrix} x_1 \oplus x_2 \cdot \bar{k}_2 \oplus k_1 \oplus k_2 \oplus 1 \\ x_1 \oplus x_2 \cdot k_2 \oplus k_1 \end{bmatrix} = O_{18,3,12,21}$$

Якщо $F^{1}_{9,12}=\begin{bmatrix} x_1 \oplus x_2 \oplus 1 \\ x_1 \oplus 1 \end{bmatrix}$ – операція перетворення першого операнда, а $F^{2.6}_{пк}=\begin{bmatrix} x_2 \cdot k_2 \oplus k_1 \oplus k_2 \\ x_2 \cdot k_2 \oplus k_1 \end{bmatrix}$ – операція перетворення другого операнда, тоді

$$F^{1}_{9,12} \oplus F^{2.6}_{пк}=\begin{bmatrix} x_1 \oplus x_2 \oplus 1 \\ x_1 \oplus 1 \end{bmatrix} \oplus \begin{bmatrix} x_2 \cdot k_2 \oplus k_1 \oplus k_2 \\ x_2 \cdot k_2 \oplus k_1 \end{bmatrix} = \begin{bmatrix} x_1 \oplus x_2 \oplus x_2 \cdot k_2 \oplus k_1 \oplus k_2 \oplus 1 \\ x_1 \oplus x_2 \cdot k_2 \oplus k_1 \oplus 1 \end{bmatrix}.$$

Так як

$$F^{1}_{9,12} \oplus F^{2.6}_{пк}=\begin{bmatrix} x_1 \oplus x_2 \oplus x_2 \cdot k_2 \oplus k_1 \oplus k_2 \oplus 1 \\ x_1 \oplus x_2 \cdot k_2 \oplus k_1 \oplus 1 \end{bmatrix} = \begin{bmatrix} x_1 \oplus x_2 \cdot \bar{k}_2 \oplus k_1 \oplus k_2 \oplus 1 \\ x_1 \oplus x_2 \cdot k_2 \oplus k_1 \oplus 1 \end{bmatrix} = O_{24,9,6,15}$$

Синтез операцій шостого рядка табл. 4.3. реалізується шляхом додавання по модулю два до операцій шостого рядка табл. 4.1 операції $F^{2.6}_{пк}=\begin{bmatrix} x_2 \cdot k_2 \oplus k_1 \oplus k_2 \\ x_2 \cdot k_2 \oplus k_1 \end{bmatrix}$.

Отримані результати дозволили розробити аналогічний метод синтезу групи двохрозрядних двохоперандних операцій для симетричного потокового шифрування, який полягає в наступному:

- синтез двохоперандних операцій базової групи на основі додавання за модулем два одноопераднних операцій обробки кожного операнда. Виконується перетворення на основі моделі $F=\begin{bmatrix} k_1 \oplus x_2 \cdot k_2 \\ k_2 \end{bmatrix}$ замість перетворення на основі моделі $F=\begin{bmatrix} k_1 \\ k_2 \end{bmatrix}$. Виходячи з цього перетворення операції базової групи будуть представлені:

$$O_{1,8,13,20} = F_{3,5}^{1} \oplus F_{nk}^{2.1} = \begin{bmatrix} x_1 \\ x_2 \end{bmatrix} \oplus \begin{bmatrix} k_1 \oplus x_2 \cdot k_2 \\ k_2 \end{bmatrix} = \begin{bmatrix} x_1 \oplus x_2 \cdot k_2 \oplus k_1 \\ x_2 \oplus k_2 \end{bmatrix},$$

$$O_{2,19,14,7} = F_{6,5}^{1} \oplus F_{nk}^{2.2} = \begin{bmatrix} x_1 \oplus x_2 \\ x_2 \end{bmatrix} \oplus \begin{bmatrix} x_2 \cdot k_2 \oplus k_1 \oplus k_2 \\ k_2 \end{bmatrix} = \begin{bmatrix} x_1 \oplus x_2 \oplus x_2 \cdot k_2 \oplus k_1 \oplus k_2 \\ x_2 \oplus k_2 \end{bmatrix},$$

$$O_{3,12,21,18} = F_{3,6}^{1} \oplus F_{nk}^{2.3} = \begin{bmatrix} x_1 \\ x_1 \oplus x_2 \end{bmatrix} \oplus \begin{bmatrix} x_2 \cdot k_2 \oplus k_1 \\ x_2 \cdot k_2 \oplus k_1 \oplus k_2 \end{bmatrix} = \begin{bmatrix} x_1 \oplus x_2 \cdot k_2 \oplus k_1 \\ x_1 \oplus x_2 \oplus x_2 \cdot k_2 \oplus k_1 \oplus k_2 \end{bmatrix}$$

- виконання над операціями базової групи операцій перестановок;
- виконання над операціями базової групи в поєднанні з операціями перестановок операцій інверсії.

Так як основною операцією цієї групи є операція додавання за модулем чотири, то і група була названа симетричною групою двохоперандних двохрозрядних операцій криптографічного додавання за модулем чотири.

Синтезовані групи моделей операцій можуть бути реалізовані в блокових і потокових шифрах.

4.3 Реалізація синтезованих двохоперандних операцій криптоперетворення

Синтезовані математичні моделі симетричних двохрозрядних двохоперандних операцій криптографічного перетворення інформації не викликають складності. Вони базуються на простому й повному математичному описі кожної операції, а також повному математичному описі процесу синтезу груп операцій [7]. Тому ці дослідження не було включено в дисертаційну роботу, а розроблені програмні засоби застосовано для генерації послідовностей для системи тестування NIST STS.

Значно більшу зацікавленість викликають результати дослідження реалізації отриманих моделей на програмному рівні [9].

На рис 4.1 представлена функціональна схема пристрою реалізації груп операцій додавання за модулем два (першої групи).

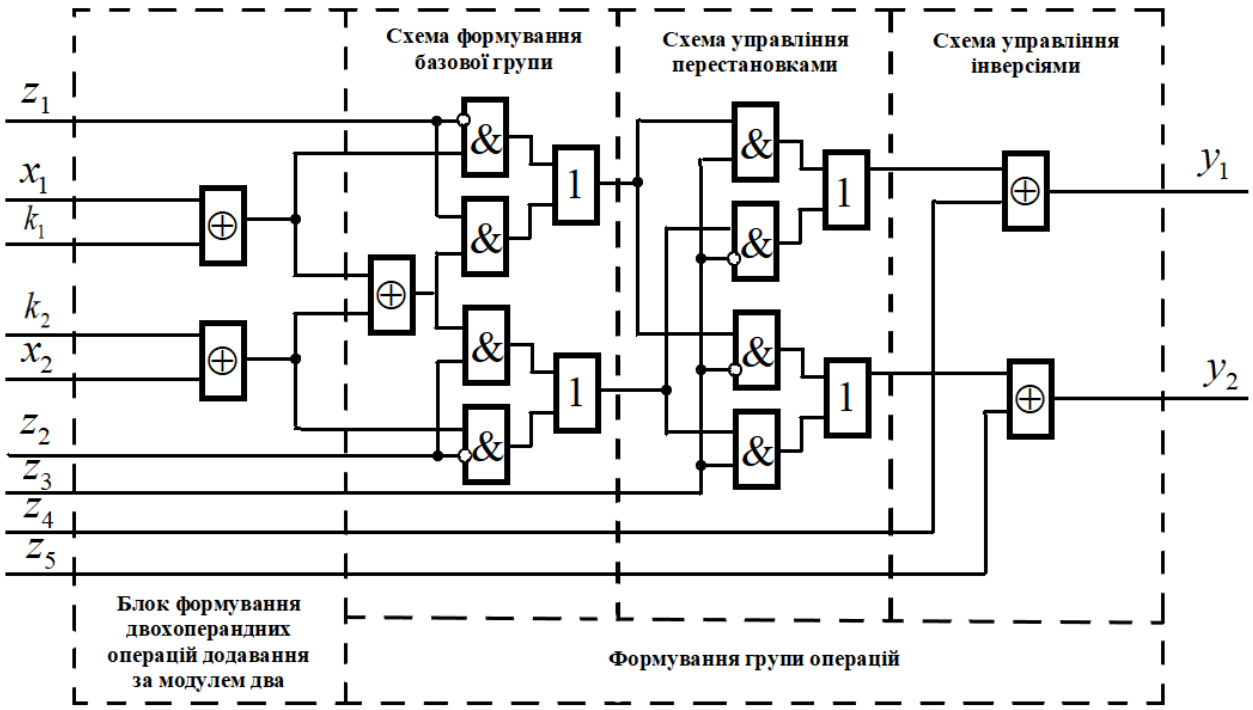


Рис. 4.1 Функціональна схема пристрою реалізації груп операцій додавання за модулем два

Функціональна схема пристрою може бути розбита на чотири функціонально незалежні модулі: блок формування двохоперандних операцій на основі одноопераднних шляхом додавання відповіднох розрядів операндів за модулем два (об'єднуються відповідні розряди першого операнда x_1 і x_2, з відповідними розрядами другого операнда k_1 і k_2); схеми формування операцій базової групи (схема працює в залежності від значень команди управління заданої вхідними сигналами z_1 і z_2); схеми управління перестановками (перестановка задається значенням вхідного сигналу z_3) ; та схеми управління інверсіями (наявність інверсій виходів визначається сигналами управління z_4 і z_5). Три останні схеми умовно можна поєднати в об'єднаний блок формування групи операцій. Функціональна схема пристрою реалізації груп операцій додавання за модулем два працює таким чином: при подачі на входи інформації та сигналів управління на виході буде результат виконання операції заданої сигналами управління.

На рис 4.2 представлена функціональна схема пристрою реалізації груп операцій додавання за модулем чотири (другої групи). Ця функціональна схема відрізняється від функціональна схема пристрою реалізації груп операцій додавання за модулем два лише блоком формування двохоперандних операцій за модулем. Цей блок забезпечує поєднання операцій відповідно до методу синтезу групи другої операції. Схеми формування групи операцій залишені без зміни. Функціонування цієї схеми аналогічне попередній.

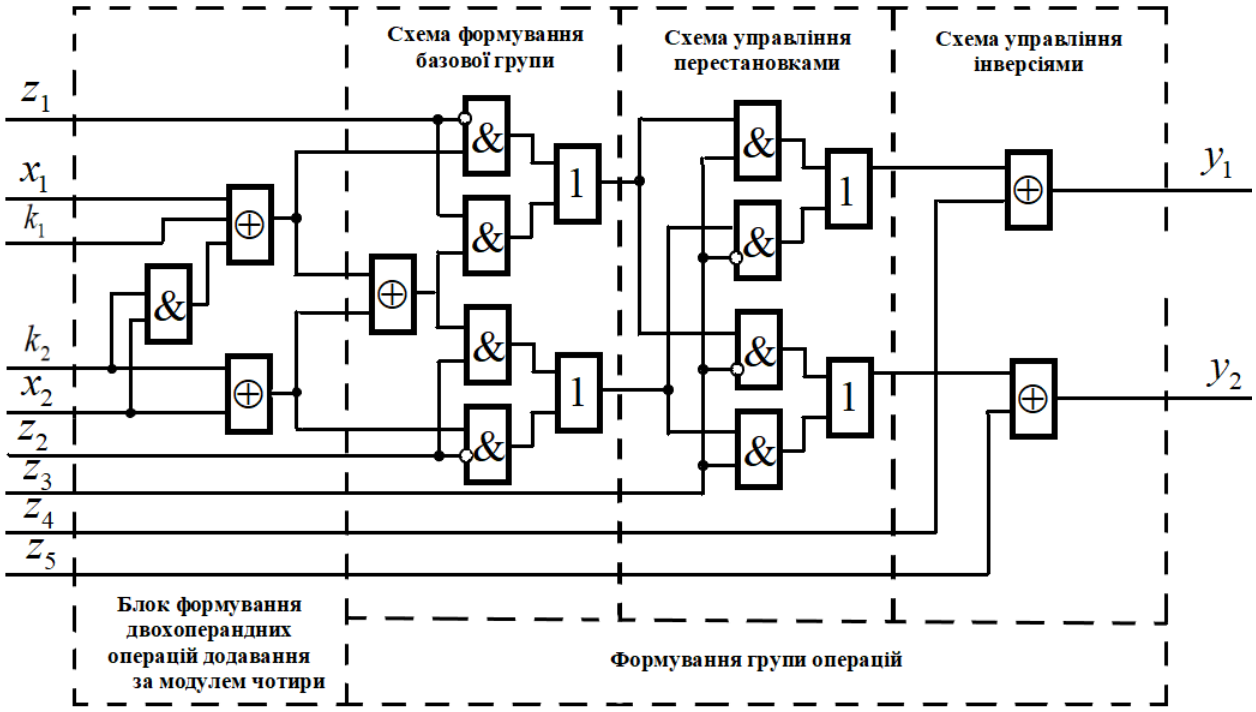


Рис. 4.2 Функціональна схема пристрою реалізації груп операцій додавання за модулем чотири

Об’єднавши під управлінням сигналу z_6 поєднання блоків формування двохоперандних операцій додавання за модулем два та чотири було отримано функціональну схему пристрою реалізації груп операцій додавання за модулями два та чотири (рис.4.3). Ця функціональна схема реалізує 48 симетричних двохрозрядних двохоперандних операцій криптоперетворення замість 24, що реалізують дві попередні функціональні схеми.

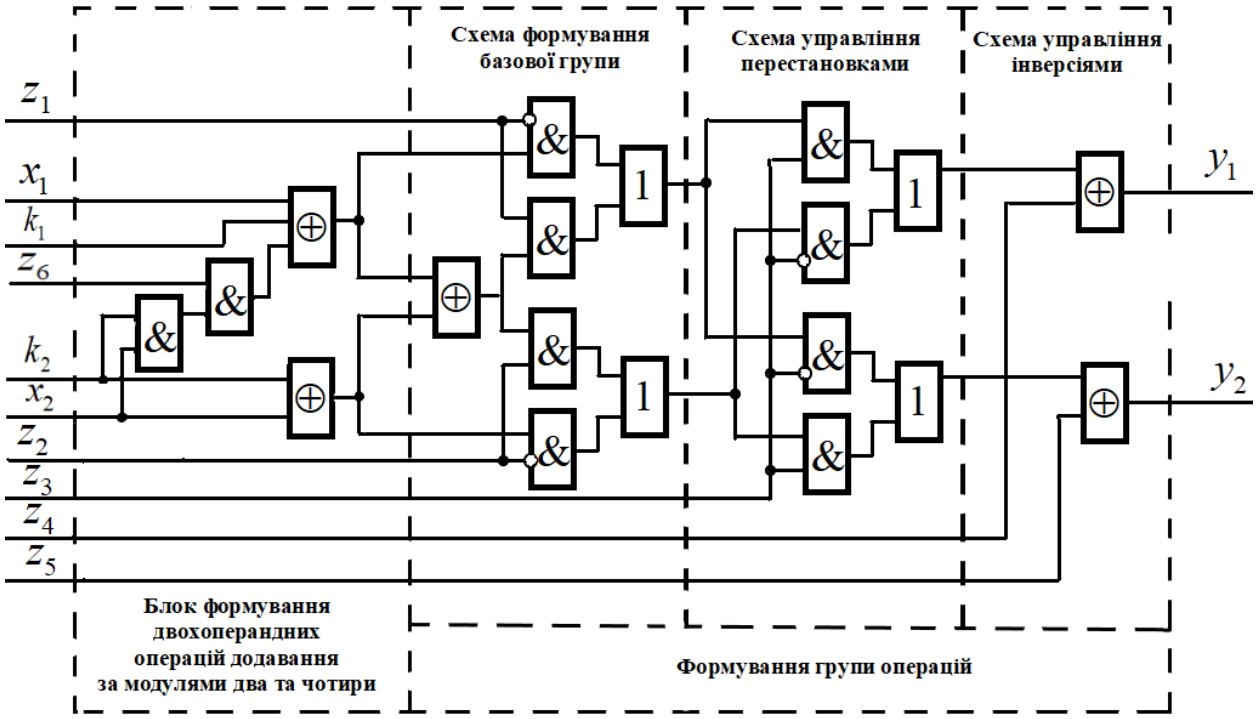


Рис. 4.3 Функціональна схема пристрою реалізації груп операцій додавання за модулями два та чотири

В процесі дослідження встановлено, що побудований пристрій доцільно застосовувати в блоці криптоперетворення при реалізації методу підвищення стійкості та надійності потокового шифрування (рис.4.4) [3, 106-108].

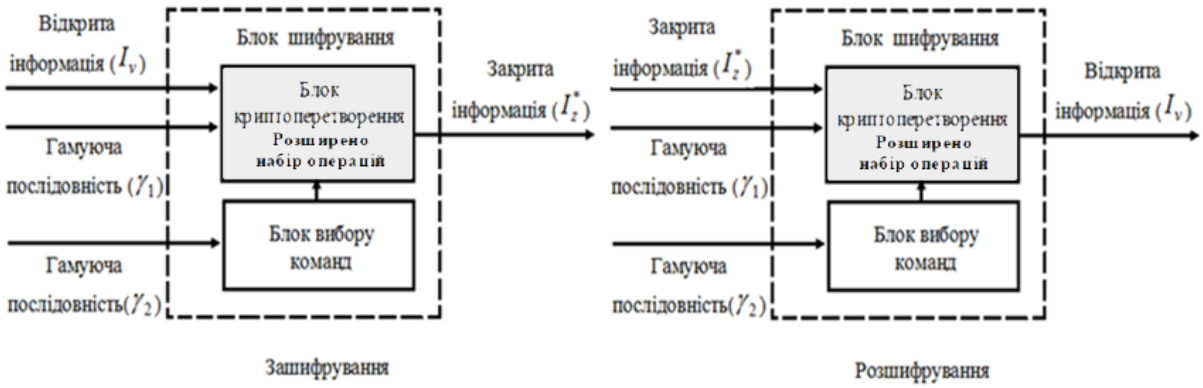


Рис.4.4. Застосування синтезованих груп операцій в методі підвищення стійкості та надійності потокового шифрування

В процесі дослідження встановлено, що сумісне застосування операцій вп’ятеро збільшує варіативність потокового шифрування.

4.4 Оцінка ефективності застосування синтезованих двохоперандних операцій криптоперетворення в потокових шифрах

Для статистичного тестування генераторів псевдовипадкової послідовності, а саме, визначення якісних та кількісних ознак випадковості послідовності чисел, фахівцями Національного інституту стандартів і технологій (НІСТ) США в рамках проекта AES (Advanced Encryption Standard) розроблено статистичні тести «NIST STS» (NIST Statistical Test Suite) [106].

Тести «NIST STS» орієнтовані на використання в задачах криптографічного захисту інформації, які, на думку більшості фахівців цієї сфери, насьогодні найкращим чином відповідають вимогам якісної перевірки ефективності криптоалгоритмів, методів шифрування тощо. Пакет NIST STS містить 15-ть статистичних тестів, які були розроблені для перевірки гіпотези про випадковість двійкової послідовності довільної довжини, що утворює псевдовипадкову послідовність. Усі 15-ть тестів спрямовані на виявлення різних дефектів випадковості. Основним принципом тестування є перевірка нульової гіпотези, суть якої в тому, що випадковість, що тестується, дійсно є випадковою. Альтернативною гіпотезою є гіпотеза про те, що випадковість, що тестується, є не випадковою. За результатами виконання кожного тесту нульова гіпотеза або підтверджується, або ні. Рішення про те, що задана послідовність нулів та одиниць є випадковою, ухвалюється за результатами усіх тестів [107-108].

В процесі тестування проводилася оцінка відповідності згенерованих текстових файлів вимогам NIST STS [5]. Текстові файли формувалися на основі потокового шифрування інформації з використанням наборів операцій [5, 8]. Вхідні дані для тестування формувалися на основі алгоритму (рис 4.1). Алгоритм має такі режими генерації наборів операцій для тестування:

1. Відомої групи з 12-ти операцій криптографічного додавання за модулем два з точністю до перестановки (аналог). Результати наведено на рис.4.2 (додаток А);

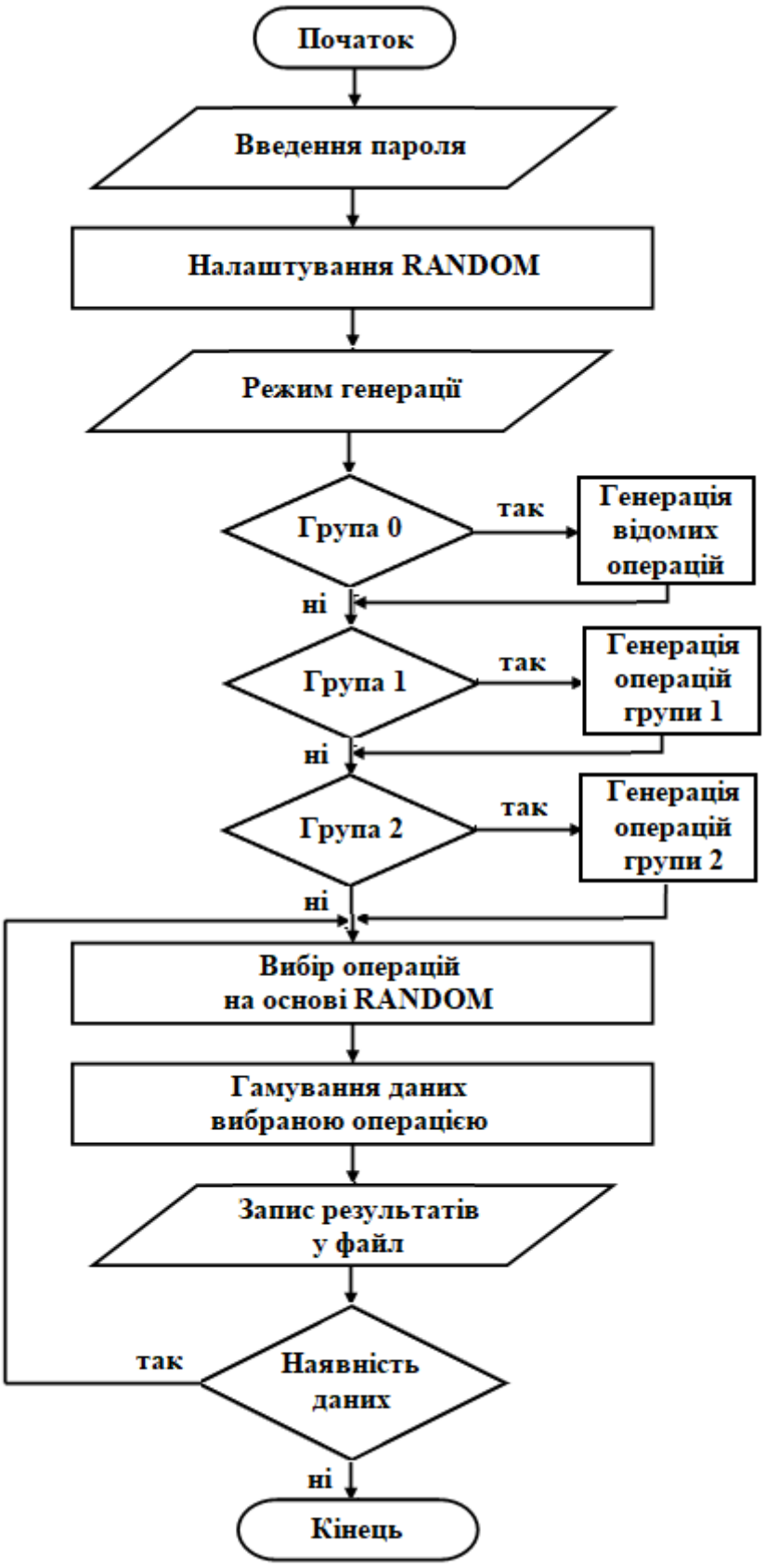


Рис 4.1. Алгоритм генерації результатів шифрування для тестування

2. Першої синтезованої групи з 24-ох операцій криптографічного додавання за модулем два. Результати наведено на рис.4.3;
3. Другої синтезованої групи з 24-ох операцій криптографічного додавання за модулем чотири. Результати наведено на рис.4.4;
4. Сумісного використання першої і другої синтезованих груп операцій криптографічного додавання (48 операцій). Результати наведено на рис.4.5;
5. Сумісного використання наявних операцій криптографічного додавання (60 операцій). Результати наведено на рис.4.6.

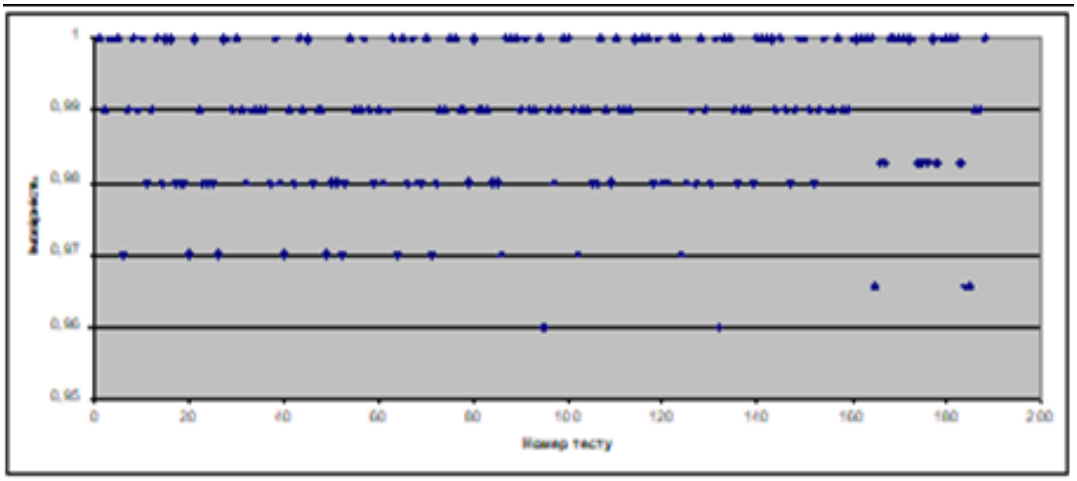


Рис.4.2. Результати тестування методу підвищення стійкості та надійності потокового шифрування відомої групи з 12-ти операцій криптографічного додавання за модулем два з точністю до перестановки (аналог)

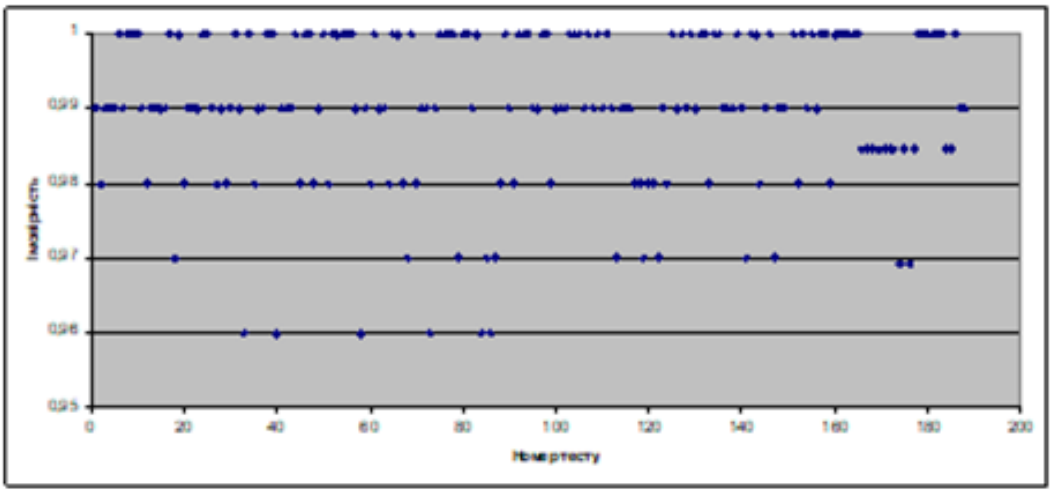


Рис.4.3. Результати тестування методу підвищення стійкості та надійності потокового шифрування першої синтезованої групи з 24-ох операцій криптографічного додавання за модулем два

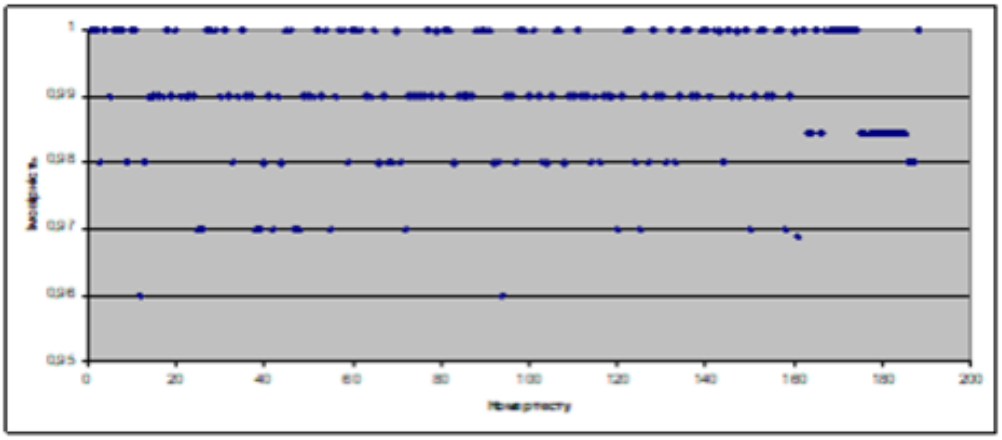


Рис.4.4. Результати тестування методу підвищення стійкості та надійності потокового шифрування другої синтезованої групи з 24-ох операцій криптографічного додавання за модулем чотири

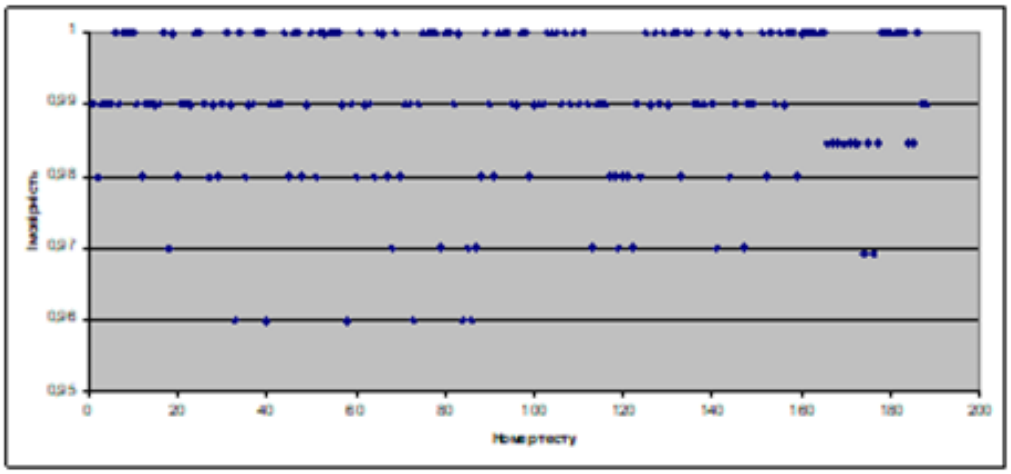


Рис.4.5. Результати тестування методу підвищення стійкості та надійності потокового шифрування сумісного використання першої і другої синтезованих груп операцій криптографічного додавання (48 операцій)

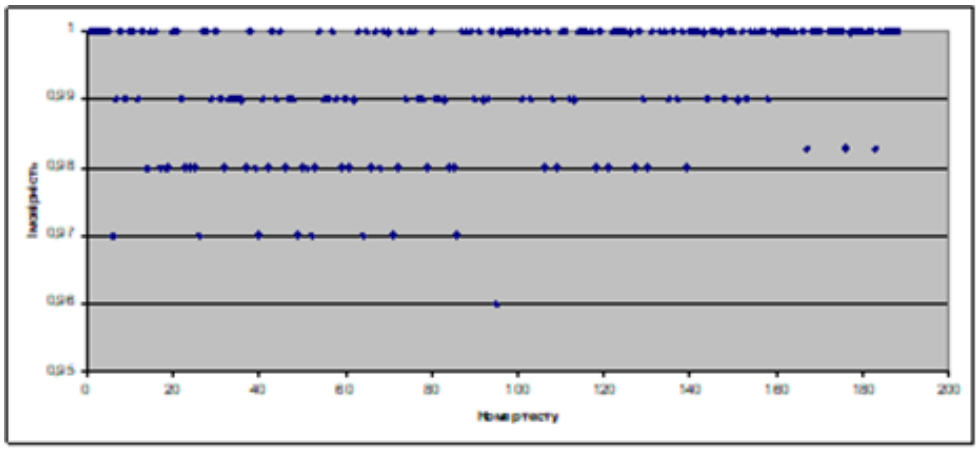


Рис.4.6. Результати тестування методу підвищення стійкості та надійності потокового шифрування сумісного використання наявних операцій криптографічного додавання (60 операцій)

Результати тестування наведено в додатках А-Д відповідно.

Зведені результати тестування NIST STS методу підвищення стійкості та надійності потокового шифрування за різних наборів операцій криптоперетворення подано в табл. 4.4.

Таблиця 4.4

Зведені результати тестування методу підвищення стійкості та надійності потокового шифрування за різних наборів операцій криптоперетворення

Генерація послідовності на основі застосування	Кількість тестів, в яких пройшло тестування	
	99% послід.	96% послід.
Відомої групи з 12-ти операцій криптографічного додавання за модулем два з точністю до перестановки (аналог)	126 (67 %)	188 (100 %)
Першої синтезованої група з 24-ох операцій криптографічного додавання за модулем два	131 (69,7 %)	188 (100 %)
Другої синтезованої група з 24-ох операцій криптографічного додавання за модулем чотири	132(70,2 %)	187 (99,5 %)
Сумісного використання першої і другої синтезованих груп операцій криптографічного додавання (48 операцій)	131 (69,7 %)	188 (100 %)
Сумісного використання наявних операцій криптографічного додавання (60 операцій)	142 (75,5 %)	188 (100 %)

Наведені результати статистичних досліджень практичних результатів дисертаційної роботи свідчать про те, що досліджувані послідовності пройшли комплексний контроль за методикою випробувань пакетом тестів NIST STS [8]. Найкращі результати тестування отримано при застосуванні 12-ти відомих та 48-ми синтезованих в роботі операцій криптоперетворення.

Висновки з розділу 4

1. Розроблено метод синтезу групи операцій додавання за модулем два для потокового шифрування на основі операції додавання за модулем два на основі результатів обчислювального експерименту, шляхом застосування результатів реалізації методу побудови та дослідження двохоперандних операцій криптоперетворення та табличного представлення класифікації групи одноопераднних двохрозрядних операцій криптографічного перетворення, а також встановлення нових раніше невідомих взаємозв'язків між одноопераднними та двохоперандними операціями, що забезпечило синтез нової математичної групи симетричних двохоперандних операцій криптоперетворення.

2. Розроблено метод синтезу групи операцій додавання за модулем чотири для потокового шифрування, метод синтезу групи операцій додавання за модулем два для потокового шифрування, шляхом встановлення нових раніше невідомих взаємозв'язків між одноопераднними та двохоперандними операціями, що забезпечило синтез нової математичної групи симетричних двохоперандних операцій криптоперетворення.

3. При реалізації синтезованих операцій в методі підвищення стійкості та надійності потокового шифрування забезпечується збільшення варіативності потокового шифрування вп'ятеро. Розроблені функціональні схеми забезпечують сумісне використання обох груп синтезованих операцій з 12-ма раніше відомими операціями в блоці криптоперетворення.

4. Результати статистичних досліджень результатів програмної реалізації методу підвищення стійкості та надійності потокового шифрування при застосуванні відомих та вперше синтезованих симетричних операцій показав, що їх застосування забезпечує необхідну стійкість до лінійного криптоаналізу. Найкращі результати тестування отримано при застосуванні 12-ти відомих та 48-ми синтезованих в роботі операцій криптоперетворення.

5. Результати розділу опубліковано [3, 5, 7- 9, 11].

ВИСНОВКИ

У дисертаційній роботі вирішено важливу науково-технічну задачу підвищення якості систем потокового шифрування конфіденційної інформації за рахунок збільшення стійкості та варіативності перетворення на основі додаткового використання груп двохоперандних двохрозрядних операцій, синтезованих на основі додавання за модулями два та чотири. А саме:

1) розроблено метод побудови та дослідження двохоперандних операцій криптоперетворення на основі результатів обчислювального експерименту, шляхом формального опису та класифікації наборів та груп операцій, з подальшим дослідженням виокремлених сукупностей на основі математичного опису та визначеної послідовності математичних перетворень, а також побудови перестановочних схем, що забезпечило виявлення сутності операції на основі встановлення нових взаємозв’язків між операндами й результатами, а також можливість застосування відомих раніше одноопераднних операцій в потоковому шифруванні на апаратному і програмному рівнях;

2) вперше розроблено методи синтезу груп симетричних двохрозрядних двохоперандних операцій потокового шифрування на основі результатів обчислювального експерименту шляхом застосування результатів реалізації методу побудови та дослідження двохоперандних операцій криптоперетворення і табличного представлення класифікації групи одноопераднних двохрозрядних операцій криптографічного перетворення, а також встановлення нових раніше невідомих взаємозв’язків між одноопераднними та двохоперандними операціями, що забезпечило синтез математичних груп симетричних двохоперандних операцій на основі додавання за модулем два та додавання за модулем чотири. Побудова нових математичних груп операцій реалізована шляхом математичних перетворень трьох відомих двохрозрядних одноопераднних операцій базової групи.

Побудова групи перестановочних схем таблиці істинності забезпечила можливість побудови невідомої математичної групи операцій на основі однієї операції, яка належить цій групі;

3) удосконалено метод підвищення стійкості та надійності потокового шифрування на основі додаткового застосування синтезованих груп симетричних двохоперандних операцій криптографічного перетворення інформації, що забезпечило підвищення стійкості та варіативності потокового шифрування;

4) практична цінність роботи полягає в тому, що отримані наукові результати доведенні здобувачем до конкретних інженерних методик, моделей та варіантів функціональних схем спеціалізованих дискретних пристроїв, які реалізують криптографічне перетворення інформації на основі застосування синтезованих груп операцій потокового шифрування та забезпечують підвищення варіативності й стійкості до лінійного криптоаналізу. На підставі проведених досліджень одержано такі практичні результати: побудовано математичні моделі, алгоритми функціонування та функціональні схеми реалізації груп операцій криптографічного додавання за модулем два та модулем чотири, що дає можливість підвищувати якість систем потокового й блокового шифрування інформації. У разі застосуванні синтезованих груп операцій в методі підвищення стійкості та надійності потокового шифрування найкращі результати тестування пакетом тестів NIST STS отримано під час застосування 12-ти відомих та 48-ми синтезованих операцій криптоперетворення. Крім того сумісне застосування операцій вп’ятеро збільшує варіативність потокового шофрування.

Результати роботи впроваджено у Центральному конструкторському бюро «Сокіл» Науково-виробничого комплексу «ФОТОПРИЛАД» (м. Черкаси) під час проектування спеціалізованого модуля операційної системи, а також в навчальному процесі Черкаського державного технологічного університету.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Бабенко В. Г., Козловська С. Г. Особливості використання матричних операцій криптографічного перетворення інформації. *Системи обробки інформації.* 2015. № 3 (128). С. 84–87.

2. Рудницький В. М., Лада Н. В., Козловська С. Г. Технологія побудови двохоперандних операцій криптографічного перетворення інформації за результатами моделювання. *Сучасні інформаційні системи*. 2018. Т. 2, № 4. С. 26–30.

3. Лада Н. В., Козловська С. Г. Застосування операцій криптографічного додавання за модулем два з точністю до перестановки в потокових шифрах. *Системи управління, навігації та зв'язку :* зб. наук. пр. Полтава : ПНТУ, 2018. Т. 1 (47). С. 127–130.

4. Козловська С. Г. Синтез груп двохоперандних операцій криптоперетворення на основі перестановочних схем. *Сучасна спеціальна техніка.* 2018. № 4 (55). С. 44–50.

5. Зажома В. М., Козловська С. Г. Спосіб підвищення достовірності передачі ключового елементу стегоконтейнера. *Smart and Young.* 2016. № 11-12. Частина 1. С. 42–48.

6. Криптографічне кодування: обробка та захист інформації: колективна монографія / за ред. В. М. Рудницького. Харків : ТОВ «ДІСА ПЛЮС», 2018. 139 с.

7. Козловська С. Г. Лада С. В., Аскеров Р. В. Засоби захисту програм від несанкціонованого доступу. *Проблеми інформатизації* : матеріали Першої міжнар. наук.-техн. конф.: тези доп., (Черкаси – Київ – Тольятті – Полтава, 19–20 грудня. 2013 р.). Черкаси: ЧДТУ; Київ: ДУТ, Тольятті: ТДУ, Полтава: ПНТУ, 2013. С. 25.

8. Козловська С. Г. Проблеми захисту управлінської інформації. *Теоретико-методологічні і науково-практичні засади інформаційного, фінансового та облікового забезпечення розвитку економіки* : зб. тез доп. наук.-практ. конф., м. Черкаси, 21–22 лист. 2013 р. Черкаси, 2013. С. 50-51.

9. Козловська С. Г. Технічні способи запобігання просочуванню інформації. *Проблеми моделювання структури і процесів економічних систем* : зб. тез доп. міжнар. наук.-практ. конф., м. Черкаси, 17–18 квіт. 2014 р. Черкаси, 2014. С. 93–95.

10. Козловська С. Г. Персонал підприємства як основне джерело втрати конфіденційної інформації. *Управління економіко-соціальними системами розвитку суспільства в умовах євроінтеграції* : зб. тез доп. наук.-практ. конф., м. Черкаси, 15–17 квіт. 2015 р. Черкаси, 2015. С. 79–80.

11. Козловська С. Г. Особливості криптографічного захисту інформації. *Фінансово-економічне та обліково-аналітичне забезпечення підприємницької діяльності* : зб. тез доп. Всеукр. наук.-практ. конф., м. Черкаси, 20–21 квіт. 2016 р. Черкаси, 2016. С. 360–363.

12. 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.

13. Василенко О. Н. Теоретико-числовые алгоритмы в криптографии / О.Н. Василенко. М.: МЦНМО, 2003. 328 с.

14. Болотов А. А. Гашков С. Б., Фролов А. Б. Элементарное введение в эллиптическую криптографию: Протоколы криптографии на эллиптических кривых. М.: КомКнига, 2006. 280 с.

15. Ковтун В. Ю. Введение в криптоанализ. Криптоанализ симетричных криптосистем: блочные шифры. URL: http://www.nrjetix.com/fileadmin/doc/ publications/Lectures_security/Lecture4-1.pdf.

16. Панасенко С. П. Алгоритмы шифрования: специальный справочник. СПб. : БХВ-Петербург, 2009. 576 с.

17. Брилюк Д. В. Подход к созданию трудноанализируемых шифров. URL: http://www.nestor.minsk.by/kg/2000/26/kg02613.html.

18. Нечаев В. И. Элементы криптографии. Основы теории защиты информации : учеб. пособие. М.: Высшая школа, 1999. 109 с.

19. Ященко В.В. Введение в криптологию. Сбп. : Питер, 2000. 271 с.

20. ДСТУ 4145-2002. Інформаційні технології. Криптографічний захист інформації. Цифровий підпис, що грунтується на еліптичних кривих. Формування та перевіряння. [Чинний від 2003-07-01]. Київ, 2002. 39 с.

21. Нильсен М., Чанг И. Квантовые вычисления и квантовая информация : монографія / пер. с англ. М.: Мир, 2006. 824 с.

22. Корченко О. Г., Васіліу Є. В., Гнатюк С. О. Сучасні квантові технології захисту інформації. *Захист інформації*. 2010. № 1. С. 77–89.

23. Diffie, Whitfield; Hellman, Martin E. (June 1977). “Exhaustive Cryptanalysis of the NBS Data Encryption Standard”. Computer. 10 (6): 74–84. DOI:10.1109/C-M.1977.217750.

24. 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.

25. Криптографическое кодирование : кол. монография / за ред. В. Н. Рудницкого, В. Я. Мильчевича. Х. : Щедрая усадьба плюс, 2014. 240 с.

26. Брюс Шнайер. Прикладная криптография. Протоколы, алгоритмы и исходные тексты на языке Си. М. : Триумф, 2002. 816 с.

27. Шеннон К. Работы по теории информации и кибернетике. М.: Изд-во иностранной литературы, 1963. 830 с.

28. Панасенко С. П. Алгоритмы шифрования. Специальный справочник. СПб. : БХВ-Петербург, 2009. 576 с.

29. Eli Biham, Orr Dunkelman, Nathan Keller. Improved Slide Attacks. *Fast Software Encryption*. 14th International Workshop, FSE 2007, Luxembourg, Luxembourg, March 26–28, 2007, Revised Selected Papers. Springer Berlin Heidelberg, 2007. P. 153–166.

30. Рябко Б. Я., Фионов А. Н. Криптографические методы защиты информации : учеб. пособ. М. : Горячая линия-Телеком, 2005. 229 с.

31. Andriy Lagun Cryptographic Strength of a New Symmetric Block Cipher Based on Feistel Network. *Technical Transactions*. Series "Automatic Control". 2013. Vol. 2-AC (10). P. 67–80.

32. Вербіцький О. В. Вступ до криптології. Львів : Науково-технічна література, 1998. 249 с.

33. Основы криптографии : учеб. пособ. / Алферов А. П., Зубов А. Ю., Кузьмин А. С., Черемушкин А. В. М. : Гелиос АРВ, 2002. 480 с.

34. Soichi Furuya. Slide Attacks with a Known-Plaintext Cryptanalysis. *Information Security and Cryptology – ICISC 2001*. 4th International Conference Seoul, Korea, December 6–7, 2001 Proceedings. Springer Berlin Heidelberg, 2002. P. 214–225.

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

36. Ільєнко А. В., Зюбіна Р. В. Забезпечення конфіденційності інформаційних ресурсів на основі методів гомоморфного шифрування. *Авіа-2015:* тези доп. XII міжнар. наук.-техн. конф., 28–29 квітня 2015 р. К., 2015. С. 5.25–5.29.

37. Чунарьова А. В., Миколишин Д. М. Аналіз сучасних алгоритмів гомоморфного шифрування. *Naukpwa przestrzen europy – 2014*: X miedzynar. nauk.-prakt. konf., 07–15 kwiet. 2014 r.: abstracts. Przemysl (Polska), 2014. V. 33. P. 98–101.

38. Анна Ільєнко. Сучасні методи гомоморфного шифрування інформаційних ресурсів. *Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні*. 2015. Вип. 2 (30). С. 52–57.

39. Задірака В. К., Олексюк О. С. Комп'ютерна криптологія : підручник. К., 2002. 504 с.

40. 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.

41. Математичні основи криптографії : навч. посіб. / Кузнецов Г. В., Фомичов В. В., Сушко С. О., Фомичова Л. Я. Дніпропетровськ: Націон. гірничий ун-т, 2004. Ч. 1. 391 с.

42. 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.

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

44. 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.

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

46. 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.

47. Рудницький В. М., Миронець І. В., Бабенко В. Г. Технологія побудови пристрою реалізації методу підвищення оперативності доступу до конфіденційних інформаційних ресурсів. 2011. Вип. 3 (29). С. 145–150.

48. 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. Первой междунар. заочной научно-практ. конф. Тольятти: ПВГУС, 2012. С. 67–77.

49. Миронець І. В., Рудницький В. М. Дослідження алгоритмів синтезу функцій перекодування. *Вісник Черкаського державного технологічного університету*. *Сер. Технічні науки.* 2010. Вип. №4. С. 60–64.

50. 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.

51. 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.

52. Бабенко В. Г. Складності та особливості побудови ефективних крипто алгоритмів. *Вісник Черкаського державного технологічного університету*. *Сер. Технічні науки.* 2014. № 3. С. 87–91.

53. 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.

54. 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.

55. 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.

56. 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.

57. 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.

58. 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.

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

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

61. 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. 1–54.

62. Рудницький В. М., Миронець І. В., Бабенко В. Г. Реалізація методу підвищення оперативності доступу до конфіденційних інформаційних

ресурсів. *Вісник Черкаського державного технологічного університету*. *Сер. Технічні науки*. 2010. Вип. №3. С. 60–65.

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

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

65. Ланських Є. В., Сисоєнко С. В., Пустовіт М. О. Оцінка якості псевдовипадкових послідовностей на основі використання операцій додавання за модулем два. *Наука і техніка Повітряних Сил Збройних Сил України*. 2015. №4(21). С. 147–150.

66. Фауре Е. В., Сисоєнко С. В., Миронюк Т. В. Синтез і аналіз псевдовипадкових послідовностей на основі операцій криптографічного перетворення. *Системи управління, навігації та зв'язку*. 2015. Вип. 4 (36). С. 85–87.

67. Фауре Е. В., Сисоєнко С. В. Метод підвищення стійкості псевдовипадкових послідовностей до лінійного криптоаналізу. *The scientific potential of the present*: proceedings of the International Scientific Conference (St. Andrews, Scotland, UK, December 1, 2016) / ed. N. P. Kazmyna. NGO «European Scientific Platform». Vinnytsia: PE Rogalska I. O., 2016. P. 119–122.

68. Рудницький В. М., Миронець І. В., Бабенко В. Г., Миронюк Т. В., Сисоєнко С. В. Реалізація вершинної мінімізації булевих функцій для моделювання процесів, що не формалізуються. *Science and Education a New Dimension. Natural and Technical Sciences*. V(14). Issue: 132. Budapest, 2017. P. 85–88.

69. Миронец И. В., Бабенко В. Г., Миронюк Т. В., Сысоенко С. В. Особенности применения операций перестановок, управляемых

информацией, для криптографического преобразования. *Wschodnioeuropejskie Czasopismo Naukowe*: East European Scientific Journal (Warsaw, Poland)#11(27), 2017, part 1. P. 85–92.

70. Эвристические алгоритмы и распределённые вычисления в прикладных задачах: кол. монография / под ред. Б. Ф. Мельникова. Ульяновск, 2013. Вып. 2. 202 с.

71. Рудницький В. М., Сисоєнко С. В., Миронець І. В. Синтез невиродженого криптографічного перетворення на основі групового використання дворозрядних матричних операцій. *Наукоемкие технологии в инфокоммуникациях: обработка информации, кибербезопасность, информационная борьба :* монография / под общ. ред. В. М. Безрука, В. В. Баранника. Х. : Лидер, 2017. С. 516-532.

72. Миронець І. В., Миронюк Т. В., Сисоєнко С. В. Апаратна реалізація базової групи операцій перестановок, керованих інформацією. *Актуальні задачі та досягнення у галузі кібербезпеки* : матеріали Всеукр. наук.-практ. конф. (м. Кропивницький, 23–25 листоп. 2016 р.). Кропивницький: КНТУ, 2016. С. 141–142.

73. Стабецька Т. А. Математичне обґрунтування узагальненого методу синтезу обернених операцій нелінійного розширеного матричного криптографічного перетворення. *Наукові праці. Сер. Комп'ютерні технології.* 2014. Т. 250, Вип. 238. С. 10–114.

74. 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.

75. Стабецька Т. А. Умови невиродженості нелінійних операцій розширеного матричного криптографічного перетворення, що містять неповні функції РМКП. *Системи обробки інформації.* 2016. Вип. 1(138). С.131–133.

76. Бабенко В. Г., Мельник О. Г., Стабецька Т. А. Синтез нелінійних

операцій криптографічного перетворення. *Безпека інформації*. 2014. № 2. Т. 20. С. 143–147.

77. Стабецька Т. А. Умови невиродженості операцій розширеного матричного криптографічного перетворення. *Сучасні напрями розвитку інформаційно-комунікаційних технологій та засобів управління* : матеріали П'ятої міжнар. наук.-техн. конф.: тези доп. (Полтава – Баку – Кіровоград – Харків, 23–24 квітня 2015 р.). С. 61.

78. Стабецька Т.А. Побудова обернених нелінійних операцій розширеного матричного криптографічного перетворення. *Проблеми інформатизації*: матеріали Першої міжнар. наук.-техн. конф.: тези доп. (Черкаси – Київ – Тольятті – Полтава, 9–20 грудня 2013 р.). Черкаси: ЧДТУ, 2013. С. 24–25.

79. Рудницький В. М., Шувалова Л. А., Нестеренко О. Б. Синтез операцій криптографічного перетворення за критерієм строгого стійкого кодування. *Вісник інженерної академії України: часопис.* 2016. Вип. 3. С. 105–108.

80. 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. (Черкаси – Баку – Бельсько-Бяла – Полтава, 14–16 листоп. 2018 р.). Черкаси: ЧДТУ; Баку: ВА ЗС АР; Бельсько-Бяла: УТіГН; Полтава: ПНТУ, 2018. С. 9–10.

81. 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.

82. Лада Н. В. Аналіз коректності взаємозв'язків між прямими та оберненими матричними моделями операцій криптографічного перетворення інформації. *Системи управління, навігації та зв'язку*. 2015. Вип. 4 (36). С. 73–

78.

83. 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.

84. 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.

85. 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.

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

87. Лада Н. В., Рудницька Ю. В. Класифікація груп несиметричних двохоперандних операцій криптоперетворення інформації на основі перестановочних схем їх синтезу. *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.

88. Бабенко В. Г., Лада Н. В. Дослідження симетричних дворозрядних двохоперандних операцій для криптоперетворення. *Сучасні напрями розвитку інформаційно-комунікаційних технологій та засобів управління* : матеріали П'ятої міжнар. наук.-техн. конф.: тези доп., (Полтава – Баку – Кіровоград – Харків, 23–24 квіт. 2015 р.). С. 59.

89. 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*: матеріали Першої міжнар. наук.-практ. конф. : тези доп., (Харків – Київ – Кіровоград – Вінниця – Софія – Баку – Бельсько-Бяла, 30 березня-1 квітня 2016 р.). С. 17.

90. Бабенко В. Г., Лада Н. В., Лада С. В. Розширення множини двохоперандних операцій додавання за модулем для криптографічного перетворення інформації. *Проблеми інформатизації* : матеріали Третої міжнар. наук.-техн. конф.: тези доп., (Черкаси – Баку – Бельсько-Бяла – Полтава, 12–13 листоп. 2015 р.). Черкаси: ЧДТУ, 2015. С. 16.

91. Бабенко В. Г., Лада Н. В., Лада С. В. Аналіз множин операцій, синтезованих на основі додавання за модулем два. *Методи та засоби кодування, захисту й ущільнення інформації :* матеріали П’ятої Міжнар. наук.-практ. конф.: тези доп. (м. Вінниця, 19–21 квіт. 2016 р.). Вінниця: ТОВ «Нілан-ЛТД», 2016. С. 54–57.

92. Лада Н. В. Використання графічного представлення операцій для виявлення їх взаємозв’язків в моделях операцій криптографічного перетворення. *Проблеми інформатизації* : матер. четвертої міжнар. наук.-техн. конф.: тези доп. (Черкаси – Баку – Бельсько-Бяла – Полтава, 3–4 листоп. 2016 р.). Черкаси: ЧДТУ, 2016. С. 9–10.

93. Лада Н. В. Аналіз коректності взаємозв’язків між прямими та оберненими матричними моделями операцій криптографічного перетворення інформації. *Системи управління, навігації та зв’язку.* 2015. Вип. 4 (36). С. 73–78.

94. 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* : матер.

Першої міжнар. наук.-практич. конф.: тези доп. (Харків –Київ – Кіровоград – Вінниця – Софія – Баку – Бельсько-Бяла; 30 берез.–1 квіт. 2016 р.). С. 17.

95. Бабенко В. Г., Лада Н. В. Синтез і аналіз операцій криптографічного додавання за модулем два. *Системи обробки інформації*. 2014. №. 2 (118). С. 116–118.

96. 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*: the Internat. sci. conf., (St. Andrews, Scotland, UK, December, 1, 2016) / ed. N. P. Kazmyna. NGO «European Scientific Platform». Vinnytsia: PE Rogal ska I. O., 2016. С. 108–111. (Шотландия, Логос).

97. Лада Н. В. Аналіз коректності взаємозв'язків між прямими та оберненими матричними моделями операцій криптографічного перетворення інформації. *Системи управління, навігації та зв'язку.* 2015. Вип. 4 (36). С. 73–78.

98. Бабенко В. Г., Лада Н. В. Технологія дослідження операцій додавання за модулем. *Smart and Young.* 2016. № 11–12, ч. 1. С. 49–54.

99. Бабенко В. Г., Лада Н. В., Лада С. В. Аналіз множини операцій синтезованих на основі додавання за модулем два. *Вісник Черкаського державного технологічного університету. Сер. Технічні науки*. 2016. Вип. №1. С. 5–11.

100. 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.

101. Криптографическое кодирование: кол. монография / под ред. В. Н. Рудницкого, В. Я. Мильчевича. Х. : Щедрая усадьба плюс, 2014. 240 с.

102. 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.

103. Рудницький В. М., Бабенко В. Г., Рудницький С. В. Метод синтезу матричних моделей операцій криптографічного кодування та декодування інформації. *Зб. наук. пр. Харків. ун-ту Повітряних Сил*. 2012. Вип. 4 (33). С. 198–200.

104. Криптографическое кодирование: методы и средства реализации: монография / Рудницкий В.Н. и др. Тольятти, 2013. 196 с.

105. Ланських Є. В., Сисоєнко С. В. Дослідження математичної моделі двохоперандного групового матричного криптографічного перетворення. *Вісник Черкаського державного технологічного університету. Сер. Технічні науки.* Черкаси: ЧДТУ, 2018. Вип. 1. С. 67–74.

106. Soto J. Statistical testing of random number generators. *The 22nd National Information Systems Security Conference*. 1999. Vol. 10. P. 12.

107. Потій А. В. Статистичне тестування генераторів випадкових і псевдовипадкових чисел з використанням набору статистичних тестів NIST STS. URL: www.kiev-security.org.ua.

108. Потий А., Орлова С., Гриненко Т. Статистическое тестирование генераторов случайных и псевдослучайных чисел с использованием набора статистических тестов NIST STS. Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні. 2001. Вип. 2. С. 206–214.

ДОДАТОК А

Результати тестування методу підвищення стійкості та надійності потокового шифрування відомої групи з 12-ти операцій криптографічного додавання за модулем два з точністю до перестановки (аналог) за допомогою статистичного пакету NIST STS

RESULTS FOR THE UNIFORMITY OF P-VALUES AND THE PROPORTION OF PASSING SEQUENCES

generator is <12_kz_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	0.9900	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	0.9900	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.
- -

ДОДАТОК Б

Результати тестування методу підвищення стійкості та надійнсті потокового шифрування першої синтезованої групи з 24-ох операцій криптографічного додавання за модулем два за допомогою статистичного пакету NIST STS

RESULTS FOR THE UNIFORMITY OF P-VALUES AND THE PROPORTION OF PASSING SEQUENCES

generator is <24_2_kz_TXT,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	0.9900	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.
- -

ДОДАТОК В

Результати тестування методу підвищення стійкості та надійності потокового шифрування другої синтезованої групи з 24-ох операцій криптографічного додавання за модулем чотири за допомогою статистичного пакету NIST STS

```
------------------------------------------------------------------------------
RESULTS FOR THE UNIFORMITY OF P-VALUES AND THE PROPORTION OF PASSING SEQUENCES
------------------------------------------------------------------------------
   generator is <24_4_kz_TXT,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   0.9800    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
 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
 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
  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
 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   0.9800    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
 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
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	0.9800	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
12	8	6	10	14	7	8	10	13	12	0.678686	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
13	12	13	8	7	9	4	12	9	13	0.474986	0.9800	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
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	0.9800	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
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   0.9590    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   0.9800    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
  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   0.9800    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
  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 Г

Результати тестування методу підвищення стійкості та надійності потокового шифрування сумісного використання першої і другої синтезованих груп операцій криптографічного додавання (48 операцій) за допомогою статистичного пакету NIST STS

RESULTS FOR THE UNIFORMITY OF P-VALUES AND THE PROPORTION OF PASSING SEQUENCES

generator is <48_kz_TXT,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
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	0.9800	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
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
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
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
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
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
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
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	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
  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
 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
  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   0.9800    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
  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
  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  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.
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
```

ДОДАТОК Д

Результати тестування методу підвищення стійкості та надійності потокового шифрування сумісного використання наявних операцій криптографічного додавання (60 операцій) за допомогою статистичного пакету NIST STS

```
------------------------------------------------------------------------------
RESULTS FOR THE UNIFORMITY OF P-VALUES AND THE PROPORTION OF PASSING SEQUENCES
------------------------------------------------------------------------------
   generator is <60_kz_TXT,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
 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
  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
 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   0.9900    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
```

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
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
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	1.0000	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   0.9900    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   1.0000    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   1.0000    RandomExcursionsVariant
  8   5   1   7   7   8   3   9   9   4  0.264458   0.9900    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   0.9900    RandomExcursionsVariant
  7   6   4   3  11   9   3   4   6   8  0.287306   1.0000    RandomExcursionsVariant
  8   5   3   5   6   7   4   6   8   9  0.788728   0.9900    RandomExcursionsVariant
  2  11   2   8   7   4   3   9   7   8  0.095617   0.9900    RandomExcursionsVariant
  3   6  10   7   4   5   5   5   8   8  0.654467   1.0000    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   0.9900    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.
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
```

ДОДАТОК Е

Список публікацій здобувача за темою дисертації

1. Бабенко В. Г., Козловська С. Г. Особливості використання матричних операцій криптографічного перетворення інформації. *Системи обробки інформації.* 2015. № 3 (128). С. 84–87.
2. Рудницький В. М., Лада Н. В., Козловська С. Г. Технологія побудови двохоперандних операцій криптографічного перетворення інформації за результатами моделювання. *Сучасні інформаційні системи*. 2018. Т. 2, № 4. С. 26–30.
3. Лада Н. В., Козловська С. Г. Застосування операцій криптографічного додавання за модулем два з точністю до перестановки в потокових шифрах. *Системи управління, навігації та зв'язку :* зб. наук. пр. Полтава : ПНТУ, 2018. Т. 1 (47). С. 127–130.
4. Козловська С. Г. Синтез груп двохоперандних операцій криптоперетворення на основі перестановочних схем. *Сучасна спеціальна техніка.* 2018. № 4 (55). С. 44–50.
5. Зажома В. М., Козловська С. Г. Спосіб підвищення достовірності передачі ключового елементу стегоконтейнера. *Smart and Young.* 2016. № 11-12. Частина 1. С. 42–48.
6. Криптографічне кодування: обробка та захист інформації: колективна монографія / за ред. В. М. Рудницького. Харків : ТОВ «ДІСА ПЛЮС», 2018. 139 с.
7. Козловська С. Г. Лада С. В., Аскеров Р. В. Засоби захисту програм від несанкціонованого доступу. *Проблеми інформатизації* : матеріали Першої міжнар. наук.-техн. конф. : тези доп., (Черкаси – Київ – Тольятті – Полтава, 19–20 грудня 2013 р.). Черкаси: ЧДТУ; Київ: ДУТ, Тольятті: ТДУ, Полтава: ПНТУ, 2013. С. 25.
8. Козловська С. Г. Проблеми захисту управлінської інформації. *Теоретико-методологічні і науково-практичні засади інформаційного, фінансового*

та облікового забезпечення розвитку економіки : зб. тез доп. наук.-практ. конф., м. Черкаси, 21–22 лист. 2013 р. Черкаси, 2013. С. 50-51.

9. Козловська С. Г. Технічні способи запобігання просочуванню інформації. *Проблеми моделювання структури і процесів економічних систем* : зб. тез доп. міжнар. наук.-практ. конф., м. Черкаси, 17–18 квіт. 2014 р. Черкаси, 2014. С. 93–95.
10. Козловська С. Г. Персонал підприємства як основне джерело втрати конфіденційної інформації. *Управління економіко-соціальними системами розвитку суспільства в умовах євроінтеграції* : зб. тез доп. наук.-практ. конф., м. Черкаси, 15–17 квіт. 2015 р. Черкаси, 2015. С. 79–80.
11. Козловська С. Г. Особливості криптографічного захисту інформації. *Фінансово-економічне та обліково-аналітичне забезпечення підприємницької діяльності* : зб. тез доп. Всеукр. наук.-практ. конф., м. Черкаси, 20–21 квіт. 2016 р. Черкаси, 2016. С. 360–363.
12. 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.

Відомості про апробацію результатів дисертації

1. Козловська С. Г. Лада С.В., Аскеров Р.В. Засоби захисту програм від несанкціонованого доступу. *Проблеми інформатизації*: матеріали Першої міжнар. наук.-техн. конф.: тези доп., (Черкаси – Київ – Тольятті – Полтава, 19–20 грудня. 2013 р.). Черкаси: ЧДТУ; Київ: ДУТ, Тольятті: ТДУ, Полтава: ПНТУ, 2013. С. 25. – очна участь.
2. Козловська С. Г. Проблеми захисту управлінської інформації. *Теоретико-методологічні і науково-практичні засади інформаційного, фінансового*

та облікового забезпечення розвитку економіки: зб. тез доп. наук.-практ. конф., м. Черкаси, 21–22 лист. 2013 р. Черкаси, 2013. С.50–51. – очна участь.

3. Козловська С. Г. Технічні способи запобігання просочуванню інформації. *Проблеми моделювання структури і процесів економічних систем*: зб. тез доп. міжнар. наук.-практ. конф., м. Черкаси, 17–18 квіт. 2014 р. Черкаси, 2014. С. 93–95. – очна участь.
4. Козловська С. Г. Персонал підприємства як основне джерело втрати конфіденційної інформації. *Управління економіко-соціальними системами розвитку суспільства в умовах євроінтеграції*: зб. тез доп. наук.-практ. конф., м. Черкаси, 15–17 квіт. 2015 р. Черкаси, 2015. С.79–80. – очна участь.
5. Козловська С. Г. Особливості криптографічного захисту інформації. *Фінансово-економічне та обліково-аналітичне забезпечення підприємницької діяльності* : зб. тез доп. Всеукр. наук.-практ. конф., м. Черкаси, 20–21 квіт. 2016 р. Черкаси, 2016. С. 360–363. – очна участь.
6. 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. – очна участь.

ДОДАТОК Ж

Акт впровадження результатів дисертаційної роботи

в ЦКБ «Сокіл» НВК «Фотоприлад»

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
"20" листопада 2012 р.

АКТ
впровадження результатів дисертаційної роботи
Козловської Світлани Григорівни
в ЦКБ "Сокіл" НВК "Фотоприлад"

Для забезпечення конфіденційності та достовірності передачі команд в оптичній лінії звязку з допомогою виробу 1К118 були використані наступні наукові результати отримані Козловською Світланою Григорівною, а саме:

– метод криптографічного кодування інформації на основі керуючих перестановок.

Дані наукові результати реалізовані на основі спеціалізованого модуля операційної системи.

Начальник відділу ЦКБ "Сокіл"
НВК "Фотоприлад" _____ О.Я. Хомченко

ДОДАТОК И

Акт впровадження результатів дисертаційної роботи в навчальний процес Черкаського державного технологічного університету

«ЗАТВЕРДЖУЮ»
Ректор Черкаського
державного технологічного
університету
_____ О.О. Григор
«10» січня 2019р.

АКТ
впровадження результатів дисертаційної роботи
Козловської Світлани Григорівни в навчальний процес
Черкаського державного технологічного університету

Комісія у складі: завідувача кафедри інформаційних технологій проектування д.т.н., доцента Прокопенко Т.О., доцента кафедри інформаційної безпеки та комп'ютерної інженерії к.т.н., доцента Федотової-Півень І.М., доцента кафедри інформаційної безпеки та комп'ютерної інженерії к.т.н., доцента Миронець І.В., розглянувши матеріали дисертаційного дослідження Козловської Світлани Григорівни, встановила наступне:

1. При підготовці бакалаврів за напрямом 6.170103 «Управління інформаційною безпекою» в курсі лекцій з дисциплін «Основи криптографічного захисту інформації» та «Криптографічні методи та засоби захисту інформації» використовуються результати дисертаційного дослідження, а саме:

– методи синтезу груп симетричних двохрозрядних двохоперандних операцій потокового шифрування;

– удосконалений метод підвищення стійкості та надійності потокового шифрування на основі додаткового застосування синтезованих груп симетричних двохоперандних операцій криптографічного перетворення інформації.

2. При виконанні курсових і кваліфікаційних робіт використовуються запропоновані методики синтезу прямих та обернених операцій розширеного матричного криптографічного перетворення.

Завідувач кафедри ІТП, д.т.н., доц. Т.О. Прокопенко
Доцент кафедри ІБ та КІ, к.т.н., доц. І.М.Федотова-Півень
Доцент кафедри ІБ та КІ, к.т.н., доц. І.В. Миронець