ЧЕРКАСЬКИЙ ДЕРЖАВНИЙ ТЕХНОЛОГІЧНИЙ УНІВЕРСИТЕТ
МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

Кваліфікаційна наукова
праця на правах рукопису

Короткий Тимофій Констянтинович

УДК 004.421.5:004.056.55

ДИСЕРТАЦІЯ

ІЄРАРХІЧНА ІНФОРМАЦІЙНА СИСТЕМА МОДЕЛЮВАННЯ І ДОСЛІДЖЕННЯ АЛГОРИТМІВ ПОТОКОВОГО СЕТ-ШИФРУВАННЯ

126 – інформаційні системи та технології

Подається на здобуття наукового ступеня доктора філософії.

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

_____Т.К. Короткий

Наукові керівники:
Бабенко Віра Григорівна,
доктор технічних наук, професор;
Рудницький Сергій Володимирович,
кандидат технічних наук, доцент

Черкаси – 2026

АНОТАЦІЯ

Короткий Т.К. Ієрархічна інформаційна система моделювання і дослідження алгоритмів потокового СЕТ-шифрування. – Кваліфікаційна наукова праця на правах рукопису.

Дисертація на здобуття наукового ступеня доктора філософії за спеціальністю 126 «Інформаційні системи та технології». – Черкаський державний технологічний університет, Черкаси, 2026

Дисертаційна робота присвячена підвищенню продуктивності наукових досліджень СЕТ-операцій при побудові перспективних стійких алгоритмів потокового шифрування на основі розширення можливостей ієрархічної інформаційної системи моделювання і дослідження СЕТ-операцій за рахунок встановлення нових і уточнення існуючих взаємозв'язків між моделями ієрархічних рівнів, які в сукупності забезпечать автоматизований синтез і аналіз симетричних та несиметричних одноопераднних і багатоопераднних СЕТ-операцій, а також генераторів їх псевдовипадкових послідовностей для потокового СЕТ-шифрування.

У першому розділі за результатами проведеного аналізу встановлено, що розбудова малоресурсних систем криптографічного захисту інформації на сьогоднішній день відноситься до найбільш актуальних задач розвитку захищених інформаційних і телекомунікаційних систем. Проаналізовано основні напрямки розвитку і області застосування малоресурсної криптографії. Проведено детальний аналіз відомих результатів дослідження СЕТ-операцій і алгоритмів СЕТ-шифрування, які відносяться до малоресурсної криптографії. Проаналізовано сучасний стан розвитку автоматизованих інформаційних систем моделювання і дослідження СЕТ-операцій та алгоритмів шифрування. Визначено їх переваги і недоліки. За результатами проведеного аналізу сформульована мета і завдання дисертаційного дослідження.

Другий розділ присвячений дослідженню особливостей застосування несиметричних двохоперандних СЕТ-операцій, які допускають перестановку операндів в потокових системах шифрування. Проаналізовано два сценарії потокового шифрування, які базуються на використанні комутативних і не комутативних двохоперандних СЕТ-операцій. Наведено структури систем потокового шифрування на основі реалізації даних сценаріїв. Для забезпечення однозначного сприйняття задач і результатів дослідження наводяться основні поняття і визначення стосовно потокового СЕТ-шифрування, які необхідні для даної дисертаційної роботи. На основі реалізації послідовності дискретних перетворень побудована група моделей некомутативних двохоперандних двохрозрядних СЕТ-операціях подвійного циклу, кожна з яких забезпечує перестановку операндів. В основу побудови даної групи було покладено групу СЕТ-операцій з точністю до перестановки результатів перетворення. Дану групу було отримано на основі повного перебору можливих варіантів розміщення 2Сі-квантових одноопераднних СЕТ-операціях в 2Сі-квантовій двохоперандній СЕТ-операції. Отримані результати забезпечили можливість удосконалення технології побудови удосконалених моделей некомутативних двохоперандних СЕТ-операцій. Сутність удосконалено полягає в заміні повторного використання технології для знаходження удосконаленої моделі після перестановки операндів на зміну змінних в удосконаленій моделі СЕТ-операції до перестановки операндів. Це забезпечує прямий перехід від моделі СЕТ-операції до перестановки операндів, до моделі СЕТ-операції після перестановки операндів.

В третьому розділі запропоновано послідовність перетворень результатів обчислювального експерименту для побудови удосконалених моделей операцій несиметричного криптографічного кодування і декодування. На прикладі однієї з класифікованих множин операцій криптографічного кодування з точністю до перестановки представлених кортежами одноопераднних операцій отримано математичні моделі

удосконалених несиметричних двохоперандних двохрозрядних операцій подвійного циклу. Запропоновано використати метод синтезу симетричних двохоперандних двохрозрядних операцій для побудови групи несиметричних двохоперандних двохрозрядних операцій. Удосконалений метод синтезу двохоперандних двохрозрядних операцій криптографічного перетворення забезпечив синтез груп несиметричних операцій подвійного циклу. Коректність реалізації даного методу підтверджена класифікованими результатами обчислювального експерименту та збігом отриманих різними методами синтезу математичних моделей на приведеному прикладі однієї з множин операцій. Результати дослідження можливості синтезу множин несиметричних двохоперандних двохрозрядних операцій потрійного циклу показали обмеженість даного методу побудовою лише груп симетричних операцій та несиметричних операцій подвійного циклу.

Четвертий розділ присвячено моделюванню множини несиметричних двохоперандних двохрозрядних операцій подвійного циклу на основі дублювання операцій для різних сценаріїв шифрування. Була встановлена можливість синтезу двохоперандних СЕТ-операцій, які допускають перестановку операндів шляхом поєднання одноопераднних операцій. Досліджено можливість синтезу множини симетричних двохрозрядних двохоперандних СЕТ-операцій на шляхом поєднання одноопераднних операцій. Досліджено особливості синтезу прямих і обернених двохрозрядних двохоперандних СЕТ-операцій, які допускають перестановку операндів, шляхом поєднання одноопераднних СЕТ-операцій, перша з яких є симетричною, а також шляхом поєднання одноопераднних СЕТ-операцій, перша з яких є несиметричною. Встановлено взаємозв’язки і обмеження які відображають особливості синтезу двохрозрядних двохоперандних операцій криптографічного перетворення, які допускають перестановку операндів при різних моделях перетворення першого операнду.

П’ятий розділ присвячено побудові моделі ієрархічної інформаційної системи моделювання і дослідження симетричних і несиметричних СЕТ-

операцій. Основним елементом малоресурсної системи потокового СЕТ-шифрування е генератор псевдовипадкової послідовності СЕТ-операцій з точністю до перестановки. В процесі дослідження генераторів послідовності несиметричних СЕТ-операцій з точністю до перестановки другого операнда було встановлено наступне: в процесі модифікації двохоперандної СЕТ-операції набір одноопераднних операцій не змінюється, а змінюється лише їх послідовність, отримані модифіковані СЕТ-операції будуть мати однакові криптографічні властивості, тому що реалізують однакові набори таблиць підстановок; реалізація генераторів груп прямих обернених несиметричних двохоперандних СЕТ-операцій з точністю до перестановки другого операнда вимагає застосування в криптографічному алгоритмі лише прямої і оберненої несиметричних двохоперандних СЕТ-операцій і набору прямих одноопераднних СЕТ-операцій, що забезпечує суттєве спрощення алгоритмів СЕТ-шифрування. В процесі дослідження генераторів послідовності несиметричних СЕТ-операцій з точністю до перестановки першого операнда було встановлено наступне: в процесі модифікації несиметричної двохоперандної СЕТ-операцій з змінюється математична модель двохоперандної СЕТ-операції за рахунок модифікації моделей одноопераднх СЕТ-операцій, що приводить до модифікації таблиць підстановки; якщо при шифруванні інформації генератор реалізує модифікацію СЕТ-операції з точністю до перестановки першого операнда, то для розшифрування необхідно використовувати генератор обернених СЕТ-операцій з точністю до перестановки результату криптографічного перетворення; збільшення кількості одноопераднних СЕТ-операцій при використанні групи модифікованих несиметричних СЕТ-операцій з точністю до перестановки першого операнду забезпечує збільшення кількості таблиць підстановки, які реалізується в процесі шифрування і як наслідок збільшення криптостійкості алгоритму шифрування. Отримані результати досліджень стали теоретичною основою для побудови моделі ієрархічної інформаційної системи моделювання і дослідження симетричних і несиметричних СЕТ-

операцій. Для уніфікації програмної реалізації інформаційної системи запропоновано використати базу даних, і базу знань. База даних забезпечить зберігання параметрів синтезу, синтезовані СЕТ-операцій, і їх властивості. База знань наповнюється моделями синтезу операцій, моделями синтезу груп операцій і моделями генерації псевдовипадкових послідовностей СЕТ-операцій. Під вимогами до процесу функціонування системи розглядаються формалізовані обмеження на реалізацію конкретних задач моделювання і дослідження. Обмеження напряму взаємодіють як з базою даних так і з базою знань. Вирішення нової задачі дослідження забезпечує розширення бази знань. Застосування запропонованих баз даних і знань забезпечать простоту подальшого вдосконалення інформаційної системи та можливість її адаптації до вирішення нових задач по синтезу і дослідженню СЕТ-операцій.

Наукова новизна отриманих результатів:

- вперше побудована модель ієрархічної інформаційної системи моделювання і дослідження симетричних і несиметричних СЕТ-операцій, на основі методів синтезу СЕТ-операцій і груп СЕТ-операцій, шляхом вдосконалення моделей, методів і технології побудови комутативних і некомутативних СЕТ-операції, а також генераторів псевдовипадкових наборів СЕТ-операцій, що дозволило встановлювати нові залежності між моделями синтезу симетричних і несиметричних операцій, які приводять до розширення взаємозв’язків між моделями ієрархічних рівнів інформаційної системи, реалізація якої забезпечить експериментальну підтримку для побудову перспективних стійких малоресурсних алгоритмів потокового шифрування;
- удосконалено технологію побудови удосконалених моделей некомутативних двохрозрядних двохоперандних СЕТ-операції за результатами експерименту, на основі побудови удосконалених моделей СЕТ-операцій за результатами експерименту, шляхом встановлення взаємозв’язків між моделями до і після перестановки

операндів, що забезпечило зменшення складності моделювання некомутативних СЕТ-операцій на основі реалізації прямого переході від побудованої моделі СЕТ-операції до моделі СЕТ-операції з переставленими операндами;

– удосконалено метод синтезу двохоперандних двохрозрядних операцій криптографічного перетворення на основі метод синтезу симетричних операцій, шляхом застосування в якості першої базової операції несиметричної операції криптоперетворення та додаткової побудови оберненої операції за результатами обчислювального експерименту, що забезпечили можливість додаткового синтезу несиметричних двохоперандних двохрозрядних операцій подвійного циклу;
– удосконалено метод побудови двохрозрядних двохоперандних операцій, які допускають перестановку операндів на основі об'єднання двохрозрядних одноопераднних операцій криптографічного перетворення, шляхом встановлення взаємозв'язків між прямими і оберненими операціями, що дозволило змоделювати всі двохрозрядні двохоперандні операції, які допускають перестановку операндів.

Практичне значення отриманих результатів.

Практична цінність дисертаційної роботи полягає в тому, що отримані наукові результати доведено здобувачем до конкретних моделей, інженерних методик розрахунку, та отриманих варіантів застосування моделей генераторів псевдовипадкових послідовностей СЕТ-операцій.

На підставі проведених досліджень побудовано програмний макет ієрархічної інформаційної системи моделювання і дослідження алгоритмів потокового СЕТ-шифрування. Дана інформаційна система забезпечує розширення спектру 2Сі-квантових СЕТ-операцій, що аналізуються, та які допускають перестановку операндів з 96 симетричних до 576 симетричних та несиметричних 2Сі-квантових СЕТ-операцій, які допускають перестановку операндів, а також до 10623 2Сі-квантових СЕТ-операцій, які не допускають перестановку операндів. Дана інформаційна система забезпечить

дослідження систем потокового шифрування в яких може бути використано до $65 \cdot 10^{35}$ несиметричних двохоперандних СЕТ-операцій, з яких 1 625 702 400 3Сі-квантові СЕТ-операції що допускають перестановку операндів.

Реалізація. Результати дисертаційного дослідження впроваджено в навчальний процес Черкаського державного технологічного університету:

- на кафедрі інформаційних технологій проектування при підготовці бакалаврів за спеціальністю 126 «Інформаційні системи та технології» в курсі лекцій з дисциплін «Системи інформаційної безпеки», а також при виконанні курсових і кваліфікаційних робіт;
- на кафедрі інформаційної безпеки та комп'ютерної інженерії при підготовці бакалаврів за спеціальністю 123 «Комп'ютерна інженерія» в курсі лекцій з дисциплін: «Безпека програмного забезпечення», «Арифметичні та логічні структури комп'ютерів», а також при виконанні кваліфікаційних робіт магістрів за спеціальністю 123 «Комп'ютерна інженерія» освітньої програми «Системне програмування».

Ключові слова: ієрархічна інформаційна технологія, інформаційна система, криптографія, потокове шифрування, двохоперандні операції, синтез груп операцій, генерація послідовностей операцій криптоперетворення, кібербезпека.

ABSTRACT

Korotkyi T.K. Hierarchical information system for modeling and research of stream CET encryption algorithms. – Qualification scientific work submitted as a manuscript.

Dissertation for the degree of Doctor of Philosophy in specialty 126 "Information Systems and Technologies" – Cherkasy State Technological University, Cherkasy, 2026.

The dissertation is devoted to improving the efficiency of research on CET-operations in the development of advanced, resilient stream cipher algorithms. The approach is based on expanding the capabilities of a hierarchical information system for modeling and analyzing CET-operations by establishing new and refining existing interrelations between hierarchical models. Collectively, this ensures automated synthesis and analysis of symmetric and asymmetric single-operand and multi-operand CET-operations, as well as generators of their pseudorandom sequences for stream CET-encryption.

In the first chapter, presents an analytical review establishing that the development of resource-efficient cryptographic systems is one of the most pressing challenges in secure information and telecommunication technologies. The chapter surveys the main trends and application areas of lightweight cryptography, providing a detailed analysis of existing research on CET-operations and CET-encryption algorithms in this domain. The current state of automated information systems for modeling and analyzing CET-operations is examined, highlighting strengths and weaknesses. Based on this analysis, the research objectives and tasks of the dissertation are formulated.

The second chapter investigates the application of asymmetric two-operand CET-operations permitting operand permutation in stream encryption systems. Two encryption scenarios based on commutative and non-commutative two-operand CET-operations are analyzed, and system structures for their implementation are presented. To ensure clarity, key concepts and definitions relevant to stream CET-encryption are introduced. A group of models of non-

commutative two-operand two-bit double-cycle CET-operations was constructed, each supporting operand permutation. The construction was based on a group of CET-operations defined up to the permutation of transformation results, obtained by exhaustively enumerating all possible placements of 2Ci-quantum single-operand operations within a 2Ci-quantum two-operand operation. These results enabled refinement of the technology for constructing advanced models of non-commutative two-operand CET-operations, allowing a direct transition from an operation model to its permuted form by variable substitution rather than repeated application of the synthesis method.

In the third chapter, introduces a sequence of transformations of computational experiment results to construct advanced models of asymmetric encryption and decryption operations. Using an example of a classified set of encryption operations (defined up to operand permutation and represented by tuples of single-operand operations), mathematical models of advanced asymmetric two-operand two-bit double-cycle operations were obtained. A method originally intended for synthesizing symmetric two-operand two-bit operations was adapted to construct groups of asymmetric two-operand two-bit operations. The improved synthesis method produced groups of asymmetric double-cycle operations, with correctness validated through classified experimental results and consistency across different synthesis approaches. Further experiments on synthesizing sets of asymmetric two-operand two-bit triple-cycle operations demonstrated limitations of the method, showing that it can construct only groups of symmetric operations and asymmetric double-cycle operations.

The fourth chapter focuses on modeling sets of asymmetric two-operand two-bit double-cycle operations through operation duplication for various encryption scenarios. The study confirmed the feasibility of synthesizing two-operand CET-operations that allow operand permutation by combining single-operand operations. The synthesis of symmetric two-bit two-operand CET-operations through such combinations was also explored. Specific attention was given to direct and inverse two-bit two-operand CET-operations permitting operand

permutation, constructed either by combining single-operand operations where the first is symmetric or where it is asymmetric. The research established interrelations and constraints characterizing the synthesis of two-bit two-operand cryptographic transformations permitting operand permutation under different models of first-operand transformation.

The fifth chapter presents the construction of a hierarchical information system for modeling and analyzing symmetric and asymmetric CET-operations. The central element of a lightweight stream CET-encryption system is a pseudorandom sequence generator of CET-operations defined up to operand permutation. The study of generators of asymmetric operations with second-operand permutation showed that modification alters only the sequence of single-operand operations, not their set. Thus, the resulting operations preserve identical cryptographic properties since they implement the same substitution tables. Generators of groups of direct and inverse asymmetric operations with second-operand permutation therefore require only the direct and inverse asymmetric operations together with a set of single-operand operations, significantly simplifying encryption algorithms.

In contrast, with first-operand permutation, modification changes the mathematical model itself through changes to single-operand components, leading to new substitution tables. In this case, decryption requires generators of inverse operations defined with respect to permutation of the cryptographic result. Increasing the number of single-operand operations in such groups expands the number of substitution tables realized during encryption, thereby enhancing algorithmic cryptographic strength. The research results formed the theoretical basis for the hierarchical information system. For unified implementation, both a database and a knowledge base are proposed. The database stores synthesis parameters, generated operations, and their properties, while the knowledge base contains models of operation synthesis, groups of operations, and pseudorandom sequence generation. System requirements are formulated as formalized constraints on modeling and research tasks, directly interacting with both repositories. Solving

new tasks expands the knowledge base, ensuring adaptability and continuous improvement of the system.

Scientific novelty of the obtained results:

- For the first time, a model of a hierarchical information system for modeling and analyzing symmetric and asymmetric CET-operations has been developed, based on synthesis methods for individual operations and operation groups. This refinement of models, methods, and technologies for constructing commutative and non-commutative operations, as well as pseudorandom operation generators, established new dependencies between synthesis models, broadening interrelations between hierarchical levels of the system. The implementation provides experimental support for developing lightweight, resilient stream cipher algorithms.
- The technology for constructing advanced models of non-commutative two-bit two-operand CET-operations has been improved by establishing interrelations between models before and after operand permutation. This reduced the complexity of modeling non-commutative operations by enabling direct transition from an operation model to its permuted form.
- The method of synthesizing two-operand two-bit cryptographic transformations has been refined by applying an asymmetric transformation as the first base operation and additionally constructing an inverse operation from experimental results. This enabled synthesis of new asymmetric two-operand two-bit double-cycle operations.
- The method of constructing two-bit two-operand operations permitting operand permutation has been improved by combining single-operand cryptographic transformations, with interrelations established between direct and inverse operations. This allowed modeling of all two-bit two-operand operations that permit operand permutation.

The practical value of the obtained results. The practical significance of this research lies in the translation of theoretical results into concrete models, engineering calculation methods, and applied variants of pseudorandom CET-

operation generators. A prototype hierarchical information system for modeling and studying stream CET-encryption algorithms was implemented. The system expands the range of analyzable 2Ci-quantum CET-operations permitting operand permutation from 96 symmetric to 576 symmetric and asymmetric operations, and up to 10,623 2Ci-quantum operations that do not permit permutation. The system also supports the study of stream cipher systems employing up to $65 \cdot 10^{35}$ asymmetric two-operand CET-operations, including 1,625,702,400 3Ci-quantum operations permitting operand permutation.

Implementation. The results of the dissertation research have been integrated into the educational process of Cherkasy State Technological University:

- at the Department of Information Technologies in Design in the training of bachelors majoring in 126 *"*Information Systems and Technologies*"*, within the lecture courses *"*Information Security Systems*"*, as well as in the execution of course projects and qualification theses;
- at the Department of Information Security and Computer Engineering in the training of bachelors majoring in 123 *"*Computer Engineering*"*, within the lecture courses *"*Software Security*"*, *"*Arithmetic and Logical Structures of Computers*"*, as well as in the preparation of master's theses in specialty 123 *"*Computer Engineering*"* under the educational program *"*System Programming."

Keywords: hierarchical information technology, information system, cryptography, stream encryption, two-operand operations, synthesis of operation groups, generation of sequences of cryptographic transformation operations, cybersecurity.

Список публікацій здобувача:

1. Rudnytskyi V., Semenov S., Lada N., Babenko V., Larin V., Korotkyi T. The model for constructing a set of symmetric two-operand set operations that allow perversion of operands by combining one-operand operations. *Innovative Technologies and Scientific Solutions for Industries*. 2025. № 3(33). P. 126–136. DOI: https://doi.org/10.30837/2522-9818.2025.3.126. URL: https://journals.uran.ua/itssi/article/view/340558 (Scopus, фахове видання)

2. Rudnytskyi V., Lada N., Herashchenko M., Korotkyi T., Stabetska T. Modeling relationships in non-commutative two-operand two-bit CET-operations of a double cycle when permuting the operands. *Technology Audit and Production Reserves*. 2024. Vol. 3, No. 2(77). P. 30–35. DOI: https://doi.org/10.15587/2706-5448.2024.306980. URL: https://journals.uran.ua/tarp/article/view/306980 (Scopus, фахове видання)

3. Ларін В. В., Гусак М. Ю., Короткий Т. К., Гук О. М., Кащишин О. Л. Моделювання множин двохоперандних трьохрозрядних операцій криптоперетворення шляхом поєднання одноопераднних СЕТ-операцій. *Збірник наукових праць Харківського національного університету Повітряних Сил*. 2025. № 1(83). С. 56–62. DOI: https://doi.org/10.30748/zhups.2025.83.06. Режим доступу: https://journal-hnups.com.ua/index.php/zhups/article/view/1922 (фахове видання)

4. Рудницький С. В., Ларін В. В., Підласий Д. А., Короткий Т. К. Синтез двохоперандних двохрозрядних СЕТ-операцій шляхом поєднання одноопераднних двохрозрядних СЕТ-операцій. *Наука і техніка Повітряних* Сил України. 2024. № 4(57). С. 71–79. DOI: https://doi.org/10.30748/nitps.2024.57.09. Режим доступу: https://journal-hnups.com.ua/index.php/nitps/article/view/1868 (фахове видання)

5. Рудницький В., Бабенко В., Рудницький С., Короткий Т. Генерація послідовності несиметричних СЕТ-операцій з точністю до перестановки другого операнда. *Інформаційні технології та суспільство*. 2025. Вип. 1(16).

С. 221–226. DOI: https://doi.org/10.32689/maup.it.2025.1.28. Режим доступу: https://journals.maup.com.ua/index.php/it/article/view/4827 (фахове видання)

6. Рудницький В. М., Бабенко В. Г., Рудницький С. В., Короткий Т. К., Ковтюх В. А. Особливості груп несиметричних СЕТ-операцій синтезованих з точністю до перестановки першого операнда. *Вчені записки ТНУ імені В. І. Вернадського. Серія: Технічні науки*. 2025. Т. 36(75), № 4. С. 265–271. DOI: https://doi.org/10.32782/2663-5941/2025.4.2/35. Режим доступу: https://www.tech.vernadskyjournals.in.ua/journals/2025/4_2025/part_2/37.pdf (фахове видання)

7. Semenov S., Rudnytskyi V., Lada N., Krivtsun V., Korotkyi T., Zazhoma V., Wasiuta O. Stream Encryption Cryptographic Systems Based on Asymmetric CET Operations with an Accuracy of Permutation. *Applied Sciences*. 2026. Vol. 16. Article 4987. DOI: https://doi.org/10.3390/app16104987. URL: https://www.mdpi.com/2076-3417/16/10/4987 (Scopus, WoS)

8. Рудницький В. М., Лада Н. В., Рудницька Ю. В., Короткий Т. К. Моделювання симетричних двохоперандних операцій криптографічного кодування на основі об’єднання одноопераднних операцій. *Сучасна спеціальна техніка*. 2021. № 4. С. 32–38. (фахове видання)

9. Короткий Т. К. Дослідження і синтез некомутативних двохрозрядних двохоперандних СЕТ-операцій які допускають перестановку операндів. *Технології розвитку безпілотних систем. Том 1. Малоресурсний захист інформації в безпілотних системах : монографія* / за ред. В. М. Рудницького. Черкаси : Видавець Вовчок О. Ю., 2025. С. 165–205. (розділ монографії)

10. Rudnytskyi V., Lada N., Larin V., Melnyk O., Stebetska T., Korotkyi T., Pidlasyi D. Usage of non-commutative two-operand CET-operations in limited resources stream ciphers. *Journal of Xidian University*. 2024. Vol. 18, Issue 5. P. 1105–1120. DOI: https://doi.org/10.5281/Zenodo.11253625. URL: https://repositsc.nuczu.edu.ua/bitstream/123456789/21303/1/110-May-10807.pdf

11. Rudnytskyi V., Lada N., Larin V., Tkachenko V., Korotkyi T., Pidlasyi D., Tarasenko D. Information system for modeling and research of

pseudorandom sequences of CET-operations for post quantum stream encryption systems. *Journal of Xidian University*. 2024. Vol. 18, Issue 7. P. 1284–1298. DOI: https://doi.org/10.5281/Zenodo.13096683. URL: https://xadzkjdx.cn/index.php/volume-18-issue-7-july-24/.

12. Рудницька Ю. В., Короткий Т. К. Інформаційна технологія моделювання та дослідження симетричних СЕТ-операцій. *Проблеми інформатизації : тези доп. Десятої міжнар. наук.-техн. конф.* Черкаси – Баку – Бельсько-Бяла – Харків, 24–25 листопада 2022 р. Черкаси : ЧДТУ, 2022. Т. 1. С. 40.

13. Рудницький В. М., Ларін В. В., Лада Н. В., Короткий Т. К. Сучасний стан та перспективи розвитку СЕТ-шифрування. *Воєнні інновації в сучасних війнах : збірник тез Міжнародного академічного форуму*. Київ : Центральний науково-дослідний інститут Збройних Сил України, 2024. С. 39–40.

14. Короткий Т. К., Ковтюх В. А. Моделювання і дослідження генераторів двохоперандних СЕТ-операцій для малоресурсної криптографії. *Актуальні проблеми розвитку сучасної науки: виклики та перспективи : збірник тез Міжнародної науково-практичної конференції здобувачів вищої освіти і молодих вчених*. Запоріжжя, 29 квітня 2025 р. Запоріжжя : ЗНУ, 2025. С. 472. URL: https://dspace.znu.edu.ua/jspui/handle/12345/25952.

15. Рудницький В. М., Лада Н. В., Короткий Т. К. Вдосконалення технології побудови некомутативних СЕТ-операцій. *Сучасні напрямки розвитку інформаційно-комунікаційних технологій та засобів управління : тези доповідей 15-ї міжнародної науково-технічної конференції*. Баку–Харків–Жиліна, 24–25 квітня 2025 р. Т. 1. Харків, 2025. С. 41. DOI: https://doi.org/10.32620/ICT.25.t1.

16. Рудницький В. М., Ларін В. В., Нікорчук А. І., Короткий Т. К. Особливості застосування малоресурсної криптографії в безпілотних комплексах. *Проблемні питання щодо експлуатації та відновлення автобронетанкової техніки в Національній гвардії України : матеріали наук.-практ. конф.*. Золочів, 27 травня 2025 р. Харків : НАНГУ, 2025.

ЗМІСТ

ВСТУП

Актуальність теми.

Кібербезпека стала однією з необхідних умов для цифровізації суспільства і забезпечення належного функціонування простору цифрових даних. Таким чином, підвищення рівня безпеки інформації є дуже важливою справою як для пересічного громадянина, так і для держави. Сьогодні як і в минулому криптографічний захист залишається найпоширенішим способом захисту інформації.

В наш час особливо актуальним стають питання пошуку методів та засобів постквантових та малоресурсних криптографічних систем. Проте знаходити ефективні рішення для побудови даних криптографічних систем без застосування інформаційних систем і технологій неможливо.

На сьогоднішній день значний внесок у розвиток інформаційних систем зробили вітчизняних і зарубіжних науковців: В.М., Глушков, Б.М. Маліновський, Є.П. Угрюмов, Є.С. Согомонян, В.І. Хаханов, Д.О. Поспєлов, Е.В. Попова, В. К. Задірака, В.Н. Вагін, А.П. Перегудова Ф.І., Тарасенко Ф.П., М.П. Бусленко, А. А. Молдовян, М.М. Моісєєва, Я.Г. Неуйміна, Е.Г. Петрова, А.С.Кулика, О. Г. Додонов, О. В. Коваль, О. Ю. Петропавловський, У. Пірс, J. Allen, P. van Beek, L. Vila, E. Schwalb, P. Ladkin, D. McDermott, Y. Shoham, G. Ferguson та ін..

Проте будувати інформаційні системи для моделювання і дослідження криптографічних алгоритмів неможливо без глибокого знання предметної області. Суттєвий внесок у розвиток інформаційної безпеки та захисту інформації зробили І. Д. Горбенко, Ю. В. Кузнецов, П. В. Дорошкевич, О. А. Логачов, Р. А. Хаді, В. В. Ященко, С. О. Шестаков, А. Н. Фіонов, О. Г. Корченко, Б. Я. Рябко, К. Є. Шеннон, Дж. Л. Месси, Брюс Шнайер, Жиль Брассар, Чарльз Г. Беннет, M. E. Hellman, U. M. Maurer, W. Diffie, B. Chor, A. Shamir, R. L. Rivest, N. Koblitz та ін.

На сьогоднішній день існують програмно-апаратні засоби синтезу і дослідження груп симетричних одно і двохоперандних СЕТ-операцій і симетричних СЕТ-операцій які допускають перестановку операндів. Але Симетричні двохоперандні СЕТ-операції, які допускають перестановку операндів, складають не більше 20% від несиметричних СЕТ-операцій, які допускають перестановку операндів. Загальна кількість симетричних двохоперандних СЕТ-операцій не перевищує декількох процентів від загальної кількості СЕТ-операцій (симетричних і несиметричних). Проте методи побудови несиметричних СЕТ-операцій і моделі генерації їх псевдовипадкових послідовностей не досліджувалися.

Таким чином, можна стверджувати, що тема дисертаційного дослідження «Ієрархічна інформаційна система моделювання і дослідження алгоритмів потокового СЕТ-шифрування» є актуальною.

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

Дисертаційна робота виконана відповідно до Закону України «Про перспективні напрямки наукових досліджень» від 2006 року зі змінами від 2022 року, а також відповідно до плану науково-дослідних робіт Черкаського державного технологічного університету. Результати дисертаційної роботи включені в НДР Черкаського державного технологічного університету: «Дослідження шляхів розвитку потокового шифрування на основі криптографічного кодування» (ДР № 0121U114389), і НДР «Інформаційна технологія психолінгвістичного аналізу тексту для стеганографічних систем» (ДР № 0123U102085), у яких автор брав участь як виконавець.

Мета і задачі дослідження. Основною метою дослідження є підвищення продуктивності дослідження СЕТ-операцій при побудові перспективних стійких алгоритмів потокового шифрування на основі розширення можливостей ієрархічної інформаційної системи моделювання і дослідження СЕТ-операцій за рахунок встановлення нових і уточнення існуючих взаємозв’язків між моделями ієрархічних рівнів, які в сукупності забезпечать автоматизований синтез і аналіз симетричних та несиметричних

одноопераднних і багатоопераднних СЕТ-операцій, а також генераторів їх псевдовипадкових послідовностей для потокового СЕТ-шифрування.

Для досягнення поставленої мети сформульовано і вирішено такі задачі:

1. Удосконалити технологію побудови удосконалених моделей некомутативних двохрозрядних двохоперандних СЕТ-операції за результатами обчислювального експерименту;

2. Удосконалити метод синтезу двохоперандних двохрозрядних операцій криптографічного перетворення для забезпечення можливості побудови як симетричних так і несиметричних СЕТ-операцій;

3. Удосконалити метод побудови двохрозрядних двохоперандних операцій, які допускають перестановку операндів на основі об’єднання двохрозрядних одноопераднних операцій криптографічного перетворення;

4. Розробити модель ієрархічної інформаційної системи моделювання і дослідження симетричних і несиметричних СЕТ-операцій, реалізація якої забезпечить побудову перспективних стійких малоресурсних алгоритмів потокового шифрування.

Об’єкт дослідження – процеси автоматизації моделювання і дослідження малоресурсного шифрування.

Предмет дослідження – моделі, методи і засоби побудови ієрархічної інформаційної системи моделювання і дослідження алгоритмів потокового СЕТ-шифрування.

Методи дослідження. У процесі удосконалення технології побудови удосконалених моделей некомутативних двохрозрядних двохоперандних СЕТ-операції за результатами обчислювального експерименту використовувався математичний апарат теорії інформації, теорії алгоритмів, криптографії, логіки, методи комп’ютерного моделювання та дискретної математики.

Для удосконалення методу синтезу двохоперандних двохрозрядних операцій криптографічного перетворення і забезпечення можливості

побудови як симетричних так і несиметричних СЕТ-операцій використовувалися: теорія алгоритмів, теорії інформації, криптографія, та дискретна математика.

Для удосконалення методу побудови двохрозрядних двохоперандних операцій, які допускають перестановку операндів на основі об’єднання двохрозрядних одноопераднних операцій криптографічного перетворення використовувалися: теорія алгоритмів, теорії інформації, криптографія, та дискретна математика.

Для розробки моделі ієрархічної інформаційної системи моделювання і дослідження симетричних і несиметричних СЕТ-операцій, реалізація якої забезпечить побудову перспективних стійких мало ресурсних алгоритмів потокового шифрування використано теорії: інформації, алгоритмів, ймовірності, криптографії із застосуванням методів дискретної математики, математичної статистики та комп’ютерного моделювання.

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

1) вперше побудована модель ієрархічної інформаційної системи моделювання і дослідження симетричних і несиметричних СЕТ-операцій, на основі методів синтезу СЕТ-операцій і груп СЕТ-операцій, шляхом вдосконалення моделей, методів і технології побудови комутативних і некомутативних СЕТ-операції, а також генераторів псевдовипадкових наборів СЕТ-операцій, що дозволило встановлювати нові залежності між моделями синтезу симетричних і несиметричних операцій, які приводять до розширення взаємозв’язків між моделями ієрархічних рівнів інформаційної системи, реалізація якої забезпечить експериментальну підтримку для побудову перспективних стійких мало ресурсних алгоритмів потокового шифрування;

2) удосконалено технологію побудови удосконалених моделей некомутативних двохрозрядних двохоперандних СЕТ-операції за результатами експерименту, на основі побудови удосконалених моделей

СЕТ-операцій за результатами експерименту, шляхом встановлення взаємозв’язків між моделями до і після перестановки операндів, що забезпечило зменшення складності моделювання некомутативних СЕТ-операцій на основі реалізації прямого переході від побудованої моделі СЕТ-операції до моделі СЕТ-операції з переставленими операндами;

3) удосконалено метод синтезу двохоперандних двохрозрядних операцій криптографічного перетворення на основі метод синтезу симетричних операцій, шляхом застосування в якості першої базової операції несиметричної операції криптоперетворення та додаткової побудови оберненої операції за результатами обчислювального експерименту, що забезпечили можливість додаткового синтезу несиметричних двохоперандних двохрозрядних операцій подвійного циклу;

4) удосконалено метод побудови двохрозрядних двохоперандних операцій, які допускають перестановку операндів, на основі об’єднання двохрозрядних одноопераднних операцій криптографічного перетворення, шляхом встановлення взаємозв’язків між прямими і оберненими операціями, що дозволило змоделювати всі двохрозрядні двохоперандні операцій, які допускають перестановку операндів.

Практичне значення отриманих результатів.

Практична цінність дисертаційної роботи полягає в тому, що отримані наукові результати доведено здобувачем до конкретних моделей, інженерних методик розрахунку, та отриманих варіантів застосування моделей генераторів псевдовипадкових послідовностей СЕТ-операцій.

На підставі проведених досліджень побудовано програмний макет ієрархічної інформаційної системи моделювання і дослідження алгоритмів потокового СЕТ-шифрування. Дана інформаційна система забезпечує розширення спектру 2Сі-квантових СЕТ-операцій, що аналізуються, та які допускають перестановку операндів з 96 симетричних до 576 симетричних та несиметричних 2Сі-квантових СЕТ-операцій які допускають перестановку операндів, а також до 10623 2Сі-квантових СЕТ-операцій які не допускають перестановку операндів. Дана інформаційна система забезпечить

дослідження систем потокового шифрування в яких може бути використано до $65 \cdot 10^{35}$ несиметричних двохоперандних СЕТ-операцій, з яких 1 625 702 400 3Сі-квантові СЕТ-операції що допускають перестановку операндів.

Реалізація. Результати дисертаційного дослідження впроваджено в навчальний процес Черкаського державного технологічного університету:

– на кафедрі інформаційних технологій проектування при підготовці бакалаврів за спеціальністю 126 «Інформаційні системи та технології» в курсі лекцій з дисциплін «Системи інформаційної безпеки», а також при виконанні курсових і кваліфікаційних робіт;
– на кафедрі інформаційної безпеки та комп'ютерної інженерії при підготовці бакалаврів за спеціальністю 123 «Комп'ютерна інженерія» в курсі лекцій з дисциплін «Безпека програмного забезпечення», «Арифметичні та логічні структури комп'ютерів», а також при виконанні кваліфікаційних робіт магістрів за спеціальністю 123 «Комп'ютерна інженерія» освітньої програми «Системне програмування».

Особистий внесок здобувача. Всі нові результати дисертаційної роботи отримано автором самостійно. У наукових працях, опублікованих у співавторстві, з питань, що стосуються цього дослідження, автору належать: побудова моделей комутативних і некомутативних двохоперандних СЕТ-операцій на основі об'єднання одноопераднних операцій за результатами обчислювального експерименту [1, 8, 9], встановлені взаємозв'язки в моделях некомутативних СЕТ-операціях при перестановці операндів [2], побудова множин 2 і 3 Сі-квантових СЕТ-операцій з точністю до перестановки на основі поєднання одноопераднних двохрозрядних СЕТ-операцій [3, 4], моделювання результатів генерацій псевдовипадкових послідовностей не комутативних СЕТ-операцій з точністю до перестановки другого операнда [5] і першого операнда [6], модифікація СЕТ-операцій і статистичний аналіз [7], розробка та оцінка різних сценаріїв використання шифрування потоків з обмеженими ресурсами на основі некомутативних

СЕТ-операцій [10], виявлення залежностей між моделями синтезу симетричних/несиметричних операцій та рівнями ієрархії, а також визначення шляхів вдосконалення ієрархічно структурованої моделі ІТ-системи, придатної для моделювання та дослідження симетричних і несиметричних СЕТ-операцій [11], структура, архітектура та модель інформаційної системи моделювання і дослідження алгоритмів потокового СЕТ-шифрування [12, 13, 16], взаємозв'язок між рінням ієрархії системи при моделюванні генераторів СЕТ-операцій [15], особливості застосування генераторів СЕТ-операцій в безпілотних комплексах [16], результати аналізу напрямків дослідження не комутативних СЕТ-операцій [12, 14].

Апробація результатів дисертації. Результати дисертаційної роботи доповідалися й обговорювалися на Десятій міжнародній науково-технічній конференції «Проблеми інформатизації» (Черкаси – Баку – Бельсько-Бяла – Харків, 2022), Міжнародному академічному форумі «Воєнні інновації в сучасних війнах» (Київ, 2024), Міжнародній науково-практичній конференції здобувачів вищої освіти і молодих вчених «Актуальні проблеми розвитку сучасної науки: виклики та перспектив» (Запоріжжя, 2025), Пятнадцята міжнародна науково-технічна конференція «Сучасні напрямки розвитку інформаційно-комунікаційних технологій та засобів управління» (Баку-Харків-Жиліна, 2025), Науково-практичній конференції «Проблемні питання щодо експлуатації та відновлення автобронетанкової техніки в Національній гвардії України» (Золочів, 2025).

Публікації. Основні положення дисертації опубліковано у 16 друкованих працях, зокрема: у 7 статтях у фахових виданнях України із яких 2 статті в фахових журналах категорії А і проіндексовані в науково-метричній базі SCOPUS, 3 статтях опублікованих за кордоном, із яких 1 стаття включена до науково-метричної бази SCOPUS (1 квартіль) та WoS, одноосібному розділі колективної монографії, і в матеріалах двох міжнародних науково-технічних конференцій, однієї міжнародної науково-практичної конференції, міжнародного академічного форума та науково-практичної конференції Національної Академії Національної гвардії України.

Структура і обсяг дисертації. Робота складається зі вступу, пяти розділів, висновків, списку використаних джерел, додатків. Загальний обсяг дисертації – 190 сторінок. Основний зміст викладений на 158 сторінках, у тому числі – 15 таблиць, 13 рисунків. Список використаних джерел містить 103 найменування. Робота містить 3 додатки.

РОЗДІЛ 1. СУЧАСНИЙ СТАН ТА ПЕРСПЕКТИВИ РОЗВИТКУ ІНФОРМАЦІЙНИХ СИСТЕМ ПРОЕКТУВАННЯ МАЛОРЕСУРСНИХ КРИПТОГРАФІЧНИХ АЛГОРИТМІВ

1.1. Напрямки розвитку моделей і систем малоресурсної (легкої) криптографії

В теперішньому стані криптографічний захист інформації залишається одним з найбільш дієвих варіантів захисту інформаційного ресурсу [18-19]. Однак вищезазначені вимоги до програмно-апаратних технологічних обмежень робить застосування значної кількості криптоалгоритмів вкрай складним або з низькою ефективністю. В наш час одним із найперспективніших напрямів розвитку інформаційної безпеки є так звана «малоресурсна» (low-resource) або «полегшена» («легковагова») криптографія (lightweight cryptography) [20–22], використання яої орієнтовано на пристрої з обмеженими апаратними та енергетичними ресурсами. Актуальність розроблення ефективних та безпечних легковагових криптографічних рішень зумовлена стрімким поширенням вбудованих систем, бездротових сенсорних мереж, мобільних пристроїв та технологій Інтернету речей, для яких традиційні криптографічні алгоритми часто виявляються надто ресурсомісткими. В галузі інформаційної безпеки значна кількість наукових досліджень присвячена вдосконаленню саме показників криптографічного захисту інформації [24], аналізу можливостей застосування малоресурсних криптографічних алгоритмів у вбудованих системах [25], модернізації та оптимізації мало ресурсних криптографічних систем [26], а також визначенню найкращих сучасних легких криптографічних алгоритмів за рахунок проведення їх порівняльного аналізу [27–28]. Окрему увагу дослідники приділяють питанням зменшення

енергоспоживання, скорочення обчислювальної складності та забезпечення належного рівня захисту даних у середовищах з обмеженими ресурсами.

За останні роки було створено низку малоресурсних криптографічних примітивів, які перевершують традиційні криптографічні стандарти за показниками продуктивності. На відміну від класичних алгоритмів, такі примітиви орієнтовані на вузькоспеціалізовані сфери застосування та можуть враховувати обмежені можливості потенційного зловмисника. Малоресурсна криптографія є напрямом криптографії, спрямованим на розробку алгоритмів для пристроїв з обмеженими ресурсами пам’яті, обчислювальної потужності та фізичних можливостей [29].

В роботі [29] наведено класифікацію добре відомих типів доступних для практичного використання полехшених криптопримітивів (Див. рис 1.1).

Рис. 1.1. Класифікація відомих малоресурсних криптографічних примітивів [29].

Основними характеристиками малоресурсних криптографічних примітивів є розмір блоку, довжина ключа, структура алгоритму та кількість

раундів. Одним із прикладів малоресурсної криптографії є ECC, який, будучи асиметричним шифром, забезпечує автентифікацію та неспростовність. Властивості таких алгоритмів розглядаються у стандарті ISO/IEC 29192 [30], де малоресурсність визначається за вимогами до пам’яті, енергоспоживання та апаратної реалізації.

Для зменшення ресурсних витрат малоресурсні алгоритми зазвичай використовують менші розміри блоків і ключів порівняно з традиційними шифрами. Водночас важливими критеріями залишаються продуктивність, вартість реалізації та рівень безпеки. Стійкість алгоритмів до атак оцінюється за допомогою криптоаналізу, метою якого є виявлення слабких місць і розробка методів дешифрування [30].

В роботі [31] наведено класифікацію основних типів атак на блоковий шифр (Див. рис 1.2).

Рис. 1.2. Класифікація основних типів атак на блоковий шифр [29].

Представлені на рисунку 1.2 атаки використовують методи: «відомого відкритого тексту», «тільки шифрованого тексту», «обраного шифрованого

тексту», «обраного відкритого тексту», «людина посередині», «атаки грубою силою» та «атаки побічного каналу» [32].

Основними напрямками малоресурсної криптографії є.

- Асиметричні алгоритми на основі кривих Еліптичної кривої **(**ECC)**:** ECC дозволяє отримувати той самий рівень безпеки, що і традиційні алгоритми (RSA, DH), при меншому розмірі ключів. Це знижує вимоги до обчислювальних ресурсів і пам'яті.
- Стійкі до квантових обчислень алгоритми: Поява квантових комп'ютерів створює загрозу для традиційних криптосистем. Малоресурсна криптографія активно розвиває квантово-стійкі алгоритми, такі як NTRU або McEliece, з акцентом на економію ресурсів.
- Блокові шифри з низькими ресурсними вимогами: Алгоритми, такі як PRESENT, LEA, і SIMON/SPECK, були спеціально розроблені для малих пристроїв з обмеженими обчислювальними можливостями.
- Алгоритми хешування для обмежених ресурсів: Полегшені хеш-функції, такі як SPONGENT і PHOTON, розробляються для роботи на малих пристроях, з мінімальним використанням пам'яті і процесорного часу.
- Протоколи аутентифікації: Важливий напрямок у розробці малоресурсної криптографії — це створення легких аутентифікаційних протоколів для забезпечення безпеки IoT-пристроїв і сенсорних мереж з обмеженими ресурсами. До таких відносяться протоколи PUF (Physical Unclonable Function).
- Оптимізація енергоспоживання: Малоресурсна криптографія також зосереджується на мінімізації енергоспоживання під час виконання криптографічних операцій, що є критичним для пристроїв з автономним живленням (напр., сенсорні вузли або портативні пристрої).
- Інтеграція криптографії з апаратними рішеннями**:** Використання апаратних акселераторів, таких як FPGA або ASIC, для виконання криптографічних операцій є ще одним напрямком розвитку, який дозволяє суттєво знизити обчислювальні ресурси для криптографії.

1.2. СЕТ-шифрування.

Перспективним напрямом сучасного розвитку малоресурсної криптографії є СЕТ-шифрування, в основі якого лежать СЕТ-операції, що забезпечують перетворення вхідних Сі-квантів інформації у шифрограму [33]. СЕТ-операція – це операція криптографічного кодування (від англ. Cryptographic Encoding Theory – СЕТ). Вона представляє собою набір елементарних функцій кожна з яких в залежності від вхідних Сі-квантів інформації формує відповідний вихідний Сі-квантів інформації, перша елементарна функція –перший; друга елементарна функція – другий; і т.д. [33]. Позначення операцій криптографічного кодування як СЕТ-операцій було викликано необхідністю підвищення коректності розуміння англомовних статей по криптографічному кодуванню, а також виникнення тавтології при перекладі. СЕТ-операція представляє собою математичну модель таблиці підстановки. А елементарна функція – модель реалізації розряду в таблиці підстановки. Використання в СЕТ-операціях Сі-квантів інформації замість бітів, або байтів базується на тому, що дискретні моделі операцій забезпечують перетворення інформації бітами, байтами, словами і т.д. [34]. В роботі [33]. Показано що навіть в самій багатооперандній операції Сі-кванити операцій можуть мати різну сутність. Наприклад Сі-кванти першого операнду і Сі-кванти результату перетворення представляють байти вхідної інформації і результати перетворення, а Сі-кванти другого операнду – це біти управління вибором одноопераднних операцій. Також необхідно відмітити, що кількості Сі-квантів в операндах багатооперандних СЕТ-операцій можуть відрізнятися. За результатами наукових досліджень, наведених в [33] можна зробити висновок що СЕТ-шифрування є наступним етапом розвитку криптографічного кодування (криптографічного перетворення інформації).

Криптографічному кодування, або СЕТ-шифруванню присвячено цілий ряд наукових робіт [14]. Перші результати дослідження операцій

криптографічного кодування були оприлюднені в 2006 році [35]. В цій роботі ключову увагу приділено дослідженню моделей логічних пристроїв, що виконують криптографічне перетворення інформації розміром 2 біта. Модель операції криптографічного перетворення будується на основі елементарних функцій. У роботі [35] представлено технологію побудови логічних функцій для двохрозрядних дискретних криптографічних пристроїв, а подальші дослідження були спрямовані на вивчення закономірностей об'єднання елементарних функцій та розробку методів побудови операцій криптографічного перетворення [36]. Після встановлення взаємозв'язків між прямими і обернене ними операціями було запропоновано модель уніфікованого пристрою криптографічного перетворення інформації [37]. Узагальнивши результати досліджень двохррозрядних елементарних функцій і побудованих на їх основі двох розрядних операцій криптографічного кодування була встановлена алгебраїчна структура множини логічних операцій кодування [38]. В даній роботі було доведено що досліджена сукупність перетворень представляє групу перестановок в полі G_4 , а моделі операцій формалізують таблиці підстановок, які реалізують дані підстановки [33]. Узагальнені результати дослідження двохррозрядних елементарних функцій і двох розрядних операцій криптографічного кодування наведені в [40].

Слід відмітити, що всі отримані наукові результати по дослідженню двох розрядних елементарних функцій і двох розрядних операцій криптографічного перетворення були отримані лише після формування бази функцій і операцій на основі обчислювального експерименту.

Для забезпечення можливості дослідження трьох розрядних елементарних функцій і трьох розрядних операцій криптографічного кодування виникла необхідність проведення додаткового обчислювального експерименту. За його результатами було отримано 70 трьохрозрядних елементарних функцій і 40320 трьохрозрядних операцій криптографічного кодування [41].

Для спрощення досліджень всієї сукупності отриманих елементарних функцій, вони були поділені на симетричні (35 елементарних функцій) і несиметричні (35 елементарних функцій). Поділ було реалізовано аналогічно з поділом двох розрядних елементарних функцій [40]. Проте при дослідженні операцій криптографічного кодування побудованих на основі лише прямих або лише обернених елементарних функцій необхідно досліджувати по 5040 операцій. Одночасний аналіз такої кількості операцій значно ускладнює процес дослідження. Для зменшення кількості операцій криптографічного кодування які необхідно одночасно досліджувати необхідно поділити групи прямих і обернених елементарних функцій на підгрупи. В роботі [42] для класифікації трьох розрядних елементарних функцій було запропоновано використовувати складність їх дискретних моделей. Результати класифікації наведені на рис 1.3.

Наведена на рис.1.3 класифікація дозволила синтезувати і досліджувати групи операції криптографічного кодування, побудованих на основі класифікованих підгруп елементарних функцій.

Слід відмітити що необхідність класифікація трьох розрядних елементарних функцій і трьох розрядних операцій криптографічного пов’язана не стільки з великою кількістю операцій, а з необхідністю використання різного математичного апарату для їх опису і дослідження [43].

Основні результати дослідження операцій матричного криптографічного кодування наведені в роботах [44], [45]. Операцій матричного криптографічного кодування це єдина група операцій яка реалізує лінійні перетворення інформації. Дані перетворенні інформації описуються поєднанням дискретних лінійних перетворень на основі додавання по модулю два, та додаткового гамування по модулю два [46].

Основні результати дослідження операцій нелінійного розширеного матричного криптографічного кодування наведені в роботах [47], [48] . Опис нелінійних операцій розширеного матричного криптографічного кодування

може бути зведено до об’єднання лінійного криптографічного перетворення з наступним додаванням по модулю результату нелінійного перетворення.

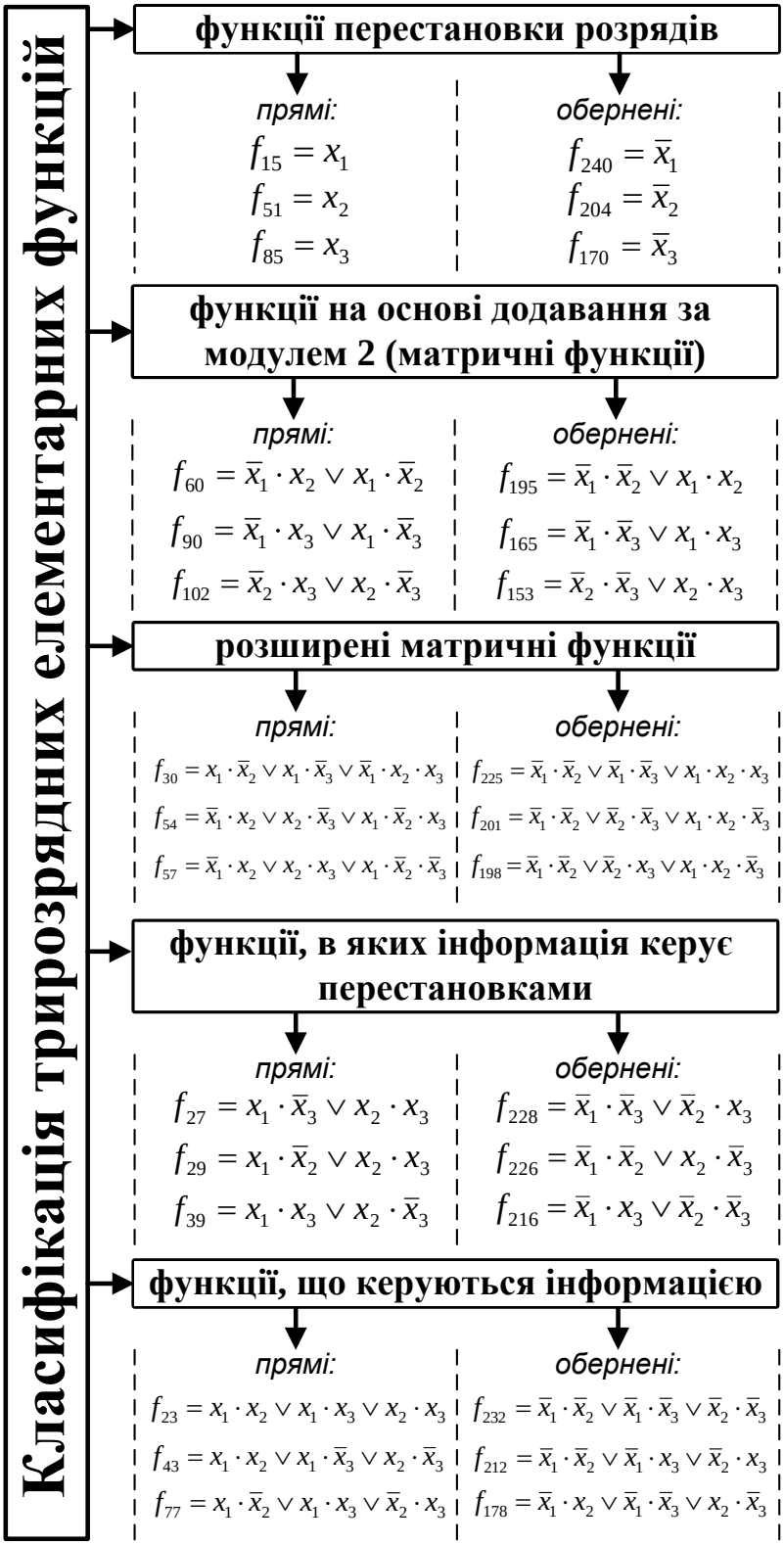

Рис. 1.3. Класифікація трирозрядних елементарних функцій [42]

Дослідженню операцій в яких інформація керую вибором перестановок і операцій перетворення присвячені роботи [49] – [51]. В основу проведенню наукових досліджень також було покладено результати обчислювального експерименту по моделюванню операцій в яких інформація керує процесом криптографічного перетворення.

При узагальненні і наведених результатів побудови і дослідження СЕТ-операцій було встановлено, що дані операції можна класифікувати як одноопернадні СЕТ-операції [33]. Дані операції перетворюють Сі-кванти вхідної інформації в Сі-кванти результати перетворення. Необхідність зміни алгоритму перетворення приводить до необхідності зміни СЕТ-операції.

Алгоритми потокового шифрування реалізуються на основі послідовного додавання по модулю два інформації з псевдовипадковою послідовністю. Основна операція – операція додавання по модулю два є однією із СЕТ-операцій. Дана операція містить два операнда, перший операнд – це операнд в який поступає інформація і другий операнд – операнд для псевдовипадкової послідовності.

Подальший розвиток СЕТ-шифрування привів до необхідності переходу від одноопернадних до багатоопернадних СЕТ-операцій. Розширення можливостей моделювання і дослідження СЕТ-операцій неможливе без вдосконалення засобів комп’ютерного моделювання. Вирішити дані питання без використання інформаційних технологій достатньо складно.

1.3. Інформаційні системи моделювання СЕТ-операцій

СЕТ-операція представляє собою математичну модель таблиці, або декількох таблиць підстановки. Елементарні функції представляють собою моделі реалізації розрядів в таблицях підстановки. В залежності від кількості таблиць підстановки, які та взаємозв’язків між таблицями підстановки СЕТ-

операції діляться на одноопераднді, двохоперандні і багатоопераднді [33]. Одноопераднда СЕТ-операція реалізує одну таблицю підстановки.

Серед груп одноопераднднх СЕТ-операцій самою простою групою є група 2Сі-квантових СЕТ-операцій. Математичні моделі даної групи СЕТ-операцій наведені в табл.1.1.

Таблиця 1.1

Дискретні моделі 2Сі-квантових одноопераднднх СЕТ-операцій

$C_1(x)=\begin{bmatrix} x_1 \\ x_2 \end{bmatrix}$	$C_7(x)=\begin{bmatrix} x_1 \\ x_2 \oplus 1 \end{bmatrix}$	$C_{13}(x)=\begin{bmatrix} x_1 \oplus 1 \\ x_2 \end{bmatrix}$	$C_{19}(x)=\begin{bmatrix} x_1 \oplus 1 \\ x_2 \oplus 1 \end{bmatrix}$
$C_2(x)=\begin{bmatrix} x_1 \oplus x_2 \\ x_2 \end{bmatrix}$	$C_8(x)=\begin{bmatrix} x_1 \oplus x_2 \\ x_2 \oplus 1 \end{bmatrix}$	$C_{14}(x)=\begin{bmatrix} x_1 \oplus x_2 \oplus 1 \\ x_2 \end{bmatrix}$	$C_{20}(x)=\begin{bmatrix} x_1 \oplus x_2 \oplus 1 \\ x_2 \oplus 1 \end{bmatrix}$
$C_3(x)=\begin{bmatrix} x_1 \\ x_1 \oplus x_2 \end{bmatrix}$	$C_9(x)=\begin{bmatrix} x_1 \\ x_1 \oplus x_2 \oplus 1 \end{bmatrix}$	$C_{15}(x)=\begin{bmatrix} x_1 \oplus 1 \\ x_1 \oplus x_2 \end{bmatrix}$	$C_{21}(x)=\begin{bmatrix} x_1 \oplus 1 \\ x_1 \oplus x_2 \oplus 1 \end{bmatrix}$
$C_4\begin{pmatrix} x_1 \\ x_2 \end{pmatrix}=\begin{bmatrix} x_2 \\ x_1 \end{bmatrix}$	$C_{10}(x)=\begin{bmatrix} x_2 \\ x_1 \oplus 1 \end{bmatrix}$	$C_{16}(x)=\begin{bmatrix} x_2 \oplus 1 \\ x_1 \end{bmatrix}$	$C_{22}(x)=\begin{bmatrix} x_2 \oplus 1 \\ x_1 \oplus 1 \end{bmatrix}$
$C_5(x)=\begin{bmatrix} x_2 \\ x_1 \oplus x_2 \end{bmatrix}$	$C_{11}(x)=\begin{bmatrix} x_2 \\ x_1 \oplus x_2 \oplus 1 \end{bmatrix}$	$C_{17}(x)=\begin{bmatrix} x_2 \oplus 1 \\ x_1 \oplus x_2 \end{bmatrix}$	$C_{23}(x)=\begin{bmatrix} x_2 \oplus 1 \\ x_1 \oplus x_2 \oplus 1 \end{bmatrix}$
$C_6(x)=\begin{bmatrix} x_1 \oplus x_2 \\ x_1 \end{bmatrix}$	$C_{12}(x)=\begin{bmatrix} x_1 \oplus x_2 \\ x_1 \oplus 1 \end{bmatrix}$	$C_{18}(x)=\begin{bmatrix} x_1 \oplus x_2 \oplus 1 \\ x_1 \end{bmatrix}$	$C_{24}(x_1)=\begin{bmatrix} x_1 \oplus x_2 \oplus 1 \\ x_1 \oplus 1 \end{bmatrix}$

Як видно з табл.1.1, дана група СЕТ-операцій включає в себе всього 24 операції які описуються елементарними функціями побудованими на основі додавання за модулем 2. Дану групу СЕТ-операцій можна будо досліджувати буз застосування засобів автоматизованого моделювання.

Група 3Сі-квантових СЕТ-операцій включає в себе 40320 операцій. По аналогії з класифікацією елементарних функцій, дані операції можна поділити на матричні СЕТ-операції, розширені матричні СЕТ-операції, СЕТ-операції перестановок керованих інформацією та інші. В табл. 1.2 [52] наведені дискретні моделі базової групи 3Сі-квантових матричних СЕТ-операцій.

Особливу складність при проведенні дослідження викликають СЕТ-операції побудовані з елементарних функцій, які належать до різних

класифікаційних груп. Їх дослідження практично не можливо проводити без засобів автоматизації моделювання.

Таблиця 1.2

Базова група ЗСі-квантових одноопераднних матричних СЕТ-операцій [52]

$C_1(x)=\begin{bmatrix} x_1 \\ x_2 \\ x_3 \end{bmatrix}$	$C_2(x)=\begin{bmatrix} x_1 \\ x_1 \oplus x_2 \\ x_3 \end{bmatrix}$	$C_3(x)=\begin{bmatrix} x_1 \\ x_2 \\ x_1 \oplus x_3 \end{bmatrix}$	$C_4(x)=\begin{bmatrix} x_1 \oplus x_2 \\ x_2 \\ x_3 \end{bmatrix}$
$C_5(x)=\begin{bmatrix} x_1 \\ x_2 \\ x_2 \oplus x_3 \end{bmatrix}$	$C_6(x)=\begin{bmatrix} x_1 \oplus x_3 \\ x_2 \\ x_3 \end{bmatrix}$	$C_7(x)=\begin{bmatrix} x_1 \\ x_2 \oplus x_3 \\ x_3 \end{bmatrix}$	$C_8(x)=\begin{bmatrix} x_1 \oplus x_2 \oplus x_3 \\ x_2 \\ x_3 \end{bmatrix}$
$C_9(x)=\begin{bmatrix} x_1 \\ x_1 \oplus x_2 \oplus x_3 \\ x_3 \end{bmatrix}$	$C_{10}(x)=\begin{bmatrix} x_1 \\ x_2 \\ x_1 \oplus x_2 \oplus x_3 \end{bmatrix}$	$C_{11}(x)=\begin{bmatrix} x_1 \\ x_1 \oplus x_2 \\ x_1 \oplus x_3 \end{bmatrix}$	$C_{12}(x)=\begin{bmatrix} x_1 \oplus x_2 \\ x_2 \\ x_2 \oplus x_3 \end{bmatrix}$
$C_{13}(x)=\begin{bmatrix} x_1 \oplus x_3 \\ x_2 \oplus x_3 \\ x_3 \end{bmatrix}$	$C_{14}(x)=\begin{bmatrix} x_1 \\ x_1 \oplus x_2 \\ x_1 \oplus x_2 \oplus x_3 \end{bmatrix}$ $C'_{14}(x)=\begin{bmatrix} x_1 \\ x_1 \oplus x_2 \\ x_2 \oplus x_3 \end{bmatrix}$	$C_{15}(x)=\begin{bmatrix} x_1 \\ x_1 \oplus x_3 \\ x_1 \oplus x_2 \oplus x_3 \end{bmatrix}$ $C'_{15}(x)=\begin{bmatrix} x_1 \\ x_2 \oplus x_3 \\ x_1 \oplus x_2 \end{bmatrix}$	$C_{16}(x)=\begin{bmatrix} x_1 \oplus x_2 \\ x_2 \\ x_1 \oplus x_2 \oplus x_3 \end{bmatrix}$ $C'_{16}(x)=\begin{bmatrix} x_1 \oplus x_2 \\ x_2 \\ x_1 \oplus x_3 \end{bmatrix}$
$C_{17}(x)=\begin{bmatrix} x_1 \oplus x_2 \oplus x_3 \\ x_2 \\ x_2 \oplus x_3 \end{bmatrix}$ $C'_{17}(x)=\begin{bmatrix} x_1 \oplus x_3 \\ x_2 \\ x_2 \oplus x_3 \end{bmatrix}$	$C_{18}(x)=\begin{bmatrix} x_1 \oplus x_2 \oplus x_3 \\ x_2 \oplus x_3 \\ x_3 \end{bmatrix}$ $C'_{18}(x)=\begin{bmatrix} x_1 \oplus x_2 \\ x_2 \oplus x_3 \\ x_3 \end{bmatrix}$	$C_{19}(x)=\begin{bmatrix} x_1 \oplus x_3 \\ x_1 \oplus x_2 \oplus x_3 \\ x_3 \end{bmatrix}$ $C'_{19}(x)=\begin{bmatrix} x_1 \oplus x_3 \\ x_1 \oplus x_2 \\ x_3 \end{bmatrix}$	$C_{20}(x)=\begin{bmatrix} x_1 \\ x_1 \oplus x_2 \\ x_2 \oplus x_3 \end{bmatrix}$ $C'_{20}(x)=\begin{bmatrix} x_1 \\ x_1 \oplus x_2 \\ x_1 \oplus x_2 \oplus x_3 \end{bmatrix}$
$C_{21}(x)=\begin{bmatrix} x_1 \\ x_2 \oplus x_3 \\ x_1 \oplus x_3 \end{bmatrix}$ $C'_{21}(x)=\begin{bmatrix} x_1 \\ x_1 \oplus x_2 \oplus x_3 \\ x_1 \oplus x_3 \end{bmatrix}$	$C_{22}(x)=\begin{bmatrix} x_1 \oplus x_3 \\ x_2 \\ x_2 \oplus x_3 \end{bmatrix}$ $C'_{22}(x)=\begin{bmatrix} x_1 \oplus x_2 \oplus x_3 \\ x_2 \\ x_2 \oplus x_3 \end{bmatrix}$	$C_{23}(x)=\begin{bmatrix} x_1 \oplus x_2 \\ x_2 \\ x_1 \oplus x_3 \end{bmatrix}$ $C'_{23}(x)=\begin{bmatrix} x_1 \oplus x_2 \\ x_2 \\ x_1 \oplus x_2 \oplus x_3 \end{bmatrix}$	$C_{24}(x)=\begin{bmatrix} x_1 \oplus x_2 \\ x_2 \oplus x_3 \\ x_3 \end{bmatrix}$ $C'_{24}(x)=\begin{bmatrix} x_1 \oplus x_2 \oplus x_3 \\ x_2 \oplus x_3 \\ x_3 \end{bmatrix}$
$C_{25}(x)=\begin{bmatrix} x_1 \oplus x_3 \\ x_1 \oplus x_2 \\ x_3 \end{bmatrix}$ $C'_{25}(x)=\begin{bmatrix} x_1 \oplus x_3 \\ x_1 \oplus x_2 \oplus x_3 \\ x_3 \end{bmatrix}$	$C_{26}(x)=\begin{bmatrix} x_1 \oplus x_3 \\ x_1 \oplus x_2 \\ x_1 \oplus x_2 \oplus x_3 \end{bmatrix}$ $C'_{26}(x)=\begin{bmatrix} x_1 \oplus x_2 \oplus x_3 \\ x_1 \oplus x_3 \\ x_2 \oplus x_3 \end{bmatrix}$	$C_{27}(x)=\begin{bmatrix} x_1 \oplus x_2 \oplus x_3 \\ x_2 \oplus x_3 \\ x_1 \oplus x_3 \end{bmatrix}$ $C'_{27}(x)=\begin{bmatrix} x_1 \oplus x_2 \\ x_1 \oplus x_3 \\ x_1 \oplus x_2 \oplus x_3 \end{bmatrix}$	$C_{28}(x)=\begin{bmatrix} x_1 \oplus x_2 \\ x_2 \oplus x_3 \\ x_1 \oplus x_2 \oplus x_3 \end{bmatrix}$ $C'_{28}(x)=\begin{bmatrix} x_2 \oplus x_3 \\ x_1 \oplus x_2 \oplus x_3 \\ x_1 \oplus x_3 \end{bmatrix}$

Проте виникає питання навіщо досліджувати одноопераднді операції, адже кожна така операція представляє собою лише таблицю підстановки. Щоб відповісти на дане питання проаналізуємо особливості практичної реалізації одноопераднди СЕТ-операцій.

Шифр на основі однієї одноопераднді СЕТ-операції можна розглядати як шифр прямої підстановки [53]. Проте якщо кількість Сі-квантів СЕТ-операції не співпадає з кількістю біт представлення символів з алфавіту повідомлення даний шифр буде реалізовувати підстановку з між символьним перемішуванням. Якщо в потоковому шифрі використовується декілька одноопераднди СЕТ-операцій, то він може розглядатися як однозвучний підстановочний шифр, або поліалфавітний шифр. [53]. Проте при використанні СЕТ-операцій кількість біт перетворення як правило не співпадає з кількість біт, які використовуються для кодування символів, тому дані шифри можуть розглядатися як модифіковані поліграмні підстановні шифри, які забезпечують між символьне перемішування [22]. Використання одноопераднди СЕТ-операцій з різною кількістю Сі-квантів інформації, яка перетворюється, забезпечить побудову шифрів з плаваючим блоком перетворювання. [33].

Криптографічному кодування, або СЕТ перетворенню інформації присвячено цілий ряд наукових робіт. Дані роботи можуть бути поділені на роботи присвячені методам синтезу аналізу та застосування одноопераднди операцій [46, 54], і наукові роботи присвячені методам синтезу аналізу та застосування двохоперандних операцій [55, 56]. Отримані наукові результати базуються на результатах комп'ютерного моделювання, яке забезпечує пошук вхідних даних для проведення дослідження. Тому питанням побудови інформаційних технологій моделювання і дослідження СЕТ-операцій присвячено ряд робіт [57 - 59]. Розглянемо дані роботи більш детально.

Перша інформаційна система для побудови і дослідження логічних функцій та одноопераднди операцій була описана в [57]. Інформаційна система включала блок кодування-декодування і логічний аналізатор команд.

Для забезпечення простоти і ефективності моделювання одноопераднних СЕТ-операцій дана система була доповнена графічним інтерфейсом користувача та засобами збереження отриманих формалізованих моделей. Наявність бази синтезованих моделей одноопераднних СЕТ-операцій в подальшому дозволили розширити можливості системи за рахунок впровадження засобів моделювання груп елементарних функцій, а також можливостей додаткового аналізу статистичного аналізу, включаючи лавинний ефект [58].

Застосування в потокових шифрах одноопераднних СЕТ-операцій забезпечує реалізацію однієї, або декількох таблиць підстановки. В класичній криптографії існує чотири типи підстановочних шифрів [59]. По своїй сутності потокові шифри на основі одноопераднних СЕТ-операцій поділяються на [323, 60]:

– простий підстановочний шифр, в якому кожен символ відкритого тексту при шифруванні заміняється іншим символом з таблиці підстановки [33];

– однозвучний підстановочний шифр, в якому кожен символ відкритого тексту при шифруванні може замінятися одним з декількох символів [62]. Його реалізація пов’язана з збільшенням кількості символів які використовуються в шифрограмі, порівняно з відкритим текстом [33];

– поліграмний підстановочний шифр, в якогму групи символів відкритого тексту заміняються групами інших символів з таблиці підстановки [61];

– поліалфавітний підстановочний шифр, в якому послідовно виконується декілька простих підстановочних шифрів, послідовність яких визначаються ключем [62].

Генеруємі інформаційною системою операції можуть використовуватися при побудові блокових і потокових шифрів. Проте дані операції представляють лише незначну частину двохоперандних СЕТ-операцій. На сьогоднішній день відсутні засоби автоматизації досліджень несиметричних двохоперандних СЕТ-операцій для побудови потокових

систем шифрування. Подальший розвиток СЕТ-шифрування привів до необхідності переходу від одноопераднних до багатоопераднних СЕТ-операцій. Розширення можливостей моделювання і дослідження СЕТ-операцій неможливе без вдосконалення засобів комп'ютерного моделювання.

1.4. Ієрархічна технології моделювання симетричних двохоперандних операцій криптографічного кодування

Не зважаючи на всі переваги підстановочний шифрів на основі одноопераднних СЕТ-операцій, їх криптостійкість суттєво менша на основі шифрів побудованих на основі додавання по модулю інформації з псевдовипадковою послідовністю.

Реалізувати аналогічні криптографічні системи можна замінивши операцію додавання за модулем двохоперандною СЕТ-операцією [63, 64]. Необхідно відмітити, що будь яка операція додавання за модулем також є СЕТ-операцією, тому що вона реалізує набір таблиць підстановки які вибираються в залежності від значень біт псевдовипадкової послідовності.

Перші результати дослідження множини операцій аналогічних додаванню за модулем два були опубліковані в [65]. В процесі дослідження множини синтезованих операцій встановлювалися взаємозв'язки між операціями криптографічного перетворення [66 - 68]. Для отримання необхідних результатів на початковому етапі використовувалися різні методи дослідження, включаючи графічне представлення операцій [69]. В результаті була розроблена технологія дослідження модифікованих операцій додавання за модулем два яка опублікована в [70, 71].

В результаті проведених досліджень була синтезована множина модифікованих операцій додавання за модулем два з точністю до перестановки, яка включає в себе 16 СЕТ-операцій, які забезпечують стійкість до лінійного криптоаналізу аналогічну стійкості потокових шифрів на основі додавання за модулем два [72, 73].

Синтезовані двохоперандні СЕТ-операції на основі модифікації додавання за модулем два мають одну особливість, вони допускають перестановку операндів. Подальші дослідження операцій, які допускають перестановку операндів пов’язані з вирішенням трудомістких переборних задач, які практично неможливо вирішити без використання засобів обчислювальної техніки і спеціалізованого програмного забезпечення [74].

Отримані перші математичні моделі симетричних двохоперандних СЕТ-операцій стали основою для створення програмного забезпечення для проведення обчислювального експерименту по пошуку кортежів одноопераднних операцій на основі яких будуються двохоперандні операції .

За результатами дослідження результатів моделювання 2Сі-квантових СЕТ-операцій були побудовані 4 групи симетричних 2Сі-квантових СЕТ-операцій по 24 операції в кожній групі.

Була побудована група двохоперандні симетричних 2Сі-квантових СЕТ-операцій, синтезована на основі порозрядного додавання за модулем два наведена в табл. 1.3 [75]. При побудові даної групи симетричних СЕТ-операцій були використані наукові результати опубліковані в [76 - 78].

На основі даних результатів та побудованої групи СЕТ-операцій було розроблено технологію побудови двохоперандних операцій криптографічного перетворення інформації за результатами моделювання [79]. Застосувавши дану технологію були побудовані групи симетричних 2Сі-квантових СЕТ-операцій на основі правостороннього і лівостороннього додавання за модулем 4, які наведені в табл.1.4 і табл. 1.5

За результатами аналізу експериментально отриманих кортежів була встановлена четверта група симетричних 2Сі-квантових СЕТ-операцій яка будується не на основі операцій додавання за модулем [82]. Математичні моделі даної групи СЕТ-операцій наведені в табл. 1.6 [74].

Необхідно відмітити що побудувати моделі всіх груп симетричних двохоперандних СЕТ-операцій можливо на основі методу синтезу двохоперандних СЕТ-операцій на основі дублювання одноопераднних СЕТ-операцій [55].

Таблиця 1.3

Група двохоперандних симетричних 2Сі-квантових СЕТ-операцій, синтезованих на основі порозрядного додавання за модулем два [75]

Класифікатор операцій		Операції інверсії	
		$\begin{bmatrix}0\\0\end{bmatrix}$ / $\begin{bmatrix}1\\0\end{bmatrix}$	$\begin{bmatrix}0\\1\end{bmatrix}$ / $\begin{bmatrix}1\\1\end{bmatrix}$
Базові операції	$F_1=\begin{bmatrix}x_1\\x_2\end{bmatrix}$	$O_1^{\text{mod}2}=\begin{bmatrix}x_1\oplus k_1\\x_2\oplus k_2\end{bmatrix}$	$O_7^{\text{mod}2}=\begin{bmatrix}x_1\oplus k_1\\x_2\oplus k_2\oplus 1\end{bmatrix}$
		$O_{13}^{\text{mod}2}=\begin{bmatrix}x_1\oplus k_1\oplus 1\\x_2\oplus k_2\end{bmatrix}$	$O_{19}^{\text{mod}2}=\begin{bmatrix}x_1\oplus k_1\oplus 1\\x_2\oplus k_2\oplus 1\end{bmatrix}$
	$F_2=\begin{bmatrix}x_1\oplus x_2\\x_2\end{bmatrix}$	$O_2^{\text{mod}2}=\begin{bmatrix}x_1\oplus x_2\oplus k_1\oplus k_2\\x_2\oplus k_2\end{bmatrix}$	$O_8^{\text{mod}2}=\begin{bmatrix}x_1\oplus x_2\oplus k_1\oplus k_2\\x_2\oplus k_2\oplus 1\end{bmatrix}$
		$O_{14}^{\text{mod}2}=\begin{bmatrix}x_1\oplus x_2\oplus k_1\oplus k_2\oplus 1\\x_2\oplus k_2\end{bmatrix}$	$O_{20}^{\text{mod}2}=\begin{bmatrix}x_1\oplus x_2\oplus k_1\oplus k_2\oplus 1\\x_2\oplus k_2\oplus 1\end{bmatrix}$
	$F_3=\begin{bmatrix}x_1\\x_1\oplus x_2\end{bmatrix}$	$O_3^{\text{mod}2}=\begin{bmatrix}x_1\oplus k_1\\x_1\oplus x_2\oplus k_1\oplus k_2\end{bmatrix}$	$O_9^{\text{mod}2}=\begin{bmatrix}x_1\oplus k_1\\x_1\oplus x_2\oplus k_1\oplus k_2\oplus 1\end{bmatrix}$
		$O_{15}^{\text{mod}2}=\begin{bmatrix}x_1\oplus k_1\oplus 1\\x_1\oplus x_2\oplus k_1\oplus k_2\end{bmatrix}$	$O_{21}^{\text{mod}2}=\begin{bmatrix}x_1\oplus k_1\oplus 1\\x_1\oplus x_2\oplus k_1\oplus k_2\oplus 1\end{bmatrix}$
Операції перестановок	$F_4=\begin{bmatrix}x_2\\x_1\end{bmatrix}$	$O_4^{\text{mod}2}=\begin{bmatrix}x_2\oplus k_2\\x_1\oplus k_1\end{bmatrix}$	$O_{10}^{\text{mod}2}=\begin{bmatrix}x_2\oplus k_2\\x_1\oplus k_1\oplus 1\end{bmatrix}$
		$O_{16}^{\text{mod}2}=\begin{bmatrix}x_2\oplus k_2\oplus 1\\x_1\oplus k_1\end{bmatrix}$	$O_{22}^{\text{mod}2}=\begin{bmatrix}x_2\oplus k_2\oplus 1\\x_1\oplus k_1\oplus 1\end{bmatrix}$
	$F_5=\begin{bmatrix}x_2\\x_1\oplus x_2\end{bmatrix}$	$O_5^{\text{mod}2}=\begin{bmatrix}x_2\oplus k_2\\x_1\oplus x_2\oplus k_1\oplus k_2\end{bmatrix}$	$O_{11}^{\text{mod}2}=\begin{bmatrix}x_2\oplus k_2\\x_1\oplus x_2\oplus k_1\oplus k_2\oplus 1\end{bmatrix}$
		$O_{17}^{\text{mod}2}=\begin{bmatrix}x_2\oplus k_2\oplus 1\\x_1\oplus x_2\oplus k_1\oplus k_2\end{bmatrix}$	$O_{23}^{\text{mod}2}=\begin{bmatrix}x_2\oplus k_2\oplus 1\\x_1\oplus x_2\oplus k_1\oplus k_2\oplus 1\end{bmatrix}$
	$F_6=\begin{bmatrix}x_1\oplus x_2\\x_1\end{bmatrix}$	$O_6^{\text{mod}2}=\begin{bmatrix}x_1\oplus x_2\oplus k_1\oplus k_2\\x_1\oplus k_1\end{bmatrix}$	$O_{12}^{\text{mod}2}=\begin{bmatrix}x_1\oplus x_2\oplus k_1\oplus k_2\\x_1\oplus k_1\oplus 1\end{bmatrix}$
		$O_{18}^{\text{mod}2}=\begin{bmatrix}x_1\oplus x_2\oplus k_1\oplus k_2\oplus 1\\x_1\oplus k_1\end{bmatrix}$	$O_{24}^{\text{mod}2}=\begin{bmatrix}x_1\oplus x_2\oplus k_1\oplus k_2\oplus 1\\x_1\oplus k_1\oplus 1\end{bmatrix}$

Таблиця 1.4

Група двохоперандних симетричних 2Сі-квантових СЕТ-операцій, синтезованих на основі лівостороннього додавання за модулем чотири [80]

Класифікатор операцій		Операції інверсії	
		$\begin{bmatrix}0\\0\end{bmatrix}$ / $\begin{bmatrix}1\\0\end{bmatrix}$	$\begin{bmatrix}0\\1\end{bmatrix}$ / $\begin{bmatrix}1\\1\end{bmatrix}$
Базові операції	$F_1=\begin{bmatrix}x_1\\x_2\end{bmatrix}$	$O_1^{\text{mod}4\leftarrow}=\begin{bmatrix}x_1\oplus x_2\cdot k_2\oplus k_1\\x_2\oplus k_2\end{bmatrix}$	$O_7^{\text{mod}4\leftarrow}=\begin{bmatrix}x_1\oplus x_2\cdot k_2\oplus k_1\\x_2\oplus k_2\oplus 1\end{bmatrix}$
		$O_{13}^{\text{mod}4\leftarrow}=\begin{bmatrix}x_1\oplus x_2\cdot k_2\oplus k_1\oplus 1\\x_2\oplus k_2\end{bmatrix}$	$O_{19}^{\text{mod}4\leftarrow}=\begin{bmatrix}x_1\oplus x_2\cdot k_2\oplus k_1\oplus 1\\x_2\oplus k_2\oplus 1\end{bmatrix}$
	$F_2=\begin{bmatrix}x_1\oplus x_2\\x_2\end{bmatrix}$	$O_2^{\text{mod}4\leftarrow}=\begin{bmatrix}x_1\oplus x_2\cdot\bar{k}_2\oplus k_1\oplus k_2\\x_2\oplus k_2\end{bmatrix}$	$O_8^{\text{mod}4\leftarrow}=\begin{bmatrix}x_1\oplus x_2\cdot\bar{k}_2\oplus k_1\oplus k_2\\x_2\oplus k_2\oplus 1\end{bmatrix}$
		$O_{14}^{\text{mod}4\leftarrow}=\begin{bmatrix}x_1\oplus x_2\cdot\bar{k}_2\oplus k_1\oplus k_2\oplus 1\\x_2\oplus k_2\end{bmatrix}$	$O_{20}^{\text{mod}4\leftarrow}=\begin{bmatrix}x_1\oplus x_2\cdot\bar{k}_2\oplus k_1\oplus k_2\oplus 1\\x_2\oplus k_2\oplus 1\end{bmatrix}$
	$F_3=\begin{bmatrix}x_1\\x_1\oplus x_2\end{bmatrix}$	$O_3^{\text{mod}4\leftarrow}=\begin{bmatrix}x_1\oplus x_2\cdot k_2\oplus k_1\\x_1\oplus x_2\cdot\bar{k}_2\oplus k_1\oplus k_2\end{bmatrix}$	$O_9^{\text{mod}4\leftarrow}=\begin{bmatrix}x_1\oplus x_2\cdot k_2\oplus k_1\\x_1\oplus x_2\cdot\bar{k}_2\oplus k_1\oplus k_2\oplus 1\end{bmatrix}$
		$O_{15}^{\text{mod}4\leftarrow}=\begin{bmatrix}x_1\oplus x_2\cdot k_2\oplus k_1\oplus 1\\x_1\oplus x_2\cdot\bar{k}_2\oplus k_1\oplus k_2\end{bmatrix}$	$O_{21}^{\text{mod}4\leftarrow}=\begin{bmatrix}x_1\oplus x_2\cdot k_2\oplus k_1\oplus 1\\x_1\oplus x_2\cdot\bar{k}_2\oplus k_1\oplus k_2\oplus 1\end{bmatrix}$
Операції перестановок	$F_4=\begin{bmatrix}x_2\\x_1\end{bmatrix}$	$O_4^{\text{mod}4\leftarrow}=\begin{bmatrix}x_2\oplus k_2\\x_1\oplus x_2\cdot k_2\oplus k_1\end{bmatrix}$	$O_{10}^{\text{mod}4\leftarrow}=\begin{bmatrix}x_2\oplus k_2\\x_1\oplus x_2\cdot k_2\oplus k_1\oplus 1\end{bmatrix}$
		$O_{16}^{\text{mod}4\leftarrow}=\begin{bmatrix}x_2\oplus k_2\oplus 1\\x_1\oplus x_2\cdot k_2\oplus k_1\end{bmatrix}$	$O_{22}^{\text{mod}4\leftarrow}=\begin{bmatrix}x_2\oplus k_2\oplus 1\\x_1\oplus x_2\cdot k_2\oplus k_1\oplus 1\end{bmatrix}$
	$F_5=\begin{bmatrix}x_2\\x_1\oplus x_2\end{bmatrix}$	$O_5^{\text{mod}4\leftarrow}=\begin{bmatrix}x_2\oplus k_2\\x_1\oplus x_2\cdot\bar{k}_2\oplus k_1\oplus k_2\end{bmatrix}$	$O_{11}^{\text{mod}4\leftarrow}=\begin{bmatrix}x_2\oplus k_2\\x_1\oplus x_2\cdot\bar{k}_2\oplus k_1\oplus k_2\oplus 1\end{bmatrix}$
		$O_{17}^{\text{mod}4\leftarrow}=\begin{bmatrix}x_2\oplus k_2\oplus 1\\x_1\oplus x_2\cdot\bar{k}_2\oplus k_1\oplus k_2\end{bmatrix}$	$O_{23}^{\text{mod}4\leftarrow}=\begin{bmatrix}x_2\oplus k_2\oplus 1\\x_1\oplus x_2\cdot\bar{k}_2\oplus k_1\oplus k_2\oplus 1\end{bmatrix}$
	$F_6=\begin{bmatrix}x_1\oplus x_2\\x_1\end{bmatrix}$	$O_6^{\text{mod}4\leftarrow}=\begin{bmatrix}x_1\oplus x_2\cdot\bar{k}_2\oplus k_1\oplus k_2\\x_1\oplus x_2\cdot k_2\oplus k_1\end{bmatrix}$	$O_{12}^{\text{mod}4\leftarrow}=\begin{bmatrix}x_1\oplus x_2\cdot\bar{k}_2\oplus k_1\oplus k_2\\x_1\oplus x_2\cdot k_2\oplus k_1\oplus 1\end{bmatrix}$
		$O_{18}^{\text{mod}4\leftarrow}=\begin{bmatrix}x_1\oplus x_2\cdot\bar{k}_2\oplus k_1\oplus k_2\oplus 1\\x_1\oplus x_2\cdot k_2\oplus k_1\end{bmatrix}$	$O_{24}^{\text{mod}4\leftarrow}=\begin{bmatrix}x_1\oplus x_2\cdot\bar{k}_2\oplus k_1\oplus k_2\oplus 1\\x_1\oplus x_2\cdot k_2\oplus k_1\oplus 1\end{bmatrix}$

Таблиця 1.5

Група двохоперандних симетричних 2Сі-квантових СЕТ-операцій, синтезованих на основі правостороннього додавання за модулем чотири [80]

Класифікатор операцій		Операції інверсії	
		$\begin{bmatrix}0\\0\end{bmatrix}\diagup\begin{bmatrix}1\\0\end{bmatrix}$	$\begin{bmatrix}0\\1\end{bmatrix}\diagup\begin{bmatrix}1\\1\end{bmatrix}$
Базові операції	$F_1=\begin{bmatrix}x_1\\x_2\end{bmatrix}$	$O_{1,7,15,21}=\begin{bmatrix}x_1\oplus k_1\\x_1\cdot k_1\oplus x_2\oplus k_2\end{bmatrix}$	$O_{7,1,21,15}=\begin{bmatrix}x_1\oplus k_1\\x_1\cdot k_1\oplus x_2\oplus k_2\oplus 1\end{bmatrix}$
		$O_{13,19,3,9}=\begin{bmatrix}x_1\oplus k_1\oplus 1\\x_1\cdot k_1\oplus x_2\oplus k_2\end{bmatrix}$	$O_{13,19,3,9}=\begin{bmatrix}x_1\oplus k_1\oplus 1\\x_1\cdot k_1\oplus x_2\oplus k_2\oplus 1\end{bmatrix}$
	$F_2=\begin{bmatrix}x_1\oplus x_2\\x_2\end{bmatrix}$	$O_{2,20,17,11}=\begin{bmatrix}x_1\cdot\bar{k}_1\oplus x_2\oplus k_1\oplus k_2\\x_1\cdot k_1\oplus x_2\oplus k_2\end{bmatrix}$	$O_{8,14,23,5}=\begin{bmatrix}x_1\cdot\bar{k}_1\oplus x_2\oplus k_1\oplus k_2\\x_1\cdot k_1\oplus x_2\oplus k_2\oplus 1\end{bmatrix}$
		$O_{14,8,5,23}=\begin{bmatrix}x_1\cdot\bar{k}_1\oplus x_2\oplus k_1\oplus k_2\oplus 1\\x_1\cdot k_1\oplus x_2\oplus k_2\end{bmatrix}$	$O_{20,2,11,17}=\begin{bmatrix}x_1\cdot\bar{k}_1\oplus x_2\oplus k_1\oplus k_2\oplus 1\\x_1\cdot k_1\oplus x_2\oplus k_2\oplus 1\end{bmatrix}$
	$F_3=\begin{bmatrix}x_1\\x_1\oplus x_2\end{bmatrix}$	$O_{3,9,19,13}=\begin{bmatrix}x_1\oplus k_1\\x_1\cdot\bar{k}_1\oplus x_2\oplus k_1\oplus k_2\end{bmatrix}$	$O_{9,3,13,19}=\begin{bmatrix}x_1\oplus k_1\\x_1\cdot\bar{k}_1\oplus x_2\oplus k_1\oplus k_2\oplus 1\end{bmatrix}$
		$O_{15,21,7,1}=\begin{bmatrix}x_1\oplus k_1\oplus 1\\x_1\cdot\bar{k}_1\oplus x_2\oplus k_1\oplus k_2\end{bmatrix}$	$O_{121,15,1,7}=\begin{bmatrix}x_1\oplus k_1\oplus 1\\x_1\cdot\bar{k}_1\oplus x_2\oplus k_1\oplus k_2\oplus 1\end{bmatrix}$
Операції перестановок	$F_4=\begin{bmatrix}x_2\\x_1\end{bmatrix}$	$O_{4,16,12,24}=\begin{bmatrix}x_1\cdot k_1\oplus x_2\oplus k_2\\x_1\oplus k_1\end{bmatrix}$	$O_{10,22,6,18}=\begin{bmatrix}x_1\cdot k_1\oplus x_2\oplus k_2\\x_1\oplus k_1\oplus 1\end{bmatrix}$
		$O_{16,4,24,12}=\begin{bmatrix}x_1\cdot k_1\oplus x_2\oplus k_2\oplus 1\\x_1\oplus k_1\end{bmatrix}$	$O_{22,10,18,6}=\begin{bmatrix}x_1\cdot k_1\oplus x_2\oplus k_2\oplus 1\\x_1\oplus k_1\oplus 1\end{bmatrix}$
	$F_5=\begin{bmatrix}x_2\\x_1\oplus x_2\end{bmatrix}$	$O_{5,23,8,14}=\begin{bmatrix}x_1\cdot k_1\oplus x_2\oplus k_2\\x_1\cdot\bar{k}_1\oplus x_2\oplus k_1\oplus k_2\end{bmatrix}$	$O_{11,17,2,20}=\begin{bmatrix}x_1\cdot k_1\oplus x_2\oplus k_2\\x_1\cdot\bar{k}_1\oplus x_2\oplus k_1\oplus k_2\oplus 1\end{bmatrix}$
		$O_{17,11,20,2}=\begin{bmatrix}x_1\cdot k_1\oplus x_2\oplus k_2\oplus 1\\x_1\cdot\bar{k}_1\oplus x_2\oplus k_1\oplus k_2\end{bmatrix}$	$O_{23,5,14,8}=\begin{bmatrix}x_1\cdot k_1\oplus x_2\oplus k_2\oplus 1\\x_1\cdot\bar{k}_1\oplus x_2\oplus k_1\oplus k_2\oplus 1\end{bmatrix}$
	$F_6=\begin{bmatrix}x_1\oplus x_2\\x_1\end{bmatrix}$	$O_{6,18,22,10}=\begin{bmatrix}x_1\cdot\bar{k}_1\oplus x_2\oplus k_1\oplus k_2\\x_1\oplus k_1\end{bmatrix}$	$O_{12,24,16,4}=\begin{bmatrix}x_1\cdot\bar{k}_1\oplus x_2\oplus k_1\oplus k_2\\x_1\oplus k_1\oplus 1\end{bmatrix}$
		$O_{18,6,10,22}=\begin{bmatrix}x_1\cdot\bar{k}_1\oplus x_2\oplus k_1\oplus k_2\oplus 1\\x_1\oplus k_1\end{bmatrix}$	$O_{24,12,4,16}=\begin{bmatrix}x_1\cdot\bar{k}_1\oplus x_2\oplus k_1\oplus k_2\oplus 1\\x_1\oplus k_1\oplus 1\end{bmatrix}$

Таблиця 1.6

Четверта група двохоперандних симетричних 2Сі-квантових СЕТ-операцій, синтезованих на основі основі операції $O_1^{4\oplus}$ [76]

Класифікатор операцій		**Операції інверсії**	
		$\begin{bmatrix}0\\0\end{bmatrix}\diagup\begin{bmatrix}1\\0\end{bmatrix}$	$\begin{bmatrix}0\\1\end{bmatrix}\diagup\begin{bmatrix}1\\1\end{bmatrix}$
Базові операції	$F_1=\begin{bmatrix}x_1\\x_2\end{bmatrix}$	$O_1^{4\oplus}=\begin{bmatrix}x_1\cdot(\overline{k_1\oplus k_2})\oplus x_2\cdot(k_1\oplus k_2)\oplus k_1\\x_1\cdot(k_1\oplus k_2)\oplus x_2\cdot(\overline{k_1\oplus k_2})\oplus k_2\end{bmatrix}$	$O_7^{4\oplus}=\begin{bmatrix}x_1\cdot(\overline{k_1\oplus k_2})\oplus x_2\cdot(k_1\oplus k_2)\oplus k_1\\x_1\cdot(k_1\oplus k_2)\oplus x_2\cdot(\overline{k_1\oplus k_2})\oplus k_2\oplus 1\end{bmatrix}$
		$O_{13}^{4\oplus}=\begin{bmatrix}x_1\cdot(\overline{k_1\oplus k_2})\oplus x_2\cdot(k_1\oplus k_2)\oplus k_1\oplus 1\\x_1\cdot(k_1\oplus k_2)\oplus x_2\cdot(\overline{k_1\oplus k_2})\oplus k_2\end{bmatrix}$	$O_{19}^{4\oplus}=\begin{bmatrix}x_1\cdot(\overline{k_1\oplus k_2})\oplus x_2\cdot(k_1\oplus k_2)\oplus k_1\oplus 1\\x_1\cdot(k_1\oplus k_2)\oplus x_2\cdot(\overline{k_1\oplus k_2})\oplus k_2\oplus 1\end{bmatrix}$
	$F_2=\begin{bmatrix}x_1\oplus x_2\\x_2\end{bmatrix}$	$O_2^{4\oplus}=\begin{bmatrix}x_1\oplus x_2\oplus k_1\oplus k_2\\x_1\cdot(k_1\oplus k_2)\oplus x_2\cdot(\overline{k_1\oplus k_2})\oplus k_2\end{bmatrix}$	$O_8^{4\oplus}=\begin{bmatrix}x_1\oplus x_2\oplus k_1\oplus k_2\\x_1\cdot(k_1\oplus k_2)\oplus x_2\cdot(\overline{k_1\oplus k_2})\oplus k_2\oplus 1\end{bmatrix}$
		$O_{14}^{4\oplus}=\begin{bmatrix}x_1\oplus x_2\oplus k_1\oplus k_2\oplus 1\\x_1\cdot(k_1\oplus k_2)\oplus x_2\cdot(\overline{k_1\oplus k_2})\oplus k_2\end{bmatrix}$	$O_{20}^{4\oplus}=\begin{bmatrix}x_1\oplus x_2\oplus k_1\oplus k_2\oplus 1\\x_1\cdot(k_1\oplus k_2)\oplus x_2\cdot(\overline{k_1\oplus k_2})\oplus k_2\oplus 1\end{bmatrix}$
	$F_3=\begin{bmatrix}x_1\\x_1\oplus x_2\end{bmatrix}$	$O_3^{4\oplus}=\begin{bmatrix}x_1\cdot(\overline{k_1\oplus k_2})\oplus x_2\cdot(k_1\oplus k_2)\oplus k_1\\x_1\oplus x_2\oplus k_1\oplus k_2\end{bmatrix}$	$O_9^{4\oplus}=\begin{bmatrix}x_1\cdot(\overline{k_1\oplus k_2})\oplus x_2\cdot(k_1\oplus k_2)\oplus k_1\\x_1\oplus x_2\oplus k_1\oplus k_2\oplus 1\end{bmatrix}$
		$O_{15}^{4\oplus}=\begin{bmatrix}x_1\cdot(\overline{k_1\oplus k_2})\oplus x_2\cdot(k_1\oplus k_2)\oplus k_1\oplus 1\\x_1\oplus x_2\oplus k_1\oplus k_2\end{bmatrix}$	$O_{21}^{4\oplus}=\begin{bmatrix}x_1\cdot(\overline{k_1\oplus k_2})\oplus x_2\cdot(k_1\oplus k_2)\oplus k_1\oplus 1\\x_1\oplus x_2\oplus k_1\oplus k_2\oplus 1\end{bmatrix}$
Операції перестановок	$F_4=\begin{bmatrix}x_2\\x_1\end{bmatrix}$	$O_4^{4\oplus}=\begin{bmatrix}x_1\cdot(k_1\oplus k_2)\oplus x_2\cdot(\overline{k_1\oplus k_2})\oplus k_2\\x_1\cdot(\overline{k_1\oplus k_2})\oplus x_2\cdot(k_1\oplus k_2)\oplus k_1\end{bmatrix}$	$O_{10}^{4\oplus}=\begin{bmatrix}x_1\cdot(k_1\oplus k_2)\oplus x_2\cdot(\overline{k_1\oplus k_2})\oplus k_2\\x_1\cdot(\overline{k_1\oplus k_2})\oplus x_2\cdot(k_1\oplus k_2)\oplus k_1\oplus 1\end{bmatrix}$
		$O_{16}^{4\oplus}=\begin{bmatrix}x_1\cdot(k_1\oplus k_2)\oplus x_2\cdot(\overline{k_1\oplus k_2})\oplus k_2\oplus 1\\x_1\cdot(\overline{k_1\oplus k_2})\oplus x_2\cdot(k_1\oplus k_2)\oplus k_1\end{bmatrix}$	$O_{22}^{4\oplus}=\begin{bmatrix}x_1\cdot(k_1\oplus k_2)\oplus x_2\cdot(\overline{k_1\oplus k_2})\oplus k_2\oplus 1\\x_1\cdot(\overline{k_1\oplus k_2})\oplus x_2\cdot(k_1\oplus k_2)\oplus k_1\oplus 1\end{bmatrix}$
	$F_5=\begin{bmatrix}x_2\\x_1\oplus x_2\end{bmatrix}$	$O_5^{4\oplus}=\begin{bmatrix}x_1\cdot(k_1\oplus k_2)\oplus x_2\cdot(\overline{k_1\oplus k_2})\oplus k_2\\x_1\oplus x_2\oplus k_1\oplus k_2\end{bmatrix}$	$O_{11}^{4\oplus}=\begin{bmatrix}x_1\cdot(k_1\oplus k_2)\oplus x_2\cdot(\overline{k_1\oplus k_2})\oplus k_2\\x_1\oplus x_2\oplus k_1\oplus k_2\oplus 1\end{bmatrix}$
		$O_{17}^{4\oplus}=\begin{bmatrix}x_1\cdot(k_1\oplus k_2)\oplus x_2\cdot(\overline{k_1\oplus k_2})\oplus k_2\oplus 1\\x_1\oplus x_2\oplus k_1\oplus k_2\end{bmatrix}$	$O_{23}^{4\oplus}=\begin{bmatrix}x_1\cdot(k_1\oplus k_2)\oplus x_2\cdot(\overline{k_1\oplus k_2})\oplus k_2\oplus 1\\x_1\oplus x_2\oplus k_1\oplus k_2\oplus 1\end{bmatrix}$
	$F_6=\begin{bmatrix}x_1\oplus x_2\\x_1\end{bmatrix}$	$O_6^{4\oplus}=\begin{bmatrix}x_1\oplus x_2\oplus k_1\oplus k_2\\x_1\cdot(\overline{k_1\oplus k_2})\oplus x_2\cdot(k_1\oplus k_2)\oplus k_1\end{bmatrix}$	$O_{12}^{4\oplus}=\begin{bmatrix}x_1\oplus x_2\oplus k_1\oplus k_2\\x_1\cdot(\overline{k_1\oplus k_2})\oplus x_2\cdot(k_1\oplus k_2)\oplus k_1\oplus 1\end{bmatrix}$
		$O_{18}^{4\oplus}=\begin{bmatrix}x_1\oplus x_2\oplus k_1\oplus k_2\oplus 1\\x_1\cdot(\overline{k_1\oplus k_2})\oplus x_2\cdot(k_1\oplus k_2)\oplus k_1\end{bmatrix}$	$O_{24}^{4\oplus}=\begin{bmatrix}x_1\oplus x_2\oplus k_1\oplus k_2\oplus 1\\x_1\cdot(\overline{k_1\oplus k_2})\oplus x_2\cdot(k_1\oplus k_2)\oplus k_1\oplus 1\end{bmatrix}$

Даний метод став основою для побудови ієрархічної інформаційної технології моделювання і дослідження симетричних двохоперандних СЕТ-операцій, які допускають перестановку операндів [82].

Структура інформаційної системи яка реалізує ієрархічну інформаційну технологію моделювання і дослідження симетричних двохоперандних СЕТ-операцій, які допускають перестановку операндів включає в себе три рівні ієрархії (рис.1.4) [83]:

- рівень одноопераднних СЕТ-операцій;
- рівень двохоперандних СЕТ-операцій;
- рівень груп СЕТ-операцій, або псевдовипадкових послідовностей СЕТ-операцій.

Кожен наступний рівень базується на результатах синтезованих на попередньому рівні. Правила синтезу СЕТ-операцій на кожному рівні різні проте структура системи контролю результатів синтезу одна і представлена на рис.1.5. [83] .

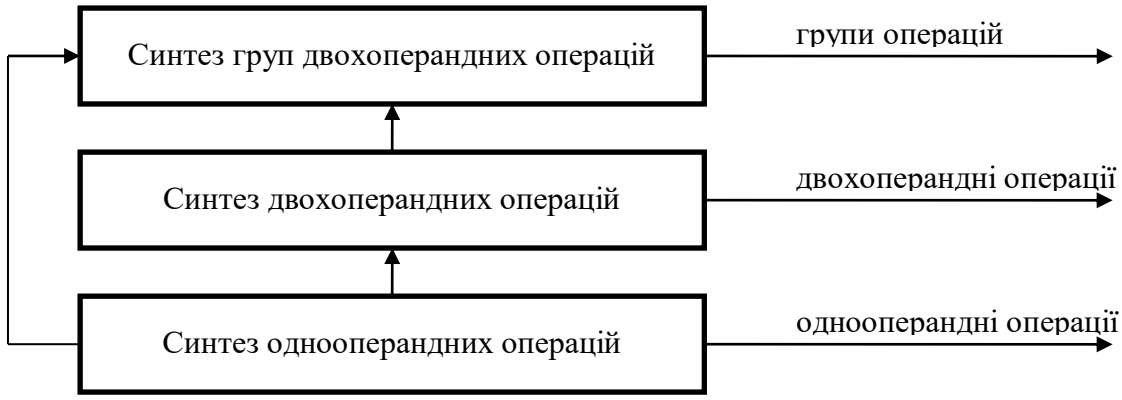

Рис. 1.4. Ієрархічна структура технології моделювання симетричних двохоперандних операцій криптографічного кодування [83]

Структура інформаційної системи для реалізації технології моделювання симетричних двохоперандних операцій криптографічного кодування має включати [83]: підсистему введення-виведення даних (моделей, параметрів, оцінок, запитів системи тощо); підсистему керування режимами роботи; підсистему пошуку (введення) базових симетричних

двохоперандних операцій; базу даних; базу знань; підсистему синтезу операцій; підсистему статистичного дослідження та класифікації операцій; підсистему генерації послідовностей симетричних двохоперандних операцій.

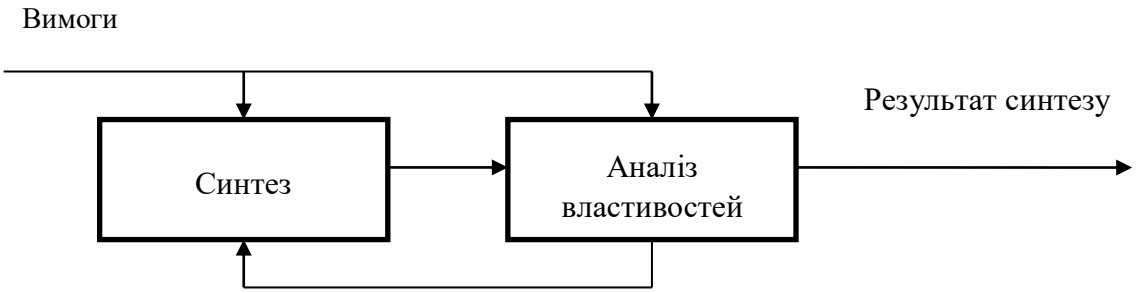

Рис. 1.5. Структура системи контролю результатів синтезу [83]

Правильне встановлення зв’язків між алгоритмами та програмами, що реалізують ієрархічні рівні, необхідне для ефективної роботи інформаційної технології, можливе лише за умови вибору єдиного підходу для представлення [83]: елементарних функцій; одноопераднних операцій; двохоперандних симетричних операцій; послідовностей двохоперандних симетричних операцій.

Ця інформаційна система дозволяє вирішувати значну частину завдань, пов’язаних з моделюванням і оцінкою результатів, які виникають під час дослідження симетричних двохоперандних операцій криптографічного кодування. Проте вона не дозволяє моделювання і досліджувати несиметричних двохоперандних операцій криптографічного кодування.

1.5. Мета і задачі дослідження

Якість та ефективність малоресурсних систем потокового шифрування можна покращувати за рахунок застосування двохоперандних СЕТ-операцій, що забезпечують покращення характеристик криптографічного перетворення без значних ресурсних витрат. У низці наукових праць [76, 84–87] доведено ефективність використання СЕТ-операцій, побудованих на основі додавання за модулем два. Особливу роль серед них відіграють операції

криптографічного перетворення інформації, які допускають перестановку операндів. Саме ця властивість дає можливість реалізовувати у системах як блокового так і потокового шифрування як шифрування вхідних даних, так і шифрування гамуючої послідовності [33].

Особливе місце серед СЕТ-операцій належить операціям криптоперетворення, які допускають перестановку операндів. Їх важливість обумовлена тим, що такі СЕТ-операції забезпечують більш гнучку реалізацію процесів криптографічного перетворення у системах потокового шифрування. Можливість зміни порядку операндів дозволяє ефективно виконувати як шифрування вхідної інформації, так і перетворення гамуючої послідовності, в наслідок чого може бути підвищена функціональність і адаптивність систем потокового шифрування при збереженні невисоких ресурсних витрат [33].

Для виявлення кортежів двохрозрядних двохоперандних СЕТ-операцій, що допускають перестановку операндів, було проведено обчислювальний експеримент, у межах якого попередньо здійснено нумерацію групи двохрозрядних одноопераднихних СЕТ-операцій, поданих у табл. 1.1 [76, 86].

В роботах [76, 88, 89] наведені результати моделювання 576 двохрозрядних двохоперандних СЕТ-операцій, що допускають перестановку операндів, серед яких 96 симетричних операцій, що є комутативними ($C(x, y) = C(y, x)$) та 480 несиметричних операцій, що є некомутативними ($C(x, y) = C(y, x)$).

В роботах [66, 76, 88] Синтезовані в результаті експерименту СЕТ-операції було класифіковано на 24 групи з урахуванням перестановки результатів, серед яких в подальших дослідженнях [90, 91] виокремлено 4 групи симетричних і 20 груп несиметричних операцій. У роботах [89, 91] досліджено симетричні двохрозрядні двохоперандні СЕТ-операції та виділено серед несиметричних операцій 6 груп подвійного циклу і 14 груп потрійного циклу. Водночас некомутативні СЕТ-операції, що допускають перестановку операндів, залишаються недостатньо вивченими, хоча саме

вони дають змогу реалізувати потокові шифри для взаємного криптографічного перетворення вхідних даних і гамуючої послідовності [33].

За результатами експерименту на основі 24 одноопераднних 2Сі-квантовтових СЕТ-операцій за результатами експерименту існує 24 групи двохоперандних СЕТ-операцій які допускають перестановку операндів, по 24 СЕТ-операції в кожній групі. Можна допустити, що на основі 40320 [41, 45] одноопераднних 3Сі-квантовтових СЕТ-операцій може бути побудовано до 40320 груп двохоперандних СЕТ-операцій які допускають перестановку операндів, по 40320 СЕТ-операції в кожній групі. Можна також допустити що на що на основі 2092289888000 [41, 92] одноопераднних 4Сі-квантовтових СЕТ-операцій може бути побудовано до 2092289888000 груп двохоперандних СЕТ-операцій які допускають перестановку операндів, по 2092289888000 СЕТ-операції в кожній групі.

Якщо навіть кількість груп двохоперандних СЕТ-операцій які допускають перестановку операндів, не співпадає, а пропорційна кількості одноопераднних СЕТ-операцій з яких будуються то дослідити і визначити підгрупи СЕТ-операцій для застосування в потокових шифрах можна лише при використанні інформаційних систем та спеціалізованої технології для вирішення задач дослідження і проектування.

Дана технологія повинні будуватися на основі відомої технології дослідження і проектування симетричних СЕТ-операцій які допускають перестановку операндів. Крім того, дана технологія повинна забезпечити моделювання як симетричних так і не симетричних двохоперандних СЕТ-операцій, які допускають перестановку операндів. Дана технологія повинна забезпечити можливість дослідження генераторів псевдовипадкових послідовностей симетричних двохоперандних СЕТ-операцій, генераторів псевдовипадкових послідовностей несиметричних двохоперандних СЕТ-операцій, а також генерувати псевдовипадкові послідовності із симетричних і несиметричних двохоперандних СЕТ-операцій, які допускають перестановку операндів.

Виходячи з цього метою дисертаційної роботи є підвищення продуктивності дослідження СЕТ-операцій при побудові перспективних стійких алгоритмів потокового шифрування на основі розширення можливостей ієрархічної інформаційної системи моделювання і дослідження СЕТ-операцій за рахунок встановлення нових і уточнення існуючих взаємозв'язків між моделями ієрархічних рівнів які в сукупності забезпечать автоматизований синтез і аналіз симетричних та несиметричних одноопераднних і багатоопераднних СЕТ-операцій, а також генераторів їх псевдовипадкових послідовностей для потокового СЕТ-шифрування.

Для досягнення поставленої мети в дисертаційному дослідженні необхідно вирішити наступні завдання:

1. Удосконалити технології побудови удосконалених моделей некомутативних двохрозрядних двохоперандних СЕТ-операції за результатами обчислювального експерименту;

2. Удосконалити метод синтезу двохоперандних двохрозрядних операцій криптографічного перетворення для забезпечення можливості побудови як симетричних так і несиметричних СЕТ-операцій;

3. Удосконалити метод побудови двохрозрядних двохоперандних операцій які допускають перестановку операндів на основі об'єднання двохрозрядних одноопераднних операцій криптографічного перетворення;

4. Розробити модель ієрархічної інформаційної системи моделювання і дослідження симетричних і несиметричних СЕТ-операцій реалізація якої забезпечить побудову перспективних стійких мало ресурсних алгоритмів потокового шифрування.

Висновки до розділу 1

1. За результатами проведеного аналізу встановлено, що розбудова мало ресурсних систем криптографічного захисту інформації на сьогоднішній день відноситься до найбільш актуальних задач розвитку захищених інформаційних і телекомунікаційних систем. Проаналізовано

основні напрямки розвитку і області застосування мало ресурсної криптографії.

2. Проведено детальний аналіз відомих результатів дослідження СЕТ-операцій і алгоритмів СЕТ-шифрування, які відносяться до мало ресурсної криптографії.

3. Проаналізовано сучасний стан розвитку автоматизованих інформаційних систем моделювання і дослідження СЕТ-операцій та алгоритмів шифрування. Визначено їх переваги і недоліки.

4. Сформульована мета і завдання дисертаційного дослідження.

5. Результати розділу опубліковані в [14].

РОЗДІЛ 2. НЕКОМУТАТИВНІ ДВОХРОЗРЯДНІ ДВОХОПЕРАНДНІ СЕТ-ОПЕРАЦІЇ ЯКІ ДОПУСКАЮТЬ ПЕРЕСТАНОВКУ ОПЕРАНДІВ

2.1. Особливості застосування несиметричних двохоперандних СЕТ-операцій, які допускають перестановку операндів в потокових системах шифрування

Підвищення якості криптосистем можливе за рахунок збільшення варіативності крипто алгоритмів шляхом застосування в них додатково несиметричних СЕТ-операцій. Застосовувати СЕТ-операції представлені кортежами вимагає зберігання в пам’яті таблиць істинності, що не дозволяє застосовувати їх в мало ресурсній криптографії, крім того це забезпечить криптоперетворення інформації представленої лише на рівні біт. Доцільно для практичної реалізації несиметричних СЕТ-операцій перейти від таблиць істинності до моделей, що забезпечить можливість застосування даних операцій як на апаратному так і програмному рівнях [14, 93].

Серед несиметричних двохоперандних СЕТ-операцій особливе місце займають СЕТ-операції, які допускають перестановку операндів [11].

Відповідно до визначення [33] двохоперандна СЕТ-операція представляє собою кортеж одноопераднних операцій які реалізують перетворення першого операнда в залежності від значення другого операнда.

В несиметричних операціях, так як

$$C(x, y) \neq C(y, x), \tag{2.1}$$

то перестановка операндів місцями приводить до зміни результату крипто перетворення [33] В моделі позначено: x - значення першого операнда; y - значення другого операнда.

Розглянемо зміну алгоритму криптографічного перетворення при перестановці операндів місцями на прикладі.

Нехай криптографічне перетворення реалізується на основі моделі:

$$C(x, y) = \begin{cases} \begin{bmatrix} x_1 \oplus 1 \\ x_2 \end{bmatrix}, \text{ якщо } y_1 = 0;\ y_2 = 0 \\ \begin{bmatrix} x_1 \oplus 1 \\ x_2 \oplus 1 \end{bmatrix}, \text{якщо } y_1 = 0;\ y_2 = 1 \\ \begin{bmatrix} x_1 \\ x_2 \oplus 1 \end{bmatrix}, \text{ якщо } y_1 = 1;\ k_2 = 0 \\ \begin{bmatrix} x_1 \\ x_2 \end{bmatrix}, \text{якщо } y_1 = 1;\ y_2 = 1 \end{cases} \tag{2.2}$$

Модель несиметричної двохоперандної СЕТ-операції (2.2) отримана за результатами обчислювального експерименту [89]. При побудові дискретних моделей СЕТ- операції було використано технологію побудови двох розрядних двохоперандних операцій строгого стійкого криптографічного кодування, наведену в [94].

Переставивши в моделі несиметричної двохоперандної СЕТ-операції (2.2) операнди місцями отримаємо:

$$C(y, x) = \begin{cases} \begin{bmatrix} y_1 \oplus 1 \\ y_2 \end{bmatrix}, \text{ якщо } x_1 = 0;\ x_2 = 0 \\ \begin{bmatrix} y_1 \oplus 1 \\ y_2 \oplus 1 \end{bmatrix}, \text{якщо } x_1 = 0;\ x_2 = 1 \\ \begin{bmatrix} y_1 \\ y_2 \oplus 1 \end{bmatrix}, \text{ якщо } x_1 = 1;\ x_2 = 0 \\ \begin{bmatrix} y_1 \\ y_2 \end{bmatrix}, \text{якщо } x_1 = 1;\ x_2 = 1 \end{cases} = \begin{cases} \begin{bmatrix} x_1 \oplus 1 \\ x_1 \oplus x_2 \end{bmatrix}, \text{ якщо } y_1 = 0;\ y_2 = 0 \\ \begin{bmatrix} x_1 \oplus 1 \\ x_1 \oplus x_2 \oplus 1 \end{bmatrix}, \text{якщо } y_1 = 0;\ y_2 = 1 \\ \begin{bmatrix} x_1 \\ x_1 \oplus x_2 \end{bmatrix}, \text{ якщо } y_1 = 1;\ y_2 = 0 \\ \begin{bmatrix} x_1 \\ x_1 \oplus x_2 \oplus 1 \end{bmatrix}, \text{якщо } y_1 = 1;\ y_2 = 1 \end{cases} \tag{2.3}$$

Як видно з наведеного прикладу перетворення вхідної інформації x, при перестановці операндів місцями буде реалізовано різними СЕТ-операціями.

Розглянемо варіанти використання несиметричних двохоперандних СЕТ-операцій, які допускають перестановку операндів в потокових шифрах.

В потоковому шифруванні криптографічне перетворення вхідної інформації реалізується шляхом додавання до неї гамуючої (γ) послідовності. В якості гамуючої послідовності використовується

псевдовипадкова послідовність, яка повинна бути однаковою як при шифруванні, так і при розшифруванні інформації.

При перестановці операндів місцями одна і та сама несиметрична двохоперандна СЕТ-операція реалізує дві різні моделі криптографічного перетворення інформації (наприклад моделі криптографічного перетворення інформації (2.2) і (2.3)). Тому можна допустити, що двохоперандні СЕТ-операції, які допускають перестановку операндів місцями можуть забезпечити існування двох різних сценаріїв потокового шифрування. В першому сценарію шифрування операнди двохоперандної СЕТ-операції не переставлені місцями. В другому сценарію шифрування операнди двохоперандної СЕТ-операції повинні бути переставленими місцями. Дослідимо дане питання більш детально.

Нехай в двохоперандній СЕТ-операції операнди не переставлялися місцями [14].

Якщо для потокового шифрування використовується двохоперандна СЕТ-операція, то вхідна (відкрита) інформація повинна заноситись в перший операнд, а гамуючи послідовність, під управлінням якої буду перетворюватися вхідна інформація буде заноситися в другий операнд. Відповідно до розглянутого прикладу, шифрування інформації буде реалізовано на основі моделі [10]:

$$C(x,\gamma)=\begin{cases}\begin{bmatrix}x_1\oplus 1\\ x_2\end{bmatrix}, \text{ якщо } \gamma_1=0;\ \gamma_2=0\\ \begin{bmatrix}x_1\oplus 1\\ x_2\oplus 1\end{bmatrix}, \text{якщо } \gamma_1=0;\ \gamma_2=1\\ \begin{bmatrix}x_1\\ x_2\oplus 1\end{bmatrix}, \text{ якщо } \gamma_1=1;\ \gamma_2=0\\ \begin{bmatrix}x_1\\ x_2\end{bmatrix}, \text{якщо } \gamma_1=1;\ \gamma_2=1\end{cases} \tag{2.4}$$

Так як СЕТ-операції криптографічного кодування можуть бути як симетричними, так і несиметричними [33, 74], то для розшифрування інформації використовувати обернену СЕТ-оперцію. Так як в СЕТ-операції

(2.2) всі одноопераднідні операції будуть симетричним, то і двохоперандна операція буде симетричною [33, 95]:

$$C'(x,\gamma)=C(x,\gamma)=\begin{cases}\begin{bmatrix}x_1\oplus 1\\ x_2\end{bmatrix}, \text{ якщо } \gamma_1=0;\ \gamma_2=0\\ \begin{bmatrix}x_1\oplus 1\\ x_2\oplus 1\end{bmatrix}, \text{якщо } \gamma_1=0;\ \gamma_2=1\\ \begin{bmatrix}x_1\\ x_2\oplus 1\end{bmatrix}, \text{ якщо } \gamma_1=1;\ \gamma_2=0\\ \begin{bmatrix}x_1\\ x_2\end{bmatrix}, \text{якщо } \gamma_1=1;\ \gamma_2=1\end{cases} \quad (2.5)$$

Якщо СЕТ-операція для потокового шифрування буде несиметричною, тобі $C'(x,\gamma)\neq C(x,\gamma)$ [33].

Відповідно до розглянутого прикладу шифрування відкритої інформацію несиметричною СЕТ-операцією, яка допускає перестановку операндів реалізовано моделлю (2.4). Шифрування проводиться під управлінням гамуючої послідовності. Після реалізації даної моделі буде отримана зашифрована (закрита) інформація. Розшифрування зашифрованої (закритої) інформації реалізується оберненою несиметричною СЕТ-операцією, яка допускає перестановку операндів реалізовано моделлю (2.5). Разшифрування інформації також проводиться під управлінням гамуючої послідовності. Після реалізації даної моделі буде отримана розшифрована (відкрита) інформація.

Структура пристрою який реалізує перший сценарій потокового шифрування/розшифрування інформації наведена на рис.2.1. [11]

Пристрій працює наступним чином. При шифруванні на вхід блоку перетворення інформації поступає відкрита інформація. На вхід блоку формування інформації поступає гамуючи послідовність. В залежності від значення біт гамуючої послідовності в блоці формування операцій буде визначено порядковий номер одноопераднідної СЕТ операції, для реалізації крипто перетворення, переданий у блок перетворення інформації. По своїй

сутності блок формування операцій представляє собою дешифратор коду гамуючої послідовності (γ). В блоці перетворення інформації поступивши відкрита інформація буде зашифрована одноопераднною СЕТ-операцією із кортежу двохоперандної СЕТ-операції, відповідно до її порядкового номеру, який поступив з блоку формування операції. З виходу блоку перетворення інформації на вихід пристрою поступить закрита (зашифрована) інформація.

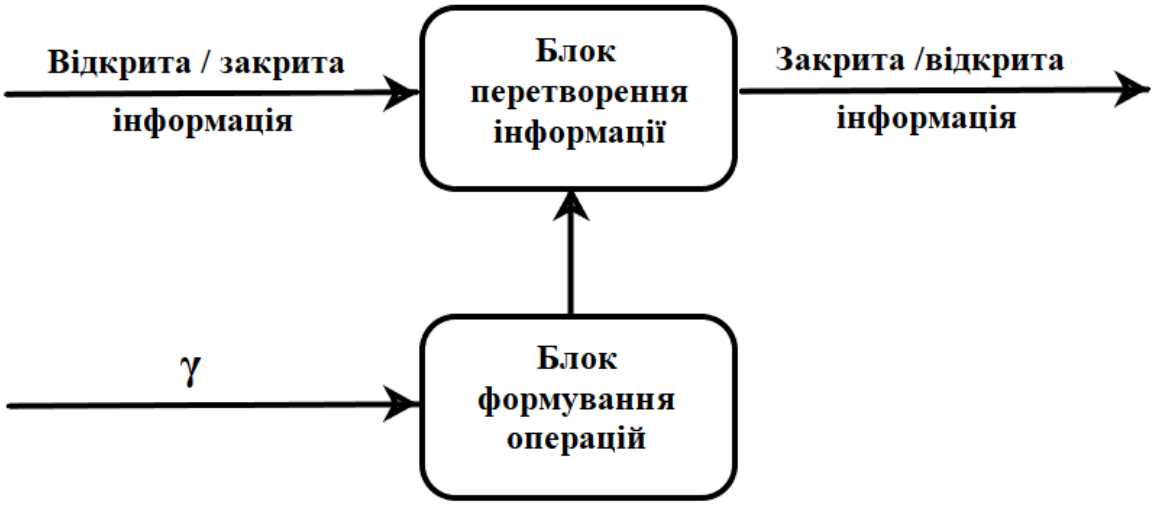

Рис. 2.1 Структура пристрою який реалізує перший сценарій потокового шифрування [11]

При розшифруванні закритої інформації пристрій працює наступним чином. При розшифруванні на вхід блоку перетворення інформації поступає закрита інформація. На вхід блоку формування інформації поступає гамуючи послідовність. В залежності від значення біт гамуючої послідовності в блоці формування операцій буде визначено порядковий номер оберненої одноопераднної СЕТ-операції. Отриманий порядковий номер з визоду блоку буде переданий у блок перетворення інформації. Так як гамуючи послідовність при шифруванні і розшифруванні однакові то в блок перетворення інформації поступить такий самий порядковий номер одноопераднної СЕТ-операції. В блоці перетворення інформації поступивши закрита інформація буде розшифрована оберненою одноопераднною СЕТ-операцією із кортежу оберненої двохоперандної СЕТ-операції, відповідно до

її порядкового номеру, який поступив з блоку формування операції. З виходу блоку перетворення інформації на вихід пристрою поступить відкрита (розшифрована) інформація. [11]

В першому сценарії шифрування можуть бути використанні як симетричні так і несиметричні операції криптоперетворення.

В другому сценарії шифрування операнда поміняно місцями, і над гамуючою послідовністю (перший операнда) буде виконана одноопераднда операція криптоперетворення, яку визначає відкрита інформація. В канал передачі інформації буде передаватися не зашифрована інформація, а зашифрована гамуюча послідовність. Розшифрування інформації проводиться шляхом криптоперетворення гамуючої послідовності одноопераднними операціями криптоперетворення, які визначаються зашифрованою гамуючою послідовністю. Структура другого сценарію потокового шифрування наведена на рис.2.2 [11]. Дана структура шифрування може бути реалізована лише при використанні несиметричних операцій криптоперетворення.

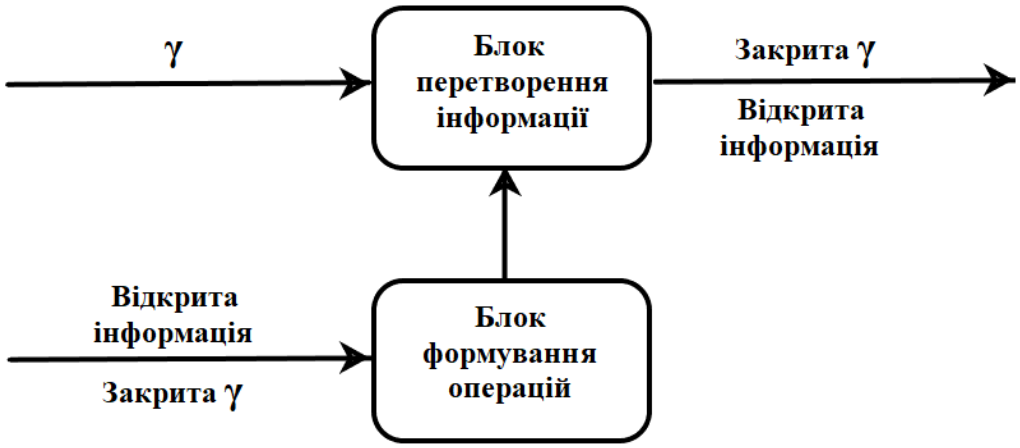

Рис. 2.2 Структура другого сценарію потокового шифрування [11]

Для застосування запропонованих структур потокового шифрування необхідно знайти взаємозв’язок між прямими і оберненими операціями при потоковому шифруванні.

Реалізувати другий сценарій потокового шифрування можна на основі використання не комутативних СЕТ-операцій подвійного, або потрійного циклу.

Розглянемо сутність СЕТ-операцій подвійного і потрійного циклу і визначимося з термінологією.

Будь яка СЕТ-операція переставляє собою дискретну модель однієї, або декількох таблиць підстановки [33]. Одноопераднда СЕТ-операція реалізує одну таблицю підстановки. Для одноопераднодної СЕТ-операції $C(x)$ існує обернена СЕТ-операція $C'(x)$ така, що $C'(C(x)) = x$. Двохоперандна операндна СЕТ-операція представляє собою кортеж одноопераднодних операцій $C(x, y) = C(C_1(x), C_2(x), C_3(x),..., C_n(x))$ і реалізує декілька таблиць підстановки. Для двохоперандної СЕТ-операції $C(x, y)$ існує обернена СЕТ-операція $C'(x, y) = C(C_1'(x), C_2'(x), C_3'(x),..., C_n'(x))$ така, що $C'(C(x, y), y) = x$.

Серед двохоперандних СЕТ-операцій існують операції які допускають перестановку операндів. За результатами обчислювального експерименту [66] було виявлено 24 групи двохрозрядних двохоперандних СЕТ-операцій з точністю до перестановки результатів, які допускають перестановку операндів. Двохоперандна СЕТ-операція $C(x, y)$ допускає перестановку операндів якщо існує СЕТ-операція $C(y, x)$.

Двохоперандна СЕТ-операція $C(x, y)$ буде комутативною, якщо $C(x, y) = C(y, x)$ [11]. Двохоперандна комутативна СЕТ-операція $C(x, y)$ буде симетричною, якщо $C(x, y) = C(y, x) = C'(x, y) = C'(y, x)$. За результатами обчислювального експерименту було побудовано 4 групи симетричних комутативних СЕТ-операцій з точністю до перестановки результату перетворення.

Двохоперандна СЕТ-операція $C(x, y)$ буде не комутативною, якщо $C(x, y) \neq C(y, x)$ [33]. За результатами обчислювального експерименту було побудовано 20 груп не комутативних СЕТ-операцій з точністю до

перестановки результату перетворення. Саме для цих груп операцій і були введені поняття подвійного і потрійного циклу [78].

Не комутативна двохоперандна СЕТ-операція $C(x, y)$ буде СЕТ-операцією подвійного циклу, якщо $C(x, y) \in C^*(x, y)$; $C(y, x) \in C^*(x, y)$, де $C^*(x, y)$ - група операцій з точністю до перестановки результату. В не комутативних двохоперандних СЕТ-операціях подвійного циклу прямі і обернені операції належать до однієї і тієї групи операцій з точністю до перестановки результатів [96].

Серед не комутативних двохоперандних СЕТ-операціях подвійного циклу доцільно виділити групу взаємно обернених операцій [14]. Не комутативна двохоперандна СЕТ-операція $C(x, y)$ подвійного циклу буде взаємно оберненою, якщо $C(y, x) = C'(x, y)$. Так як $C(x, y) \in C^*(x, y)$ і $C(y, x) \in C^*(x, y)$, то буде справедлива рівність $C(x, y) = C'(y, x)$. Для взаємно обернених не комутативних двохоперандних СЕТ-операцій подвійного циклу перестановка операндів забезпечує взаємне перетворення прямих і обернених операції. Якщо інформація була зашифрована прямою операцією (без перестановки операндів) то вона буде розшифрована оберненою операцією (з переставленими операндами). Якщо інформація була зашифрована оберненою операцією (з переставленими операндами) то вона буде розшифрована прямою операцією (без перестановки операндів).

Множина не комутативних взаємно обернених двохоперандних СЕТ-операцій подвійного циклу є підмножиною не комутативних двохоперандних СЕТ-операцій потрійного циклу [96]. За результатами обчислювального експерименту множини не комутативних двохоперандних СЕТ-операцій подвійного циклу утворюють групи СЕТ-операцій з точністю до перестановки результатів [2]. Дослідимо можливість синтезу груп не комутативних двохрозрядних двохоперандних СЕТ-операціях подвійного циклу.

Не комутативна двохоперандна СЕТ-операція $C(x, y)$ буде СЕТ-операцією потрійного циклу, якщо $C(x, y) \in C^*(x, y)$; $C(y, x) \notin C^*(x, y)$, де $C^*(x, y)$ - група операцій з точністю до перестановки результату [96]. В не комутативних двохоперандних СЕТ-операціях потрійного циклу перестановка операндів приводить до необхідності пошуку оберненої операції серед інших груп операцій з точністю до перестановки результату [96].

2.2. Компьютерне моделювання комутативних і не комутативних СЕТ-операцій подвійного і потрійного циклу

Практична реалізація другого сценарію шифрування вимагає проведення дослідження не комутативних двохоперандних СЕТ-операціцй. Для проведення дослідження по встановлення взаємозвязків між прямими і обереними некомутативними СЕТ-операціями необхідно отримати класифіковані множини даних операцій за результатами обчислювального експерименту. Крім того в процесі моделювання необхідно реалізувати пошук і сортування двохоперандних СЕТ-операцій на комутативні і не комутативні, а не комутативні СЕТ-операції в свою чергу поділити на СЕТ-операції подвійного і потрійного циклу.

Виходячи з цього алгоритм моделювання і класифікації СЕТ-операцій які допускають перестановку операндів повинен включати:

- синтез елементарних функцій;
- синтез одноопераднних СЕТ-операцій;
- синтез двохоперандних СЕТ-операцій;
- класифікацію двохоперандних СЕТ-операцій;
    - перевірка можливості перестановки операндів, для СЕТ-операцій які допускають перестановку операндів:

- перевірка комутативності СЕТ-операції, для не комутативних СЕТ-операцій:
  - визначення групи з точністю до перестановки результату до якої належить СЕТ-операції;
  - визначення значення циклу СЕТ-операції;
- збереження СЕТ-операції в базі даних відповідно до визначених показників класифікації.

Блок схема алгоритму моделювання і класифікації СЕТ-операцій які допускають перестановку операндів представлена на рис. 2.3.

Деталізуємо даний алгоритм для синтезу і аналізу двохоперандних двохрозрядних СЕТ-операціях, та визначення циклу не комутативних СЕТ-операцій.

Синтез елементарниз функцій реалізується на рівні табльці істинності. Для цього необхідно в наборі елементарних функцій визначити ті елементарні функції які в таблиці істинності мають однакову кількість нулів і одиниць.

Елементарна функція яка перетворює 2 вхідних Сі-квантів інформації повинна мати в таблиці істинності 2 нулі і 2 одиниці [40]. На основі цього елементарна функція яка використовується в побудові двохрозрядних одноопераднди СЕТ-операцій повинна відповідати умові $\sum_{i=1}^{4} b_i = 2$, де b_i значення i –го рядка таблиці істинності елементарної функції.

Елементарні функції для побудови 2Сі-квантових одноопераднди СЕТ-операцій відомі і їх всього 6. На основі 6 елементарних функцій будуються 24 одноопераднді СЕТ-операції. При цьому взаємозв’язки між прямими і оберненими СЕТ-операціями відомі. Виходячи з цього доцільно побудову елементарних функцій і одноопераднди СЕТ-операції ввести в якості вхідних даних, або представити набором констант, які відобразять моделф СЕТ-операцій як таблиці істинності.

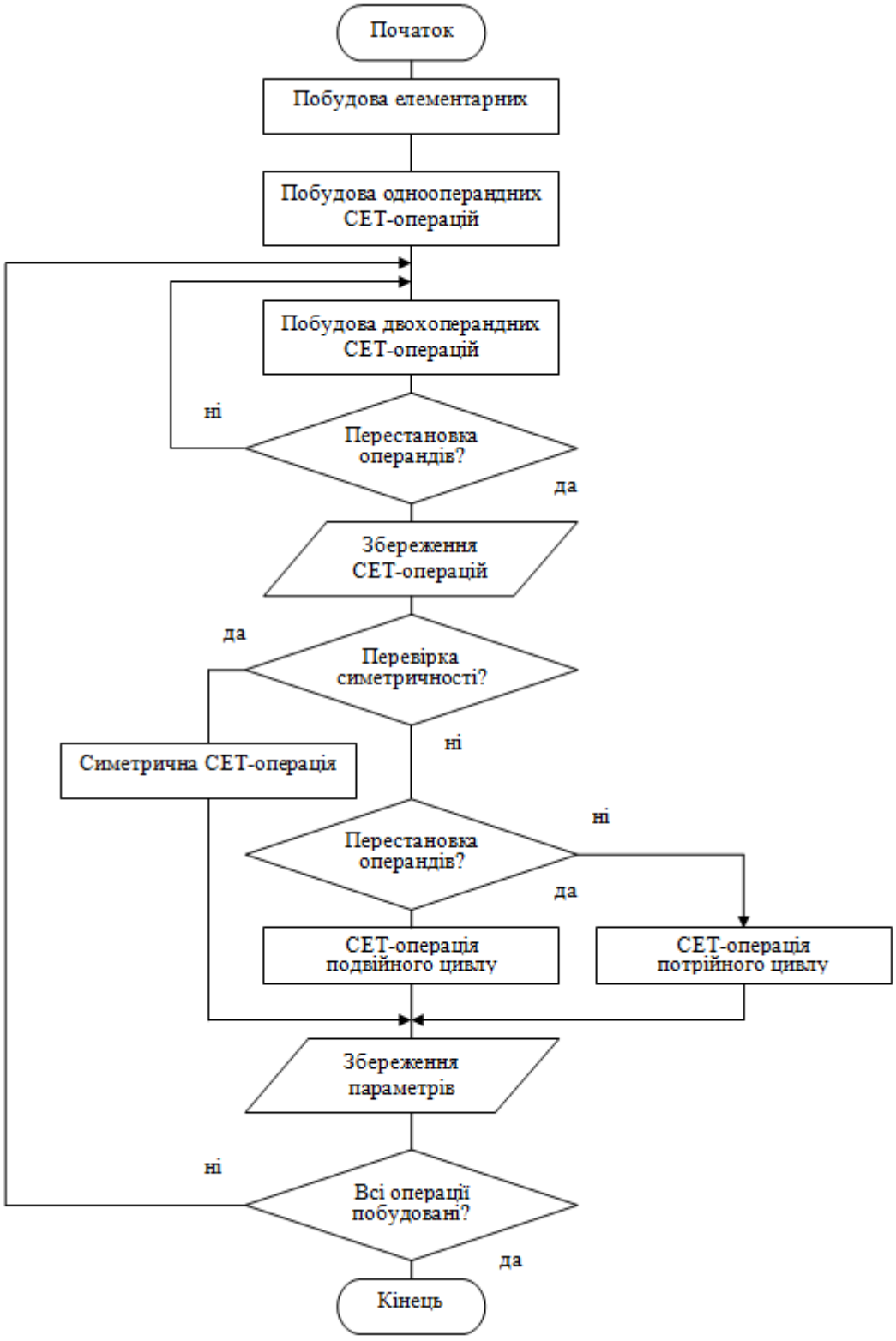

Рис. 2.3. Блок схема алгоритму моделювання і класифікації СЕТ-операцій які допускають перестановку операндів

Побудова двохоперендної 2Сі-квантової СЕТ-операції представляє собою поєднання чотирьох одноопераднних СЕТ-операцій в двохоперандну. Програмна модель 2Сі-квантової двохоперандної СЕТ-операції представляє мобою двохвимірний масив (таблицю) з результатами перетворення чотирьох одноопераднних СЕТ-операцій. Для простоти реалізації програми доцільно результатами перетворення чотирьох одноопераднних СЕТ-операцій представити в четверичній системі числення (від 0 до 3). Двохоперандна СЕТ-операція забезпечує можливість перестановки операндів ,якщо в рядках і стовпціх таблиці істинності двохоперандної операції будуть представлені таблиці істинності одноопераднних операцій. Властивість таблиці істинності одноопераднної СЕТ-операції полягає в тому що вона взаємозв'язок маж вхідними даними і результатами перетворення. Так як вхідні дані в таблиці істинності не повторяються, то не будуть повторятися і результати перетворення. Для того щоб в двохоперандній СЕТ-операції можна було переставляти операнди в її таблиці істинності результати перетворення в рядках а також в стовпцях не повинні повторюватися.

Нехай c_{ij} - результат перетворення i-ю 2Сі-квантовою одноопераднною СЕТ-операцією j-го значення вхідних даних. Даний результат буде знаходитись на перетині i-го рядка і j-го стовпця таблиці істинності. При програмній реалізації таблиці істинності даний результат матиме указники зміщення i і j відносно початку двохвимірного масиву.

Двохоперандна 2Сі-квант СЕТ-операція допускає перестановку операндів за умови $\begin{cases} c_{ij} \neq c_{lj} \\ c_{ij} \neq c_{il} \end{cases}$, де $i, j, l \in \{1; 2; ...; 4\}$ [33]. Дана модель була взята для визначення можливості перестановки операндів в двохоперандній СЕТ-операції.

Двохоперндна 2Сі-квант СЕТ-операція буде комутативною, якщо її таблиця істинності буде симетричною відносно діагоналі в задовольнятиме умові $c_{ij} = c_{ji}$, де $i, j \in \{1; 2; ...; 4\}$ [79]. Якщо хоч один результат перевірки

беде відповідати умові $c_{ij} \neq c_{ji}$, де $i, j \in \{1; 2; ...; 4\}$. Дані моделі і було взято за основу для поділу 2Сі-квантових СЕТ-операцій на комутативні і не комутативні.

Для поділу двохоперандних не комутативних СЕТ-операцій на операції подвійного циулу і протрійного циклу використаємо модель синтезу групи СЕТ-операцій з точністю до результату перетворення $C_i(x, y) = C_i(C(x, y))$ [33]. Відповідно до даної моделі до групи СЕТ-операцій з точністю до перестановки результата входять лише СЕТ-операції, в яких таблиці істинності взаємозв'язані підстановкою результатів. Другими словами таблиці істинності двох двохоперандних СЕТ-операцій, які належіть до групи операцій точністю до перестановки будуються шляхом однозначної підстановки значень результату в шаблон операції без модифікації шаблону. В якості шаблону можна взяти будь яку СЕТ-операцію з даної групи. Якщо пряма і обернена не комутативні СЕТ-операції належать до однієї групи, то дані операції будуть СЕТ-операціями подвійного циклу, якщо на то будуть СЕТ-операціями потрійного циклу. Використання прямої 2Сі-квантової СЕТ--операції в якості шаблону для визначення належності оберненої 2Сі-квантової СЕТ-операції до групи операцій з точністю до перестановки результатту перетворення стало основою для поділу на операції подвійного і потрійного циклу.

Результати моделювання двохоперандних 2Сі-квантових СЕТ-операцій які допускають перестановку операндів і їх поділ на комутативні і не комутативні, а такод поділ не комутативних СЕТ-операцій на операції подвійного циклу представлені в додатку 1. В даному додатку всі синтезовані СЕТ-операції поділені на групи операцій з точністю до перестановки результату перетворення.

Отримана на за результатами комп'ютерного моделювання база не комутативних двохоперндних 2Сі-квантових СЕТ-операцій дозволяє перейти до узагальнення результатів обчислювального експерименту і встановлення нових, раніше невідомих взаємозв'язків між СЕТ-операціями.

2.3. Моделювання взаємозв'язків в некомутативних двохоперандних двохрозрядних СЕТ-операціях подвійного циклу при перестановці операндів

Базуючись на результатах обчислювального експерименту буде сформовано модель взаємозв'язків для некомутативних двохоперандних двохрозрядних СЕТ-операцій подвійного циклу що допускають перестановку операндів. Побудова такої моделі дасть змогу реалізувати криптографічні системи, у яких здійснюється шифрування гамуючої послідовності, що забезпечить підтримку другого сценарію потокового шифрування.

Для встановлення взаємозв'язків між двох розрядними двохоперандними СЕТ-операціями подвійного циклу отриманими при перестановці операндів місцями дослідимо групу операцій з точністю до перестановки результату виділену на основі СЕТ-операції $C_{1,7,19,13}(x,y)$ [2]. Дана двохоперандна СЕТ-операція представляє собою кортеж одноопераднних СЕТ-операцій перетворення операнду x ($C_1(x)$; $C_7(x)$; $C_{19}(x)$; $C_{13}(x)$), об'єднаних другим операндом y. За результатами ексеременту СЕТ-операції $C_{1,7,19,13}(x,y)$ відповідає СЕТ операція $C_{3,9,15,21}(x,y)$, так як $C_{3,9,15,21}(x,y)= C_{1,7,19,13}(y,x)$. Взаємозв'язок між СЕТ-операціями перетворення вхідної інформації x, при перестановці операндів місцями позначимо як $C_{1,7,19,13}(x,y) \leftrightarrow C_{3,9,15,21}(x,y)$. Група СЕТ-операцій, яку будемо досліджувати є групою операцій подвійного циклу. Особливість груп операцій подвійного циклу полягає в наявності взаємопов'язаних перетворень, яка полягає в наступному: якщо $C_{1,7,19,13}(x,y) \leftrightarrow C_{3,9,15,21}(x,y)$, то $C_{3,9,15,21}(x,y) \leftrightarrow C_{1,7,19,13}(x,y)$ [2]. В СЕТ-операціях подвійного циклу повторна перестановка операндів місцями приведе до повернення початкової операції: $C_{1,7,19,13}(x,y) \leftrightarrow C_{3,9,15,21}(x,y) \leftrightarrow C_{1,7,19,13}(x,y)$ [2].

Група несиметричних двохрозрядних двохоперандних СЕТ-операцій подвійного циклу, яку будемо досліджувати наведена в табл. 2.1.

Таблиця 2.1

Група несиметричних двохрозрядних двохоперандних СЕТ-операцій подвійного циклу [2]

СЕТ-операція		**СЕТ-операція**	
$C(x,y)$	$C(y,x)$	$C(x,y)$	$C(y,x)$
$C_{1,7,19,13}(x,y)$	$C_{3,9,15,21}(x,y)$	$C_{3,9,15,21}(x,y)$	$C_{1,7,19,13}(x,y)$
$C_{7,1,13,19}(x,y)$	$C_{9,3,21,15}(x,y)$	$C_{9,3,21,15}(x,y)$	$C_{7,1,13,19}(x,y)$
$C_{13,19,7,1}(x,y)$	$C_{15,21,3,9}(y,x)$	$C_{15,21,3,9}(x,y)$	$C_{13,19,7,1}(x,y)$
$C_{19,13,1,7}(x,y)$	$C_{21,15,9,3}(x,y)$	$C_{21,15,9,3}(x,y)$	$C_{19,13,1,7}(x,y)$
$C_{6,18,12,24}(x,y)$	$C_{4,16,22,10}(y,x)$	$C_{4,16,22,10}(x,y)$	$C_{6,18,12,24}(x,y)$
$C_{12,24,6,18}(x,y)$	$C_{10,22,16,4}(x,y)$	$C_{10,22,16,4}(x,y)$	$C_{12,24,6,18}(x,y)$
$C_{18,6,24,12}(x,y)$	$C_{16,4,10,22}(x,y)$	$C_{16,4,10,22}(x,y)$	$C_{18,6,24,12}(x,y)$
$C_{24,12,18,6}(x,y)$	$C_{22,10,4,16}(x,y)$	$C_{22,10,4,16}(x,y)$	$C_{24,12,18,6}(x,y)$
$C_{5,23,17,11}(x,y)$	$C_{2,20,8,14}(x,y)$	$C_{2,20,8,14}(x,y)$	$C_{5,23,17,11}(x,y)$
$C_{11,17,23,5}(x,y)$	$C_{8,14,2,20}(x,y)$	$C_{8,14,2,20}(x,y)$	$C_{11,17,23,5}(x,y)$
$C_{17,11,5,23}(x,y)$	$C_{14,8,20,2}(x,y)$	$C_{14,8,20,2}(x,y)$	$C_{17,11,5,23}(x,y)$
$C_{23,5,11,17}(x,y)$	$C_{20,2,14,8}(x,y)$	$C_{20,2,14,8}(x,y)$	$C_{23,5,11,17}(x,y)$

Застосуємо технологію синтезу і дослідження двохоперандних СЕТ-операцій на основі одноопераднних [97]. Модифіковані варіанти даної технології наведені в [98 - 101].

Дослідимо пару взаємозв'язаних операцій $C_{7,1,13,19}(x,y) \leftrightarrow C_{9,3,21,15}(x,y) = C_{7,1,13,19}(y,x)$ представлену другим рядком табл..2.1.

Побудуємо модель операції $C_{7,1,13,19}(x,y)$ [2]:

$$C_{7,1,13,19}(x,y)=\begin{cases}\begin{bmatrix}x_1\\ x_2\oplus 1\end{bmatrix}, \text{ якщо } y_1=0;\ y_2=0\\ \begin{bmatrix}x_1\\ x_2\end{bmatrix}, \text{якщо } y_1=0;\ y_2=1\\ \begin{bmatrix}x_1\oplus 1\\ x_2\end{bmatrix}, \text{ якщо } y_1=1;\ y_2=0\\ \begin{bmatrix}x_1\oplus 1\\ x_2\oplus 1\end{bmatrix}, \text{якщо } y_1=1;\ y_2=1\end{cases}=\begin{cases}\begin{bmatrix}x_1\\ x_2\oplus 1\end{bmatrix}=\begin{bmatrix}x_1\oplus y_1\\ x_2\oplus y_1\oplus y_2\oplus 1\end{bmatrix}, \text{ якщо } y_1=0;\ y_2=0\\ \begin{bmatrix}x_1\\ x_2\end{bmatrix}=\begin{bmatrix}x_1\oplus y_1\\ x_2\oplus y_1\oplus y_2\oplus 1\end{bmatrix}, \text{якщо } y_1=0;\ y_2=1\\ \begin{bmatrix}x_1\oplus 1\\ x_2\end{bmatrix}=\begin{bmatrix}x_1\oplus y_1\\ x_2\oplus y_1\oplus y_2\oplus 1\end{bmatrix}, \text{ якщо } y_1=1;\ y_2=0\\ \begin{bmatrix}x_1\oplus 1\\ x_2\oplus 1\end{bmatrix}=\begin{bmatrix}x_1\oplus y_1\\ x_2\oplus y_1\oplus k_2\oplus 1\end{bmatrix}, \text{якщо } y_1=1;\ y_2=1\end{cases}. \quad (2.6)$$

На основі виразу (2.6) отримаємо вдосконалену модель операції :

$$C_{7,1,13,19}(x,y)=\begin{bmatrix}x_1\oplus y_1\\ x_2\oplus y_1\oplus y_2\oplus 1\end{bmatrix} \quad (2.7)$$

Побудуємо вдосконалену модель операції $C_{9,3,21,15}(x,y)$:

$$C_{9,3,21,15}(x,y)=\begin{cases}\begin{bmatrix}x_1\\ x_1\oplus x_2\oplus 1\end{bmatrix}, \text{ якщо } y_1=0;\ y_2=0\\ \begin{bmatrix}x_1\\ x_1\oplus x_2\end{bmatrix}, \text{ якщо } y_1=0;\ y_2=1\\ \begin{bmatrix}x_1\oplus 1\\ x_1\oplus x_2\oplus 1\end{bmatrix}, \text{ якщо } y_1=1;\ y_2=0\\ \begin{bmatrix}x_1\oplus 1\\ x_1\oplus x_2\end{bmatrix}, \text{ якщо } y_1=1;\ y_2=1\end{cases}=\begin{cases}\begin{bmatrix}x_1\\ x_1\oplus x_2\oplus 1\end{bmatrix}=\begin{bmatrix}x_1\oplus y_1\\ x_1\oplus x_2\oplus y_2\oplus 1\end{bmatrix}, \text{ якщо } y_1=0;\ y_2=0\\ \begin{bmatrix}x_1\\ x_1\oplus x_2\end{bmatrix}=\begin{bmatrix}x_1\oplus y_1\\ x_1\oplus x_2\oplus y_2\oplus 1\end{bmatrix}, \text{ якщо } y_1=0;\ y_2=1\\ \begin{bmatrix}x_1\oplus 1\\ x_1\oplus x_2\oplus 1\end{bmatrix}=\begin{bmatrix}x_1\oplus y_1\\ x_1\oplus x_2\oplus y_2\oplus 1\end{bmatrix}, \text{ якщо } y_1=1;\ y_2=0\\ \begin{bmatrix}x_1\oplus 1\\ x_1\oplus x_2\end{bmatrix}=\begin{bmatrix}x_1\oplus y_1\\ x_1\oplus x_2\oplus y_2\oplus 1\end{bmatrix}, \text{ якщо } y_1=1;\ y_2=1\end{cases} \quad (2.8)$$

Отримана на основі виразу (2.8) вдосконалена модель операції буде представлена:

$$C_{9,3,21,15}(x,y)=\begin{bmatrix}x_1\oplus y_1\\ x_1\oplus x_2\oplus y_2\oplus 1\end{bmatrix} \quad (2.9)$$

Виходячи виразів (2.7) і (2.9) можна стверджувати, що перестановка операндів приведе до реалізації наступних взаємозв'язків між СЕТ-операціями [2]:

$$C_{7,1,13,19}(x,y)=\begin{bmatrix}x_1\oplus y_1\\ x_2\oplus y_1\oplus y_2\oplus 1\end{bmatrix} \Rightarrow C_{7,1,13,19}(y,x)=C_{9,3,21,15}(x,y)=\begin{bmatrix}x_1\oplus y_1\\ x_1\oplus x_2\oplus y_2\oplus 1\end{bmatrix}; \quad (2.10)$$

$$C_{9,3,21,15}(x,y)=\begin{bmatrix}x_1\oplus y_1\\ x_1\oplus x_2\oplus y_2\oplus 1\end{bmatrix} \Rightarrow C_{9,3,21,15}(y,x)=C_{7,1,13,19}(x,y)=\begin{bmatrix}x_1\oplus y_1\\ x_2\oplus y_1\oplus y_2\oplus 1\end{bmatrix}. \quad (2.11)$$

Дослідимо пару взаємозв'язаних операцій $C_{13,19,7,1}(x,y)\leftrightarrow C_{15,21,3,9}(x,y)$ представлену третім рядком табл..2.1 [2].

Побудуємо вдосконалену модель операції $C_{13,19,7,1}(x,y)$:

$$C_{13,19,7,1}(x,y)=\begin{cases}\begin{bmatrix}x_1\oplus 1\\ x_2\end{bmatrix}, \text{ якщо } y_1=0;\ y_2=0\\ \begin{bmatrix}x_1\oplus 1\\ x_2\oplus 1\end{bmatrix}, \text{ якщо } y_1=0;\ y_2=1\\ \begin{bmatrix}x_1\\ x_2\oplus 1\end{bmatrix}, \text{ якщо } y_1=1;\ y_2=0\\ \begin{bmatrix}x_1\\ x_2\end{bmatrix}, \text{ якщо } y_1=1;\ y_2=1\end{cases}=\begin{cases}\begin{bmatrix}x_1\oplus 1\\ x_2\end{bmatrix}=\begin{bmatrix}x_1\oplus y_1\oplus 1\\ x_2\oplus y_1\oplus y_2\end{bmatrix}, \text{ якщо } y_1=0;\ y_2=0\\ \begin{bmatrix}x_1\oplus 1\\ x_2\oplus 1\end{bmatrix}=\begin{bmatrix}x_1\oplus y_1\oplus 1\\ x_2\oplus y_1\oplus y_2\end{bmatrix}, \text{ якщо } y_1=0;\ y_2=1\\ \begin{bmatrix}x_1\\ x_2\oplus 1\end{bmatrix}=\begin{bmatrix}x_1\oplus y_1\oplus 1\\ x_2\oplus y_1\oplus y_2\end{bmatrix}, \text{ якщо } y_1=1;\ y_2=0\\ \begin{bmatrix}x_1\\ x_2\end{bmatrix}=\begin{bmatrix}x_1\oplus y_1\oplus 1\\ x_2\oplus y_1\oplus y_2\end{bmatrix}, \text{ якщо } y_1=1;\ y_2=1\end{cases} \quad (2.12)$$

Вдосконалену модель операції, на основі виразу (2.12), буде представлена виразом:

$$C_{13,19,7,1}(x,y)=\begin{bmatrix}x_1\oplus y_1\oplus 1\\ x_2\oplus y_1\oplus y_2\end{bmatrix} \quad (2.13)$$

Побудуємо вдосконалену модель операції $C_{15,21,3,9}(x,y)$:

$$C_{15,21,3,9}(x,y)=\begin{cases}\begin{bmatrix}x_1\oplus 1\\ x_1\oplus x_2\end{bmatrix}, \text{ якщо } y_1=0;\ y_2=0\\ \begin{bmatrix}x_1\oplus 1\\ x_1\oplus x_2\oplus 1\end{bmatrix}, \text{ якщо } y_1=0;\ y_2=1\\ \begin{bmatrix}x_1\\ x_1\oplus x_2\end{bmatrix}, \text{ якщо } y_1=1;\ y_2=0\\ \begin{bmatrix}x_1\\ x_1\oplus x_2\oplus 1\end{bmatrix}, \text{ якщо } y_1=1;\ y_2=1\end{cases}=\begin{cases}\begin{bmatrix}x_1\oplus 1\\ x_1\oplus x_2\end{bmatrix}=\begin{bmatrix}x_1\oplus y_1\oplus 1\\ x_1\oplus x_2\oplus y_2\end{bmatrix}, \text{ якщо } y_1=0;\ y_2=0\\ \begin{bmatrix}x_1\oplus 1\\ x_1\oplus x_2\oplus 1\end{bmatrix}=\begin{bmatrix}x_1\oplus y_1\oplus 1\\ x_1\oplus x_2\oplus y_2\end{bmatrix}, \text{ якщо } y_1=0;\ y_2=1\\ \begin{bmatrix}x_1\\ x_1\oplus x_2\end{bmatrix}=\begin{bmatrix}x_1\oplus y_1\oplus 1\\ x_1\oplus x_2\oplus y_2\end{bmatrix}, \text{ якщо } y_1=1;\ y_2=0\\ \begin{bmatrix}x_1\\ x_1\oplus x_2\oplus 1\end{bmatrix}=\begin{bmatrix}x_1\oplus y_1\oplus 1\\ x_1\oplus x_2\oplus y_2\end{bmatrix}, \text{ якщо } y_1=1;\ y_2=1\end{cases} \quad (2.14)$$

Отримаємо на основі виразу (2.14)

$$C_{15,21,3,9}(x,y)=\begin{bmatrix}x_1\oplus y_1\oplus 1\\ x_1\oplus x_2\oplus y_2\end{bmatrix} \quad (2.15)$$

Отримано на основі виразів (2.13) і (2.15) наступні взаємозв'язки:

$$C_{13,19,7,1}(x,y)=\begin{bmatrix}x_1\oplus y_1\oplus 1\\ x_2\oplus y_1\oplus y_2\end{bmatrix} \Rightarrow C_{13,19,7,1}(y,x)=C_{15,21,3,9}(x,y)=\begin{bmatrix}x_1\oplus y_1\oplus 1\\ x_1\oplus x_2\oplus y_2\end{bmatrix}; \quad (2.16)$$

$$C_{15,21,3,9}(x,y)=\begin{bmatrix}x_1\oplus y_1\oplus 1\\ x_1\oplus x_2\oplus y_2\end{bmatrix} \Rightarrow C_{15,21,3,9}(y,x)=C_{13,19,7,1}(x,y)=\begin{bmatrix}x_1\oplus y_1\oplus 1\\ x_2\oplus y_1\oplus y_2\end{bmatrix}. \quad (2.17)$$

Побудуємо моделі взаємозв'язаних операцій $C_{19,13,1,7}(x,y)\leftrightarrow C_{21,15,9,3}(x,y)$ згідно з четвертим рядком табл..2.1.

Побудуємо вдосконалену модель операції: $C_{19,13,1,7}(x,y)$

$$C_{19,13,1,7}(x,y)=\begin{cases}\begin{bmatrix}x_1\oplus 1\\ x_2\oplus 1\end{bmatrix}, \text{ якщо } y_1=0;\ y_2=0\\ \begin{bmatrix}x_1\oplus 1\\ x_2\end{bmatrix}, \text{якщу } y_1=0; y_2=1\\ \begin{bmatrix}x_1\\ x_2\end{bmatrix}, \text{ якщо } y_1=1;\ y_2=0\\ \begin{bmatrix}x_1\\ x_2\oplus 1\end{bmatrix}, \text{якщо } y_1=1;\ y_2=1\end{cases}=\begin{cases}\begin{bmatrix}x_1\oplus 1\\ x_2\oplus 1\end{bmatrix}=\begin{bmatrix}x_1\oplus y_1\oplus 1\\ x_2\oplus y_1\oplus y_2\oplus 1\end{bmatrix}, \text{ якщо } y_1=0;\ y_2=0\\ \begin{bmatrix}x_1\oplus 1\\ x_2\end{bmatrix}=\begin{bmatrix}x_1\oplus y_1\oplus 1\\ x_2\oplus y_1\oplus y_2\oplus 1\end{bmatrix}, \text{якщо } y_1=0;\ y_2=1\\ \begin{bmatrix}x_1\\ x_2\end{bmatrix}=\begin{bmatrix}x_1\oplus y_1\oplus 1\\ x_2\oplus y_1\oplus y_2\oplus 1\end{bmatrix}, \text{ якщо } y_1=1;\ y_2=0\\ \begin{bmatrix}x_1\\ x_2\oplus 1\end{bmatrix}=\begin{bmatrix}x_1\oplus y_1\oplus 1\\ x_2\oplus y_1\oplus y_2\oplus 1\end{bmatrix}, \text{якщо } y_1=1;\ y_2=1\end{cases} \quad (2.18)$$

Отримаємо на основі виразу (2.18)

$$C_{19,13,1,7}(x,y)=\begin{bmatrix}x_1\oplus y_1\oplus 1\\ x_2\oplus y_1\oplus y_2\oplus 1\end{bmatrix} \quad (2.19)$$

Побудуємо вдосконалену модель операції : $C_{21,15,9,3}(x,y)$

$$C_{21,15,9,3}(x,y)=\begin{cases}\begin{bmatrix}x_1\oplus 1\\ x_1\oplus x_2\oplus 1\end{bmatrix}, \text{ якщо } y_1=0;\ y_2=0\\ \begin{bmatrix}x_1\oplus 1\\ x_1\oplus x_2\end{bmatrix}, \text{якщо } y_1=0;\ y_2=1\\ \begin{bmatrix}x_1\\ x_1\oplus x_2\oplus 1\end{bmatrix}, \text{ якщо } y_1=1;\ y_2=0\\ \begin{bmatrix}x_1\\ x_1\oplus x_2\end{bmatrix}, \text{якщо } y_1=1;\ y_2=1\end{cases}=\begin{cases}\begin{bmatrix}x_1\oplus 1\\ x_1\oplus x_2\oplus 1\end{bmatrix}=\begin{bmatrix}x_1\oplus y_1\oplus 1\\ x_1\oplus x_2\oplus y_2\oplus 1\end{bmatrix}, \text{ якщо } y_1=0;\ y_2=0\\ \begin{bmatrix}x_1\oplus 1\\ x_1\oplus x_2\end{bmatrix}=\begin{bmatrix}x_1\oplus y_1\oplus 1\\ x_1\oplus x_2\oplus y_2\oplus 1\end{bmatrix}, \text{якщо } y_1=0;\ y_2=1\\ \begin{bmatrix}x_1\\ x_1\oplus x_2\oplus 1\end{bmatrix}=\begin{bmatrix}x_1\oplus y_1\oplus 1\\ x_1\oplus x_2\oplus y_2\oplus 1\end{bmatrix}, \text{ якщо } y_1=1;\ y_2=0\\ \begin{bmatrix}x_1\\ x_1\oplus x_2\end{bmatrix}=\begin{bmatrix}x_1\oplus y_1\oplus 1\\ x_1\oplus x_2\oplus y_2\oplus 1\end{bmatrix}, \text{якщо } y_1=1;\ y_2=1\end{cases} \quad (2.20)$$

Отримаємо вдосконалену модель операції $C_{21,15,9,3}(x,y)$:

$$C_{21,15,9,3}(x,y)=\begin{bmatrix}x_1\oplus y_1\oplus 1\\ x_1\oplus x_2\oplus y_2\oplus 1\end{bmatrix} \quad (2.21)$$

Вирази (2.19) і (2.21) забезпечують відображення наступних взаємозв’язків між операціями:

$$C_{19,13,1,7}(x,y)=\begin{bmatrix}x_1\oplus y_1\oplus 1\\ x_2\oplus y_1\oplus y_2\oplus 1\end{bmatrix} \Rightarrow C_{19,13,1,7}(y,x)=C_{21,15,9,3}(x,y)=\begin{bmatrix}x_1\oplus y_1\oplus 1\\ x_1\oplus x_2\oplus y_2\oplus 1\end{bmatrix} \quad (2.22)$$

$$C_{21,15,9,3}(x,y)=\begin{bmatrix}x_1\oplus y_1\oplus 1\\ x_1\oplus x_2\oplus y_2\oplus 1\end{bmatrix} \Rightarrow C_{21,15,9,3}(y,x)=C_{19,13,1,7}(x,y)=\begin{bmatrix}x_1\oplus y_1\oplus 1\\ x_2\oplus y_1\oplus y_2\oplus 1\end{bmatrix}. \quad (2.23)$$

Побудуємо моделі взаємозв’язаних операцій згідно з четвертим рядком табл..2.1: $C_{6,18,12,24}(x,y) \leftrightarrow C_{4,16,22,10}(x,y)$

Побудуємо вдосконалену модель операції $C_{6,18,12,24}(x,y)$:

$$C_{6,18,12,24}(x,y)=\begin{cases}\begin{bmatrix}x_1\oplus x_2\\ x_1\end{bmatrix}, \text{ якщо } y_1=0;\ y_2=0\\ \begin{bmatrix}x_1\oplus x_2\oplus 1\\ x_1\end{bmatrix}, \text{якщо } y_1=0;\ y_2=1\\ \begin{bmatrix}x_1\oplus x_2\\ x_1\oplus 1\end{bmatrix}, \text{ якщо } y_1=1;\ y_2=0\\ \begin{bmatrix}x_1\oplus x_2\oplus 1\\ x_1\oplus 1\end{bmatrix}, \text{якщо } y_1=1;\ y_2=1\end{cases}=\begin{cases}\begin{bmatrix}x_1\oplus x_2\\ x_1\end{bmatrix}=\begin{bmatrix}x_1\oplus x_2\oplus y_2\\ x_2\oplus y_1\end{bmatrix}, \text{ якщо } y_1=0;\ y_2=0\\ \begin{bmatrix}x_1\oplus x_2\oplus 1\\ x_1\end{bmatrix}=\begin{bmatrix}x_1\oplus x_2\oplus y_2\\ x_2\oplus y_1\end{bmatrix}, \text{якщо } y_1=0;\ y_2=1\\ \begin{bmatrix}x_1\oplus x_2\\ x_1\oplus 1\end{bmatrix}=\begin{bmatrix}x_1\oplus x_2\oplus y_2\\ x_2\oplus y_1\end{bmatrix}, \text{ якщо } y_1=1;\ y_2=0\\ \begin{bmatrix}x_1\oplus x_2\oplus 1\\ x_1\oplus 1\end{bmatrix}=\begin{bmatrix}x_1\oplus x_2\oplus y_2\\ x_2\oplus y_1\end{bmatrix}, \text{якщо } y_1=1;\ y_2=1\end{cases} \quad (2.24)$$

Вдосконалена модель операції $C_{6,18,12,24}(x,y)$ буде задана виразом:

$$C_{6,18,12,24}(x,y)=\begin{bmatrix}x_1\oplus x_2\oplus y_2\\ x_1\oplus y_1\end{bmatrix} \quad (2.25)$$

Побудуємо модель операції $C_{4,16,22,10}(x,y)$

$$C_{4,16,22,10}(x,y)=\begin{cases}\begin{bmatrix}x_2\\ x_1\end{bmatrix} \text{ якщо } y_1=0;\ y_2=0\\ \begin{bmatrix}x_2\oplus 1\\ x_1\end{bmatrix} \text{ якщо } y_1=0;\ y_2=1\\ \begin{bmatrix}x_2\oplus 1\\ x_1\oplus 1\end{bmatrix} \text{ якщо } y_1=1;\ y_2=0\\ \begin{bmatrix}x_2\\ x_1\oplus 1\end{bmatrix} \text{ якщо } y_1=1;\ y_2=1\end{cases}=\begin{cases}\begin{bmatrix}x_2\\ x_1\end{bmatrix}=\begin{bmatrix}x_2\oplus y_1\oplus y_2\\ x_1\oplus y_1\end{bmatrix} \text{ якщо } y_1=0;\ y_2=0\\ \begin{bmatrix}x_2\oplus 1\\ x_1\end{bmatrix}=\begin{bmatrix}x_2\oplus y_1\oplus y_2\\ x_1\oplus y_1\end{bmatrix} \text{ якщо } y_1=0;\ y_2=1\\ \begin{bmatrix}x_2\oplus 1\\ x_1\oplus 1\end{bmatrix}=\begin{bmatrix}x_2\oplus y_1\oplus y_2\\ x_1\oplus y_1\end{bmatrix} \text{ якщо } y_1=1;\ y_2=0\\ \begin{bmatrix}x_2\\ x_1\oplus 1\end{bmatrix}=\begin{bmatrix}x_2\oplus y_1\oplus y_2\\ x_1\oplus y_1\end{bmatrix} \text{ якщо } y_1=1;\ y_2=1\end{cases} \quad (2.26)$$

Вдосконалена модель операції буде задана:

$$C_{4,16,22,10}(x,y)=\begin{bmatrix}x_2\oplus y_1\oplus y_2\\ x_1\oplus y_1\end{bmatrix} \quad (2.27)$$

Отримано на основі виразів (2.25) і (2.27) наступні взаємозв'язки:

$$C_{6,18,12,24}(x.y)=\begin{bmatrix}x_1\oplus x_2\oplus y_2\\ x_1\oplus y_1\end{bmatrix} \quad \Rightarrow \quad C_{6,18,12,24}(y.x)=C_{4,16,22,10}(x,y)=\begin{bmatrix}x_2\oplus y_1\oplus y_2\\ x_1\oplus y_1\end{bmatrix}; \quad (2.28)$$

$$C_{4,16,22,10}(x,y)=\begin{bmatrix}x_2\oplus y_1\oplus y_2\\ x_1\oplus y_1\end{bmatrix} \quad \Rightarrow \quad C_{4,16,22,10}(y,x)=C_{6,18,12,24}(x,y)=\begin{bmatrix}x_1\oplus x_2\oplus y_2\\ x_1\oplus y_1\end{bmatrix}. \quad (2.29)$$

Побудуємо моделі взаємозв'язаних операцій $C_{12,24,6,18}(x,y)\leftrightarrow C_{10,22,16,4}(x,y)$.

Побудуємо модель операції $C_{12,24,6,18}(x,y)$:

$$C_{12,24,6,18}(x,y)=\begin{cases}\begin{bmatrix}x_1\oplus x_2\oplus y_2\\ x_2\oplus y_1\oplus 1\end{bmatrix}, \text{якщо } y_1=0;\ y_2=0\\ \begin{bmatrix}x_1\oplus x_2\oplus y_2\\ x_2\oplus y_1\oplus 1\end{bmatrix}, \text{якщо } y_1=0;\ y_2=1\\ \begin{bmatrix}x_1\oplus x_2\oplus y_2\\ x_2\oplus y_1\oplus 1\end{bmatrix}, \text{якщо } y_1=1;\ y_2=0\\ \begin{bmatrix}x_1\oplus x_2\oplus y_2\\ x_2\oplus y_1\oplus 1\end{bmatrix}, \text{якщо } y_1=1;\ y_2=1\end{cases}=\begin{cases}\begin{bmatrix}x_1\oplus x_2\oplus y_2\\ x_2\oplus y_1\oplus 1\end{bmatrix}=\begin{bmatrix}x_1\oplus x_2\\ x_1\oplus 1\end{bmatrix}, \text{якщо } y_1=0;\ y_2=0\\ \begin{bmatrix}x_1\oplus x_2\oplus y_2\\ x_2\oplus y_1\oplus 1\end{bmatrix}=\begin{bmatrix}x_1\oplus x_2\oplus 1\\ x_1\oplus 1\end{bmatrix}, \text{якщо } y_1=0;\ y_2=1\\ \begin{bmatrix}x_1\oplus x_2\oplus y_2\\ x_2\oplus y_1\oplus 1\end{bmatrix}=\begin{bmatrix}x_1\oplus x_2\\ x_1\end{bmatrix}, \text{якщо } y_1=1;\ y_2=0\\ \begin{bmatrix}x_1\oplus x_2\oplus y_2\\ x_2\oplus y_1\oplus 1\end{bmatrix}=\begin{bmatrix}x_1\oplus x_2\oplus 1\\ x_1\end{bmatrix}, \text{якщо } y_1=1;\ y_2=1\end{cases} \quad (2.30)$$

Вдосконалена модель операції буде представлена виразом:

$$C_{12,24,6,18}(x,y)=\begin{bmatrix}x_1\oplus x_2\oplus y_2\\ x_1\oplus y_1\oplus 1\end{bmatrix} \quad (2.31)$$

Побудуємо модель операції $C_{10,22,16,4}(x,y)$:

$$C_{10,22,16,4}(x,y)=\begin{cases}\begin{bmatrix}x_2\\ x_1\oplus 1\end{bmatrix}, \text{ якщо } y_1=0;\ y_2=0\\ \begin{bmatrix}x_2\oplus 1\\ x_1\oplus 1\end{bmatrix}, \text{якщо } y_1=0;\ y_2=1\\ \begin{bmatrix}x_2\oplus 1\\ x_1\end{bmatrix}, \text{ якщо } y_1=1;\ y_2=0\\ \begin{bmatrix}x_2\\ x_1\end{bmatrix}, \text{якщо } y_1=1;\ y_2=1\end{cases}=\begin{cases}\begin{bmatrix}x_2\\ x_1\oplus 1\end{bmatrix}=\begin{bmatrix}x_2\oplus y_1\oplus y_2\\ x_1\oplus y_1\oplus 1\end{bmatrix}, \text{ якщо } y_1=0;\ y_2=0\\ \begin{bmatrix}x_2\oplus 1\\ x_1\oplus 1\end{bmatrix}=\begin{bmatrix}x_2\oplus y_1\oplus k_2\\ x_1\oplus y_1\oplus 1\end{bmatrix}, \text{якщо } y_1=0;\ y_2=1\\ \begin{bmatrix}x_2\oplus 1\\ x_1\end{bmatrix}=\begin{bmatrix}x_2\oplus y_1\oplus y_2\\ x_1\oplus y_1\oplus 1\end{bmatrix}, \text{якщо } y_1=1;\ y_2=0\\ \begin{bmatrix}x_2\\ x_1\end{bmatrix}=\begin{bmatrix}x_2\oplus y_1\oplus y_2\\ x_1\oplus y_1\oplus 1\end{bmatrix}, \text{якщо } y_1=1;\ y_2=1\end{cases} \quad (2.32$$

Вдосконалена модель операції буде представлена виразом:

$$C_{10,22,16,4}(x,y)=\begin{bmatrix}x_2\oplus k_1\oplus k_2\\ x_1\oplus k_1\oplus 1\end{bmatrix} \quad (2.33)$$

Отримано на основі виразів (2.31) і (2.33) наступні взаємозв'язки:

$$C_{12,24,6,18}(x,y)=\begin{bmatrix}x_1\oplus x_2\oplus y_2\\ x_1\oplus y_1\oplus 1\end{bmatrix} \quad \Rightarrow \quad C_{12,24,6,18}(y,x)=C_{10,22,16,4}(x,y)=\begin{bmatrix}x_2\oplus y_1\oplus y_2\\ x_1\oplus y_1\oplus 1\end{bmatrix}; \quad (2.34)$$

$$C_{10,22,16,4}(\mathrm{x},\mathrm{y})=\begin{bmatrix}x_2\oplus y_1\oplus y_2\\ x_1\oplus y_1\oplus 1\end{bmatrix} \quad \Rightarrow \quad C_{10,22,16,4}(y,x)=C_{12,24,6,18}(x,y)=\begin{bmatrix}x_1\oplus x_2\oplus y_2\\ x_1\oplus y_1\oplus 1\end{bmatrix}. \quad (2.35)$$

Побудуємо моделі взаємозв'язаних операцій $C_{18,6,24,12}(x,y)\leftrightarrow C_{16,4,10,22}(x,y)$ згідно з сьомим рядком табл..2.1.

Побудуємо модель операції: $C_{18,6,24,12}(x,y)$

$$C_{18,6,24,12}(x,y)=\begin{cases}\begin{bmatrix}x_1\oplus x_2\oplus 1\\ x_1\end{bmatrix}, \text{ якщо } y_1=0;\ y_2=0\\ \begin{bmatrix}x_1\oplus x_2\\ x_1\end{bmatrix}, \text{якщо } y_1=0;\ y_2=1\\ \begin{bmatrix}x_1\oplus x_2\oplus 1\\ x_1\oplus 1\end{bmatrix}, \text{ якщо } y_1=1;\ y_2=0\\ \begin{bmatrix}x_1\oplus x_2\\ x_1\oplus 1\end{bmatrix}, \text{якщо } y_1=1;\ y_2=1\end{cases}=\begin{cases}\begin{bmatrix}x_1\oplus x_2\oplus 1\\ x_1\end{bmatrix}=\begin{bmatrix}x_1\oplus x_2\oplus y_2\oplus 1\\ x_1\oplus y_1\end{bmatrix}, \text{ якщо } y_1=0;\ y_2=0\\ \begin{bmatrix}x_1\oplus x_2\\ x_1\end{bmatrix}=\begin{bmatrix}x_1\oplus x_2\oplus y_2\oplus 1\\ x_1\oplus y_1\end{bmatrix}, \text{якщо } y_1=0;\ y_2=1\\ \begin{bmatrix}x_1\oplus x_2\oplus 1\\ x_1\oplus 1\end{bmatrix}=\begin{bmatrix}x_1\oplus x_2\oplus y_2\oplus 1\\ x_1\oplus y_1\end{bmatrix}, \text{ якщо } y_1=1;\ y_2=0\\ \begin{bmatrix}x_1\oplus x_2\\ x_1\oplus 1\end{bmatrix}=\begin{bmatrix}x_1\oplus x_2\oplus y_2\oplus 1\\ x_1\oplus y_1\end{bmatrix}, \text{якщо } y_1=1;\ y_2=1\end{cases} \tag{2.36}$$

Вдосконалена модель операції буде представлена виразом:

$$C_{18,6,24,12}(x,y)=\begin{bmatrix}x_1\oplus x_2\oplus y_2\oplus 1\\ x_1\oplus y_1\end{bmatrix} \tag{2.37}$$

Побудуємо модель операції $C_{16,4,10,22}(x,y)$:

$$C_{16,4,10,22}(x,y)=\begin{cases}\begin{bmatrix}x_2\oplus 1\\ x_1\end{bmatrix}, \text{ якщо } y_1=0;\ y_2=0\\ \begin{bmatrix}x_2\\ x_1\end{bmatrix}, \text{якщо } y_1=0;\ y_2=1\\ \begin{bmatrix}x_2\\ x_1\oplus 1\end{bmatrix}, \text{ якщо } y_1=1;\ y_2=0\\ \begin{bmatrix}x_2\oplus 1\\ x_1\oplus 1\end{bmatrix}, \text{якщо } y_1=1;\ y_2=1\end{cases}=\begin{cases}\begin{bmatrix}x_2\oplus 1\\ x_1\end{bmatrix}=\begin{bmatrix}x_2\oplus y_1\oplus y_2\oplus 1\\ x_1\oplus y_1\end{bmatrix}, \text{ якщо } y_1=0;\ y_2=0\\ \begin{bmatrix}x_2\\ x_1\end{bmatrix}=\begin{bmatrix}x_2\oplus y_1\oplus y_2\oplus 1\\ x_1\oplus y_1\end{bmatrix}, \text{якщо } y_1=0;\ y_2=1\\ \begin{bmatrix}x_2\\ x_1\oplus 1\end{bmatrix}=\begin{bmatrix}x_2\oplus y_1\oplus y_2\oplus 1\\ x_1\oplus y_1\end{bmatrix}, \text{ якщо } y_1=1;\ y_2=0\\ \begin{bmatrix}x_2\oplus 1\\ x_1\oplus 1\end{bmatrix}=\begin{bmatrix}x_2\oplus y_1\oplus y_2\oplus 1\\ x_1\oplus y_1\end{bmatrix}, \text{якщо } y_1=1;\ y_2=1\end{cases} \tag{2.38}$$

Вдосконалена модель операції буде представлена виразом:

$$C_{16,4,10,22}(x,y)=\begin{bmatrix}x_2\oplus y_1\oplus y_2\oplus 1\\ x_1\oplus y_1\end{bmatrix} \tag{2.39}$$

Отримано на основі виразів (2.37) і (2.39) наступні взаємозв'язки:

$$C_{18,6,24,12}(x,y)=\begin{bmatrix}x_1\oplus x_2\oplus y_2\oplus 1\\ x_1\oplus y_1\end{bmatrix} \Rightarrow C_{18,6,24,12}(y,x)=C_{16,4,10,22}(x,y)=\begin{bmatrix}x_2\oplus y_1\oplus y_2\oplus 1\\ x_1\oplus y_1\end{bmatrix}; \tag{2.40}$$

$$C_{16,4,10,22}(x,y)=\begin{bmatrix}x_2\oplus y_1\oplus y_2\oplus 1\\ x_1\oplus y_1\end{bmatrix} \Rightarrow C_{16,4,10,22}(y,x)=C_{18,6,24,12}(x,y)=\begin{bmatrix}x_1\oplus x_2\oplus y_2\oplus 1\\ x_1\oplus y_1\end{bmatrix}. \tag{2.41}$$

Побудуємо моделі взаємозв'язаних операцій $C_{24,12,18,6}(x,y)\leftrightarrow C_{22,10,4,16}(x,y)$ згідно з восьмим рядком табл..2.1.

Побудуємо модель операції $C_{24,12,18,6}(x,y)$:

$$C_{24,12,18,6}(x,y)=\begin{cases}\begin{bmatrix}x_1\oplus x_2\oplus 1\\ x_1\oplus 1\end{bmatrix}, \text{якщо } y_1=0;\ y_2=0\\ \begin{bmatrix}x_1\oplus x_2\\ x_1\oplus 1\end{bmatrix}, \text{якщо } y_1=0;\ y_2=1\\ \begin{bmatrix}x_1\oplus x_2\oplus 1\\ x_1\end{bmatrix}, \text{якщо } y_1=1;\ y_2=0\\ \begin{bmatrix}x_1\oplus x_2\\ x_1\end{bmatrix}, \text{якщо } y_1=1;\ y_2=1\end{cases}=\begin{cases}\begin{bmatrix}x_1\oplus x_2\oplus 1\\ x_1\oplus 1\end{bmatrix}=\begin{bmatrix}x_1\oplus x_2\oplus y_2\oplus 1\\ x_2\oplus y_1\oplus 1\end{bmatrix}, \text{якщо } y_1=0;\ y_2=0\\ \begin{bmatrix}x_1\oplus x_2\\ x_1\oplus 1\end{bmatrix}=\begin{bmatrix}x_1\oplus x_2\oplus y_2\oplus 1\\ x_2\oplus y_1\oplus 1\end{bmatrix}, \text{якщо } y_1=0;\ y_2=1\\ \begin{bmatrix}x_1\oplus x_2\oplus 1\\ x_1\end{bmatrix}=\begin{bmatrix}x_1\oplus x_2\oplus y_2\oplus 1\\ x_2\oplus y_1\oplus 1\end{bmatrix}, \text{якщо } y_1=1;\ y_2=0\\ \begin{bmatrix}x_1\oplus x_2\\ x_1\end{bmatrix}=\begin{bmatrix}x_1\oplus x_2\oplus y_2\oplus 1\\ x_2\oplus y_1\oplus 1\end{bmatrix}, \text{якщо } y_1=1;\ y_2=1\end{cases} \quad (2.42)$$

Вдосконалена модель операції буде представлена виразом:

$$C_{24,12,18,6}(x,y)=\begin{bmatrix}x_1\oplus x_2\oplus y_2\oplus 1\\ x_1\oplus y_1\oplus 1\end{bmatrix} \quad (2.43)$$

Побудуємо модель операції $C_{22,10,4,16}(x,y)$:

$$C_{22,10,4,16}(x,y)=\begin{cases}\begin{bmatrix}x_2\oplus 1\\ x_1\oplus 1\end{bmatrix}, \text{якщо } y_1=0;\ y_2=0\\ \begin{bmatrix}x_2\\ x_1\oplus 1\end{bmatrix}, \text{якщо } y_1=0;\ y_2=1\\ \begin{bmatrix}x_2\\ x_1\end{bmatrix}, \text{якщо } y_1=1;\ y_2=0\\ \begin{bmatrix}x_2\oplus 1\\ x_1\end{bmatrix}, \text{якщо } y_1=1;\ y_2=1\end{cases}=\begin{cases}\begin{bmatrix}x_2\oplus 1\\ x_1\oplus 1\end{bmatrix}=\begin{bmatrix}x_2\oplus y_1\oplus y_2\oplus 1\\ x_1\oplus y_1\oplus 1\end{bmatrix}, \text{якщо } y_1=0;\ y_2=0\\ \begin{bmatrix}x_2\\ x_1\oplus 1\end{bmatrix}=\begin{bmatrix}x_2\oplus y_1\oplus y_2\oplus 1\\ x_1\oplus y_1\oplus 1\end{bmatrix}, \text{якщо } y_1=0;\ y_2=1\\ \begin{bmatrix}x_2\\ x_1\end{bmatrix}=\begin{bmatrix}x_2\oplus y_1\oplus y_2\oplus 1\\ x_1\oplus y_1\oplus 1\end{bmatrix}, \text{якщо } y_1=1;\ y_2=0\\ \begin{bmatrix}x_2\oplus 1\\ x_1\end{bmatrix}=\begin{bmatrix}x_2\oplus y_1\oplus y_2\oplus 1\\ x_1\oplus y_1\oplus 1\end{bmatrix}, \text{якщо } y_1=1;\ y_2=1\end{cases} \quad (2.44)$$

Вдосконалена модель операції буде представлена виразом:

$$C_{22,10,4,16}(x,y)=\begin{bmatrix}x_2\oplus y_1\oplus y_2\oplus 1\\ x_1\oplus y_1\oplus 1\end{bmatrix} \quad (2.45)$$

На основі виразів (2.43) і (2.45) отримано наступні взаємозв'язки:

$$C_{24,12,18,6}(x,y)=\begin{bmatrix}x_1\oplus x_2\oplus y_2\oplus 1\\ x_1\oplus y_1\oplus 1\end{bmatrix} \Rightarrow C_{24,12,18,6}(y,x)=C_{22,10,4,16}(x,y)=\begin{bmatrix}x_2\oplus y_1\oplus y_2\oplus 1\\ x_1\oplus y_1\oplus 1\end{bmatrix}; \quad (2.46)$$

$$C_{22,10,4,16}(x,y)=\begin{bmatrix}x_2\oplus y_1\oplus y_2\oplus 1\\ x_1\oplus y_1\oplus 1\end{bmatrix} \Rightarrow C_{22,10,4,16}(y,x)=C_{24,12,18,6}(x,y)=\begin{bmatrix}x_1\oplus x_2\oplus y_2\oplus 1\\ x_1\oplus y_1\oplus 1\end{bmatrix}. \quad (2.47)$$

Побудуємо моделі взаємозв'язаних операцій $C_{5,23,17,11}(x,y)\leftrightarrow C_{2,20,8,14}(x,y)$ згідно з дев'ятим рядком табл..2.1.

Побудуємо модель операції $C_{5,23,17,11}(x,y)$:

$$C_{5,23,17,11}(x,y)=\begin{cases}\begin{bmatrix}x_2\\ x_1\oplus x_2\end{bmatrix}, \text{ якщо } y_1=0;\ y_2=0\\ \begin{bmatrix}x_2\oplus 1\\ x_1\oplus x_2\oplus 1\end{bmatrix}, \text{якщо } y_1=0;\ y_2=1\\ \begin{bmatrix}x_2\oplus 1\\ x_1\oplus x_2\end{bmatrix}, \text{ якщо } y_1=1;\ y_2=0\\ \begin{bmatrix}x_2\\ x_1\oplus x_2\oplus 1\end{bmatrix}, \text{якщо } y_1=1;\ y_2=1\end{cases}=\begin{cases}\begin{bmatrix}x_2\\ x_1\oplus x_2\end{bmatrix}=\begin{bmatrix}x_2\oplus y_1\oplus y_2\\ x_1\oplus x_2\oplus y_2\end{bmatrix}, \text{ якщо } y_1=0;\ y_2=0\\ \begin{bmatrix}x_2\oplus 1\\ x_1\oplus x_2\oplus 1\end{bmatrix}=\begin{bmatrix}x_2\oplus y_1\oplus y_2\\ x_1\oplus x_2\oplus y_2\end{bmatrix}, \text{якщо } y_1=0;\ y_2=1\\ \begin{bmatrix}x_2\oplus 1\\ x_1\oplus x_2\end{bmatrix}=\begin{bmatrix}x_2\oplus y_1\oplus y_2\\ x_1\oplus x_2\oplus y_2\end{bmatrix}, \text{ якщо } y_1=1;\ y_2=0\\ \begin{bmatrix}x_2\\ x_1\oplus x_2\oplus 1\end{bmatrix}=\begin{bmatrix}x_2\oplus y_1\oplus y_2\\ x_1\oplus x_2\oplus y_2\end{bmatrix}, \text{якщо } y_1=1;\ y_2=1\end{cases} \quad (2.48)$$

Вдосконалена модель операції буде представлена виразом:

$$C_{5,23,17,11}(x,y)=\begin{bmatrix}x_2\oplus y_1\oplus y_2\\ x_1\oplus x_2\oplus y_2\end{bmatrix} \quad (2.49)$$

Побудуємо модель операції $C_{2,20,8,14}(x,y)$:

$$C_{2,20,8,14}(x,y)=\begin{cases}\begin{bmatrix}x_1\oplus x_2\\ x_2\end{bmatrix}, \text{ якщо } y_1=0;\ y_2=0\\ \begin{bmatrix}x_1\oplus x_2\oplus 1\\ x_2\oplus 1\end{bmatrix}, \text{якщо } y_1=0;\ y_2=1\\ \begin{bmatrix}x_1\oplus x_2\\ x_2\oplus 1\end{bmatrix}, \text{ якщо } y_1=1;\ y_2=0\\ \begin{bmatrix}x_1\oplus x_2\oplus 1\\ x_2\end{bmatrix}, \text{якщо } y_1=1;\ y_2=1\end{cases}=\begin{cases}\begin{bmatrix}x_1\oplus x_2\\ x_2\end{bmatrix}=\begin{bmatrix}x_1\oplus x_2\oplus y_2\\ x_2\oplus y_1\oplus y_2\end{bmatrix}, \text{ якщо } y_1=0;\ y_2=0\\ \begin{bmatrix}x_1\oplus x_2\oplus 1\\ x_2\oplus 1\end{bmatrix}=\begin{bmatrix}x_1\oplus x_2\oplus y_2\\ x_2\oplus y_1\oplus y_2\end{bmatrix}, \text{якщо } k_1=0;\ k_2=1\\ \begin{bmatrix}x_1\oplus x_2\\ x_2\oplus 1\end{bmatrix}=\begin{bmatrix}x_1\oplus x_2\oplus y_2\\ x_2\oplus y_1\oplus y_2\end{bmatrix}, \text{ якщо } y_1=1;\ y_2=0\\ \begin{bmatrix}x_1\oplus x_2\oplus 1\\ x_2\end{bmatrix}=\begin{bmatrix}x_1\oplus x_2\oplus y_2\\ x_2\oplus y_1\oplus y_2\end{bmatrix}, \text{якщо } y_1=1;\ y_2=1\end{cases} \quad (2.50)$$

Вдосконалена модель операції буде представлена виразом:

$$C_{2,20,8,14}(x,y)=\begin{bmatrix}x_1\oplus x_2\oplus y_2\\ x_2\oplus y_1\oplus y_2\end{bmatrix} \quad (2.51)$$

На основі виразів (2.49) і (2.51) отримано наступні взаємозв'язки:

$$C_{5,23,17,11}(x,y)=\begin{bmatrix}x_2\oplus y_1\oplus y_2\\ x_1\oplus x_2\oplus y_2\end{bmatrix} \Rightarrow C_{5,23,17,11}(y,x)=C_{2,20,8,14}(x,y)=\begin{bmatrix}x_1\oplus x_2\oplus y_2\\ x_2\oplus y_1\oplus y_2\end{bmatrix}; \quad (2.52)$$

$$C_{2,20,8,14}(x,y)=\begin{bmatrix}x_1\oplus x_2\oplus y_2\\ x_2\oplus y_1\oplus y_2\end{bmatrix} \Rightarrow C_{2,20,8,14}(y,x)=C_{5,23,17,11}(x,y)=\begin{bmatrix}x_2\oplus y_1\oplus y_2\\ x_1\oplus x_2\oplus y_2\end{bmatrix}. \quad (2.53)$$

Побудуємо моделі взаємозв'язаних операцій $C_{11,17,23,5}(x,y) \leftrightarrow C_{8,14,2,20}(x,y)$ згідно з десятим рядком табл..2.1.

Побудуємо модель операції $C_{11,17,23,5}(x,y)$:

$$C_{11,17,23,5}(x,y)=\begin{cases}\begin{bmatrix}x_2\\ x_1\oplus x_2\oplus 1\end{bmatrix}, \text{ якщо } y_1=0;\ y_2=0\\ \begin{bmatrix}x_2\oplus 1\\ x_1\oplus x_2\end{bmatrix}, \text{якщо } y_1=0;\ y_2=1\\ \begin{bmatrix}x_2\oplus 1\\ x_1\oplus x_2\oplus 1\end{bmatrix}, \text{ якщо } y_1=1;\ y_2=0\\ \begin{bmatrix}x_2\\ x_1\oplus x_2\end{bmatrix}, \text{якщо } y_1=1;\ y_2=1\end{cases}=\begin{cases}\begin{bmatrix}x_2\\ x_1\oplus x_2\oplus 1\end{bmatrix}=\begin{bmatrix}x_2\oplus y_1\oplus y_2\\ x_1\oplus x_2\oplus y_2\oplus 1\end{bmatrix}, \text{ якщо } y_1=0;\ y_2=0\\ \begin{bmatrix}x_2\oplus 1\\ x_1\oplus x_2\end{bmatrix}=\begin{bmatrix}x_2\oplus y_1\oplus y_2\\ x_1\oplus x_2\oplus y_2\oplus 1\end{bmatrix}, \text{якщо } y_1=0;\ y_2=1\\ \begin{bmatrix}x_2\oplus 1\\ x_1\oplus x_2\oplus 1\end{bmatrix}=\begin{bmatrix}x_2\oplus y_1\oplus y_2\\ x_1\oplus x_2\oplus y_2\oplus 1\end{bmatrix}, \text{ якщо } y_1=1;\ y_2=0\\ \begin{bmatrix}x_2\\ x_1\oplus x_2\end{bmatrix}=\begin{bmatrix}x_2\oplus y_1\oplus y_2\\ x_1\oplus x_2\oplus y_2\oplus 1\end{bmatrix}, \text{якщо } y_1=1;\ y_2=1\end{cases} \quad (2.54)$$

Вдосконалена модель операції (3.49) буде представлена виразом:

$$C_{11,17,23,5}(x,y)=\begin{bmatrix}x_2\oplus y_1\oplus y_2\\ x_1\oplus x_2\oplus y_2\oplus 1\end{bmatrix} \quad (2.55)$$

Побудуємо модель операції $C_{8,14,2,20}(x,y)$:

$$C_{8,14,2,20}(x,y)=\begin{cases}\begin{bmatrix}x_1\oplus x_2\\ x_2\oplus 1\end{bmatrix}, \text{ якщо } y_1=0;\ y_2=0\\ \begin{bmatrix}x_1\oplus x_2\oplus 1\\ x_2\end{bmatrix}, \text{якщо } y_1=0;\ y_2=1\\ \begin{bmatrix}x_1\oplus x_2\\ x_2\end{bmatrix}, \text{ якщо } y_1=1;\ y_2=0\\ \begin{bmatrix}x_1\oplus x_2\oplus 1\\ x_2\oplus 1\end{bmatrix}, \text{якщо } y_1=1;\ y_2=1\end{cases}=\begin{cases}\begin{bmatrix}x_1\oplus x_2\\ x_2\oplus 1\end{bmatrix}=\begin{bmatrix}x_1\oplus x_2\oplus y_2\\ x_2\oplus y_1\oplus y_2\oplus 1\end{bmatrix}, \text{ якщо } y_1=0;\ y_2=0\\ \begin{bmatrix}x_1\oplus x_2\oplus 1\\ x_2\end{bmatrix}=\begin{bmatrix}x_1\oplus x_2\oplus y_2\\ x_2\oplus y_1\oplus y_2\oplus 1\end{bmatrix}, \text{якщо } y_1=0;\ y_2=1\\ \begin{bmatrix}x_1\oplus x_2\\ x_2\end{bmatrix}=\begin{bmatrix}x_1\oplus x_2\oplus y_2\\ x_2\oplus k_1\oplus y_2\oplus 1\end{bmatrix}, \text{ якщо } y_1=1;\ y_2=0\\ \begin{bmatrix}x_1\oplus x_2\oplus 1\\ x_2\oplus 1\end{bmatrix}=\begin{bmatrix}x_1\oplus x_2\oplus y_2\\ x_2\oplus y_1\oplus y_2\oplus 1\end{bmatrix}, \text{якщо } y_1=1;\ y_2=1\end{cases} \quad (2.56)$$

Вдосконалена модель операції буде представлена виразом:

$$C_{8,14,2,20}(x,y)=\begin{bmatrix}x_1\oplus x_2\oplus y_2\\ x_2\oplus y_1\oplus y_2\oplus 1\end{bmatrix} \quad (2.57)$$

На основі виразів (2.55) і (2.57) отримано наступні взаємозв'язки:

$$C_{11,17,23,5}(x,y)=\begin{bmatrix}x_2\oplus y_1\oplus y_2\\ x_1\oplus x_2\oplus y_2\oplus 1\end{bmatrix} \Rightarrow C_{11,17,23,5}(y,x)=C_{8,14,2,20}(x,y)=\begin{bmatrix}x_1\oplus x_2\oplus y_2\\ x_2\oplus y_1\oplus y_2\oplus 1\end{bmatrix}; \quad (2.58)$$

$$C_{8,14,2,20}(x,y)=\begin{bmatrix}x_1\oplus x_2\oplus y_2\\ x_2\oplus y_1\oplus y_2\oplus 1\end{bmatrix} \Rightarrow C_{8,14,2,20}(y,x)=C_{11,17,23,5}(x,y)=\begin{bmatrix}x_2\oplus y_1\oplus y_2\\ x_1\oplus y_2\oplus y_2\oplus 1\end{bmatrix}. \quad (2.59)$$

Побудуємо моделі взаємозв'язаних операцій $C_{17,11,5,23}(x,y)\leftrightarrow C_{14,8,20,2}(x,y)$.

Побудуємо модель операції $C_{17,11,5,23}(x,y)$:

$$C_{17,11,5,23}(x,y)=\begin{cases}\begin{bmatrix}x_2\oplus 1\\ x_1\oplus x_2\end{bmatrix}, \text{ якщо } y_1=0;\ y_2=0\\ \begin{bmatrix}x_2\\ x_1\oplus x_2\oplus 1\end{bmatrix}, \text{якщо } y_1=0;\ y_2=1\\ \begin{bmatrix}x_2\\ x_1\oplus x_2\end{bmatrix}, \text{ якщо } y_1=1;\ y_2=0\\ \begin{bmatrix}x_2\oplus 1\\ x_1\oplus x_2\oplus 1\end{bmatrix}, \text{якщо } y_1=1;\ y_2=1\end{cases}=\begin{cases}\begin{bmatrix}x_2\oplus 1\\ x_1\oplus x_2\end{bmatrix}=\begin{bmatrix}x_2\oplus y_1\oplus y_2\oplus 1\\ x_1\oplus x_2\oplus y_2\end{bmatrix}, \text{ якщо } y_1=0;\ y_2=0\\ \begin{bmatrix}x_2\\ x_1\oplus x_2\oplus 1\end{bmatrix}=\begin{bmatrix}x_2\oplus y_1\oplus y_2\oplus 1\\ x_1\oplus x_2\oplus y_2\end{bmatrix}, \text{якщо } y_1=0;\ y_2=1\\ \begin{bmatrix}x_2\\ x_1\oplus x_2\end{bmatrix}=\begin{bmatrix}x_2\oplus y_1\oplus y_2\oplus 1\\ x_1\oplus x_2\oplus y_2\end{bmatrix}, \text{ якщо } y_1=1;\ y_2=0\\ \begin{bmatrix}x_2\oplus 1\\ x_1\oplus x_2\oplus 1\end{bmatrix}=\begin{bmatrix}x_2\oplus y_1\oplus y_2\oplus 1\\ x_1\oplus x_2\oplus y_2\end{bmatrix}, \text{якщо } y_1=1;\ y_2=1\end{cases} \quad (2.60)$$

Вдосконалена модель операції буде представлена виразом:

$$C_{17,11,5,23}(x,y)=\begin{bmatrix}x_2\oplus y_1\oplus y_2\oplus 1\\ x_1\oplus x_2\oplus y_2\end{bmatrix} \quad (2.61)$$

Побудуємо модель операції $C_{14,8,20,2}(x,y)$:

$$C_{14,8,20,2}(y,x)=\begin{cases}\begin{bmatrix}x_1\oplus x_2\oplus 1\\ x_2\end{bmatrix}, \text{ якщо } y_1=0;\ y_2=0\\ \begin{bmatrix}x_1\oplus x_2\\ x_2\oplus 1\end{bmatrix}, \text{якщо } y_1=0;\ y_2=1\\ \begin{bmatrix}x_1\oplus x_2\oplus 1\\ x_2\oplus 1\end{bmatrix}, \text{ якщо } y_1=1;\ y_2=0\\ \begin{bmatrix}x_1\oplus x_2\\ x_2\end{bmatrix}, \text{якщо } y_1=1;\ y_2=1\end{cases}=\begin{cases}\begin{bmatrix}x_1\oplus x_2\oplus 1\\ x_2\end{bmatrix}=\begin{bmatrix}x_1\oplus x_2\oplus y_2\oplus 1\\ x_2\oplus y_1\oplus y_2\end{bmatrix}, \text{ якщо } y_1=0;\ y_2=0\\ \begin{bmatrix}x_1\oplus x_2\\ x_2\oplus 1\end{bmatrix}=\begin{bmatrix}x_1\oplus x_2\oplus y_2\oplus 1\\ x_2\oplus y_1\oplus y_2\end{bmatrix}, \text{якщо } y_1=0;\ y_2=1\\ \begin{bmatrix}x_1\oplus x_2\oplus 1\\ x_2\oplus 1\end{bmatrix}=\begin{bmatrix}x_1\oplus x_2\oplus y_2\oplus 1\\ x_2\oplus y_1\oplus y_2\end{bmatrix}, \text{ якщо } y_1=1;\ y_2=0\\ \begin{bmatrix}x_1\oplus x_2\\ x_2\end{bmatrix}=\begin{bmatrix}x_1\oplus x_2\oplus y_2\oplus 1\\ x_2\oplus y_1\oplus y_2\end{bmatrix}, \text{якщо } y_1=1;\ y_2=1\end{cases} \quad 2.62)$$

Вдосконалена модель операції буде представлена виразом:

$$C_{14,8,20,2}(x,y)=\begin{bmatrix}x_1\oplus x_2\oplus y_2\oplus 1\\ x_2\oplus y_1\oplus y_2\end{bmatrix} \quad (2.63)$$

На основі виразів (2.61) і (2.63) отримано наступні взаємозв'язки:

$$C_{17,11,5,23}(x,y)=\begin{bmatrix}x_2\oplus y_1\oplus y_2\oplus 1\\ x_1\oplus x_2\oplus y_2\end{bmatrix} \Rightarrow C_{17,11,5,23}(y,x)=C_{14,8,20,2}(x,y)=\begin{bmatrix}x_1\oplus x_2\oplus y_2\oplus 1\\ x_2\oplus y_1\oplus y_2\end{bmatrix}; \quad (2.64)$$

$$C_{14,8,20,2}(x,y)=\begin{bmatrix}x_1\oplus x_2\oplus y_2\oplus 1\\ x_2\oplus y_1\oplus y_2\end{bmatrix} \Rightarrow C_{14,8,20,2}(y,x)=C_{17,11,5,23}(x,y)=\begin{bmatrix}x_2\oplus y_1\oplus y_2\oplus 1\\ x_1\oplus x_2\oplus y_2\end{bmatrix}. \quad (2.65)$$

Побудуємо моделі взаємозв'язаних операцій $C_{23,5,11,17}(x,y)\leftrightarrow C_{20,2,14,8}(x,y)$ згідно з останнім дванадцятим рядком табл..2.1.

Побудуємо модель операції $C_{23,5,11,17}(x,y)$:

$$C_{23,5,11,17}(x,y)=\begin{cases}\begin{bmatrix}x_2\oplus 1\\ x_1\oplus x_2\oplus 1\end{bmatrix}, \text{ якщо } y_1=0;\ y_2=0\\ \begin{bmatrix}x_2\\ x_1\oplus x_2\end{bmatrix}, \text{якщо } y_1=0;\ y_2=1\\ \begin{bmatrix}x_2\\ x_1\oplus x_2\oplus 1\end{bmatrix}, \text{ якщо } y_1=1;\ y_2=0\\ \begin{bmatrix}x_2\oplus 1\\ x_1\oplus x_2\end{bmatrix}, \text{якщо } y_1=1;\ y_2=1\end{cases}=\begin{cases}\begin{bmatrix}x_2\oplus 1\\ x_1\oplus x_2\oplus 1\end{bmatrix}=\begin{bmatrix}x_2\oplus y_1\oplus y_2\oplus 1\\ x_1\oplus x_2\oplus y_2\oplus 1\end{bmatrix}, \text{ якщо } y_1=0;\ y_2=0\\ \begin{bmatrix}x_2\\ x_1\oplus x_2\end{bmatrix}=\begin{bmatrix}x_2\oplus y_1\oplus y_2\oplus 1\\ x_1\oplus x_2\oplus y_2\oplus 1\end{bmatrix}, \text{якщо } y_1=0;\ y_2=1\\ \begin{bmatrix}x_2\\ x_1\oplus x_2\oplus 1\end{bmatrix}=\begin{bmatrix}x_2\oplus y_1\oplus y_2\oplus 1\\ x_1\oplus x_2\oplus y_2\oplus 1\end{bmatrix}, \text{ якщо } y_1=1;\ y_2=0\\ \begin{bmatrix}x_2\oplus 1\\ x_1\oplus x_2\end{bmatrix}=\begin{bmatrix}x_2\oplus y_1\oplus y_2\oplus 1\\ x_1\oplus x_2\oplus y_2\oplus 1\end{bmatrix}, \text{якщо } y_1=1;\ y_2=1\end{cases} \quad (2.66)$$

Вдосконалена модель операції буде представлена виразом:

$$C_{23,5,11,17}(x,y)=\begin{bmatrix}x_2\oplus y_1\oplus y_2\oplus 1\\ x_1\oplus x_2\oplus y_2\oplus 1\end{bmatrix} \quad (2.67)$$

Побудуємо модель операції $C_{20,2,14,8}(x,y)$:

$$C_{20,2,14,8}(x,y)=\begin{cases}\begin{bmatrix}x_1\oplus x_2\oplus 1\\ x_2\oplus 1\end{bmatrix}, \text{ якщо } y_1=0;\ y_2=0\\ \begin{bmatrix}x_1\oplus x_2\\ x_2\end{bmatrix}, \text{якщо } y_1=0;\ y_2=1\\ \begin{bmatrix}x_1\oplus x_2\oplus 1\\ x_2\end{bmatrix}, \text{ якщо } y_1=1;\ y_2=0\\ \begin{bmatrix}x_1\oplus x_2\\ x_2\oplus 1\end{bmatrix}, \text{якщо } y_1=1;\ y_2=1\end{cases}=\begin{cases}\begin{bmatrix}x_1\oplus x_2\oplus 1\\ x_2\oplus 1\end{bmatrix}=\begin{bmatrix}x_1\oplus x_2\oplus y_2\oplus 1\\ x_2\oplus y_1\oplus y_2\oplus 1\end{bmatrix}, \text{ якщо } y_1=0;\ y_2=0\\ \begin{bmatrix}x_1\oplus x_2\\ x_2\end{bmatrix}=\begin{bmatrix}x_1\oplus x_2\oplus y_2\oplus 1\\ x_2\oplus y_1\oplus y_2\oplus 1\end{bmatrix}, \text{якщо } y_1=0;\ y_2=1\\ \begin{bmatrix}x_1\oplus x_2\oplus 1\\ x_2\end{bmatrix}=\begin{bmatrix}x_1\oplus x_2\oplus y_2\oplus 1\\ x_2\oplus y_1\oplus y_2\oplus 1\end{bmatrix}, \text{ якщо } y_1=1;\ y_2=0\\ \begin{bmatrix}x_1\oplus x_2\\ x_2\oplus 1\end{bmatrix}=\begin{bmatrix}x_1\oplus x_2\oplus y_2\oplus 1\\ x_2\oplus y_1\oplus y_2\oplus 1\end{bmatrix}, \text{якщо } y_1=1;\ y_2=1\end{cases} \quad (2.68)$$

Вдосконалена модель операції буде представлена виразом:

$$C_{20,2,14,8}(x,y)=\begin{bmatrix}x_1\oplus x_2\oplus y_2\oplus 1\\ x_2\oplus y_1\oplus y_2\oplus 1\end{bmatrix} \quad (2.69)$$

Вирази (2.67) і (2.69) забезпечують відображення наступних взаємозв'язків між операціями:

$$C_{23,5,11,17}(x,y)=\begin{bmatrix}x_2\oplus y_1\oplus y_2\oplus 1\\ x_1\oplus x_2\oplus y_2\oplus 1\end{bmatrix} \Rightarrow C_{23,5,11,17}(y,x)=C_{20,2,14,8}(x,y)=\begin{bmatrix}x_1\oplus x_2\oplus y_2\oplus 1\\ x_2\oplus y_1\oplus y_2\oplus 1\end{bmatrix}; \quad (2.70)$$

$$C_{20,2,14,8}(x,y)=\begin{bmatrix}x_1\oplus x_2\oplus y_2\oplus 1\\ x_2\oplus y_1\oplus y_2\oplus 1\end{bmatrix} \Rightarrow C_{20,2,14,8}(y,x)=C_{23,5,11,17}(x,y)=\begin{bmatrix}x_2\oplus y_1\oplus y_2\oplus 1\\ x_1\oplus x_2\oplus y_2\oplus 1\end{bmatrix}. \quad (2.71)$$

Відобразимо отримані вдосконалені моделі та взаємозв'язки між ними згідно виразів (2.10) і (2.11), (2.16) і (2.17), (2.22) і (2.23), (2.28) і (2.29), (2.34) і (2.35), (2.40) і (2.41), (2.46) і (2.47), (2.52) і (2.53), (2.58) і (2.59), (2.64) і (2.65), (2.70) і (2.71), в табл..2.2.

Таблиця 2.2

Синтезована множина моделей несиметричних двохоперандних двохрозрядних операцій подвійного циклу та взаємозв'язки між моделями [2]

	Операції криптоперетворення			
$C(x,y)$	$C_{1,7,19,13}(x,y)=\begin{bmatrix} x_1 \oplus y_1 \\ x_2 \oplus y_1 \oplus y_2 \end{bmatrix}$	$C_{7,1,13,19}(x,y)=\begin{bmatrix} x_1 \oplus y_1 \\ x_2 \oplus y_1 \oplus y_2 \oplus 1 \end{bmatrix}$	$C_{13,19,7,1}(x,y)=\begin{bmatrix} x_1 \oplus y_1 \oplus 1 \\ x_2 \oplus y_1 \oplus y_2 \end{bmatrix}$	$C_{19,13,1,7}(x,y)=\begin{bmatrix} x_1 \oplus y_1 \oplus 1 \\ x_2 \oplus y_1 \oplus y_2 \oplus 1 \end{bmatrix}$
$C(y,x)$	$C_{3,9,15,21}(x,y)=\begin{bmatrix} x_1 \oplus y_1 \\ x_1 \oplus x_2 \oplus y_2 \end{bmatrix}$	$C_{9,3,21,15}(x,y)=\begin{bmatrix} x_1 \oplus y_1 \\ x_1 \oplus x_2 \oplus y_2 \oplus 1 \end{bmatrix}$	$C_{15,21,3,9}(x,y)=\begin{bmatrix} x_1 \oplus y_1 \oplus 1 \\ x_1 \oplus x_2 \oplus y_2 \end{bmatrix}$	$C_{21,15,9,3}(x,y)=\begin{bmatrix} x_1 \oplus y_1 \oplus 1 \\ x_1 \oplus x_2 \oplus y_2 \oplus 1 \end{bmatrix}$
$C(x,y)$	$C_{6,18,12,24}(x,y)=\begin{bmatrix} x_1 \oplus x_2 \oplus y_2 \\ x_1 \oplus y_1 \end{bmatrix}$	$C_{12,24,6,18}(x,y)=\begin{bmatrix} x_1 \oplus x_2 \oplus y_2 \\ x_1 \oplus y_1 \oplus 1 \end{bmatrix}$	$C_{18,6,24,12}(x,y)=\begin{bmatrix} x_1 \oplus x_2 \oplus y_2 \oplus 1 \\ x_1 \oplus y_1 \end{bmatrix}$	$C_{24,12,18,6}(x,y)=\begin{bmatrix} x_1 \oplus x_2 \oplus y_2 \oplus 1 \\ x_1 \oplus y_1 \oplus 1 \end{bmatrix}$
$C(y,x)$	$C_{4,16,22,10}(x,y)=\begin{bmatrix} x_2 \oplus y_1 \oplus y_2 \\ x_1 \oplus y_1 \end{bmatrix}$	$C_{10,22,16,4}(x,y)=\begin{bmatrix} x_2 \oplus y_1 \oplus y_2 \\ x_1 \oplus y_1 \oplus 1 \end{bmatrix}$	$C_{16,4,10,22}(x,y)=\begin{bmatrix} x_2 \oplus y_1 \oplus y_2 \oplus 1 \\ x_1 \oplus y_1 \end{bmatrix}$	$C_{22,10,4,16}(x,y)=\begin{bmatrix} x_2 \oplus y_1 \oplus y_2 \oplus 1 \\ x_1 \oplus y_1 \oplus 1 \end{bmatrix}$
$C(x,y)$	$C_{3,9,15,21}(x,y)=\begin{bmatrix} x_1 \oplus y_1 \\ x_1 \oplus x_2 \oplus y_2 \end{bmatrix}$	$C_{9,3,21,15}(x,y)=\begin{bmatrix} x_1 \oplus y_1 \\ x_1 \oplus x_2 \oplus y_2 \oplus 1 \end{bmatrix}$	$C_{15,21,3,9}(x,y)=\begin{bmatrix} x_1 \oplus y_1 \oplus 1 \\ x_1 \oplus x_2 \oplus y_2 \end{bmatrix}$	$C_{21,15,9,3}(x,y)=\begin{bmatrix} x_1 \oplus y_1 \oplus 1 \\ x_1 \oplus x_2 \oplus y_2 \oplus 1 \end{bmatrix}$
$C(y,x)$	$C_{1,7,19,13}(x,y)=\begin{bmatrix} x_1 \oplus y_1 \\ x_2 \oplus y_1 \oplus y_2 \end{bmatrix}$	$C_{7,1,13,19}(x,y)=\begin{bmatrix} x_1 \oplus y_1 \\ x_2 \oplus y_1 \oplus y_2 \oplus 1 \end{bmatrix}$	$C_{13,19,7,1}(x,y)=\begin{bmatrix} x_1 \oplus y_1 \oplus 1 \\ x_2 \oplus y_1 \oplus y_2 \end{bmatrix}$	$C_{19,13,1,7}(x,y)=\begin{bmatrix} x_1 \oplus y_1 \oplus 1 \\ x_2 \oplus y_1 \oplus y_2 \oplus 1 \end{bmatrix}$
$C(x,y)$	$C_{4,16,22,10}(x,y)=\begin{bmatrix} x_2 \oplus y_1 \oplus y_2 \\ x_1 \oplus y_1 \end{bmatrix}$	$C_{10,22,16,4}(x,y)=\begin{bmatrix} x_2 \oplus y_1 \oplus y_2 \\ x_1 \oplus y_1 \oplus 1 \end{bmatrix}$	$C_{16,4,10,22}(x,y)=\begin{bmatrix} x_2 \oplus y_1 \oplus y_2 \oplus 1 \\ x_1 \oplus y_1 \end{bmatrix}$	$C_{22,10,4,16}(x,y)=\begin{bmatrix} x_2 \oplus y_1 \oplus y_2 \oplus 1 \\ x_1 \oplus y_1 \oplus 1 \end{bmatrix}$
$C(y,x)$	$C_{6,18,12,24}(x,y)=\begin{bmatrix} x_1 \oplus x_2 \oplus y_2 \\ x_1 \oplus y_1 \end{bmatrix}$	$C_{12,24,6,18}(x,y)=\begin{bmatrix} x_1 \oplus x_2 \oplus y_2 \\ x_1 \oplus y_1 \oplus 1 \end{bmatrix}$	$C_{18,6,24,12}(x,y)=\begin{bmatrix} x_1 \oplus x_2 \oplus y_2 \oplus 1 \\ x_1 \oplus y_1 \end{bmatrix}$	$C_{24,12,18,6}(x,y)=\begin{bmatrix} x_1 \oplus x_2 \oplus y_2 \oplus 1 \\ x_1 \oplus y_1 \oplus 1 \end{bmatrix}$
$C(x,y)$	$C_{5,23,17,11}(x,y)=\begin{bmatrix} x_2 \oplus y_1 \oplus y_2 \\ x_1 \oplus x_2 \oplus y_2 \end{bmatrix}$	$C_{11,17,23,5}(x,y)=\begin{bmatrix} x_2 \oplus y_1 \oplus y_2 \\ x_1 \oplus x_2 \oplus y_2 \oplus 1 \end{bmatrix}$	$C_{17,11,5,23}(x,y)=\begin{bmatrix} x_2 \oplus y_1 \oplus y_2 \oplus 1 \\ x_1 \oplus x_2 \oplus y_2 \end{bmatrix}$	$C_{23,5,11,17}(x,y)=\begin{bmatrix} x_2 \oplus y_1 \oplus y_2 \oplus 1 \\ x_1 \oplus x_2 \oplus y_2 \oplus 1 \end{bmatrix}$
$C(y,x)$	$C_{2,20,8,14}(x,y)=\begin{bmatrix} x_1 \oplus x_2 \oplus y_2 \\ x_2 \oplus y_1 \oplus y_2 \end{bmatrix}$	$C_{8,14,2,20}(x,y)=\begin{bmatrix} x_1 \oplus x_2 \oplus y_2 \\ x_2 \oplus y_1 \oplus y_2 \oplus 1 \end{bmatrix}$	$C_{14,8,20,2}(x,y)=\begin{bmatrix} x_1 \oplus x_2 \oplus y_2 \oplus 1 \\ x_2 \oplus y_1 \oplus y_2 \end{bmatrix}$	$C_{20,2,14,8}(x,y)=\begin{bmatrix} x_1 \oplus x_2 \oplus y_2 \oplus 1 \\ x_2 \oplus y_1 \oplus y_2 \oplus 1 \end{bmatrix}$
$C(x,y)$	$C_{2,20,8,14}(x,y)=\begin{bmatrix} x_1 \oplus x_2 \oplus y_2 \\ x_2 \oplus y_1 \oplus y_2 \end{bmatrix}$	$C_{8,14,2,20}(x,y)=\begin{bmatrix} x_1 \oplus x_2 \oplus y_2 \\ x_2 \oplus y_1 \oplus y_2 \oplus 1 \end{bmatrix}$	$C_{14,8,20,2}(x,y)=\begin{bmatrix} x_1 \oplus x_2 \oplus y_2 \oplus 1 \\ x_2 \oplus y_1 \oplus y_2 \end{bmatrix}$	$C_{20,2,14,8}(x,y)=\begin{bmatrix} x_1 \oplus x_2 \oplus y_2 \oplus 1 \\ x_2 \oplus y_1 \oplus y_2 \oplus 1 \end{bmatrix}$
$C(y,x)$	$C_{5,23,17,11}(x,y)=\begin{bmatrix} x_2 \oplus y_1 \oplus y_2 \\ x_1 \oplus x_2 \oplus y_2 \end{bmatrix}$	$C_{11,17,23,5}(x,y)=\begin{bmatrix} x_2 \oplus y_1 \oplus y_2 \\ x_1 \oplus x_2 \oplus y_2 \oplus 1 \end{bmatrix}$	$C_{17,11,5,23}(x,y)=\begin{bmatrix} x_2 \oplus y_1 \oplus y_2 \oplus 1 \\ x_1 \oplus x_2 \oplus y_2 \end{bmatrix}$	$C_{23,5,11,17}(x,y)=\begin{bmatrix} x_2 \oplus y_1 \oplus y_2 \oplus 1 \\ x_1 \oplus x_2 \oplus y_2 \oplus 1 \end{bmatrix}$

Аналіз множини удосконалених моделей несиметричних двохоперандних двохрозрядних операцій подвійного циклу не дозволив встановити всі взаємозв'язки між моделями прямих операцій та моделями прямих і обернених операцій [2]. Відсутність перелічених взаємозв'язків не забезпечує можливість моделювання аналогічних операцій криптоперетворення без наявності результатів обчислювального експерименту.

Проте представлена в табл.2.2 множини удосконалених моделей несиметричних двохоперандних двохрозрядних СЕТ-операцій до перестановки операндів і після перестановки операндів (виділено відтінками сірого) дозволяє зробити висновок що перестановка операндів на вході СЕТ-операції приводить до модифікації моделі шляхом зміни перемінних для вхідних Сі-квантів інформації. Необхідно відмітити що модифікація моделі СЕТ-операції приводить до зміни результату шифрування (значення вихідного Сі-кванту). СЕТ-операція яка допускає перестановку операндів забезпечує двох наборів одноопераднних операцій, кожна з яких реалізує свою, індивідуальну для операції таблицю підстановки.

Отриманий результат дозволив удосконалити технологію побудови двохоперандних СЕТ-операцій за результатами обчислювального експерименту.

Технологія побудови удосконалених моделей СЕТ-операцій за результатами експеременту передбачає перехід від кортежної моделі СЕТ-операції до розширеної кортежної операції з наступним переходом до удосконаленої дискретної моделі на основі мінімізації таблиці взаємозв'язків між Сі-квантами операндів .

При комп'ютерному моделюванні комутативних СЕТ-операцій було встановлено кортежні моделі СЕТ-операції до перестановки операндів і після перестановки операндів. Виходячи з цього технологію побудови удосконалених моделей СЕТ-операцій за результатами експерименту необхідно застосовувати для побудови моделі СЕТ-операції до перестановки операндів і побудови моделі СЕТ-операції після перестановки операндів.

Отримані в розділі взаємозв’язки між моделями СЕТ-операцій до і після перестановки операндів забезпечило можливість удосконалення технології побудови удосконалених моделей СЕТ- операцій.

Сутність удосконалено технології побудови СЕТ-операцій полягає в заміні повторного використання технології для знаходження удосконаленої моделі після перестановки операндів на зміну змінних в удосконаленій моделі СЕТ-операції до перестановки операндів. Дане удосконалення забезпечує прямий перехід від моделі СЕТ-операції до перестановки операндів, до моделі СЕТ-операції після перестановки операндів. Це приводить до зменшення складності процесу моделювання некомутативних СЕТ-операцій шляхом виключення переходу аналізу кортежу одноопераднних операцій, переходу до розширеної кортежної операції, та наступного переходу до удосконаленої дискретної моделі на основі мінімізації таблиці взаємозв’язків між Сі-квантами операндів після їх перестановки.

Висновки до розділу 2

Удосконалено технологію побудови удосконалених моделей некомутативних двохрозрядних двохоперандних СЕТ-операції за результатами експерименту, на основі побудови удосконалених моделей СЕТ-операцій за результатами експерименту, шляхом встановлення взаємозв’язків між моделями до і після перестановки операндів, що забезпечило зменшення складності моделювання некомутативних СЕТ-операцій на основі реалізації прямого переході від побудованої моделі СЕТ-операції до моделі СЕТ-операції з переставленими операндами.

1. Досліджені особливості застосування несиметричних двохоперандних СЕТ-операцій які допускають перестановку операндів в потокових системах шифрування.

2. Проаналізовано два сценарії потокового шифрування які базуються на використанні комутативних і не комутативних двохоперандних СЕТ-операцій. Наведено структури систем реалізації даних сценаріїв.

3. Для забезпечення однозначного сприйняття задач і результатів дослідження наводяться основні поняття і визначення стосовно потокового СЕТ-шифрування які необхідні для даної дисертаційної роботи.

4. На основі реалізації послідовності дискретних перетворень будується група моделей некомутативних двохоперандних двохрозрядних СЕТ-операціях подвійного циклу, кожна з яких забезпечує перестановку операндів. В основу побудови даної групи було покладено групу СЕТ-операцій з точністю до перестановки результатів перетворення. Дану групу було отримано на основі повного перебору можливих варіантів розміщення 2Сі-квантових одноопераднихСЕТ-операціях в 2Сі-квантовій двохоперандній СЕТ-операції.

5. Отримані результати забезпечили можливість удосконалення технології побудови удосконалених моделей некомутативних двохоперандних СЕТ-операції. Сутність удосконалено полягає в заміні повторного використання технології для знаходження удосконаленої моделі після перестановки операндів на зміну змінних в удосконаленій моделі СЕТ-операції до перестановки операндів. Це забезпечує прямий перехід від моделі СЕТ-операції до перестановки операндів, до моделі СЕТ-операції після перестановки операндів.

6. Результати розділу опубліковані: [2], [10], [11], [14].

РОЗДІЛ 3. МОДЕЛЮВАННЯ НЕСИМЕТРИЧНИХ ДВОХРОЗРЯДНИХ ДВОХОПЕРАНДНИХ ОПЕРАЦІЙ КРИПТОПЕРЕТВОРЕННЯ

Моделювання несиметричних 2Сі-квантових двохоперандних СЕТ-операцій які допускають перестановку операндів за результатами обчислювального експерименту складна і праце ємна задача. Основний недолік в вирішенні наукової задачі полягає в обмеженні можливості отримання наукових результатів наявними результатами обчислювального експерименту. Подальший розвиток синтезу і дослідження СЕТ-операцій для потокового шифрування залежить від можливості переходу від побудови моделей операцій за результатами обчислювального експерименту до побудови моделей СЕТ-операцій за встановленими правилами їх синтезу. Даний перехід дозволить суттєво зменшити обмеження на розрядність (кількість вхідних Сі-квантів інформації) СЕТ-операцій, а також автоматизувати процес їх синтезу і дослідження [10].

3.1. Моделювання групи несиметричних двохоперандних двохрозрядних операцій подвійного циклу на основі дублювання одноопераднних двохрозрядних операцій базової групи

При розробці методів синтезу симетричних двохоперандних двохрозрядних операцій застосовувався підхід який полягає в наступному [80, 81, 93, 94]:

- вибір симетричної двохоперандної операції криптоперетворення на основі якої буде будуватися група операцій;
- визначення на основі вибраної операції нульової операції групи шляхом виділення в ній частини операції для обробки першого операнда та іншої частини операції для обробки другого операнда.

Будемо вважати що визначена нульова операція була побудована на основі поєднання одноопераднних двохрозрядних нульових операцій $C(x,y)=\begin{bmatrix}x_1\\x_2\end{bmatrix}\oplus\begin{bmatrix}y_1\\y_2\end{bmatrix}=\begin{bmatrix}x_1\oplus y_1\\x_2\oplus y_2\end{bmatrix}$, де x_1 і x_2 вирази для обробки першого та другого розряду (байту) першого операнда відповідно, де y_1 і y_2 вирази для обробки першого та другого розряду (байту) другого операнда відповідно;

- синтез другої базової двохоперандної двохрозрядної операції криптоперетворення шляхом поєднання результатів перетворення першого та другого операндів нульової операції на основі другої базової одноопераднної двохрозрядної операції

$$C(x,y)=\begin{bmatrix}x_1\oplus x_2\\x_2\end{bmatrix}\oplus\begin{bmatrix}y_1\oplus y_2\\y_2\end{bmatrix};$$

- синтез третьої базової двохоперандної двохрозрядної операції криптоперетворення шляхом поєднання результатів перетворення першого та другого операндів нульової операції на основі третьої базової одноопераднної двохрозрядної операції

$$C(x,y)=\begin{bmatrix}x_1\\x_1\oplus x_2\end{bmatrix}\oplus\begin{bmatrix}y_1\\y_1\oplus y_2\end{bmatrix};$$

- використання разом з операціями базової групи операцій перестановок;
- виконання разом з операціями базової групи та з операціями базової групи в поєднанні з операціями перестановок операцій інверсії.

Використаємо даний підхід для синтезу групи несиметричних двохоперандних двохрозрядних операцій крипто перетворення [8, 10].

Визначимо в якості нульової операції пронумерований кортеж який включає в себе наступну послідовність одноопераднних операцій $C_1(x)$, $C_7(x)$, $C_{19}(x)$, $C_{13}(x)$. Цей кортеж одноопераднних СЕТ-операцій представляє собою двох розрядну двлхоперандну СЕТ-операцію

$C_{1,7,19,13}(x,y)$. Дана операція була вибрана в якості нульової тому що за результатами обчислювального експерименту. Вона була синтезована першою несиметричною операцією (додаток 1), і крім того її математична модель вже була побудована в підрозділі 2.2.. Модель оберненої операції, яка за результатами обчислювального експерименту була визначена як кортеж із $C_3(x)$, $C_9(x)$, $C_{15}(x)$, $C_{21}(x)$ (СЕТ-операція $C_{3,9,15,21}(x,y)$), також в підрозділі 2.2 побудована математична модель даної операції. Крім того в підрозділі 2.2 було побудована наперед визначена множина несиметричних двохоперандних двохрозрядних операцій подвійного циклу, яка включає дану операцію. Синтез групи двохоперандних двохрозрядних операцій на основі операції $C_{1,7,19,13}(x,y)$, забезпечить можливість порівняти синтезовану групу операцій з множиною операцій подвійного циклу визначеною підрозділі 2.2, і представлену побудованими математичними моделями в підрозділі 2.2.

Зверніть увагу, що результати обчислювального експерименту (додаток 1) встановлюють лише взаємозв'язок між кортежами, що задають пряму операцію і операцію після перестановки операндів, а синтез групи операцій встановлює взаємозв'язки лише між прямими операціями в групі. Виходячи з цього необхідно реалізувати наступний алгоритм синтезу операцій взаємоперетворення [2]:

- синтезується математична модель наступної операції в групі несиметричних двохрозрядних двохоперандних операцій криптоперетворення;
- виконується перехід від математичної моделі несиметричної двохрозрядної двохоперандної операції кодування до кортежа операції кодування;
- на основі результатів обчислювального експерименту (додаток 1) для кортежу операції кодування знаходимо відповідний йому кортеж операції декодування;

- на основі знайденого кортежу операції декодування будуємо розширену і вдосконалену математичні моделі операції декодування.

Запропонований алгоритм можна розглядати як удосконалення методу синтезу двохоперандних двохрозрядних операцій криптографічного перетворення для забезпечення можливості додаткового синтезу несиметричних двохоперандних двохрозрядних операцій.

Застосуємо даний підхід для синтезу групи несиметричних двохоперандних двохрозрядних операцій криптографічного перетворення інформації [2].

Визначимо нульову операцію групи на основі операції $C_{1,7,19,13}(x,y)$ (першу операцію базової групи) [10]:

$$C_{1,7,19,13}(x,y)=\begin{bmatrix} x_1 \oplus y_1 \\ x_2 \oplus y_1 \oplus y_2 \end{bmatrix}=\begin{bmatrix} x_1 \\ x_2 \end{bmatrix}\oplus\begin{bmatrix} y_1 \\ y_1 \oplus y_2 \end{bmatrix} \quad (3.1)$$

Синтезуємо другу двохоперандну двохрозрядну операцію криптоперетворення базової групи, на основі другої базової одноопераднної двохрозрядної базової операції $C=\begin{bmatrix} x_1 \oplus x_2 \\ x_2 \end{bmatrix}$, шляхом поєднання результатів перетворення першого та другого операндів нульової операції $C(x,y)=\begin{bmatrix} x_1 \oplus x_2 \\ x_2 \end{bmatrix}\oplus\begin{bmatrix} y_1 \oplus y_2 \\ y_2 \end{bmatrix}$. Підставивши в типову другу базову операцію вирази розрахунку операндів нульової операцію отримаємо:

$$\begin{aligned} C(x,y)&=\begin{bmatrix} x_1^* \oplus x_2^* \\ x_2^* \end{bmatrix}\oplus\begin{bmatrix} y_1^* \oplus y_2^* \\ y_2^* \end{bmatrix}=\begin{bmatrix} x_1 \oplus x_2 \\ x_2 \end{bmatrix}\oplus\begin{bmatrix} y_1 \oplus (y_1 \oplus y_2) \\ y_1 \oplus y_2 \end{bmatrix}= \\ &=\begin{bmatrix} x_1 \oplus x_2 \\ x_2 \end{bmatrix}\oplus\begin{bmatrix} y_2 \\ y_1 \oplus y_2 \end{bmatrix}=\begin{bmatrix} x_1 \oplus x_2 \oplus y_2 \\ x_2 \oplus y_1 \oplus y_2 \end{bmatrix} \end{aligned}. \quad (3.2)$$

Для знаходження оберненої операції визначимо кортеж одноопераднних операцій який реалізується синтезованою базовою операцією:

$$C(x,y)=\begin{cases}\begin{bmatrix}x_1\oplus x_2\oplus y_2\\ x_2\oplus y_1\oplus y_2\end{bmatrix}=\begin{bmatrix}x_1\oplus x_2\\ x_2\end{bmatrix}, \text{ якщо } y_1=0;\ y_2=0\\ \begin{bmatrix}x_1\oplus x_2\oplus y_2\\ x_2\oplus y_1\oplus y_2\end{bmatrix}=\begin{bmatrix}x_1\oplus x_2\oplus 1\\ x_2\oplus 1\end{bmatrix}, \text{якщо } y_1=0;\ y_2=1\\ \begin{bmatrix}x_1\oplus x_2\oplus y_2\\ x_2\oplus y_1\oplus y_2\end{bmatrix}=\begin{bmatrix}x_1\oplus x_2\\ x_2\oplus 1\end{bmatrix}, \text{якщо } y_1=1;\ y_2=0\\ \begin{bmatrix}x_1\oplus x_2\oplus y_2\\ x_2\oplus y_1\oplus y_2\end{bmatrix}=\begin{bmatrix}x_1\oplus x_2\oplus 1\\ x_2\end{bmatrix}, \text{якщо } y_1=1;\ y_2=1\end{cases}=\begin{cases}C_2, \text{ якщо } y_1=0;\ y_2=0\\ C_{20}, \text{якщо } y_1=0;\ y_2=1\\ C_8, \text{ якщо } y_1=1;\ y_2=0\\ C_{14}, \text{якщо } y_1=1;\ y_2=1\end{cases}=C_{2,20,8,14}(x,y)$$

Знайдемо обернену операцію до операції $C_{2,20,8,14}(x,y)$. Згідно виразу (2.53) оберненою операцією буде операція $C_{5,23,17,11}(x,y)=\begin{bmatrix}x_2\oplus y_1\oplus y_2\\ x_1\oplus x_2\oplus y_2\end{bmatrix}$ [10].

Синтезуємо третю двохоперандну двохрозрядну операцію криптоперетворення базової групи, на основі другої базової одноопераднної двохрозрядної базової операції $C=\begin{bmatrix}x_1\\ x_1\oplus x_2\end{bmatrix}$. Підставимо в типову третю базову операцію $C(x,y)=\begin{bmatrix}x_1\\ x_1\oplus x_2\end{bmatrix}\oplus\begin{bmatrix}y_1\\ y_1\oplus y_2\end{bmatrix}$, вирази для перетворення першого та другого операндів нульової операції:

$$C(x,y)=\begin{bmatrix}x_1^*\\ x_1^*\oplus x_2^*\end{bmatrix}\oplus\begin{bmatrix}y_1^*\\ y_1^*\oplus y_2^*\end{bmatrix}=\begin{bmatrix}x_1\\ x_1\oplus x_2\end{bmatrix}\oplus\begin{bmatrix}y_1\\ y_1\oplus(y_1\oplus y_2)\end{bmatrix}=\begin{bmatrix}x_1\\ x_1\oplus x_2\end{bmatrix}\oplus\begin{bmatrix}y_1\\ y_2\end{bmatrix}=\begin{bmatrix}x_1\oplus y_1\\ x_1\oplus x_2\oplus y_2\end{bmatrix}. \quad (3.3)$$

Визначимо кортеж одноопераднних операцій який реалізується синтезованою третьою базовою операцією [10]:

$$C(x,y)=\begin{cases}\begin{bmatrix}x_1\oplus y_1\\ x_1\oplus x_2\oplus y_2\end{bmatrix}=\begin{bmatrix}x_1\\ x_1\oplus x_2\end{bmatrix}, \text{ якщо } y_1=0;\ y_2=0\\ \begin{bmatrix}x_1\oplus y_1\\ x_1\oplus x_2\oplus y_2\end{bmatrix}=\begin{bmatrix}x_1\\ x_1\oplus x_2\oplus 1\end{bmatrix}, \text{якщо } y_1=0;\ y_2=1\\ \begin{bmatrix}x_1\oplus y_1\\ x_1\oplus x_2\oplus y_2\end{bmatrix}=\begin{bmatrix}x_1\oplus 1\\ x_1\oplus x_2\end{bmatrix}, \text{ якщо } y_1=1;\ y_2=0\\ \begin{bmatrix}x_1\oplus y_1\\ x_1\oplus x_2\oplus y_2\end{bmatrix}=\begin{bmatrix}x_1\oplus 1\\ x_1\oplus x_2\oplus 1\end{bmatrix}, \text{якщо } y_1=1;\ y_2=1\end{cases}=\begin{cases}C_3, \text{ якщо } y_1=0;\ y_2=0\\ C_9, \text{якщо } y_1=0;\ y_2=1\\ C_{15}, \text{ якщо } y_1=1;\ y_2=0\\ C_{21}, \text{якщо } y_1=1;\ y_2=1\end{cases}=C_{3,9,15,21}(x,y)$$

Знайдемо обернену операцію. Згідно табл..2.1 оберненою операцією до операції $C_{3,9,15,21}(x,y)$ буде операція $C_{1,7,19,13}(x,y)=\begin{bmatrix}x_1\oplus y_1\\ x_2\oplus y_1\oplus y_2\end{bmatrix}$.

Для знаходження наступних трьох операцій виконаємо разом з операціями базової групи операції перестановки операндів.

Переставимо перший і другий операнди нульової операції синтезованої на основі одноопераднної двохрозрядної операції $C=\begin{bmatrix} x_2 \\ x_1 \end{bmatrix}$, виконавши двохоперандну двох розрядну операцію $C=\begin{bmatrix} X_2 \\ X_1 \end{bmatrix}$ (в даній операції позначено вирази які реалізують перший і другий операнда початкової операції як X_1 і X_2 відповідно).

$$C(x,y)=\begin{bmatrix} X_2 \\ X_1 \end{bmatrix}=\begin{bmatrix} x_2 \oplus y_1 \oplus y_2 \\ x_1 \oplus y_1 \end{bmatrix}. \qquad (3.4)$$

Побудувати дану операцію можна також на основі одноопераднної двохрозрядної операції $C=\begin{bmatrix} x_2 \\ x_1 \end{bmatrix}$, якій відповідає, для даного методу синтезу, типова двохоперандна двохрозрядна операція $C(x,y)=\begin{bmatrix} x_2 \\ x_1 \end{bmatrix}\oplus\begin{bmatrix} y_2 \\ y_1 \end{bmatrix}$. Підставимо в дану типову операцію вирази для перетворення першого та другого операндів нульової операції:

$$C(x,y)=\begin{bmatrix} x_2^* \\ x_1^* \end{bmatrix}\oplus\begin{bmatrix} y_2^* \\ y_1^* \end{bmatrix}=\begin{bmatrix} x_2 \\ x_1 \end{bmatrix}\oplus\begin{bmatrix} y_1 \oplus y_2 \\ y_1 \end{bmatrix}=\begin{bmatrix} x_2 \oplus y_1 \oplus y_2 \\ x_1 \oplus y_1 \end{bmatrix}.$$

Визначимо кортеж одноопераднних операцій який реалізується синтезованою операцією

$$C(x,y)=\begin{cases} \begin{bmatrix} x_2 \oplus y_1 \oplus y_2 \\ x_1 \oplus y_1 \end{bmatrix}=\begin{bmatrix} x_2 \\ x_1 \end{bmatrix},\ якщо\ y_1=0;\ y_2=0 \\ \begin{bmatrix} x_2 \oplus y_1 \oplus y_2 \\ x_1 \oplus y_1 \end{bmatrix}=\begin{bmatrix} x_2 \oplus 1 \\ x_1 \end{bmatrix}, якщо\ y_1=0;\ y_2=1 \\ \begin{bmatrix} x_2 \oplus y_1 \oplus y_2 \\ x_1 \oplus y_1 \end{bmatrix}=\begin{bmatrix} x_2 \oplus 1 \\ x_1 \oplus 1 \end{bmatrix},\ якщо\ y_1=1;\ y_2=0 \\ \begin{bmatrix} x_2 \oplus y_1 \oplus y_2 \\ x_1 \oplus y_1 \end{bmatrix}=\begin{bmatrix} x_2 \\ x_1 \oplus 1 \end{bmatrix}, якщо\ y_1=1;\ y_2=1 \end{cases}=\begin{cases} C_4,\ якщо\ y_1=0;\ y_2=0 \\ C_{16}, якщо\ y_1=0;\ y_2=1 \\ C_{22},\ якщо\ y_1=1;\ y_2=0 \\ C_{10}, якщо\ y_1=1;\ y_2=1 \end{cases}=C_{4,16,22,10}(x,y)$$

Знайдемо обернену операцію до операції $C_{4,16,22,10}(x,y)$. Згідно виразу (2.29) оберненою операцією буде операція $C_{6,18,12,24}(x,y)=\begin{bmatrix} x_1 \oplus x_2 \oplus y_2 \\ x_1 \oplus y_1 \end{bmatrix}$.

Переставимо перший і другий операнди другої операції базової групи синтезованої на основі одноопераднної двохрозрядної операції $C=\begin{bmatrix} x_1 \oplus x_2 \\ x_2 \end{bmatrix}$, виконавши операцію $C=\begin{bmatrix} X_2 \\ X_1 \end{bmatrix}$.

$$C(x,y)=\begin{bmatrix} X_2 \\ X_1 \end{bmatrix}=\begin{bmatrix} x_2 \oplus y_1 \oplus y_2 \\ x_1 \oplus x_2 \oplus y_2 \end{bmatrix}. \qquad (3.5)$$

Дану операцію також можна побудувати на основі одноопераднної двохрозрядної операції $C=\begin{bmatrix} x_2 \\ x_1 \oplus x_2 \end{bmatrix}$, якій відповідає, для даного методу синтезу, типова двохоперандна двохрозрядна операцію $C(x,y)=\begin{bmatrix} x_2 \\ x_1 \oplus x_2 \end{bmatrix} \oplus \begin{bmatrix} y_2 \\ y_1 \oplus y_2 \end{bmatrix}$.

$$C(x,y)=\begin{bmatrix} x_2^* \\ x_1^* \oplus x_2^* \end{bmatrix} \oplus \begin{bmatrix} y_2^* \\ y_1^* \oplus y_2^* \end{bmatrix}=\begin{bmatrix} x_2 \\ x_1 \oplus x_2 \end{bmatrix} \oplus \begin{bmatrix} y_2 \\ y_1 \oplus (y_1 \oplus y_2) \end{bmatrix}=\begin{bmatrix} x_2 \oplus y_1 \oplus y_2 \\ x_1 \oplus x_2 \oplus y_1 \end{bmatrix}$$

Знайдемо кортеж одноопераднних операцій який реалізується синтезованою операцією [10]

$$C(x,y)=\begin{cases} \begin{bmatrix} x_2 \oplus y_1 \oplus y_2 \\ x_1 \oplus x_2 \oplus y_2 \end{bmatrix}=\begin{bmatrix} x_2 \\ x_1 \oplus x_2 \end{bmatrix}, \text{ якщо } y_1=0;\ y_2=0 \\ \begin{bmatrix} x_2 \oplus y_1 \oplus y_2 \\ x_1 \oplus x_2 \oplus y_2 \end{bmatrix}=\begin{bmatrix} x_2 \oplus 1 \\ x_1 \oplus x_2 \oplus 1 \end{bmatrix}, \text{якщо } y_1=0;\ y_2=1 \\ \begin{bmatrix} x_2 \oplus y_1 \oplus y_2 \\ x_1 \oplus x_2 \oplus y_2 \end{bmatrix}=\begin{bmatrix} x_2 \oplus 1 \\ x_1 \oplus x_2 \end{bmatrix}, \text{якщо } y_1=1;\ y_2=0 \\ \begin{bmatrix} x_2 \oplus y_1 \oplus y_2 \\ x_1 \oplus x_2 \oplus y_2 \end{bmatrix}=\begin{bmatrix} x_2 \\ x_1 \oplus x_2 \oplus 1 \end{bmatrix}, \text{якщо } y_1=1;\ y_2=1 \end{cases} = \begin{cases} C_5, \text{ якщо } y_1=0;\ y_2=0 \\ C_{23}, \text{якщо } y_1=0;\ y_2=1 \\ C_{17}, \text{ якщо } y_1=1;\ y_2=0 \\ C_{11}, \text{якщо } y_1=1;\ y_2=1 \end{cases} = C_{5,23,17,11}(x,y)$$

Згідно виразу (2.52) оберненою операцією до операція $C_{5,23,17,11}(x,y)$. буде операція $C_{2,20,8,14}(x,y)=\begin{bmatrix} x_1 \oplus x_2 \oplus y_2 \\ x_2 \oplus y_1 \oplus y_2 \end{bmatrix}$.

Переставимо перший і другий операнди третьої операції базової групи синтезованої на основі одноопераднної двохрозрядної операції $C=\begin{bmatrix} x_1 \\ x_2 \oplus x_2 \end{bmatrix}$, виконавши операцію $C=\begin{bmatrix} X_2 \\ X_1 \end{bmatrix}$.

$$C(x,y)=\begin{bmatrix} X_2 \\ X_1 \end{bmatrix}=\begin{bmatrix} x_1 \oplus x_2 \oplus y_2 \\ x_1 \oplus y_1 \end{bmatrix}. \tag{3.6}$$

Дану операцію також можна побудувати на основі одноопераднної двохрозрядної операції $C=\begin{bmatrix} x_1 \oplus x_2 \\ x_1 \end{bmatrix}$, якій відповідає типова двохоперандна двохрозрядна операцію $C(x,y)=\begin{bmatrix} x_1 \oplus x_2 \\ x_1 \end{bmatrix} \oplus \begin{bmatrix} y_1 \oplus y_2 \\ y_1 \end{bmatrix}$.

$$C(x,y)=\begin{bmatrix} x_1^* \oplus x_2^* \\ x_1^* \end{bmatrix} \oplus \begin{bmatrix} y_1^* \oplus y_2^* \\ y_1^* \end{bmatrix}=\begin{bmatrix} x_1 \oplus x_2 \\ x_1 \oplus \end{bmatrix} \oplus \begin{bmatrix} y_1 \oplus (y_1 \oplus y_2) \\ y_1 \end{bmatrix}=\begin{bmatrix} x_1 \oplus x_2 \oplus y_2 \\ x_1 \oplus y_1 \end{bmatrix}$$

Знайдемо обернену операцію до синтезованої.

$$C(x,y)=\begin{cases} \begin{bmatrix} x_1 \oplus x_2 \oplus y_2 \\ x_1 \oplus y_1 \end{bmatrix}=\begin{bmatrix} x_1 \oplus x_2 \\ x_1 \end{bmatrix}, \text{ якщо } y_1=0;\ y_2=0 \\ \begin{bmatrix} x_1 \oplus x_2 \oplus y_2 \\ x_1 \oplus y_1 \end{bmatrix}=\begin{bmatrix} x_1 \oplus x_2 \oplus 1 \\ x_1 \end{bmatrix}, \text{якщо } y_1=0;\ y_2=1 \\ \begin{bmatrix} x_1 \oplus x_2 \oplus y_2 \\ x_1 \oplus y_1 \end{bmatrix}=\begin{bmatrix} x_1 \oplus x_2 \\ x_1 \oplus 1 \end{bmatrix}, \text{ якщо } y_1=1;\ y_2=0 \\ \begin{bmatrix} x_1 \oplus x_2 \oplus y_2 \\ x_1 \oplus y_1 \end{bmatrix}=\begin{bmatrix} x_1 \oplus x_2 \oplus 1 \\ x_1 \oplus 1 \end{bmatrix}, \text{якщо } y_1=1;\ y_2=1 \end{cases} = \begin{cases} C_6, \text{ якщо } y_1=0;\ y_2=0 \\ C_{18}, \text{якщо } y_1=0;\ y_2=1 \\ C_{12}, \text{ якщо } y_1=1;\ y_2=0 \\ C_{24}, \text{якщо } y_1=1;\ y_2=1 \end{cases} = C_{6,18,12,24}(x,y)$$

Згідно виразу (2.28) оберненою операцією до операції $C_{6,18,12,24}(x,y)$. буде операція $C_{4,16,22,10}(x,y)=\begin{bmatrix} x_1 \oplus y_1 \\ x_2 \oplus y_1 \oplus y_2 \end{bmatrix}$.

Виконаємо разом з операціями базової групи та з операціями базової групи в поєднанні з операціями перестановок операцій інверсії.

Синтезуємо на основі нульової операції групи ще три операції, для цього виконаємо над нею: інверсію першого операнда; інверсію другого операнда; інверсію першого та другого операндів.

- Підставивши в нульову операцію (3.1) додатково інверсію першого операнда отримаємо: $C(x,y)=\begin{bmatrix} X_1 \oplus 1 \\ X_2 \end{bmatrix}=\begin{bmatrix} x_1 \oplus y_1 \oplus 1 \\ x_2 \oplus y_1 \oplus y_2 \end{bmatrix}$

Знайдемо операцію декодування до синтезованої операції:

$$C(x,y)=\begin{cases} \begin{bmatrix} x_1 \oplus y_1 \oplus 1 \\ x_2 \oplus y_1 \oplus y_2 \end{bmatrix}=\begin{bmatrix} x_1 \oplus 1 \\ x_2 \end{bmatrix}, \text{ якщо } y_1=0;\ y_2=0 \\ \begin{bmatrix} x_1 \oplus y_1 \oplus 1 \\ x_2 \oplus y_1 \oplus y_2 \end{bmatrix}=\begin{bmatrix} x_1 \oplus 1 \\ x_2 \oplus 1 \end{bmatrix}, \text{якщо } y_1=0;\ y_2=1 \\ \begin{bmatrix} x_1 \oplus y_1 \oplus 1 \\ x_2 \oplus y_1 \oplus y_2 \end{bmatrix}=\begin{bmatrix} x_1 \\ x_2 \oplus 1 \end{bmatrix}, \text{ якщо } y_1=1;\ y_2=0 \\ \begin{bmatrix} x_1 \oplus y_1 \oplus 1 \\ x_2 \oplus y_1 \oplus y_2 \end{bmatrix}=\begin{bmatrix} x_1 \\ x_2 \end{bmatrix}, \text{якщо } y_1=1;\ y_2=1 \end{cases} = \begin{cases} C_{13}, \text{ якщо } y_1=0;\ y_2=0 \\ C_{19}, \text{якщо } y_1=0;\ y_2=1 \\ C_7, \text{ якщо } y_1=1;\ y_2=0 \\ C_1, \text{якщо } y_1=1;\ y_2=1 \end{cases} = C_{13,19,7,1}(x,y)$$

Згідно виразу (2.16) оберненою операцією буде операція $C_{15,21,3,9}(x,y)=\begin{bmatrix} x_1 \oplus y_1 \oplus 1 \\ x_1 \oplus x_2 \oplus y_2 \end{bmatrix}$.

- Підставивши в нульову операцію (3.1) додатково інверсію другого операнда отримаємо: $C(x,y)=\begin{bmatrix} X_1 \\ X_2 \oplus 1 \end{bmatrix}=\begin{bmatrix} x_1 \oplus y_1 \\ x_2 \oplus y_1 \oplus y_2 \oplus 1 \end{bmatrix}$

Знайдемо операцію декодування.

$$C(x,y)=\begin{cases} \begin{bmatrix} x_1 \oplus y_1 \\ x_2 \oplus y_1 \oplus y_2 \oplus 1 \end{bmatrix}=\begin{bmatrix} x_1 \\ x_2 \oplus 1 \end{bmatrix}, \text{ якщо } y_1=0;\ y_2=0 \\ \begin{bmatrix} x_1 \oplus y_1 \\ x_2 \oplus y_1 \oplus y_2 \oplus 1 \end{bmatrix}=\begin{bmatrix} x_1 \\ x_2 \end{bmatrix}, \text{якщо } y_1=0;\ y_2=1 \\ \begin{bmatrix} x_1 \oplus y_1 \\ x_2 \oplus y_1 \oplus y_2 \oplus 1 \end{bmatrix}=\begin{bmatrix} x_1 \oplus 1 \\ x_2 \end{bmatrix}, \text{ якщо } y_1=1;\ y_2=0 \\ \begin{bmatrix} x_1 \oplus y_1 \\ x_2 \oplus y_1 \oplus y_2 \oplus 1 \end{bmatrix}=\begin{bmatrix} x_1 \oplus 1 \\ x_2 \oplus 1 \end{bmatrix}, \text{якщо } y_1=1;\ y_2=1 \end{cases} = \begin{cases} C_7, \text{ якщо } y_1=0;\ y_2=0 \\ C_1, \text{якщо } y_1=0;\ y_2=1 \\ C_{13}, \text{ якщо } y_1=1;\ y_2=0 \\ C_{19}, \text{якщо } y_1=1;\ y_2=1 \end{cases} = C_{7,1,13,19}(x,y)$$

Згідно виразу (2.10) оберненою операцією буде операція $C_{9,3,21,15}(x,y)=\begin{bmatrix} x_1 \oplus y_1 \\ x_1 \oplus x_2 \oplus y_2 \oplus 1 \end{bmatrix}$.

- Підставивши в нульову операцію (3.1) додаткові інверсії першого другого операнда отримаємо: $C(x,y)=\begin{bmatrix} X_1 \oplus 1 \\ X_2 \oplus 1 \end{bmatrix}=\begin{bmatrix} x_1 \oplus y_1 \oplus 1 \\ x_2 \oplus y_1 \oplus y_2 \oplus 1 \end{bmatrix}$

Знайдемо операцію декодування.

$$C(x,y)=\begin{cases}\begin{bmatrix}x_1\oplus y_1\oplus 1\\ x_2\oplus y_1\oplus y_2\oplus 1\end{bmatrix}=\begin{bmatrix}x_1\oplus 1\\ x_2\oplus 1\end{bmatrix}, \text{ якщо } y_1=0;\ y_2=0\\ \begin{bmatrix}x_1\oplus y_1\oplus 1\\ x_2\oplus y_1\oplus y_2\oplus 1\end{bmatrix}=\begin{bmatrix}x_1\oplus 1\\ x_2\end{bmatrix}, \text{якщо } y_1=0;\ y_2=1\\ \begin{bmatrix}x_1\oplus y_1\oplus 1\\ x_2\oplus y_1\oplus y_2\oplus 1\end{bmatrix}=\begin{bmatrix}x_1\\ x_2\end{bmatrix}, \text{ якщо } y_1=1;\ y_2=0\\ \begin{bmatrix}x_1\oplus y_1\oplus 1\\ x_2\oplus y_1\oplus y_2\oplus 1\end{bmatrix}=\begin{bmatrix}x_1\\ x_2\oplus 1\end{bmatrix}, \text{якщо } y_1=1;\ y_2=1\end{cases}=\begin{cases}C_{19}, \text{ якщо } y_1=0;\ y_2=0\\ C_{13}, \text{якщо } y_1=0;\ y_2=1\\ C_1, \text{ якщо } y_1=1;\ y_2=0\\ C_7, \text{якщо } y_1=1;\ y_2=1\end{cases}=C_{19,13,1,7}(x,y)$$

Згідно виразу (2.23) оберненою операцією буде операція $C_{21,15,9,3}(x,y)=\begin{bmatrix}x_1\oplus y_1\oplus 1\\ x_1\oplus x_2\oplus y_2\oplus 1\end{bmatrix}$.

Синтезуємо на основі другої операції базової групи (3.2) ще три операції криптографічного перетворення [9].

- Підставивши в другу базову операцію (3.2) додатково інверсію першого операнда отримаємо: $C(x,y)=\begin{bmatrix}X_1\oplus 1\\ X_2\end{bmatrix}=\begin{bmatrix}x_1\oplus x_2\oplus y_2\oplus 1\\ x_2\oplus y_1\oplus y_2\end{bmatrix}$

Знайдемо операцію декодування до синтезованої операції:

$$C(x,y)=\begin{cases}\begin{bmatrix}x_1\oplus x_2\oplus y_2\oplus 1\\ x_2\oplus y_1\oplus y_2\end{bmatrix}=\begin{bmatrix}x_1\oplus x_2\oplus 1\\ x_2\end{bmatrix}, \text{ якщо } y_1=0;\ y_2=0\\ \begin{bmatrix}x_1\oplus x_2\oplus y_2\oplus 1\\ x_2\oplus y_1\oplus y_2\end{bmatrix}=\begin{bmatrix}x_1\oplus x_2\\ x_2\oplus 1\end{bmatrix}, \text{якщо } y_1=0;\ y_2=1\\ \begin{bmatrix}x_1\oplus x_2\oplus y_2\oplus 1\\ x_2\oplus y_1\oplus y_2\end{bmatrix}=\begin{bmatrix}x_1\oplus x_2\oplus 1\\ x_2\oplus 1\end{bmatrix}, \text{ якщо } y_1=1;\ y_2=0\\ \begin{bmatrix}x_1\oplus x_2\oplus y_2\oplus 1\\ x_2\oplus y_1\oplus y_2\end{bmatrix}=\begin{bmatrix}x_1\oplus x_2\\ x_2\end{bmatrix}, \text{якщо } y_1=1;\ y_2=1\end{cases}=\begin{cases}C_{14}, \text{ якщо } y_1=0;\ y_2=0\\ C_8, \text{якщо } y_1=0;\ y_2=1\\ C_{20}, \text{ якщо } y_1=1;\ y_2=0\\ C_2, \text{якщо } y_1=1;\ y_2=1\end{cases}=C_{14,8,20,2}(x.y)$$

Згідно виразу (2.65) оберненою операцією буде операція $C_{17,11,5,23}(x,y)=\begin{bmatrix}x_2\oplus y_1\oplus y_2\oplus 1\\ x_1\oplus x_2\oplus y_2\end{bmatrix}$.

- Підставивши в другу базову операцію (3.2) додатково інверсію другого операнда отримаємо: $C(x,y)=\begin{bmatrix}X_1\\ X_2\oplus 1\end{bmatrix}=\begin{bmatrix}x_1\oplus x_2\oplus y_2\\ x_2\oplus y_1\oplus y_2\oplus 1\end{bmatrix}$

Знайдемо операцію декодування до синтезованої операції:

$$C(x,y)=\begin{cases}\begin{bmatrix}x_1\oplus x_2\oplus y_2\\ x_2\oplus y_1\oplus y_2\oplus 1\end{bmatrix}=\begin{bmatrix}x_1\oplus x_2\\ x_2\oplus 1\end{bmatrix}, \text{ якщо } y_1=0;\ y_2=0\\ \begin{bmatrix}x_1\oplus x_2\oplus y_2\\ x_2\oplus y_1\oplus y_2\oplus 1\end{bmatrix}=\begin{bmatrix}x_1\oplus x_2\oplus 1\\ x_2\end{bmatrix}, \text{якщо } y_1=0;\ y_2=1\\ \begin{bmatrix}x_1\oplus x_2\oplus y_2\\ x_2\oplus y_1\oplus y_2\oplus 1\end{bmatrix}=\begin{bmatrix}x_1\oplus x_2\\ x_2\end{bmatrix}, \text{якщо } y_1=1;\ y_2=0\\ \begin{bmatrix}x_1\oplus x_2\oplus y_2\\ x_2\oplus y_1\oplus y_2\oplus 1\end{bmatrix}=\begin{bmatrix}x_1\oplus x_2\oplus 1\\ x_2\oplus 1\end{bmatrix}, \text{якщо } y_1=1;\ y_2=1\end{cases}=\begin{cases}C_8, \text{ якщо } y_1=0;\ y_2=0\\ C_{14}, \text{якщо } y_1=0;\ y_2=1\\ C_2, \text{ якщо } y_1=1;\ y_2=0\\ C_{20}, \text{якщо } y_1=1;\ y_2=1\end{cases}=C_{8,14,2,20}(x,y)$$

Згідно виразу (2.59) оберненою операцією буде операція $C_{11,17,23,5}(x,y)=\begin{bmatrix}x_2\oplus y_1\oplus y_2\\ x_1\oplus x_2\oplus y_2\oplus 1\end{bmatrix}$.

- Підставивши в другу базову операцію (3.2) додаткові інверсії першого та другого операндів отримаємо: $C(x,y)=\begin{bmatrix}X_1\oplus 1\\ X_2\oplus 1\end{bmatrix}=\begin{bmatrix}x_1\oplus x_2\oplus y_2\oplus 1\\ x_2\oplus y_1\oplus y_2\oplus 1\end{bmatrix}$

Знайдемо операцію декодування до синтезованої операції:

$$C(x,y)=\begin{cases}\begin{bmatrix}x_1\oplus x_2\oplus y_2\oplus 1\\ x_2\oplus y_1\oplus y_2\oplus 1\end{bmatrix}=\begin{bmatrix}x_1\oplus x_2\oplus 1\\ x_2\oplus 1\end{bmatrix}, \text{ якщо } y_1=0;\ y_2=0\\ \begin{bmatrix}x_1\oplus x_2\oplus y_2\oplus 1\\ x_2\oplus y_1\oplus y_2\oplus 1\end{bmatrix}=\begin{bmatrix}x_1\oplus x_2\\ x_2\end{bmatrix}, \text{якщо } y_1=0;\ y_2=1\\ \begin{bmatrix}x_1\oplus x_2\oplus y_2\oplus 1\\ x_2\oplus y_1\oplus y_2\oplus 1\end{bmatrix}=\begin{bmatrix}x_1\oplus x_2\oplus 1\\ x_2\end{bmatrix}, \text{ якщо } y_1=1;\ y_2=0\\ \begin{bmatrix}x_1\oplus x_2\oplus y_2\oplus 1\\ x_2\oplus y_1\oplus y_2\oplus 1\end{bmatrix}=\begin{bmatrix}x_1\oplus x_2\\ x_2\oplus 1\end{bmatrix}, \text{якщо } y_1=1;\ y_2=1\end{cases}=\begin{cases}C_{20}, \text{ якщо } y_1=0;\ y_2=0\\ C_2, \text{якщо } y_1=0;\ y_2=1\\ C_{14}, \text{ якщо } y_1=1;\ y_2=0\\ C_8, \text{якщо } y_1=1;\ y_2=1\end{cases}=C_{20,2,14,8}(x,y)$$

Згідно виразу (2.71) оберненою операцією буде операція $C_{23,5,11,17}(x,y)=\begin{bmatrix}x_2\oplus y_1\oplus y_2\oplus 1\\ x_1\oplus x_2\oplus y_2\oplus 1\end{bmatrix}$.

Синтезуємо на основі третьої операції базової групи (3.3) ще три операції криптографічного перетворення [9].

- Підставивши в третю базову операцію (3.3) додатково інверсію першого операнда отримаємо: $C(x,y)=\begin{bmatrix} X_1 \oplus 1 \\ X_2 \end{bmatrix}=\begin{bmatrix} x_1 \oplus y_1 \oplus 1 \\ x_1 \oplus x_2 \oplus y_2 \end{bmatrix}$

Знайдемо операцію декодування до синтезованої операції:

$$C(x,y)=\begin{cases} \begin{bmatrix} x_1 \oplus y_1 \oplus 1 \\ x_1 \oplus x_2 \oplus y_2 \end{bmatrix}=\begin{bmatrix} x_1 \oplus 1 \\ x_1 \oplus x_2 \end{bmatrix}, \text{ якщо } y_1=0;\ y_2=0 \\ \begin{bmatrix} x_1 \oplus y_1 \oplus 1 \\ x_1 \oplus x_2 \oplus y_2 \end{bmatrix}=\begin{bmatrix} x_1 \oplus 1 \\ x_1 \oplus x_2 \oplus 1 \end{bmatrix}, \text{якщо } y_1=0;\ y_2=1 \\ \begin{bmatrix} x_1 \oplus y_1 \oplus 1 \\ x_1 \oplus x_2 \oplus y_2 \end{bmatrix}=\begin{bmatrix} x_1 \\ x_1 \oplus x_2 \end{bmatrix}, \text{ якщо } y_1=1;\ y_2=0 \\ \begin{bmatrix} x_1 \oplus y_1 \oplus 1 \\ x_1 \oplus x_2 \oplus y_2 \end{bmatrix}=\begin{bmatrix} x_1 \\ x_1 \oplus x_2 \oplus 1 \end{bmatrix}, \text{якщо } y_1=1;\ y_2=1 \end{cases} = \begin{cases} C_{15}, \text{ якщо } y_1=0;\ y_2=0 \\ C_{21}, \text{якщо } y_1=0;\ y_2=1 \\ C_3, \text{ якщо } y_1=1;\ y_2=0 \\ C_9, \text{якщо } y_1=1;\ y_2=1 \end{cases} = C_{15,21,3,9}(x,y)$$

Згідно виразу (2.17) оберненою операцією до операції $C_{15,21,3,9}(x,y)$ буде операція $C_{13,19,7,1}(x,y)=\begin{bmatrix} x_1 \oplus y_1 \oplus 1 \\ x_2 \oplus y_1 \oplus y_2 \end{bmatrix}$.

- Підставивши в третю базову операцію (3.3) додатково інверсію другого операнда отримаємо: $C(x,y)=\begin{bmatrix} X_1 \\ X_2 \oplus 1 \end{bmatrix}=\begin{bmatrix} x_1 \oplus y_1 \\ x_1 \oplus x_2 \oplus y_2 \oplus 1 \end{bmatrix}$

Знайдемо операцію декодування до синтезованої операції:

$$C(x,y)=\begin{cases} \begin{bmatrix} x_1 \oplus y_1 \\ x_1 \oplus x_2 \oplus y_2 \oplus 1 \end{bmatrix}=\begin{bmatrix} x_1 \\ x_1 \oplus x_2 \oplus 1 \end{bmatrix}, \text{ якщо } y_1=0;\ y_2=0 \\ \begin{bmatrix} x_1 \oplus y_1 \\ x_1 \oplus x_2 \oplus y_2 \oplus 1 \end{bmatrix}=\begin{bmatrix} x_1 \\ x_1 \oplus x_2 \end{bmatrix}, \text{якщо } y_1=0;\ y_2=1 \\ \begin{bmatrix} x_1 \oplus y_1 \\ x_1 \oplus x_2 \oplus y_2 \oplus 1 \end{bmatrix}=\begin{bmatrix} x_1 \oplus 1 \\ x_1 \oplus x_2 \oplus 1 \end{bmatrix}, \text{ якщо } y_1=1;\ y_2=0 \\ \begin{bmatrix} x_1 \oplus y_1 \\ x_1 \oplus x_2 \oplus y_2 \oplus 1 \end{bmatrix}=\begin{bmatrix} x_1 \oplus 1 \\ x_1 \oplus x_2 \end{bmatrix}, \text{якщо } y_1=1;\ y_2=1 \end{cases} = \begin{cases} C_9, \text{ якщо } y_1=0;\ y_2=0 \\ C_3, \text{якщо } y_1=0;\ y_2=1 \\ C_{21}, \text{ якщо } y_1=1;\ y_2=0 \\ C_{15}, \text{якщо } y_1=1;\ y_2=1 \end{cases} = C_{9,3,21,15}(x,y)$$

Згідно виразу (2.11) оберненою операцією до операції $C_{9,3,21,15}(x,y)$ буде операція $C_{7,1,13,19}(x,y)=\begin{bmatrix} x_1 \oplus y_1 \\ x_2 \oplus y_1 \oplus y_2 \oplus 1 \end{bmatrix}$.

- Підставивши в третю базову операцію (3.3) додаткові інверсії першого та другого операндів отримаємо: $C(x,y)=\begin{bmatrix} X_1 \oplus 1 \\ X_2 \oplus 1 \end{bmatrix}=\begin{bmatrix} x_1 \oplus y_1 \oplus 1 \\ x_1 \oplus x_2 \oplus y_2 \oplus 1 \end{bmatrix}$

Знайдемо операцію декодування до синтезованої операції:

$$C(x,y)=\begin{cases} \begin{bmatrix} x_1 \oplus y_1 \oplus 1 \\ x_1 \oplus x_2 \oplus y_2 \oplus 1 \end{bmatrix}=\begin{bmatrix} x_1 \oplus 1 \\ x_1 \oplus x_2 \oplus 1 \end{bmatrix}, \text{ якщо } y_1=0;\ y_2=0 \\ \begin{bmatrix} x_1 \oplus y_1 \oplus 1 \\ x_1 \oplus x_2 \oplus y_2 \oplus 1 \end{bmatrix}=\begin{bmatrix} x_1 \oplus 1 \\ x_1 \oplus x_2 \end{bmatrix}, \text{якщо } y_1=0;\ y_2=1 \\ \begin{bmatrix} x_1 \oplus y_1 \oplus 1 \\ x_1 \oplus x_2 \oplus y_2 \oplus 1 \end{bmatrix}=\begin{bmatrix} x_1 \\ x_1 \oplus x_2 \oplus 1 \end{bmatrix}, \text{ якщо } y_1=1;\ y_2=0 \\ \begin{bmatrix} x_1 \oplus y_1 \oplus 1 \\ x_1 \oplus x_2 \oplus y_2 \oplus 1 \end{bmatrix}=\begin{bmatrix} x_1 \\ x_1 \oplus x_2 \end{bmatrix}, \text{якщо } y_1=1;\ y_2=1 \end{cases} = \begin{cases} C_{21}, \text{ якщо } y_1=0;\ y_2=0 \\ C_{15}, \text{якщо } y_1=0;\ y_2=1 \\ C_9, \text{ якщо } y_1=1;\ y_2=0 \\ C_3, \text{якщо } y_1=1;\ y_2=1 \end{cases} = C_{21,15,9,3}(x,y)$$

Згідно виразу (2.23) оберненою операцією буде операція $C_{19,13,1,7}(x,y)=\begin{bmatrix} x_1 \oplus y_1 \oplus 1 \\ x_2 \oplus y_1 \oplus y_2 \oplus 1 \end{bmatrix}$.

Синтезуємо на основі операції (2.26) ще три операції криптографічного перетворення.

- Підставивши в операцію (2.26) додатково інверсію першого операнда отримаємо: $C(x,y)=\begin{bmatrix} X_1 \oplus 1 \\ X_2 \end{bmatrix}=\begin{bmatrix} x_2 \oplus y_1 \oplus y_2 \oplus 1 \\ x_1 \oplus y_1 \end{bmatrix}$.

Знайдемо операцію декодування до синтезованої операції:

$$C=\begin{cases} \begin{bmatrix} x_2 \oplus y_1 \oplus y_2 \oplus 1 \\ x_1 \oplus y_1 \end{bmatrix}=\begin{bmatrix} x_2 \oplus 1 \\ x_1 \end{bmatrix}, \text{ якщо } y_1=0;\ y_2=0 \\ \begin{bmatrix} x_2 \oplus y_1 \oplus y_2 \oplus 1 \\ x_1 \oplus y_1 \end{bmatrix}=\begin{bmatrix} x_2 \\ x_1 \end{bmatrix}, \text{якщо } y_1=0;\ y_2=1 \\ \begin{bmatrix} x_2 \oplus y_1 \oplus y_2 \oplus 1 \\ x_1 \oplus y_1 \end{bmatrix}=\begin{bmatrix} x_2 \\ x_1 \oplus 1 \end{bmatrix}, \text{ якщо } y_1=1;\ y_2=0 \\ \begin{bmatrix} x_2 \oplus y_1 \oplus y_2 \oplus 1 \\ x_1 \oplus y_1 \end{bmatrix}=\begin{bmatrix} x_2 \oplus 1 \\ x_1 \oplus 1 \end{bmatrix}, \text{якщо } y_1=1;\ y_2=1 \end{cases} = \begin{cases} C_{16}, \text{ якщо } y_1=0;\ y_2=0 \\ C_4, \text{якщо } y_1=0;\ y_2=1 \\ C_{10}, \text{ якщо } y_1=1;\ y_2=0 \\ C_{22}, \text{якщо } y_1=1;\ y_2=1 \end{cases} = C_{16,4,10,22}(x,y)$$

Згідно виразу (2.41) оберненою операцією до операції $C_{16,4,10,22}(x,y)$ буде операція $C_{18,6,24,12}(x,y)=\begin{bmatrix} x_1 \oplus x_2 \oplus y_2 \\ x_1 \oplus y_1 \end{bmatrix}$.

- Підставивши в операцію (2.41) додатково інверсію другого операнда отримаємо: $C(x,y)=\begin{bmatrix} X_1 \\ X_2 \oplus 1 \end{bmatrix}=\begin{bmatrix} x_2 \oplus y_1 \oplus y_2 \\ x_1 \oplus y_1 \oplus 1 \end{bmatrix}$

Знайдемо операцію декодування до синтезованої операції:

$$C(x,y)=\begin{cases} \begin{bmatrix} x_2 \oplus y_1 \oplus y_2 \\ x_1 \oplus y_1 \oplus 1 \end{bmatrix}=\begin{bmatrix} x_2 \\ x_1 \oplus 1 \end{bmatrix}, \text{ якщо } y_1=0;\ y_2=0 \\ \begin{bmatrix} x_2 \oplus y_1 \oplus y_2 \\ x_1 \oplus y_1 \oplus 1 \end{bmatrix}=\begin{bmatrix} x_2 \oplus 1 \\ x_1 \oplus 1 \end{bmatrix}, \text{якщо } y_1=0;\ y_2=1 \\ \begin{bmatrix} x_2 \oplus y_1 \oplus y_2 \\ x_1 \oplus y_1 \oplus 1 \end{bmatrix}=\begin{bmatrix} x_2 \oplus 1 \\ x_1 \end{bmatrix}, \text{якщо } y_1=1;\ y_2=0 \\ \begin{bmatrix} x_2 \oplus y_1 \oplus y_2 \\ x_1 \oplus y_1 \oplus 1 \end{bmatrix}=\begin{bmatrix} x_2 \\ x_1 \end{bmatrix}, \text{якщо } y_1=1;\ y_2=1 \end{cases} = \begin{cases} C_{10}, \text{ якщо } y_1=0;\ y_2=0 \\ C_{22}, \text{якщо } y_1=0;\ y_2=1 \\ C_{16}, \text{ якщо } y_1=1;\ y_2=0 \\ C_4, \text{якщо } y_1=1;\ y_2=1 \end{cases} = C_{10,22,16,4}(x,y)$$

Згідно виразу (2.35) оберненою операцією до операції $C_{10,22,16,4}(x,y)$ буде операція $C_{12,24,6,18}(x,y)=\begin{bmatrix} x_1 \oplus x_2 \oplus y_2 \\ x_2 \oplus y_1 \oplus 1 \end{bmatrix}$. Підставивши в операцію (2.26) додаткові інверсії першого та другого операндів отримаємо: $C(x,y)=\begin{bmatrix} X_1 \oplus 1 \\ X_2 \oplus 1 \end{bmatrix}=\begin{bmatrix} x_2 \oplus y_1 \oplus y_2 \oplus 1 \\ x_1 \oplus y_1 \oplus 1 \end{bmatrix}$

Знайдемо операцію декодування до синтезованої операції:

$$C(x,y)=\begin{cases} \begin{bmatrix} x_2 \oplus y_1 \oplus y_2 \oplus 1 \\ x_1 \oplus y_1 \oplus 1 \end{bmatrix}=\begin{bmatrix} x_2 \oplus 1 \\ x_1 \oplus 1 \end{bmatrix}, \text{ якщо } y_1=0;\ y_2=0 \\ \begin{bmatrix} x_2 \oplus y_1 \oplus y_2 \oplus 1 \\ x_1 \oplus y_1 \oplus 1 \end{bmatrix}=\begin{bmatrix} x_2 \\ x_1 \oplus 1 \end{bmatrix}, \text{якщо } y_1=0;\ y_2=1 \\ \begin{bmatrix} x_2 \oplus y_1 \oplus y_2 \oplus 1 \\ x_1 \oplus y_1 \oplus 1 \end{bmatrix}=\begin{bmatrix} x_2 \\ x_1 \end{bmatrix}, \text{ якщо } y_1=1;\ y_2=0 \\ \begin{bmatrix} x_2 \oplus y_1 \oplus y_2 \oplus 1 \\ x_1 \oplus y_1 \oplus 1 \end{bmatrix}=\begin{bmatrix} x_2 \oplus 1 \\ x_1 \end{bmatrix}, \text{якщо } y_1=1;\ y_2=1 \end{cases} = \begin{cases} C_{10}, \text{ якщо } y_1=0;\ y_2=0 \\ C_{22}, \text{якщо } y_1=0;\ y_2=1 \\ C_{16}, \text{ якщо } y_1=1;\ y_2=0 \\ C_4, \text{якщо } y_1=1;\ y_2=1 \end{cases} = C_{10,22,16,4}(x,y)$$

Згідно виразу (2.47) оберненою операцією буде операція $C_{24,12,18,6}(x,y)=\begin{bmatrix} x_1 \oplus x_2 \oplus y_2 \oplus 1 \\ x_1 \oplus y_1 \oplus 1 \end{bmatrix}$.

Синтезуємо на основі операції (3.5) ще три операції криптографічного перетворення.

- Підставивши в операцію (3.5) додатково інверсію першого операнда отримаємо: $C(x,y)=\begin{bmatrix} X_1 \oplus 1 \\ X_2 \end{bmatrix}=\begin{bmatrix} x_2 \oplus y_1 \oplus y_2 \oplus 1 \\ x_1 \oplus x_2 \oplus y_2 \end{bmatrix}$

Знайдемо операцію декодування до синтезованої операції:

$$C(x,y)=\begin{cases} \begin{bmatrix} x_2 \oplus y_1 \oplus y_2 \oplus 1 \\ x_1 \oplus x_2 \oplus k_2 \end{bmatrix}=\begin{bmatrix} x_1 \oplus 1 \\ x_1 \oplus x_2 \end{bmatrix}, \text{ якщо } y_1=0;\ y_2=0 \\ \begin{bmatrix} x_2 \oplus y_1 \oplus y_2 \oplus 1 \\ x_1 \oplus x_2 \oplus y_2 \end{bmatrix}=\begin{bmatrix} x_1 \\ x_1 \oplus x_2 \oplus 1 \end{bmatrix}, \text{якщо } y_1=0;\ y_2=1 \\ \begin{bmatrix} x_2 \oplus y_1 \oplus y_2 \oplus 1 \\ x_1 \oplus x_2 \oplus y_2 \end{bmatrix}=\begin{bmatrix} x_1 \\ x_1 \oplus x_2 \end{bmatrix}, \text{ якщо } y_1=1;\ y_2=0 \\ \begin{bmatrix} x_2 \oplus y_1 \oplus y_2 \oplus 1 \\ x_1 \oplus x_2 \oplus y_2 \end{bmatrix}=\begin{bmatrix} x_1 \oplus 1 \\ x_1 \oplus x_2 \oplus 1 \end{bmatrix}, \text{якщо } y_1=1;\ y_2=1 \end{cases} = \begin{cases} C_{17}, \text{ якщо } y_1=0;\ y_2=0 \\ C_{11}, \text{якщо } y_1=0;\ y_2=1 \\ C_5, \text{ якщо } y_1=1;\ y_2=0 \\ C_{23}, \text{якщо } y_1=1;\ y_2=1 \end{cases} = C_{17,11,5,23}(x,y)$$

Згідно виразу (2.64) оберненою операцією до операції $C_{17,11,5,23}(x,y)$ буде операція $C_{14,8,20,2}(x,y)=\begin{bmatrix} x_1 \oplus x_2 \oplus y_1 \oplus 1 \\ x_2 \oplus y_1 \oplus y_2 \end{bmatrix}$.

- Підставивши в операцію (3.5) додатково інверсію другого операнда отримаємо: $C(x,y)=\begin{bmatrix} X_1 \\ X_2 \oplus 1 \end{bmatrix}=\begin{bmatrix} x_2 \oplus y_1 \oplus y_2 \\ x_1 \oplus x_2 \oplus y_2 \oplus 1 \end{bmatrix}$

Знайдемо операцію декодування до синтезованої операції:

$$C(x,y)=\begin{cases} \begin{bmatrix} x_2 \oplus y_1 \oplus y_2 \\ x_1 \oplus x_2 \oplus y_2 \oplus 1 \end{bmatrix}=\begin{bmatrix} x_2 \\ x_1 \oplus x_2 \oplus 1 \end{bmatrix}, \text{ якщо } y_1=0;\ y_2=0 \\ \begin{bmatrix} x_2 \oplus y_1 \oplus y_2 \\ x_1 \oplus x_2 \oplus y_2 \oplus 1 \end{bmatrix}=\begin{bmatrix} x_2 \oplus 1 \\ x_1 \oplus x_2 \end{bmatrix}, \text{якщо } y_1=0;\ y_2=1 \\ \begin{bmatrix} x_2 \oplus y_1 \oplus y_2 \\ x_1 \oplus x_2 \oplus y_2 \oplus 1 \end{bmatrix}=\begin{bmatrix} x_2 \oplus 1 \\ x_1 \oplus x_2 \oplus 1 \end{bmatrix}, \text{ якщо } y_1=1;\ y_2=0 \\ \begin{bmatrix} x_2 \oplus y_1 \oplus y_2 \\ x_1 \oplus x_2 \oplus y_2 \oplus 1 \end{bmatrix}=\begin{bmatrix} x_2 \\ x_1 \oplus x_2 \end{bmatrix}, \text{якщо } y_1=1;\ y_2=1 \end{cases} = \begin{cases} C_{11}, \text{ якщо } y_1=0;\ y_2=0 \\ C_{17}, \text{якщо } y_1=0;\ y_2=1 \\ C_{23}, \text{ якщо } y_1=1;\ y_2=0 \\ C_5, \text{якщо } y_1=1;\ y_2=1 \end{cases} = C_{11,17,23,5}(x,y)$$

Згідно виразу (2.58) оберненою операцією до операції $C_{11,17,23,5}(x,y)$ буде операція $C_{8,14,2,20}(x,y)=\begin{bmatrix} x_1 \oplus x_2 \oplus y_1 \\ x_2 \oplus y_1 \oplus y_2 \oplus 1 \end{bmatrix}$.

- Підставивши в операцію (3.5) додаткові інверсії першого та другого операндів отримаємо: $C(x,y)=\begin{bmatrix} X_1 \oplus 1 \\ X_2 \oplus 1 \end{bmatrix}=\begin{bmatrix} x_2 \oplus y_1 \oplus y_2 \oplus 1 \\ x_1 \oplus x_2 \oplus y_2 \oplus 1 \end{bmatrix}$

Знайдемо операцію декодування до синтезованої операції:

$$C(x,y)=\begin{cases} \begin{bmatrix} x_2 \oplus y_1 \oplus y_2 \oplus 1 \\ x_1 \oplus x_2 \oplus y_2 \oplus 1 \end{bmatrix}=\begin{bmatrix} x_2 \oplus 1 \\ x_1 \oplus x_2 \oplus 1 \end{bmatrix}, \text{ якщо } y_1=0;\ y_2=0 \\ \begin{bmatrix} x_2 \oplus y_1 \oplus y_2 \oplus 1 \\ x_1 \oplus x_2 \oplus y_2 \oplus 1 \end{bmatrix}=\begin{bmatrix} x_2 \\ x_1 \oplus x_2 \end{bmatrix}, \text{якщо } y_1=0;\ y_2=1 \\ \begin{bmatrix} x_2 \oplus y_1 \oplus y_2 \oplus 1 \\ x_1 \oplus x_2 \oplus y_2 \oplus 1 \end{bmatrix}=\begin{bmatrix} x_2 \\ x_1 \oplus x_2 \oplus 1 \end{bmatrix}, \text{ якщо } y_1=1;\ y_2=0 \\ \begin{bmatrix} x_2 \oplus y_1 \oplus y_2 \oplus 1 \\ x_1 \oplus x_2 \oplus y_2 \oplus 1 \end{bmatrix}=\begin{bmatrix} x_2 \oplus 1 \\ x_1 \oplus x_2 \end{bmatrix}, \text{якщо } y_1=1;\ y_2=1 \end{cases} = \begin{cases} C_{32}, \text{ якщо } y_1=0;\ y_2=0 \\ C_5, \text{якщо } y_1=0;\ y_2=1 \\ C_{11}, \text{ якщо } y_1=1;\ y_2=0 \\ C_{17}, \text{якщо } y_1=1;\ y_2=1 \end{cases} = C_{23,5,11,17}(x,y)$$

Згідно виразу (2.70) оберненою операцією буде операція $C_{20,2,14,8}(x,y)=\begin{bmatrix} x_1 \oplus x_2 \oplus y_1 \oplus 1 \\ x_2 \oplus y_1 \oplus y_2 \oplus 1 \end{bmatrix}$.

Синтезуємо на основі операції (3.6) ще три операції криптографічного перетворення.

- Підставивши в операцію (3.6) додатково інверсію першого операнда отримаємо: $C(x,y)=\begin{bmatrix} X_1 \oplus 1 \\ X_2 \end{bmatrix}=\begin{bmatrix} x_1 \oplus x_2 \oplus y_2 \oplus 1 \\ x_1 \oplus y_1 \end{bmatrix}$

Знайдемо операцію декодування до синтезованої операції:

$$C(x,y)=\begin{cases} \begin{bmatrix} x_1 \oplus x_2 \oplus y_2 \oplus 1 \\ x_1 \oplus y_1 \end{bmatrix}=\begin{bmatrix} x_1 \oplus x_2 \oplus 1 \\ x_1 \end{bmatrix}, \text{ якщо } y_1=0;\ y_2=0 \\ \begin{bmatrix} x_1 \oplus x_2 \oplus y_2 \oplus 1 \\ x_1 \oplus y_1 \end{bmatrix}=\begin{bmatrix} x_1 \oplus x_2 \\ x_1 \end{bmatrix}, \text{якщо } y_1=0;\ y_2=1 \\ \begin{bmatrix} x_1 \oplus x_2 \oplus y_2 \oplus 1 \\ x_1 \oplus y_1 \end{bmatrix}=\begin{bmatrix} x_1 \oplus x_2 \oplus 1 \\ x_1 \oplus 1 \end{bmatrix}, \text{ якщо } y_1=1;\ y_2=0 \\ \begin{bmatrix} x_1 \oplus x_2 \oplus y_2 \oplus 1 \\ x_1 \oplus y_1 \end{bmatrix}=\begin{bmatrix} x_1 \oplus x_2 \\ x_1 \oplus 1 \end{bmatrix}, \text{якщо } y_1=1;\ y_2=1 \end{cases} = \begin{cases} C_{18}, \text{ якщо } y_1=0;\ y_2=0 \\ C_6, \text{якщо } y_1=0;\ y_2=1 \\ C_{24}, \text{ якщо } y_1=1;\ y_2=0 \\ C_{12}, \text{якщо } y_1=1;\ y_2=1 \end{cases} = C_{18,6,24,12}(x,y)$$

Згідно виразу (2.40) оберненою операцією до операції $C_{18,6,24,12}(x,y)$ буде операція $C_{16,4,10,22}(x,y)=\begin{bmatrix} x_2 \oplus y_1 \oplus y_2 \oplus 1 \\ x_1 \oplus y_1 \end{bmatrix}$.

- Підставивши в операцію (3.6) додатково інверсію другого операнда отримаємо: $C(x,y)=\begin{bmatrix} X_1 \\ X_2 \oplus 1 \end{bmatrix}=\begin{bmatrix} x_1 \oplus x_2 \oplus y_2 \\ x_1 \oplus y_1 \oplus 1 \end{bmatrix}$

$$C(x,y)=\begin{cases} \begin{bmatrix} x_1 \oplus x_2 \oplus y_2 \\ x_1 \oplus y_1 \oplus 1 \end{bmatrix}=\begin{bmatrix} x_1 \oplus x_2 \\ x_1 \oplus 1 \end{bmatrix}, \text{ якщо } y_1=0;\ y_2=0 \\ \begin{bmatrix} x_1 \oplus x_2 \oplus y_2 \\ x_1 \oplus y_1 \oplus 1 \end{bmatrix}=\begin{bmatrix} x_1 \oplus x_2 \oplus 1 \\ x_1 \oplus 1 \end{bmatrix}, \text{якщо } y_1=0;\ y_2=1 \\ \begin{bmatrix} x_1 \oplus x_2 \oplus y_2 \\ x_1 \oplus y_1 \oplus 1 \end{bmatrix}=\begin{bmatrix} x_1 \oplus x_2 \\ x_1 \end{bmatrix}, \text{ якщо } y_1=1;\ y_2=0 \\ \begin{bmatrix} x_1 \oplus x_2 \oplus y_2 \\ x_1 \oplus y_1 \oplus 1 \end{bmatrix}=\begin{bmatrix} x_1 \oplus x_2 \oplus 1 \\ x_1 \end{bmatrix}, \text{якщо } y_1=1;\ y_2=1 \end{cases} = \begin{cases} C_{12}, \text{ якщо } y_1=0;\ y_2=0 \\ C_{24}, \text{якщо } y_1=0;\ y_2=1 \\ C_6, \text{ якщо } y_1=1;\ y_2=0 \\ C_{18}, \text{якщо } y_1=1;\ y_2=1 \end{cases} = C_{12,24,6,18}(x,y)$$

Згідно виразу (2.34) оберненою операцією до операції $C_{12,24,6,18}(x,y)$ буде операція $C_{10,22,16,4}(x,y)=\begin{bmatrix} x_2 \oplus y_1 \oplus y_2 \\ x_1 \oplus y_1 \oplus 1 \end{bmatrix}$.

- Підставивши в операцію (3.6) додаткові інверсії першого та другого операндів отримаємо: $C(x,y)=\begin{bmatrix} X_1 \oplus 1 \\ X_2 \oplus 1 \end{bmatrix}=\begin{bmatrix} x_1 \oplus x_2 \oplus y_2 \oplus 1 \\ x_1 \oplus y_1 \oplus 1 \end{bmatrix}$

Знайдемо операцію декодування до синтезованої операції:

$$C(x,y)=\begin{cases} \begin{bmatrix} x_1 \oplus x_2 \oplus y_2 \oplus 1 \\ x_1 \oplus y_1 \oplus 1 \end{bmatrix}=\begin{bmatrix} x_1 \oplus x_2 \oplus 1 \\ x_1 \oplus 1 \end{bmatrix}, \text{ якщо } y_1=0;\ y_2=0 \\ \begin{bmatrix} x_1 \oplus x_2 \oplus y_2 \oplus 1 \\ x_1 \oplus y_1 \oplus 1 \end{bmatrix}=\begin{bmatrix} x_1 \oplus x_2 \\ x_1 \oplus 1 \end{bmatrix}, \text{якщо } y_1=0;\ y_2=1 \\ \begin{bmatrix} x_1 \oplus x_2 \oplus y_2 \oplus 1 \\ x_1 \oplus y_1 \oplus 1 \end{bmatrix}=\begin{bmatrix} x_1 \oplus x_2 \oplus 1 \\ x_1 \end{bmatrix}, \text{ якщо } y_1=1;\ y_2=0 \\ \begin{bmatrix} x_1 \oplus x_2 \oplus y_2 \oplus 1 \\ x_1 \oplus y_1 \oplus 1 \end{bmatrix}=\begin{bmatrix} x_1 \oplus x_2 \\ x_1 \end{bmatrix}, \text{якщо } y_1=1;\ y_2=1 \end{cases} = \begin{cases} C_{24}, \text{ якщо } y_1=0;\ y_2=0 \\ C_{12}, \text{якщо } y_1=0;\ y_2=1 \\ C_{18}, \text{ якщо } y_1=1;\ y_2=0 \\ C_6, \text{якщо } y_1=1;\ y_2=1 \end{cases} = C_{24,12,18,6}(x,y)$$

Згідно виразу (2.46) оберненою операцією буде операція

$$C_{22,10,4,16}(x,y)=\begin{bmatrix} x_2 \oplus y_1 \oplus y_2 \oplus 1 \\ x_1 \oplus y_1 \oplus 1 \end{bmatrix}.$$

Зведемо отримані результати синтезу прямих і обернених операцій до табл..3.1. Розмістимо моделі в відповідно до груп одноопераднних операцій на основі яких вони моделювалися, по аналогії з табличною класифікацією одноопераднних двохрозрядних операцій, а також симетричних двохоперандних двохрозрядних операцій [10].

Аналіз результатів застосування методу синтезу несиметричних двохоперандних двохрозрядних операцій подвійного циклу на основі дублювання одноопераднних двохрозрядних операцій базової групи показав:

– Множини несиметричних двохоперандних двохрозрядних операцій подвійного циклу синтезованих на основі класифікації і формалізації результатів обчислювального експерименту і синтезованих на основі дублювання одноопераднних двохрозрядних операцій базової групи на прикладі наведеної групи операцій співпали. Також вони співпадають для всіх шести груп операцій подвійного циклу 10];

– Результати синтезу на основі дублювання одноопераднних двохрозрядних операцій базової групи забезпечує без додаткового дослідження таблично класифікувати отримані двохоперандні моделі повністю ідентично табличній класифікації групи одноопераднних двохрозрядних операцій [10].

– Синтез операцій кодування на основі дублювання одноопераднних двохрозрядних операцій базової групи проводиться без використання результатів обчислювального експерименту, в той час як реалізація синтезу на основі класифікації і формалізації результатів обчислювального експерименту неможлива без наявних результатів обчислювального експерименту [10].

Таблиця 3.1

Синтезована група моделей несиметричних двохоперандних двохрозрядних операцій подвійного циклу на основі дублювання одноопераднних двохрозрядних операцій базової групи згідно другого сценарію шифрування [2]

		Операції інверсії			
Бзові операції	$C(x)=\begin{bmatrix}x_1\\x_2\end{bmatrix}$	$C_{1,7,19,13}(x,y)=\begin{bmatrix}x_1\oplus y_1\\x_2\oplus y_1\oplus y_2\end{bmatrix}$	$C_{7,1,13,19}(x,y)=\begin{bmatrix}x_1\oplus y_1\\x_2\oplus y_1\oplus y_2\oplus 1\end{bmatrix}$	$C_{13,19,7,1}(x,y)=\begin{bmatrix}x_1\oplus y_1\oplus 1\\x_2\oplus y_1\oplus y_2\end{bmatrix}$	$C_{19,13,1,7}(x,y)=\begin{bmatrix}x_1\oplus y_1\oplus 1\\x_2\oplus y_1\oplus y_2\oplus 1\end{bmatrix}$
		$C_{3,9,15,21}(x,y)=\begin{bmatrix}x_1\oplus y_1\\x_1\oplus x_2\oplus y_2\end{bmatrix}$	$C_{9,3,21,15}(x,y)=\begin{bmatrix}x_1\oplus y_1\\x_1\oplus x_2\oplus y_2\oplus 1\end{bmatrix}$	$C_{15,21,3,9}(x,y)=\begin{bmatrix}x_1\oplus y_1\oplus 1\\x_1\oplus x_2\oplus y_2\end{bmatrix}$	$C_{21,15,9,3}=\begin{bmatrix}x_1\oplus y_1\oplus 1\\x_1\oplus x_2\oplus y_2\oplus 1\end{bmatrix}$
	$C(x)=\begin{bmatrix}x_1\oplus x_2\\x_2\end{bmatrix}$	$C_{2,20,8,14}(x,y)=\begin{bmatrix}x_1\oplus x_2\oplus y_2\\x_2\oplus y_1\oplus y_2\end{bmatrix}$	$C_{8,14,2,20}(x,y)=\begin{bmatrix}x_1\oplus x_2\oplus y_2\\x_2\oplus y_1\oplus y_2\oplus 1\end{bmatrix}$	$C_{14,8,20,2}(x,y)=\begin{bmatrix}x_1\oplus x_2\oplus y_2\oplus 1\\x_2\oplus y_1\oplus y_2\end{bmatrix}$	$C_{20,2,14,8}(x,y)=\begin{bmatrix}x_1\oplus x_2\oplus y_2\oplus 1\\x_2\oplus y_1\oplus y_2\oplus 1\end{bmatrix}$
		$C_{5,23,17,11}(x,y)=\begin{bmatrix}x_2\oplus y_1\oplus y_2\\x_1\oplus x_2\oplus y_2\end{bmatrix}$	$C_{11,17,23,5}(x,y)=\begin{bmatrix}x_2\oplus y_1\oplus y_2\\x_1\oplus x_2\oplus y_2\oplus 1\end{bmatrix}$	$C_{17,11,5,23}(x,y)=\begin{bmatrix}x_2\oplus y_1\oplus y_2\oplus 1\\x_1\oplus x_2\oplus y_2\end{bmatrix}$	$C_{23,5,11,17}(x,y)=\begin{bmatrix}x_2\oplus y_1\oplus y_2\oplus 1\\x_1\oplus x_2\oplus y_2\oplus 1\end{bmatrix}$
	$C(x)=\begin{bmatrix}x_1\\x_1\oplus x_2\end{bmatrix}$	$C_{3,9,15,21}(x,y)=\begin{bmatrix}x_1\oplus y_1\\x_1\oplus x_2\oplus y_2\end{bmatrix}$	$C_{9,3,21,15}(x,y)=\begin{bmatrix}x_1\oplus y_1\\x_1\oplus x_2\oplus y_2\oplus 1\end{bmatrix}$	$C_{15,21,3,9}(x,y)=\begin{bmatrix}x_1\oplus y_1\oplus 1\\x_1\oplus x_2\oplus y_2\end{bmatrix}$	$C_{21,15,9,3}(x,y)=\begin{bmatrix}x_1\oplus y_1\oplus 1\\x_1\oplus x_2\oplus y_2\oplus 1\end{bmatrix}$
		$C_{1,7,19,13}(x,y)=\begin{bmatrix}x_1\oplus y_1\\x_2\oplus y_1\oplus y_2\end{bmatrix}$	$C_{7,1,13,19}(x,y)=\begin{bmatrix}x_1\oplus y_1\\x_2\oplus y_1\oplus y_2\oplus 1\end{bmatrix}$	$C_{13,19,7,1}(x,y)=\begin{bmatrix}x_1\oplus y_1\oplus 1\\x_2\oplus y_1\oplus y_2\end{bmatrix}$	$C_{19,13,1,7}(x,y)=\begin{bmatrix}x_1\oplus y_1\oplus 1\\x_2\oplus y_1\oplus y_2\oplus 1\end{bmatrix}$
Операції інверсії	$C(x)=\begin{bmatrix}x_2\\x_1\end{bmatrix}$	$C_{4,16,22,10}(x,y)=\begin{bmatrix}x_2\oplus y_1\oplus y_2\\x_1\oplus y_1\end{bmatrix}$	$C_{10,22,16,4}(x,y)=\begin{bmatrix}x_2\oplus y_1\oplus y_2\\x_1\oplus y_1\oplus 1\end{bmatrix}$	$C_{16,4,10,22}(x,y)=\begin{bmatrix}x_2\oplus y_1\oplus y_2\oplus 1\\x_1\oplus y_1\end{bmatrix}$	$C_{22,10,4,16}(x,y)=\begin{bmatrix}x_2\oplus y_1\oplus y_2\oplus 1\\x_1\oplus y_1\oplus 1\end{bmatrix}$
		$C_{6,18,12,24}(x,y)=\begin{bmatrix}x_1\oplus x_2\oplus y_2\\x_1\oplus y_1\end{bmatrix}$	$C_{12,24,6,18}(x,y)=\begin{bmatrix}x_1\oplus x_2\oplus y_2\\x_1\oplus y_1\oplus 1\end{bmatrix}$	$C_{18,6,24,12}(x,y)=\begin{bmatrix}x_1\oplus x_2\oplus y_2\oplus 1\\x_1\oplus y_1\end{bmatrix}$	$C_{24,12,18,6}(x,y)=\begin{bmatrix}x_1\oplus x_2\oplus y_2\oplus 1\\x_1\oplus y_1\oplus 1\end{bmatrix}$
	$C(x)=\begin{bmatrix}x_2\\x_1\oplus x_2\end{bmatrix}$	$C_{5,23,17,11}(x,y)=\begin{bmatrix}x_2\oplus y_1\oplus y_2\\x_1\oplus x_2\oplus y_2\end{bmatrix}$	$C_{11,17,23,5}(x,y)=\begin{bmatrix}x_2\oplus y_1\oplus y_2\\x_1\oplus x_2\oplus y_2\oplus 1\end{bmatrix}$	$C_{17,11,5,23}(x,y)=\begin{bmatrix}x_2\oplus y_1\oplus y_2\oplus 1\\x_1\oplus x_2\oplus y_2\end{bmatrix}$	$C_{23,5,11,17}(x,y)=\begin{bmatrix}x_2\oplus y_1\oplus y_2\oplus 1\\x_1\oplus x_2\oplus y_2\oplus 1\end{bmatrix}$
		$C_{2,20,8,14}(x,y)=\begin{bmatrix}x_1\oplus x_2\oplus y_2\\x_2\oplus y_1\oplus y_2\end{bmatrix}$	$C_{8,14,2,20}(x,y)=\begin{bmatrix}x_1\oplus x_2\oplus y_2\\x_2\oplus y_1\oplus y_2\oplus 1\end{bmatrix}$	$C_{14,8,20,2}(x,y)=\begin{bmatrix}x_1\oplus x_2\oplus y_2\oplus 1\\x_2\oplus y_1\oplus y_2\end{bmatrix}$	$C_{20,2,14,8}(x,y)=\begin{bmatrix}x_1\oplus x_2\oplus y_2\oplus 1\\x_2\oplus y_1\oplus y_2\oplus 1\end{bmatrix}$
	$C(x)=\begin{bmatrix}x_1\oplus x_2\\x_1\end{bmatrix}$	$C_{6,18,12,24}(x,y)=\begin{bmatrix}x_1\oplus x_2\oplus y_2\\x_1\oplus y_1\end{bmatrix}$	$C_{12,24,6,18}(x,y)=\begin{bmatrix}x_1\oplus x_2\oplus y_2\\x_1\oplus y_1\oplus 1\end{bmatrix}$	$C_{18,6,24,12}(x,y)=\begin{bmatrix}x_1\oplus x_2\oplus y_2\oplus 1\\x_1\oplus y_1\end{bmatrix}$	$C_{24,12,18,6}(x,y)=\begin{bmatrix}x_1\oplus x_2\oplus y_2\oplus 1\\x_1\oplus y_1\oplus 1\end{bmatrix}$
		$C_{4,16,22,10}(x,y)=\begin{bmatrix}x_1\oplus y_1\\x_2\oplus y_1\oplus y_2\end{bmatrix}$	$C_{10,22,16,4}=\begin{bmatrix}x_2\oplus y_1\oplus y_2\\x_1\oplus y_1\oplus 1\end{bmatrix}$	$C_{16,4,10,22}(x,y)=\begin{bmatrix}x_2\oplus y_1\oplus y_2\oplus 1\\x_1\oplus y_1\end{bmatrix}$	$C_{22,10,4,16}(x,y)=\begin{bmatrix}x_2\oplus y_1\oplus y_2\oplus 1\\x_1\oplus y_1\oplus 1\end{bmatrix}$

– Синтез операцій розкодування інформації при відомій операції кодування при реалізації другого сценарію моделювання операцій розкодування без результатів обчислювального експерименту на даному етапі дослідження складний і математично неформалізований [10].

3.2. Моделювання множин несиметричних двохоперандних двохрозрядних операцій потрійного циклу на основі дублювання одноопераднних двохрозрядних операцій базової групи

Моделювання множин несиметричних двохоперандних двохрозрядних операцій потрійного циклу синтезованих на основі класифікації і формалізації результатів обчислювального експерименту проводиться аналогічно з моделюванням множин несиметричних двохоперандних двохрозрядних операцій подвійного циклу синтезованих на основі класифікації і формалізації результатів обчислювального експерименту наведеному в підрозділі 3.1. Дане моделювання проводиться на основі перетворення кортежів операцій в удосконалені моделі операцій. При цьому, за отриманими результатів моделювання, будуються операції кодування і відповідні їм результати декодування [10].

Множини несиметричних двохоперандних двохрозрядних операцій потрійного циклу відбиралися на основі таблиць істинності операцій з точністю до перестановки.

Синтез операцій подвійного циклу група операцій з точністю до перестановки забезпечує належність операцій до і після перестановки операндів до однієї і тієї ж групи операцій.

Для операцій потрійного циклу, є справедливою властивість: якщо операція до перестановки операндів належала до групи А, то після перестановки операндів стане належати до групи В [10].

В табл. 3.2 наведені операції до і після перестановки операндів, які належать групам операцій з точністю до перестановки отриманих на основі $C_{1,21,7,15}(x,y)$ і $C_{5,11,16,22}(x,y)$. В даній таблиці група операцій отриманих на

основі $C_{5,11,16,22}(x,y)$ виділена відтінком сірого, група операцій отриманих на основі $C_{1,21,7,15}(x,y)$ не виділялась.

Для застосування методу синтезу несиметричних двохоперандних двохрозрядних операцій на основі дублювання одноопераднних двохрозрядних операцій базової групи побудуємо вдосконалену двохоперандних двох розрядну операцію $C_{1,21,7,15}(x,y)$.

$$C_{1,21,7,15}(x,y)=\begin{cases}\begin{bmatrix}x_1\\x_2\end{bmatrix}, & якщо\ y_1=0;\ y_2=0\\ \begin{bmatrix}x_1\oplus 1\\x_1\oplus x_2\oplus 1\end{bmatrix}, & якщо\ y_1=0;\ y_2=1\\ \begin{bmatrix}x_1\\x_2\oplus 1\end{bmatrix}, & якщо\ y_1=1;\ y_2=0\\ \begin{bmatrix}x_1\oplus 1\\x_1\oplus x_2\end{bmatrix}, & якщо\ y_1=1;\ y_2=1\end{cases}=\begin{cases}\begin{bmatrix}x_1\\x_2\end{bmatrix}\oplus\begin{bmatrix}0\\0\end{bmatrix}, & якщо\ y_1=0;\ y_2=0\\ \begin{bmatrix}x_1\\x_1\oplus x_2\end{bmatrix}\oplus\begin{bmatrix}1\\1\end{bmatrix}, & якщо\ y_1=0;\ y_2=1\\ \begin{bmatrix}x_1\\x_2\end{bmatrix}\oplus\begin{bmatrix}0\\1\end{bmatrix}, & якщо\ y_1=1;\ y_2=0\\ \begin{bmatrix}x_1\\x_1\oplus x_2\end{bmatrix}\oplus\begin{bmatrix}1\\0\end{bmatrix}, & якщо\ y_1=1;\ y_2=1\end{cases}=\begin{bmatrix}x_1\oplus y_2\\x_1\oplus y_2\cdot x_2\oplus y_1\oplus y_2\end{bmatrix} \quad (3.7)$$

Використаємо дану в якості нульової операції (першої операції) базової групи.

$$C_{1,21,7,15}(x,y)=\begin{bmatrix}x_1\oplus y_2\\x_1\oplus y_2\cdot x_2\oplus y_1\oplus н_1\end{bmatrix}=\begin{bmatrix}x_1\\x_1\oplus y_2\cdot x_2\end{bmatrix}\oplus\begin{bmatrix}y_2\\y_1\oplus y_2\end{bmatrix}$$

Синтезуємо другу двохоперандну двохрозрядну операцію криптоперетворення базової групи, на основі другої базової одноопераднної двохрозрядної базової операції $C=\begin{bmatrix}x_1\oplus x_2\\x_2\end{bmatrix}$:

$$C(x,y)=\begin{bmatrix}x_1^*\oplus x_2^*\\x_2^*\end{bmatrix}\oplus\begin{bmatrix}y_1^*\oplus y_2^*\\y_2^*\end{bmatrix}=\begin{bmatrix}x_1\oplus(x_1\oplus y_2\cdot x_2)\\x_1\oplus y_2\cdot x_2\end{bmatrix}\oplus\begin{bmatrix}y_1\oplus(y_1\oplus y_2)\\y_1\oplus y_2\end{bmatrix}=\begin{bmatrix}y_2\cdot x_2\oplus y_2\\x_1\oplus y_2\cdot x_2\oplus y_1\oplus y_2\end{bmatrix}.$$

Визначимо кортеж, який визначається даною операцією:

$$C(x,y)=\begin{cases}\begin{bmatrix}y_2\cdot x_2\oplus y_2\\x_1\oplus y_2\cdot x_2\oplus y_1\oplus y_2\end{bmatrix}, & якщо\ y_1=0;\ y_2=0\\ \begin{bmatrix}y_2\cdot x_2\oplus y_2\\x_1\oplus y_2\cdot x_2\oplus y_1\oplus y_2\end{bmatrix}, & якщо\ y_1=0;\ y_2=1\\ \begin{bmatrix}y_2\cdot x_2\oplus y_2\\x_1\oplus y_2\cdot x_2\oplus y_1\oplus y_2\end{bmatrix}, & якщо\ y_1=1;\ y_2=0\\ \begin{bmatrix}y_2\cdot x_2\oplus y_2\\x_1\oplus y_2\cdot x_2\oplus y_1\oplus y_2\end{bmatrix}, & якщо\ y_1=1;\ y_2=1\end{cases}=\begin{cases}\begin{bmatrix}0\\x_1\end{bmatrix}, & якщо\ y_1=0;\ y_2=0\\ \begin{bmatrix}x_2\oplus 1\\x_1\oplus x_2\oplus 1\end{bmatrix}, & якщо\ y_1=0;\ y_2=1\\ \begin{bmatrix}0\\x_1\oplus 1\end{bmatrix}, & якщо\ y_1=1;\ y_2=0\\ \begin{bmatrix}x_2\oplus 1\\x_1\oplus x_2\end{bmatrix}, & якщо\ y_1=1;\ y_2=1\end{cases} \quad (3.8)$$

Таблиця 3.2

Множини несиметричних двохоперандних двохрозрядних операцій потрійного циклу з точністю до перестановки на основі дублювання одноопераднних двохрозрядних операцій базової групи

Пряме і обернене перетворення		Пряме і обернене перетворення	
Кодування (множина 1)	**Декодування (множина 2)**	**Кодування (множина 2)**	**Декодування (множина 1)**
$C_{1,21,7,15}(x,y)$	$C_{5,11,16,22}(x,y)$	$C_{5,11,16,22}(x,y)$	$C_{1,21,7,15}(x,y)$
$C_{7,15,1,21}(x,y)$	$C_{11,5,22,16}(x,y)$	$C_{11,5,22,16}(x,y)$	$C_{7,15,1,21}(x,y)$
$C_{15,1,21,7}(x,y)$	$C_{16,22,11,5}(x,y)$	$C_{16,22,11,5}(x,y)$	$C_{15,1,21,7}(x,y)$
$C_{21,7,15,1}(x,y)$	$C_{22,16,5,11}(x,y)$	$C_{22,16,5,11}(x,y)$	$C_{21,7,15,1}(x,y)$
$C_{2,11,20,17}(x,y)$	$C_{3,21,18,12}(x,y)$	$C_{3,21,18,12}(x,y)$	$C_{2,11,20,17}(x,y)$
$C_{11,20,17,2}(x,y)$	$C_{12,18,3,21}(x,y)$	$C_{12,18,3,21}(x,y)$	$C_{11,20,17,2}(x,y)$
$C_{17,2,11,20}(x,y)$	$C_{18,12,21,3}(x,y)$	$C_{18,12,21,3}(x,y)$	$C_{17,2,11,20}(x,y)$
$C_{20,17,2,11}(x,y)$	$C_{21,3,12,18}(x,y)$	$C_{21,3,12,18}(x,y)$	$C_{20,17,2,11}(x,y)$
$C_{4,24,16,12}(x,y)$	$C_{2,14,7,19}(x,y)$	$C_{2,14,7,19}(x,y)$	$C_{4,24,16,12}(x,y)$
$C_{12,4,24,16}(x,y)$	$C_{7,19,14,2}(x,y)$	$C_{7,19,14,2}(x,y)$	$C_{12,4,24,16}(x,y)$
$C_{16,12,4,24}(x,y)$	$C_{14,2,19,7}(x,y)$	$C_{14,2,19,7}(x,y)$	$C_{16,12,4,24}(x,y)$
$C_{24,16,12,4}(x,y)$	$C_{19,7,2,14}(x,y)$	$C_{19,7,2,14}(x,y)$	$C_{24,16,12,4}(x,y)$
$C_{3,13,9,19}(x,y)$	$C_{4,10,23,17}(x,y)$	$C_{4,10,23,17}(x,y)$	$C_{3,13,9,19}(x,y)$
$C_{9,19,3,13}(x,y)$	$C_{10,4,17,23}(x,y)$	$C_{10,4,17,23}(x,y)$	$C_{9,19,3,13}(x,y)$
$C_{13,9,19,3}(x,y)$	$C_{17,23,4,10}(x,y)$	$C_{17,23,4,10}(x,y)$	$C_{13,9,19,3}(x,y)$
$C_{19,3,13,9}(x,y)$	$C_{23,17,10,4}(x,y)$	$C_{23,17,10,4}(x,y)$	$C_{19,3,13,9}(x,y)$
$C_{5,14,23,8}(x,y)$	$C_{6,24,9,15}(x,y)$	$C_{6,24,9,15}(x,y)$	$C_{5,14,23,8}(x,y)$
$C_{8,5,14,23}(x,y)$	$C_{9,15,24,6}(x,y)$	$C_{9,15,24,6}(x,y)$	$C_{8,5,14,23}(x,y)$
$C_{14,23,8,5}(x,y)$	$C_{15,9,6,24}(x,y)$	$C_{15,9,6,24}(x,y)$	$C_{14,23,8,5}(x,y)$
$C_{23,8,5,14}(x,y)$	$C_{24,6,15,9}(x,y)$	$C_{24,6,15,9}(x,y)$	$C_{23,8,5,14}(x,y)$
$C_{6,10,18,22}(x,y)$	$C_{1,13,20,8}(x,y)$	$C_{1,13,20,8}(x,y)$	$C_{6,10,18,22}(x,y)$
$C_{10,18,22,6}(x,y)$	$C_{8,20,1,13}(x,y)$	$C_{8,20,1,13}(x,y)$	$C_{10,18,22,6}(x,y)$
$C_{18,22,6,10}(x,y)$	$C_{13,1,8,20}(x,y)$	$C_{13,1,8,20}(x,y)$	$C_{18,22,6,10}(x,y)$
$C_{22,6,10,18}(x,y)$	$C_{20,8,13,1}(x,y)$	$C_{20,8,13,1}(x,y)$	$C_{22,6,10,18}(x,y)$

Аналіз отриманого виразу (3.8) показав, що кортежа з чотирьох одноопераднних операцій не існую, тому що перша і третя одноопераднні операції вироджені, а значить при рівності нулю другого біта другого операнда ($y_2 = 0$) втрачається інформативність першого біта першого операнда і оберненого перетворення не існую, тому що не існує оберненого одноопераднного перетворення. Слід відмітити що при любому поділі моделі операції $C_{1,21,7,15}(x,y)$ на частини, які забезпечують попередню обробку, до додавання за модулем два, першого та другого операндів, застосувати її для синтезу групи операцій на основі дублювання одноопераднних двохрозрядних операцій неможливо. В результаті синтезу частина побудованих моделей операцій буде виродженою і не матиме моделей операцій оберненого перетворення [9].

Перевіримо отриманий результат на довільній операції з множини операцій синтезованої на основі операції $C_{5,11,16,22}(x,y)$ з точністю до перестановки. Наприклад $C_{3,21,18,12}(x,y)$:

$$C_{3,21,18,12}(x,y)=\begin{cases}\begin{bmatrix}x_1\\ x_1\oplus x_2\end{bmatrix}, & якщо\ y_1=0;\ y_2=0\\ \begin{bmatrix}x_1\oplus 1\\ x_1\oplus x_2\oplus 1\end{bmatrix}, & якщо\ y_1=0;\ y_2=1\\ \begin{bmatrix}x_1\oplus x_2\oplus 1\\ x_1\end{bmatrix}, & якщо\ y_1=1;\ y_2=0\\ \begin{bmatrix}x_1\oplus x_2\\ x_1\oplus 1\end{bmatrix}, & якщо\ y_1=1;\ y_2=1\end{cases}=\begin{cases}\begin{bmatrix}x_1\\ x_1\oplus x_2\end{bmatrix}\oplus\begin{bmatrix}0\\ 0\end{bmatrix}, & якщо\ y_1=0;\ y_2=0\\ \begin{bmatrix}x_1\\ x_1\oplus x_2\end{bmatrix}\oplus\begin{bmatrix}1\\ 1\end{bmatrix}, & якщо\ y_1=0;\ y_2=1\\ \begin{bmatrix}x_1\oplus x_2\\ x_2\end{bmatrix}\oplus\begin{bmatrix}1\\ 0\end{bmatrix}, & якщо\ y_1=1;\ y_2=0\\ \begin{bmatrix}x_1\oplus x_2\\ x_1\end{bmatrix}\oplus\begin{bmatrix}0\\ 1\end{bmatrix}, & якщо\ y_1=1;\ y_2=1\end{cases}=\begin{bmatrix}x_1\oplus y_1\cdot x_2\oplus y_1\oplus y_2\\ y_1\cdot y_2\cdot x_1\oplus y_2\cdot x_2\oplus y_2\end{bmatrix}$$

Синтезуємо другу двохоперандну операцію базової групи, на основі другої базової одноопераднної операції $C=\begin{bmatrix}x_1\oplus x_2\\ x_2\end{bmatrix}$

$$C(x,y)=\begin{bmatrix}x_1^*\oplus x_2^*\\ x_2^*\end{bmatrix}\oplus\begin{bmatrix}y_1^*\oplus y_2^*\\ y_2^*\end{bmatrix}=\begin{bmatrix}(x_1\oplus y_1\cdot x_2\oplus y_1\oplus y_2)\oplus(k_1\cdot y_2\cdot x_1\oplus y_2\cdot x_2\oplus y_2)\\ y_1\cdot y_2\cdot x_1\oplus y_2\cdot x_2\oplus y_2\end{bmatrix}=\begin{bmatrix}x_1\oplus y_1\cdot y_2\cdot x_1\oplus x_2\oplus y_1\\ y_1\cdot y_2\cdot x_1\oplus y_2\cdot x_2\oplus y_2\end{bmatrix}$$

Визначимо кортеж, одноопераднних операцій який визначається даною операцією:

$$C(x,y)=\begin{cases}\begin{bmatrix}x_1\oplus y_1\cdot y_2\cdot x_1\oplus x_2\oplus y_1\\ y_1\cdot y_2\cdot x_1\oplus y_2\cdot x_2\oplus y_2\end{bmatrix}, \text{якщо } y_1=0;\ y_2=0\\ \begin{bmatrix}x_1\oplus y_1\cdot y_2\cdot x_1\oplus x_2\oplus y_1\\ y_1\cdot y_2\cdot x_1\oplus y_2\cdot x_2\oplus y_2\end{bmatrix}, \text{якщо } y_1=0;\ y_2=1\\ \begin{bmatrix}x_1\oplus y_1\cdot y_2\cdot x_1\oplus x_2\oplus y_1\\ y_1\cdot y_2\cdot x_1\oplus y_2\cdot x_2\oplus y_2\end{bmatrix}, \text{якщо } y_1=1;\ y_2=0\\ \begin{bmatrix}x_1\oplus y_1\cdot y_2\cdot x_1\oplus x_2\oplus y_1\\ y_1\cdot y_2\cdot x_1\oplus y_2\cdot x_2\oplus y_2\end{bmatrix}, \text{якщо } y_1=1;\ y_2=1\end{cases}=\begin{cases}\begin{bmatrix}x_1\oplus x_2\\ x_2\end{bmatrix}, & \text{якщо } y_1=0;\ y_2=0\\ \begin{bmatrix}x_1\oplus x_2\\ x_2\oplus 1\end{bmatrix}, & \text{якщо } y_1=0;\ y_2=1\\ \begin{bmatrix}x_2\oplus 1\\ x_1\end{bmatrix}, & \text{якщо } y_1=1;\ y_2=0\\ \begin{bmatrix}x_1\oplus 1\\ 1\end{bmatrix}, & \text{якщо } y_1=1;\ y_2=1\end{cases} \quad (3.9)$$

Аналіз виразу (3.9) показав, що отриману довохоперандну операцію не можна використати в якості криптографічної операції, так як вона вироджена і не має оберненого перетворення.

Перевіримо отриманий результат ще на одній з операцій іншої множини, наприклад на множині операцій з точністю до перестановки синтезованій з операції $C_{1,15,7,21}(x,y)$. Візьмемо наприклад операцію $C_{4,12,16,24}(x,y)$

$$C_{4,12,16,24}(x,y)=\begin{cases}\begin{bmatrix}x_2\\ x_1\end{bmatrix}, & \text{якщо } y_1=0;\ y_2=0\\ \begin{bmatrix}x_1\oplus x_2\\ x_1\oplus 1\end{bmatrix}, & \text{якщо } y_1=0;\ y_2=1\\ \begin{bmatrix}x_2\oplus 1\\ x_1\end{bmatrix}, & \text{якщо } y_1=1;\ y_2=0\\ \begin{bmatrix}x_1\oplus x_2\oplus 1\\ x_1\oplus 1\end{bmatrix}, & \text{якщо } y_1=1;\ y_2=1\end{cases}=\begin{cases}\begin{bmatrix}x_2\\ x_1\oplus x_2\end{bmatrix}\oplus\begin{bmatrix}0\\ 0\end{bmatrix}, & \text{якщо } y_1=0;\ y_2=0\\ \begin{bmatrix}x_1\oplus x_2\\ x_1\end{bmatrix}\oplus\begin{bmatrix}0\\ 1\end{bmatrix}, & \text{якщо } y_1=0;\ y_2=1\\ \begin{bmatrix}x_2\\ x_1\end{bmatrix}\oplus\begin{bmatrix}1\\ 0\end{bmatrix}, & \text{якщо } y_1=1;\ y_2=0\\ \begin{bmatrix}x_1\oplus x_2\\ x_1\end{bmatrix}\oplus\begin{bmatrix}1\\ 1\end{bmatrix}, & \text{якщо } y_1=1;\ y_2=1\end{cases}=\begin{bmatrix}y_2\cdot x_1\oplus x_2\oplus y_1\\ x_1\oplus y_1\cdot y_2\cdot x_2\oplus y_2\end{bmatrix}$$

Синтезуємо другу двохоперандну операцію базової групи

$$C\ (x,y)=\begin{bmatrix}x_1^*\oplus x_2^*\\ x_2^*\end{bmatrix}\oplus\begin{bmatrix}y_1^*\oplus y_2^*\\ y_2^*\end{bmatrix}=\begin{bmatrix}(y_2\cdot x_1\oplus x_2\oplus y_1)\oplus(x_1\oplus y_1\cdot y_2\cdot x_2\oplus y_2)\\ x_1\oplus y_1\cdot y_2\cdot x_2\oplus y_2\end{bmatrix}=\begin{bmatrix}y_2\cdot x_1\oplus x_2\oplus y_1\cdot y_2\cdot x_2\oplus y_1\oplus y_2\\ x_1\oplus y_1\cdot y_2\cdot x_2\oplus y_2\end{bmatrix} \quad (3.10)$$

Визначимо кортеж, одноопераднних операцій який визначається даною операцією:

$$C(x,y)=\begin{cases}\begin{bmatrix}y_2\cdot x_1\oplus x_2\oplus y_1\cdot y_2\cdot x_2\oplus y_1\oplus y_2\\ x_1\oplus y_1\cdot y_2\cdot x_2\oplus y_2\end{bmatrix}, \text{якщо } y_1=0;\ y_2=0\\ \begin{bmatrix}y_2\cdot x_1\oplus x_2\oplus y_1\cdot y_2\cdot x_2\oplus y_1\oplus y_2\\ x_1\oplus y_1\cdot y_2\cdot x_2\oplus y_2\end{bmatrix}, \text{якщо } y_1=0;\ y_2=1\\ \begin{bmatrix}y_2\cdot x_1\oplus x_2\oplus y_1\cdot y_2\cdot x_2\oplus y_1\oplus y_2\\ x_1\oplus y_1\cdot y_2\cdot x_2\oplus y_2\end{bmatrix}, \text{якщо } y_1=1;\ y_2=0\\ \begin{bmatrix}y_2\cdot x_1\oplus x_2\oplus y_1\cdot y_2\cdot x_2\oplus y_1\oplus y_2\\ x_1\oplus y_1\cdot y_2\cdot x_2\oplus y_2\end{bmatrix}, \text{якщо } y_1=1;\ y_2=1\end{cases}=\begin{cases}\begin{bmatrix}x_1\\ x_1\oplus x_2\end{bmatrix}, & \text{якщо } y_1=0;\ y_2=0\\ \begin{bmatrix}x_2\oplus 1\\ x_1\oplus 1\end{bmatrix}, & \text{якщо } y_1=0;\ y_2=1\\ \begin{bmatrix}x_1\oplus x_2\oplus 1\\ x_1\end{bmatrix}, & \text{якщо } y_1=1;\ y_2=0\\ \begin{bmatrix}x_2\\ x_1\oplus 1\end{bmatrix}, & \text{якщо } y_1=1;\ y_2=1\end{cases} \quad (3.11)$$

Так як існують всі одноопераднді операції для (3.11) то можна стверджувати, що дана операція є не виродженою і існує для неї обернена операція.

На основі операції $C_{4,12,16,24}(x,y)$ синтезуємо третю, і останню, двохоперандну операцію базової групи, на основі третьої базової одноопераднді операції $C=\begin{bmatrix} x_1 \oplus x_2 \\ x_2 \end{bmatrix}$. Якщо синтезована операція буде не виродженою, тоді застосувавши перестановки операндів та інверсії буде синтезована вся група операцій. Синтез групи операцій буде можливий тому, що перестановки операндів та можливі варіанти інверсій операндів не приводять до виродженості результатів перетворення [9].

$$C(x,y)=\begin{bmatrix} x_1^* \\ x_1^* \oplus x_2^* \end{bmatrix} \oplus \begin{bmatrix} k_1^* \\ k_1^* \oplus k_2^* \end{bmatrix} = \begin{bmatrix} y_2 \cdot x_1 \oplus x_2 \oplus y_1 \\ (y_2 \cdot x_1 \oplus x_2 \oplus y_1) \oplus (x_1 \oplus y_1 \cdot y_2 \cdot x_2 \oplus y_2) \end{bmatrix} = \begin{bmatrix} y_2 \cdot x_1 \oplus x_2 \oplus y_1 \\ y_2 \cdot x_1 \oplus x_2 \oplus y_1 \cdot y_2 \cdot x_2 \oplus y_1 \oplus y_2) \end{bmatrix}$$

Визначимо кортеж, одноопераднді операцій який визначається даною операцією:

$$C(x,y)=\begin{cases} \begin{bmatrix} y_2 \cdot x_1 \oplus x_2 \oplus y_1 \\ y_2 \cdot x_1 \oplus x_2 \oplus y_1 \cdot y_2 \cdot x_2 \oplus y_1 \oplus y_2) \end{bmatrix}, \text{якщо } y_1=0;\ y_2=0 \\ \begin{bmatrix} y_2 \cdot x_1 \oplus x_2 \oplus y_1 \\ y_2 \cdot x_1 \oplus x_2 \oplus y_1 \cdot y_2 \cdot x_2 \oplus y_1 \oplus y_2) \end{bmatrix}, \text{якщо } y_1=0;\ y_2=1 \\ \begin{bmatrix} y_2 \cdot x_1 \oplus x_2 \oplus y_1 \\ y_2 \cdot x_1 \oplus x_2 \oplus y_1 \cdot y_2 \cdot x_2 \oplus y_1 \oplus y_2) \end{bmatrix}, \text{якщо } y_1=1;\ y_2=0 \\ \begin{bmatrix} y_2 \cdot x_1 \oplus x_2 \oplus y_1 \\ y_2 \cdot x_1 \oplus x_2 \oplus y_1 \cdot y_2 \cdot x_2 \oplus y_1 \oplus y_2) \end{bmatrix}, \text{якщо } y_1=1;\ y_2=1 \end{cases} = \begin{cases} \begin{bmatrix} x_2 \\ x_1 \end{bmatrix} & \text{якщо } y_1=0;\ y_2=0 \\ \begin{bmatrix} x_1 \oplus x_2 \\ x_2 \oplus 1 \end{bmatrix}, & \text{якщо } y_1=0;\ y_2=1 \\ \begin{bmatrix} x_2 \oplus 1 \\ x_1 \oplus x_2 \oplus 1 \end{bmatrix}, & \text{якщо } y_1=1;\ y_2=0 \\ \begin{bmatrix} x_1 \oplus x_2 \\ 0 \end{bmatrix}, & \text{якщо } y_1=1;\ y_2=1 \end{cases} \quad (3.12)$$

Так як другий операнда четвертої одноопераднді не залежно від вхідних даних буде рівним нулю, то побудована третя базова двохоперандна операція буде виродженою. Виходячи з цього можна констатувати, що даним методом неможливо синтезувати всю групу двохоперандних операцій [10].

В результаті проведення дослідження встановлено, що метод синтезу несиметричних двохоперандних двохрозрядних операцій на основі дублювання одноопераднді двохрозрядних операцій базової групи не може бути застосовано для побудови множин операцій потрійного циклу, яких за результатами модулювання більше половини (14 множин із 24) [10]. Для забезпечення можливості синтезу всіх двохоперандних криптоперетворення

отриманих на основі експерименту, необхідно шукати інші підходи, які забезпечать одноманітність синтезу симетричних операцій, несиметричних операцій подвійного циклу та несиметричних операцій потрійного циклу.

Висновки до розділу 3

Удосконалено метод синтезу двохоперандних двохрозрядних операцій криптографічного перетворення на основі метод синтезу симетричних операцій, шляхом застосування в якості першої базової операції несиметричної операції криптоперетворення та додаткової побудови оберненої операції за результатами обчислювального експерименту, що забезпечили можливість додаткового синтезу несиметричних двохоперандних двохрозрядних операцій подвійного циклу.

1. Запропоновано послідовність перетворень результатів обчислювального експерименту для побудови удосконалених моделей операцій несиметричного криптографічного кодування і декодування. На прикладі однієї з класифікованих множин операцій криптографісного кодування з точністю до перестановки представлених кортежами одноопераднних операцій отримано математичні моделі удосконалених несиметричних двохоперандних двохрозрядних операцій подвійного циклу.

2. Запропоновано використати метод синтезу симетричних двохоперандних двохрозрядних операцій для побудови групи несиметричних двохоперандних двохрозрядних операцій. Удосконалений метод синтезу двохоперандних двохрозрядних операцій криптографічного перетворення забезпечив синтез груп несиметричних операцій подвійного циклу. Коректність реалізації даного методу підтверджена класифікованими результатами обчислювального експерименту та збігом отриманих різними методами синтезу математичних моделей на приведеному прикладі однієї з множин операцій.

3. Результати дослідження можливості синтезу множин несиметричних двохоперандних двохрозрядних операцій потрійного циклу показали обмеженість даного методу побудовою лише груп симетричних операцій та несиметричних операцій подвійного циклу.

Результати розділу опубліковано [2], [8], [10].

РОЗДІЛ 4. МОДЕЛЮВАННЯ ТА ДОСЛІДЖЕННЯ МНОЖИН ДВОХОПЕРАНДНИХ ОПЕРАЦІЙ НА ОСНОВІ ПОЄДНАННЯ ОДНООПЕРАНДНИХ ОПЕРАЦІЙ КРИПТОГРАФІЧНОГО ПЕРЕТВОРЕННЯ ІНФОРМАЦІЇ

4. 1. Синтез множини симетричних двохоперандних двохрозрядних операцій шляхом поєднання одноопераднних операцій

В процесі побудови двохоперандних операцій модна поєднувати симетричні одноопераднні операції, симетричні і несиметричні одноопераднні операції, а також несиметричні одноопераднні операції.

При побудові множин двохоперандних операцій операція обробки першого операнда (x) послідовно поєднується з операціями обробки другого операнду (y). Так як при синтезі множини використовуються всі операції для обробки другого операнда, то побудова множини симетричних і несиметричних двохоперандних операцій буде залежати від першого операнду. Виходячи з цього можна допустити що при виборі для обробки першого операнду симетричну одноопераднні операцію можна отримати множину симетричних двохоперандних операцій.

Під час синтезу двохоперандних операцій використаємо принцип розміщення одноопераднних операцій, який відповідає їхньому розташуванню в табличній класифікації одноопераднних двохрозрядних операцій. Відповідна таблична класифікація одноопераднних двохрозрядних операцій, що слугує базою для виконання синтезу, наведена в табл. 4.1 [38, 78, 79].

Відповідно то розробленої техології побудови двохоперандних СЕТ-операцій на основі обьєднаннчя одноопераднних операцій побудуємо операції $C_{1,8}(x,y)$, $C_{1,14}(x,y)$, $C_{1,20}(x,y)$. Дана технологія наведена в [1].

Таблиця 4.1

Дискретні моделі прямих і обернених 2Сі-квант СЕТ-операцій [1]

$C_1(x)=\begin{bmatrix}x_1\\x_2\end{bmatrix}=C_1'(x)$	$C_7(x)=\begin{bmatrix}x_1\\x_2\oplus1\end{bmatrix}=C_7'(x)$	$C_{13}(x)=\begin{bmatrix}x_1\oplus1\\x_2\end{bmatrix}=C_{13}'(x)$	$C_{19}(x)=\begin{bmatrix}x_1\oplus1\\x_2\oplus1\end{bmatrix}=C_{19}'(x)$
$C_2(x)=\begin{bmatrix}x_1\oplus x_2\\x_2\end{bmatrix}=C_2'(x)$	$C_8(x)=\begin{bmatrix}x_1\oplus x_2\\x_2\oplus1\end{bmatrix}=C_{20}'(x)$ $C_8'(x)=\begin{bmatrix}x_1\oplus x_2\oplus1\\x_2\oplus1\end{bmatrix}=C_{20}(x)$	$C_{14}(x)=\begin{bmatrix}x_1\oplus x_2\oplus1\\x_2\end{bmatrix}=C_{14}'(x)$	$C_{20}(x)=\begin{bmatrix}x_1\oplus x_2\oplus1\\x_2\oplus1\end{bmatrix}=C_8'(x)$ $C_{20}'(x)=\begin{bmatrix}x_1\oplus x_2\\x_2\oplus1\end{bmatrix}=C_8(x)$
$C_3(x)=\begin{bmatrix}x_1\\x_1\oplus x_2\end{bmatrix}=C_3'(x)$	$C_9(x)=\begin{bmatrix}x_1\\x_1\oplus x_2\oplus1\end{bmatrix}=C_9'(x)$	$C_{15}(x)=\begin{bmatrix}x_1\oplus1\\x_1\oplus x_2\end{bmatrix}=C_{21}'(x)$ $C_{15}'(x)=\begin{bmatrix}x_1\oplus1\\x_1\oplus x_2\oplus1\end{bmatrix}=C_{21}(x)$	$C_{21}(x)=\begin{bmatrix}x_1\oplus1\\x_1\oplus x_2\oplus1\end{bmatrix}=C_{15}'(x)$ $C_{21}'(x)=\begin{bmatrix}x_1\oplus1\\x_1\oplus x_2\end{bmatrix}=C_{15}(x)$
$C_4(x)=\begin{bmatrix}x_2\\x_1\end{bmatrix}=C_4'(x)$	$C_{10}(x)=\begin{bmatrix}x_2\\x_1\oplus1\end{bmatrix}=C_{16}'(x)$ $C_{10}'(x)=\begin{bmatrix}x_2\oplus1\\x_1\end{bmatrix}=C_{16}(x)$	$C_{16}(x)=\begin{bmatrix}x_2\oplus1\\x_1\end{bmatrix}=C_{10}'(x)$ $C_{16}'(x)=\begin{bmatrix}x_2\\x_1\oplus1\end{bmatrix}=C_{10}(x)$	$C_{22}(x)=\begin{bmatrix}x_2\oplus1\\x_1\oplus1\end{bmatrix}=C_{22}'(x)$
$C_5(x)=\begin{bmatrix}x_2\\x_1\oplus x_2\end{bmatrix}=C_6'(x)$	$C_{11}(x)=\begin{bmatrix}x_2\\x_1\oplus x_2\oplus1\end{bmatrix}=C_{18}'(x)$	$C_{17}(x)=\begin{bmatrix}x_2\oplus1\\x_1\oplus x_2\end{bmatrix}=C_{24}'(x)$	$C_{23}(x)=\begin{bmatrix}x_2\oplus1\\x_1\oplus x_2\oplus1\end{bmatrix}=C_{12}'(x)$
$C_5'(x)=\begin{bmatrix}x_1\oplus x_2\\x_1\end{bmatrix}=C_6(x)$	$C_{11}'(x)=\begin{bmatrix}x_1\oplus x_2\oplus1\\x_1\end{bmatrix}=C_{18}(x)$	$C_{17}'(x)=\begin{bmatrix}x_1\oplus x_2\oplus1\\x_1\oplus1\end{bmatrix}=C_{24}(x)$	$C_{23}'(x)=\begin{bmatrix}x_1\oplus x_2\\x_1\oplus1\end{bmatrix}=C_{12}(x)$
$C_6(x)=\begin{bmatrix}x_1\oplus x_2\\x_1\end{bmatrix}=C_5'(x)$	$C_{12}(x)=\begin{bmatrix}x_1\oplus x_2\\x_1\oplus1\end{bmatrix}=C_{23}'(x)$	$C_{18}(x)=\begin{bmatrix}x_1\oplus x_2\oplus1\\x_1\end{bmatrix}=C_{11}'(x)$	$C_{24}(x)=\begin{bmatrix}x_1\oplus x_2\oplus1\\x_1\oplus1\end{bmatrix}=C_{17}'(x)$
$C_6'(x)=\begin{bmatrix}x_2\\x_1\oplus x_2\end{bmatrix}=C_5(x)$	$C_{12}'(x)=\begin{bmatrix}x_2\oplus1\\x_1\oplus x_2\oplus1\end{bmatrix}=C_{23}(x)$	$C_{18}'(x)=\begin{bmatrix}x_2\\x_1\oplus x_2\oplus1\end{bmatrix}=C_{11}(x)$	$C_{24}'(x)=\begin{bmatrix}x_2\oplus1\\x_1\oplus x_2\end{bmatrix}=C_{17}(x)$

За результатами перетворення отримаємо:

$$C_{1,8}(x,y)=C_1\begin{pmatrix}x_1\\x_2\end{pmatrix}\oplus C_8\begin{pmatrix}y_1\\y_2\end{pmatrix}=\begin{bmatrix}x_1\\x_2\end{bmatrix}\oplus\begin{bmatrix}y_1\oplus y_2\\y_2\oplus1\end{bmatrix}=C_{7,13,19,1}(x,y);$$

$$(C_{7,13,19,1}(x,y)\Rightarrow C_{7,13,19,1}'(x,y))\quad\Rightarrow\quad(C_{1,8}(x,y)\Rightarrow C_{1,8}'(x,y)).$$

$$C_{1,14}(x,y)=C_1\begin{pmatrix}x_1\\x_2\end{pmatrix}\oplus C_{14}\begin{pmatrix}y_1\\y_2\end{pmatrix}=\begin{bmatrix}x_1\\x_2\end{bmatrix}\oplus\begin{bmatrix}y_1\oplus y_2\oplus1\\y_2\end{bmatrix}=C_{13,7,1,19}(x,y);$$

$$(C_{13,7,1,19}(x,y)\Rightarrow C_{13,7,1,19}'(x,y))\quad\Rightarrow\quad(C_{1,14}(x,y)\Rightarrow C_{1,14}'(x,y)).$$

$$C_{1,20}(x,y)=C_1\begin{pmatrix}x_1\\x_2\end{pmatrix}\oplus C_{20}\begin{pmatrix}y_1\\y_2\end{pmatrix}=\begin{bmatrix}x_1\\x_2\end{bmatrix}\oplus\begin{bmatrix}y_1\oplus y_2\oplus1\\y_2\oplus1\end{bmatrix}=C_{20,1,7,13}(x,y);$$

$$(C_{20,1,7,13}(x,y)\Rightarrow C_{20,1,7,13}'(x,y))\quad\Rightarrow\quad(C_{1,20}(x,y)\Rightarrow C_{1,20}'(x,y)).$$

Знайдемо закономірності між операціями побудованими $C_{1,4}(x,y)$, $C_{1,10}(x,y)$, $C_{1,16}(x,y)$, $C_{1,22}(x,y)$ [1]

$$C_{1,4}(x,y) = C_1\begin{pmatrix}x_1\\x_2\end{pmatrix} \oplus C_4\begin{pmatrix}y_1\\y_2\end{pmatrix} = \begin{bmatrix}x_1\\x_2\end{bmatrix} \oplus \begin{bmatrix}y_2\\y_1\end{bmatrix} = C_{1,13,7,19}(x,y);$$

$$(C_{1,13,7,19}(x,y) \Rightarrow C'_{1,13,7,19}(x,y)) \Rightarrow (C_{1,4}(x,y) \Rightarrow C'_{1,4}(x,y)).$$

$$C_{1,10}(x,y) = C_1\begin{pmatrix}x_1\\x_2\end{pmatrix} \oplus C_{10}\begin{pmatrix}y_1\\y_2\end{pmatrix} = \begin{bmatrix}x_1\\x_2\end{bmatrix} \oplus \begin{bmatrix}y_2\\y_1 \oplus 1\end{bmatrix} = C_{7,19,1,13}(x,y);$$

$$(C_{7,19,1,13}(x.y) \Rightarrow C'_{7,19,1,13}(x,y)) \Rightarrow (C_{1,10}(x,y) \Rightarrow C'_{1,10}(x,y).$$

$$C_{1,16}(x,y) = C_1\begin{pmatrix}x_1\\x_2\end{pmatrix} \oplus C_{16}\begin{pmatrix}y_1\\y_2\end{pmatrix} = \begin{bmatrix}x_1\\x_2\end{bmatrix} \oplus \begin{bmatrix}y_2 \oplus 1\\y_1\end{bmatrix} = C_{13,1,19,7}(x,y);$$

$$(C_{13,1,19,7}(x,y) \Rightarrow C'_{13,1,19,7}(x,y)) \Rightarrow (C_{1,16}(x,y) \Rightarrow C'_{1,16}(x,y)).$$

$$C_{1,22}(x,y) = C_1\begin{pmatrix}x_1\\x_2\end{pmatrix} \oplus C_{22}\begin{pmatrix}y_1\\y_2\end{pmatrix} = \begin{bmatrix}x_1\\x_2\end{bmatrix} \oplus \begin{bmatrix}y_2 \oplus 1\\y_1 \oplus 1\end{bmatrix} = C_{19,7,13,1}(x,y);$$

$$(C_{19,7,13,1}(x,y) \Rightarrow C'_{19,7,13,1}(x,y) \Rightarrow (C_{1,22}(x,y) \Rightarrow C'_{1,22}(x,y)).$$

Знайдемо обернені операції $C'_{1,5}(x,y)$ $C'_{1,11}(x,y)$, $C'_{1,17}(x,y)$, $C'_{1,23}(x,y)$.

$$C_{1,5}(x,y) = C_1\begin{pmatrix}x_1\\x_2\end{pmatrix} \oplus C_5\begin{pmatrix}k_1\\k_2\end{pmatrix} = \begin{bmatrix}y_1\\y_2\end{bmatrix} \oplus \begin{bmatrix}y_2\\y_1 \oplus y_2\end{bmatrix} = C_{1,19,7,13}(x,y);$$

$$(C_{1,19,7,13}(x,y) \Rightarrow C'_{1,19,7,13}(x,y)) \Rightarrow (C_{1,5}(x,y) \Rightarrow C'_{1,5}(x,y).$$

$$C_{1,11}(x,y) = C_1\begin{pmatrix}x_1\\x_2\end{pmatrix} \oplus C_{11}\begin{pmatrix}y_1\\y_2\end{pmatrix} = \begin{bmatrix}x_1\\x_2\end{bmatrix} \oplus \begin{bmatrix}y_2\\y_1 \oplus y_2 \oplus 1\end{bmatrix} = C_{7,13,1,19}(x,y);$$

$$(C_{7,13,1,19}(x,y) \Rightarrow C'_{7,13,1,19}(x,y) \Rightarrow (C_{1,11}(x,y) \Rightarrow C'_{1,11}(x,y)).$$

$$C_{1,17} = C_1\begin{pmatrix}x_1\\x_2\end{pmatrix} \oplus C_{17}\begin{pmatrix}y_1\\y_2\end{pmatrix} = \begin{bmatrix}x_1\\x_2\end{bmatrix} \oplus \begin{bmatrix}y_2 \oplus 1\\y_1 \oplus y_2\end{bmatrix} = C_{13,7,19,1}(x,y);$$

$$(C_{13,7,19,1}(x,y) \Rightarrow C'_{13,7,19,1}(x,y)) \Rightarrow (C_{1,17}(x,y) \Rightarrow C'_{1,17}(x,y)).$$

$$C_{1,23}(x,y) = C_1\begin{pmatrix}x_1\\x_2\end{pmatrix} \oplus C_{23}\begin{pmatrix}k_1\\k_2\end{pmatrix} = \begin{bmatrix}x_1\\x_2\end{bmatrix} \oplus \begin{bmatrix}y_2 \oplus 1\\y_1 \oplus y_2 \oplus 1\end{bmatrix} = C_{19,1,13,7}(x,y);$$

$$(C_{19,1,13,7}(x,y) \Rightarrow C'_{19,1,13,7}(x,y)) \Rightarrow (C_{1,23}(x,y) \Rightarrow C'_{1,23}(x,y))$$

По аналогії побудуємо всі прямі і обернені двохоперпандні операції криптографічного перетворення на основі операції $C_1(x)$. Результати моделювання наведені в табл. 4.2.

Узагальнені результати моделювання двохоперандних операцій, синтезованих на основі першої операції обробки першого операнда (табл. 4.2), свідчать про наявність сталої закономірності. Проведений аналіз показав, що властивості сформованих двохоперандних операцій визначаються насамперед характеристиками операції обробки першого операнда. Отримані результати підтверджують визначальний вплив операції обробки першого операнда на структурні характеристики синтезованих двохоперандних криптографічних перетворень та можуть бути використані для прогнозування їхніх властивостей на етапі проєктування [1].

Формалізуємо даний висновок [1]:

$$C(x,y)=C_i(x)\oplus C_j(y)=C'(x,y)\text{, де } C_i(x)=C_i'(x). \quad (4.1)$$

Перевіримо коректність даної моделі.

Нехай перетворення першого операнду буду реалізовано на основі одноопераднної операції $C_2(x)=\begin{bmatrix}x_1\oplus x_2\\ x_2\end{bmatrix}=C_2'(x)$ [9].

Побудуємо операцію $C_{2,1}(x,y)$.

$$C_{2,1}(x,y)=C_2\begin{pmatrix}x_1\\ x_2\end{pmatrix}\oplus C_1\begin{pmatrix}y_1\\ y_2\end{pmatrix}=\begin{bmatrix}x_1\oplus x_2\\ x_2\end{bmatrix}\oplus\begin{bmatrix}y_1\\ y_2\end{bmatrix}$$

$$C_{2,1}(x,y)=\begin{cases}\begin{bmatrix}x_1\oplus x_2\\ x_2\end{bmatrix}\oplus\begin{bmatrix}y_1\\ y_2\end{bmatrix},\ якщо\ y_1=0;\ y_2=0\\ \begin{bmatrix}x_1\oplus x_2\\ x_2\end{bmatrix}\oplus\begin{bmatrix}y_1\\ y_2\end{bmatrix},якщо\ y_1=0;\ y_2=1\\ \begin{bmatrix}x_1\oplus x_2\\ x_2\end{bmatrix}\oplus\begin{bmatrix}y_1\\ y_2\end{bmatrix},\ якщо\ y_1=1;\ y_2=0\\ \begin{bmatrix}x_1\oplus x_2\\ x_2\end{bmatrix}\oplus\begin{bmatrix}y_1\\ y_2\end{bmatrix},якщо\ y_1=1;\ y_2=1\end{cases}==\begin{cases}\begin{bmatrix}x_1\oplus x_2\\ x_2\end{bmatrix},\ якщо\ y_1=0;\ y_2=0\\ \begin{bmatrix}x_1\oplus x_2\\ x_2\oplus 1\end{bmatrix},якщо\ y_1=0;\ y_2=1\\ \begin{bmatrix}x_1\oplus x_2\oplus 1\\ x_2\end{bmatrix},\ якщо\ y_1=1;\ y_2=0\\ \begin{bmatrix}x_1\oplus x_2\oplus 1\\ x_2\oplus 1\end{bmatrix},якщо\ y_1=1;\ y_2=1\end{cases}$$

$$=\begin{cases}C_2(x),\ якщо\ y_1=0;\ y_2=0\\ C_8(x),якщо\ y_1=0;\ y_2=1\\ C_{14}(x),\ якщо\ y_1=1;\ y_2=0\\ C_{20}(x),якщо\ y_1=1;\ y_2=1\end{cases}=C_{2,8,14,20}(x,y)$$

Таблиця 4.2

Синтезована група моделей двохоперандних двохрозрядних операцій отриманих шляхом поєднання одноопераднних двохрозрядних операцій криптоперетворення з операцією $C_1(x)$

$C_1(x)=\begin{bmatrix}x_1\\x_2\end{bmatrix}$		**Операції інверсії**			
Бзові операції	$C_1(x)=\begin{bmatrix}x_1\\x_2\end{bmatrix}$	$C_{1,1}(x,y)=\begin{bmatrix}x_1\\x_2\end{bmatrix}\oplus\begin{bmatrix}y_1\\y_2\end{bmatrix}$	$C_{1,7}(x,y)=\begin{bmatrix}x_1\\x_2\end{bmatrix}\oplus\begin{bmatrix}y_1\\y_2\oplus1\end{bmatrix}$	$C_{1,13}(x,y)=\begin{bmatrix}x_1\\x_2\end{bmatrix}\oplus\begin{bmatrix}y_1\oplus1\\y_2\end{bmatrix}$	$C_{1,19}(x,y)=\begin{bmatrix}x_1\\x_2\end{bmatrix}\oplus\begin{bmatrix}y_1\oplus1\\y_2\oplus1\end{bmatrix}$
	$C_2(x)=\begin{bmatrix}x_1\oplus x_2\\x_2\end{bmatrix}$	$C_{1,2}(x,y)=\begin{bmatrix}x_1\\x_2\end{bmatrix}\oplus\begin{bmatrix}y_1\oplus y_2\\y_2\end{bmatrix}$	$C_{1,8}(x,y)=\begin{bmatrix}x_1\\x_2\end{bmatrix}\oplus\begin{bmatrix}y_1\oplus y_2\\y_2\oplus1\end{bmatrix}$	$C_{1,14}(x,y)=\begin{bmatrix}x_1\\x_2\end{bmatrix}\oplus\begin{bmatrix}y_1\oplus y_2\oplus1\\y_2\end{bmatrix}$	$C_{1,20}(x,y)=\begin{bmatrix}x_1\\x_2\end{bmatrix}\oplus\begin{bmatrix}y_1\oplus y_2\oplus1\\y_2\oplus1\end{bmatrix}$
	$C_3(x)=\begin{bmatrix}x_1\\x_1\oplus x_2\end{bmatrix}$	$C_{1,3}(x,y)=\begin{bmatrix}x_1\\x_2\end{bmatrix}\oplus\begin{bmatrix}y_1\\y_1\oplus y_2\end{bmatrix}$	$C_{1,9}(x,y)=\begin{bmatrix}x_1\\x_2\end{bmatrix}\oplus\begin{bmatrix}y_1\\y_1\oplus y_2\oplus1\end{bmatrix}$	$C_{1,15}(x,y)=\begin{bmatrix}x_1\\x_2\end{bmatrix}\oplus\begin{bmatrix}y_1\oplus1\\y_1\oplus y_2\end{bmatrix}$	$C_{1,21}(x,y)=\begin{bmatrix}x_1\\x_2\end{bmatrix}\oplus\begin{bmatrix}y_1\oplus1\\y_1\oplus y_2\oplus1\end{bmatrix}$
Операції інверсії	$C_4(x)=\begin{bmatrix}x_2\\x_1\end{bmatrix}$	$C_{1,4}(x,y)=\begin{bmatrix}x_1\\x_2\end{bmatrix}\oplus\begin{bmatrix}y_2\\y_1\end{bmatrix}$	$C_{1,10}(x,y)=.\begin{bmatrix}x_1\\x_2\end{bmatrix}\oplus\begin{bmatrix}y_2\\y_1\oplus1\end{bmatrix}$	$C_{1,16}(x,y)=\begin{bmatrix}x_1\\x_2\end{bmatrix}\oplus\begin{bmatrix}y_2\oplus1\\y_1\end{bmatrix}$	$C_{1,22}(x,y)=\begin{bmatrix}x_1\\x_2\end{bmatrix}\oplus\begin{bmatrix}y_2\oplus1\\y_1\oplus1\end{bmatrix}$
	$C_5(x)=\begin{bmatrix}x_2\\x_1\oplus x_2\end{bmatrix}$	$C_{1,5}(x,y)=\begin{bmatrix}x_1\\x_2\end{bmatrix}\oplus\begin{bmatrix}y_2\\y_1\oplus y_2\end{bmatrix}$	$C_{1,11}(x,y)=\begin{bmatrix}x_1\\x_2\end{bmatrix}\oplus\begin{bmatrix}y_2\\y_1\oplus y_2\oplus1\end{bmatrix}$	$C_{1,17}(x,y)=\begin{bmatrix}x_1\\x_2\end{bmatrix}\oplus\begin{bmatrix}y_2\oplus1\\y_1\oplus y_2\end{bmatrix}$	$C_{1,23}(x,y)=\begin{bmatrix}x_1\\x_2\end{bmatrix}\oplus\begin{bmatrix}y_2\oplus1\\y_1\oplus y_2\oplus1\end{bmatrix}$
	$C_6(x)=\begin{bmatrix}x_1\oplus x_2\\x_1\end{bmatrix}$	$C_{1,6}(x,y)=\begin{bmatrix}x_1\\x_2\end{bmatrix}\oplus\begin{bmatrix}y_1\oplus y_2\\y_1\end{bmatrix}$	$C_{1,12}(x,y)=\begin{bmatrix}x_1\\x_2\end{bmatrix}\oplus\begin{bmatrix}y_1\oplus y_2\\y_1\oplus1\end{bmatrix}$	$C_{1,18}(x,y)=\begin{bmatrix}x_1\\x_2\end{bmatrix}\oplus\begin{bmatrix}y_1\oplus y_2\oplus1\\y_1\end{bmatrix}$	$C_{1,24}=\begin{bmatrix}x_1\\x_2\end{bmatrix}\oplus\begin{bmatrix}y_1\oplus y_2\oplus1\\y_1\oplus1\end{bmatrix}$

Побудуємо обернену операцію.

Так як $C_2(x) \Rightarrow C_2^{/}(x) = C_2(x)$, $C_8(x) \Rightarrow C_8^{/}(x) = C_{20}(x)$; $C_{14}(x) \Rightarrow C_{14}^{/}(x) = C_{14}(x)$, $C_{20}(x) \Rightarrow C_{20}^{/}(x) = C_8(x)$, тоді отримаємо

$$C_{2,1}^{/}(x,y) = \begin{cases} C_2^{/}(x), \text{ якщо } y_1 = 0;\ y_2 = 0 \\ C_8^{/}(x), \text{якщо } y_1 = 0;\ y_2 = 1 \\ C_{14}^{/}(x), \text{ якщо } y_1 = 1;\ y_2 = 0 \\ C_{20}^{/}(x), \text{якщо } y_1 = 1;\ y_2 = 1 \end{cases} = \begin{cases} C_2(x), \text{ якщо } y_1 = 0;\ y_2 = 0 \\ C_{20}(x), \text{якщо } y_1 = 0;\ y_2 = 1 \\ C_{14}(x), \text{ якщо } y_1 = 1;\ y_2 = 0 \\ C_8(x), \text{якщо } y_1 = 1;\ y_2 = 1 \end{cases} =$$

$$= \begin{cases} \begin{bmatrix} x_1 \oplus x_2 \\ x_2 \end{bmatrix}, \text{ якщо } y_1 = 0;\ y_2 = 0 \\ \begin{bmatrix} x_1 \oplus x_2 \oplus 1 \\ x_2 \oplus 1 \end{bmatrix}, \text{якщо } y_1 = 0;\ y_2 = 1 \\ \begin{bmatrix} x_1 \oplus x_2 \oplus 1 \\ x_2 \end{bmatrix}, \text{ якщо } y_1 = 1;\ y_2 = 0 \\ \begin{bmatrix} x_1 \oplus x_2 \\ x_2 \oplus 1 \end{bmatrix}, \text{якщо } y_1 = 1;\ y_2 = 1 \end{cases} = \begin{bmatrix} x_1 \oplus x_2 \\ x_2 \end{bmatrix} \oplus \begin{bmatrix} y_1 \oplus y_2 \\ y_2 \end{bmatrix} = C_{2,2}(x,y)$$

В результаті побудови отримано наступні взаємозв’язки [8]:

$$\begin{aligned} &C_{2,1}(x,y) = C_{2,8,14,20}(x,y); \\ &C_{2,8,14,20}(x,y) \Rightarrow C_{2,8,14,20}^{/}(x,y) = C_{2,20,14,8}(x,y); \\ &C_{2,20,14,8}(x,y) = C_{2,2}(x,y); \\ &(C_{2,1}(x,y) \Rightarrow C_{2,1}^{/}(x,y) = C_{2,2}(x,y). \end{aligned} \quad . \qquad (4.2)$$

Отримані взаємозв’язки (4.2) показали некоректність моделі (4.1) при побудові множини моделей симетричних двохоперандних операцій при об’єднанні будь якої симетричної одноопераднної операції з будь якою одноопераднної операцією для обробки другого операнда.

Обмеження на застосування моделі (4.1) встановимо в процесі синтезу множин несиметричних двохоперандних операцій шляхом поєднання одноопераднних операцій.

4.2. Синтез множини несиметричних двохоперандних двохрозрядних операцій шляхом поєднання одноопераднних операцій перша з яких є симетричною.

Так як синтезована двохоперандна операція $C_{2,1}(x,y)$ виявилася несиметричною, то будемо будувати множину несиметричних операцій криптографічного перетворення інформації на основі одноопераднної операції $C_2(x)$.

Побудуємо операцію $C_{2,7}(x,y)$.

$$C_{2,7}(x,y)=C_2\begin{pmatrix}x_1\\x_2\end{pmatrix}\oplus C_7\begin{pmatrix}y_1\\y_2\end{pmatrix}=\begin{bmatrix}x_1\oplus x_2\\x_2\end{bmatrix}\oplus\begin{bmatrix}y_1\\y_2\oplus 1\end{bmatrix};$$

$$C_{2,7}(x,y)=\begin{cases}\begin{bmatrix}x_1\oplus x_2\\x_2\end{bmatrix}\oplus\begin{bmatrix}k_1\\k_2\oplus 1\end{bmatrix}, \text{ якщо } y_1=0;\ y_2=0\\ \begin{bmatrix}x_1\oplus x_2\\x_2\end{bmatrix}\oplus\begin{bmatrix}k_1\\k_2\oplus 1\end{bmatrix}, \text{якщо } y_1=0;\ y_2=1\\ \begin{bmatrix}x_1\oplus x_2\\x_2\end{bmatrix}\oplus\begin{bmatrix}k_1\\k_2\oplus 1\end{bmatrix}, \text{ якщо } y_1=1;\ y_2=0\\ \begin{bmatrix}x_1\oplus x_2\\x_2\end{bmatrix}\oplus\begin{bmatrix}k_1\\k_2\oplus 1\end{bmatrix}, \text{якщо } y_1=1;\ y_2=1\end{cases}=\begin{cases}\begin{bmatrix}x_1\oplus x_2\\x_2\oplus 1\end{bmatrix}, \text{ якщо } y_1=0;\ y_2=0\\ \begin{bmatrix}x_1\oplus x_2\\x_2\end{bmatrix}, \text{якщо } y_1=0;\ y_2=1\\ \begin{bmatrix}x_1\oplus x_2\oplus 1\\x_2\oplus 1\end{bmatrix}, \text{ якщо } y_1=1;\ y_2=0\\ \begin{bmatrix}x_1\oplus x_2\oplus 1\\x_2\end{bmatrix}, \text{якщо } y_1=1;\ y_2=1\end{cases}=C_{8,2,20,14}(x,y)$$

$$C'_{2,7}(x,y)=\begin{cases}C'_8(x), \text{ якщо } y_1=0;\ y_2=0\\ C'_2(x), \text{якщо } y_1=0;\ y_2=1\\ C'_{20}(x), \text{ якщо } y_1=1;\ y_2=0\\ C'_{14}(x), \text{якщо } y_1=1;\ y_2=1\end{cases}=\begin{cases}C_{20}(x), \text{ якщо } y_1=0;\ y_2=0\\ C_2(x), \text{якщо } y_1=0;\ y_2=1\\ C_8(x), \text{ якщо } y_1=1;\ y_2=0\\ C_{14}(x), \text{якщо } y_1=1;\ y_2=1\end{cases}=$$

$$=\begin{cases}\begin{bmatrix}x_1\oplus x_2\oplus 1\\x_2\oplus 1\end{bmatrix}, \text{ якщо } y_1=0;\ y_2=0\\ \begin{bmatrix}x_1\oplus x_2\\x_2\end{bmatrix}, \text{якщо } y_1=0;\ y_2=1\\ \begin{bmatrix}x_1\oplus x_2\\x_2\oplus 1\end{bmatrix}, \text{ якщо } y_1=1;\ y_2=0\\ \begin{bmatrix}x_1\oplus x_2\oplus 1\\x_2\end{bmatrix}, \text{якщо } y_1=1;\ y_2=1\end{cases}=\begin{bmatrix}x_1\oplus x_2\\x_2\end{bmatrix}\oplus\begin{bmatrix}y_1\oplus y_2\oplus 1\\y_2\oplus 1\end{bmatrix}=C_{2,20}(x,y)$$

В результаті побудови отримано наступні взаємозв'язки [9]:

$$C_{2,7}(x,y) = C_{8,2,20,14}(x,y);$$
$$C_{8,2,20,14}(x,y) \Rightarrow C'_{8,2,20,14}(x,y) = C_{20,2,8,14}(x,y);$$
$$C_{20,2,8,14}(x,y) = C_{2,20}(x,y);$$
$$(C_{2,7}(x,y) \Rightarrow C'_{2,7}(x,y) = C_{2,20}(x,y).$$

Знайдемо обернену операцію для операції $C_{2,13}(x,y)$.

$$C_{2,13}(x,y) = C_2\begin{pmatrix} x_1 \\ x_2 \end{pmatrix} \oplus C_{13}\begin{pmatrix} y_1 \\ y_2 \end{pmatrix} = \begin{bmatrix} x_1 \oplus x_2 \\ x_2 \end{bmatrix} \oplus \begin{bmatrix} y_1 \oplus 1 \\ y_2 \end{bmatrix};$$

$$C_{2,13}(x,y) = \begin{cases} \begin{bmatrix} x_1 \oplus x_2 \\ x_2 \end{bmatrix} \oplus \begin{bmatrix} y_1 \oplus 1 \\ y_2 \end{bmatrix}, \text{ якщо } y_1 = 0;\ y_2 = 0 \\ \begin{bmatrix} x_1 \oplus x_2 \\ x_2 \end{bmatrix} \oplus \begin{bmatrix} y_1 \oplus 1 \\ y_2 \end{bmatrix}, \text{якщо } y_1 = 0;\ y_2 = 1 \\ \begin{bmatrix} x_1 \oplus x_2 \\ x_2 \end{bmatrix} \oplus \begin{bmatrix} y_1 \oplus 1 \\ y_2 \end{bmatrix}, \text{ якщо } y_1 = 1;\ y_2 = 0 \\ \begin{bmatrix} x_1 \oplus x_2 \\ x_2 \end{bmatrix} \oplus \begin{bmatrix} y_1 \oplus 1 \\ y_2 \end{bmatrix}, \text{якщо } y_1 = 1;\ y_2 = 1 \end{cases} = \begin{cases} \begin{bmatrix} x_1 \oplus x_2 \oplus 1 \\ x_2 \end{bmatrix}, \text{ якщо } y_1 = 0;\ y_2 = 0 \\ \begin{bmatrix} x_1 \oplus x_2 \oplus 1 \\ x_2 \oplus 1 \end{bmatrix}, \text{якщо } y_1 = 0;\ y_2 = 1 \\ \begin{bmatrix} x_1 \oplus x_2 \\ x_2 \end{bmatrix}, \text{ якщо } y_1 = 1;\ y_2 = 0 \\ \begin{bmatrix} x_1 \oplus x_2 \\ x_2 \oplus 1 \end{bmatrix}, \text{якщо } y_1 = 1;\ y_2 = 1 \end{cases} = C_{14,20,2,8}(x,y)$$

$$C'_{2,13}(x,y) = \begin{cases} C'_{14}(x), \text{ якщо } y_1 = 0;\ y_2 = 0 \\ C'_{20}(x), \text{якщо } y_1 = 0;\ y_2 = 1 \\ C'_2(x), \text{ якщо } y_1 = 1;\ y_2 = 0 \\ C'_8(x), \text{якщо } y_1 = 1;\ y_2 = 1 \end{cases} = \begin{cases} C_{14}(x), \text{ якщо } y_1 = 0;\ y_2 = 0 \\ C_8(x), \text{якщо } y_1 = 0;\ y_2 = 1 \\ C_2(x), \text{ якщо } y_1 = 1;\ y_2 = 0 \\ C_{20}(x), \text{якщо } y_1 = 1;\ y_2 = 1 \end{cases} =$$

$$= \begin{cases} \begin{bmatrix} x_1 \oplus x_2 \oplus 1 \\ x_2 \end{bmatrix}, \text{ якщо } y_1 = 0;\ y_2 = 0 \\ \begin{bmatrix} x_1 \oplus x_2 \\ x_2 \oplus 1 \end{bmatrix}, \text{якщо } y_1 = 0;\ y_2 = 1 \\ \begin{bmatrix} x_1 \oplus x_2 \\ x_2 \end{bmatrix}, \text{ якщо } y_1 = 1;\ y_2 = 0 \\ \begin{bmatrix} x_1 \oplus x_2 \oplus 1 \\ x_2 \oplus 1 \end{bmatrix}, \text{якщо } y_1 = 1;\ y_2 = 1 \end{cases} = \begin{bmatrix} x_1 \oplus x_2 \\ x_2 \end{bmatrix} \oplus \begin{bmatrix} y_1 \oplus y_2 \oplus 1 \\ y_2 \end{bmatrix} = C_{2,14}(x,y)$$

В результаті побудови отримано наступні взаємозв'язки:

$$C_{2,13}(x,y) = C_{14,20,2,8}(x,y);$$
$$C_{14,20,2,8}(x,y) \Rightarrow C'_{14,20,2,8}(x,y) = C_{14,8,2,20}(x,y);$$
$$C_{14,8,2,20}(x,y) = C_{2,20}(x,y);$$
$$(C_{2,13}(x,y) \Rightarrow C'_{2,13}(x,y) = C_{2,14}(x,y).$$

Знайдемо обернену операцію для операції $C_{2,19}(x,y)$.

$$C_{2,19}(x,y)=C_2\begin{pmatrix}x_1\\x_2\end{pmatrix}\oplus C_{13}\begin{pmatrix}y_1\\y_2\end{pmatrix}=\begin{bmatrix}x_1\oplus x_2\\x_2\end{bmatrix}\oplus\begin{bmatrix}y_1\oplus 1\\y_2\oplus 1\end{bmatrix};$$

$$C_{2,19}(x,y)=\begin{cases}\begin{bmatrix}x_1\oplus x_2\\x_2\end{bmatrix}\oplus\begin{bmatrix}y_1\oplus 1\\y_2\oplus 1\end{bmatrix},\ якщо\ y_1=0;\ y_2=0\\ \begin{bmatrix}x_1\oplus x_2\\x_2\end{bmatrix}\oplus\begin{bmatrix}y_1\oplus 1\\y_2\oplus 1\end{bmatrix},якщо\ y_1=0;\ y_2=1\\ \begin{bmatrix}x_1\oplus x_2\\x_2\end{bmatrix}\oplus\begin{bmatrix}y_1\oplus 1\\y_2\oplus 1\end{bmatrix},\ якщо\ y_1=1;\ y_2=0\\ \begin{bmatrix}x_1\oplus x_2\\x_2\end{bmatrix}\oplus\begin{bmatrix}y_1\oplus 1\\y_2\oplus 1\end{bmatrix},якщо\ y_1=1;\ y_2=1\end{cases}=\begin{cases}\begin{bmatrix}x_1\oplus x_2\oplus 1\\x_2\oplus 1\end{bmatrix},\ якщо\ y_1=0;\ y_2=0\\ \begin{bmatrix}x_1\oplus x_2\oplus 1\\x_2\end{bmatrix},якщо\ y_1=0;\ y_2=1\\ \begin{bmatrix}x_1\oplus x_2\\x_2\oplus 1\end{bmatrix},\ якщо\ y_1=1;\ y_2=0\\ \begin{bmatrix}x_1\oplus x_2\\x_2\end{bmatrix},якщо\ y_1=1;\ y_2=1\end{cases}=C_{20,14,8,2}(x,y)$$

$$C'_{2,19}(x,y)==\begin{cases}C'_{20}(x),\ якщо\ y_1=0;\ y_2=0\\ C'_{14}(x),якщо\ y_1=0;\ y_2=1\\ C'_{8}(x),\ якщо\ y_1=1;\ y_2=0\\ C'_{2}(x),якщо\ y_1=1;\ y_2=1\end{cases}=\begin{cases}C_{8}(x),\ якщо\ y_1=0;\ y_2=0\\ C_{14}(x),якщо\ y_1=0;\ y_2=1\\ C_{20}(x),\ якщо\ y_1=1;\ y_2=0\\ C_{2}(x),якщо\ y_1=1;\ y_2=1\end{cases}=$$

$$=\begin{cases}\begin{bmatrix}x_1\oplus x_2\\x_2\oplus 1\end{bmatrix},\ якщо\ y_1=0;\ y_2=0\\ \begin{bmatrix}x_1\oplus x_2\oplus 1\\x_2\end{bmatrix},якщо\ y_1=0;\ y_2=1\\ \begin{bmatrix}x_1\oplus x_2\oplus 1\\x_2\oplus 1\end{bmatrix},\ якщо\ y_1=1;\ y_2=0\\ \begin{bmatrix}x_1\oplus x_2\\x_2\end{bmatrix},якщо\ y_1=1;\ y_2=1\end{cases}=\begin{bmatrix}x_1\oplus x_2\\x_2\end{bmatrix}\oplus\begin{bmatrix}y_1\oplus y_2\\y_2\oplus 1\end{bmatrix}=C_{2,8}(x,y)$$

Отримано наступні взаємозв'язки:

$$C_{2,19}(x,y)=C_{20,14,8,2}(x,y);$$
$$C_{20,14,8,2}(x,y)\ \Rightarrow\ C'_{20,14,8,2}(x,y)=C_{8,14,20,2}(x,y);$$
$$C_{8,14,20,2}(x,y)=C_{2,8}(x,y);$$
$$(C_{2,19}(x,y)\ \Rightarrow\ C'_{2,19}(x,y)=C_{2,8}(x,y).$$

Побудуємо операцію $C_{2,2}(x,y)$ і обернену до неї операцію.

$$C_{2,2}(x,y)=C_2\begin{pmatrix}x_1\\x_2\end{pmatrix}\oplus C_2\begin{pmatrix}y_1\\y_2\end{pmatrix}=\begin{bmatrix}x_1\oplus x_2\\x_2\end{bmatrix}\oplus\begin{bmatrix}y_1\oplus y_2\\y_2\end{bmatrix}$$

$$C_{2,2}(x,y)=\begin{cases}\begin{bmatrix}x_1\oplus x_2\\ x_2\end{bmatrix}\oplus\begin{bmatrix}y_1\oplus y_2\\ y_2\end{bmatrix}, \text{ якщо } y_1=0;\ y_2=0\\ \begin{bmatrix}x_1\oplus x_2\\ x_2\end{bmatrix}\oplus\begin{bmatrix}y_1\oplus y_2\\ y_2\end{bmatrix}, \text{якщо } y_1=0;\ y_2=1\\ \begin{bmatrix}x_1\oplus x_2\\ x_2\end{bmatrix}\oplus\begin{bmatrix}y_1\oplus y_2\\ y_2\end{bmatrix}, \text{ якщо } y_1=1;\ y_2=0\\ \begin{bmatrix}x_1\oplus x_2\\ x_2\end{bmatrix}\oplus\begin{bmatrix}y_1\oplus y_2\\ y_2\end{bmatrix}, \text{якщо } y_1=1;\ y_2=1\end{cases}=\begin{cases}\begin{bmatrix}x_1\oplus x_2\\ x_2\end{bmatrix}, \text{ якщо } y_1=0;\ y_2=0\\ \begin{bmatrix}x_1\oplus x_2\oplus 1\\ x_2\oplus 1\end{bmatrix}, \text{якщо } y_1=0;\ y_2=1\\ \begin{bmatrix}x_1\oplus x_2\oplus 1\\ x_2\end{bmatrix}, \text{ якщо } y_1=1;\ y_2=0\\ \begin{bmatrix}x_1\oplus x_2\oplus 1\\ x_2\oplus 1\end{bmatrix}, \text{якщо } y_1=1;\ y_2=1\end{cases}=C_{2,20,14,8}(x,y)$$

$$C'_{2,2}(y,x)=\begin{cases}\begin{bmatrix}x_1\oplus x_2\\ x_2\end{bmatrix}, \text{ якщо } y_1=0;\ y_2=0\\ \begin{bmatrix}x_1\oplus x_2\\ x_2\oplus 1\end{bmatrix}, \text{якщо } y_1=0;\ y_2=1\\ \begin{bmatrix}x_1\oplus x_2\oplus 1\\ x_2\end{bmatrix}, \text{ якщо } y_1=1;\ y_2=0\\ \begin{bmatrix}x_1\oplus x_2\oplus 1\\ x_2\oplus 1\end{bmatrix}, \text{якщо } y_1=1;\ y_2=1\end{cases}=\begin{bmatrix}x_1\oplus x_2\\ x_2\end{bmatrix}\oplus\begin{bmatrix}y_1\\ y_2\end{bmatrix}=C_{2,8,14,20}(x,y)=C_{2,1}$$

Отримано наступні взаємозв’язки:

$$\begin{aligned}&C_{2,2}(x,y)=C_{2,20,14,8}(x,y);\\ &C_{2,20,14,8}(x,y)\ \Rightarrow\ C'_{2,20,14,8}(x,y)=C_{2,8,14,20}(x,y);\\ &C_{2,8,14,20}(x,y)=C_{2,1}(x,y);\\ &(C_{2,2}(x,y)\ \Rightarrow\ C'_{2,2}(x,y)=C_{2,1}(x,y).\end{aligned}$$

По аналогії побудуємо взаємозв’язки між всіма операціями множини операції синтезованих шляхом поєднання одноопераднних операцій на основі симетричної одноопераднної операції $C_{2,1}(x,y)$. Результати синтезу множини моделей двохопераднних двохрозрядних операцій синтезованих на основі операції $C_2(x)$ наведена в табл.4.3.

Як видно з табл.4.3 жодна з синтезованих двохрозрядних двохопераднних операцій побудованих на основі симетричної одноопераднної операції $C_{2,1}(x,y)$ не виявилась симетричною [9].

Таблиця 4.3

Синтезована множина моделей двохоперандних двохрозрядних операцій на основі операції $C_2(x)$ [8]

$C_2(x)=\begin{bmatrix}x_1\oplus x_2\\ x_2\end{bmatrix}$		**Операції інверсії**			
Базові операції	$C_1(x)=\begin{bmatrix}x_1\\ x_2\end{bmatrix}$	$C_{2,1}(x,y)=\begin{bmatrix}x_1\oplus x_2\\ x_2\end{bmatrix}\oplus\begin{bmatrix}y_1\\ y_2\end{bmatrix}$	$C_{2,7}(x,y)=\begin{bmatrix}x_1\oplus x_2\\ x_2\end{bmatrix}\oplus\begin{bmatrix}y_1\\ y_2\oplus 1\end{bmatrix}$	$C_{2,13}(x,y)=\begin{bmatrix}x_1\oplus x_2\\ x_2\end{bmatrix}\oplus\begin{bmatrix}y_1\oplus 1\\ y_2\end{bmatrix}$	$C_{2,19}(x,y)=\begin{bmatrix}x_1\oplus x_2\\ x_2\end{bmatrix}\oplus\begin{bmatrix}y_1\oplus 1\\ y_2\oplus 1\end{bmatrix}$
		$C'_{2,2}(x,y)=\begin{bmatrix}x_1\oplus x_2\\ x_2\end{bmatrix}\oplus\begin{bmatrix}y_1\oplus y_2\\ y_2\end{bmatrix}$	$C'_{2,20}(x,y)=\begin{bmatrix}x_1\oplus x_2\\ x_2\end{bmatrix}\oplus\begin{bmatrix}y_1\oplus y_2\oplus 1\\ y_2\oplus 1\end{bmatrix}$	$C'_{2,14}(x,y)=\begin{bmatrix}x_1\oplus x_2\\ x_2\end{bmatrix}\oplus\begin{bmatrix}y_1\oplus y_2\oplus 1\\ y_2\end{bmatrix}$	$C'_{2,8}(x,y)=\begin{bmatrix}x_1\oplus x_2\\ x_2\end{bmatrix}\oplus\begin{bmatrix}y_1\oplus y_2\\ y_2\oplus 1\end{bmatrix}$
	$C_2(x)=\begin{bmatrix}x_1\oplus x_2\\ x_2\end{bmatrix}$	$C_{2,2}(x,y)=\begin{bmatrix}x_1\oplus x_2\\ x_2\end{bmatrix}\oplus\begin{bmatrix}y_1\oplus y_2\\ y_2\end{bmatrix}$	$C_{2,8}=\begin{bmatrix}x_1\oplus x_2\\ x_2\end{bmatrix}\oplus\begin{bmatrix}y_1\oplus y_2\\ y_2\oplus 1\end{bmatrix}$	$C_{2,14}(x,y)=\begin{bmatrix}x_1\oplus x_2\\ x_2\end{bmatrix}\oplus\begin{bmatrix}y_1\oplus y_2\oplus 1\\ y_2\end{bmatrix}$	$C_{2,20}(x,y)=\begin{bmatrix}x_1\oplus x_2\\ x_2\end{bmatrix}\oplus\begin{bmatrix}y_1\oplus y_2\oplus 1\\ y_2\oplus 1\end{bmatrix}$
		$C'_{2,1}(x,y)=\begin{bmatrix}x_1\oplus x_2\\ x_2\end{bmatrix}\oplus\begin{bmatrix}y_1\\ y_2\end{bmatrix}$	$C'_{2,19}(x,y)=\begin{bmatrix}x_1\oplus x_2\\ x_2\end{bmatrix}\oplus\begin{bmatrix}y_1\oplus 1\\ y_2\oplus 1\end{bmatrix}$	$C'_{2,13}(x,y)=\begin{bmatrix}x_1\oplus x_2\\ x_2\end{bmatrix}\oplus\begin{bmatrix}y_1\oplus 1\\ y_2\end{bmatrix}$	$C'_{2,7}(x,y)=\begin{bmatrix}x_1\oplus x_2\\ x_2\end{bmatrix}\oplus\begin{bmatrix}y_1\\ y_2\oplus 1\end{bmatrix}$
	$C_3(x)=\begin{bmatrix}x_1\\ x_1\oplus x_2\end{bmatrix}$	$C_{2,3}(x,y)=\begin{bmatrix}x_1\oplus x_2\\ x_2\end{bmatrix}\oplus\begin{bmatrix}y_1\\ y_1\oplus y_2\end{bmatrix}$	$C_{2,9}(x,y)=\begin{bmatrix}x_1\oplus x_2\\ x_2\end{bmatrix}\oplus\begin{bmatrix}y_1\\ y_1\oplus y_2\oplus 1\end{bmatrix}$	$C_{2,15}(x,y)=\begin{bmatrix}x_1\oplus x_2\\ x_2\end{bmatrix}\oplus\begin{bmatrix}y_1\oplus 1\\ y_1\oplus y_2\end{bmatrix}$	$C_{2,21}(x,y)=\begin{bmatrix}x_1\oplus x_2\\ x_2\end{bmatrix}\oplus\begin{bmatrix}y_1\oplus 1\\ y_1\oplus y_2\oplus 1\end{bmatrix}$
		$C'_{2,5}(x,y)=\begin{bmatrix}x_1\oplus x_2\\ x_2\end{bmatrix}\oplus\begin{bmatrix}y_2\\ y_1\oplus y_2\end{bmatrix}$	$C'_{2,23}(x,y)=\begin{bmatrix}x_1\oplus x_2\\ x_2\end{bmatrix}\oplus\begin{bmatrix}y_2\oplus 1\\ y_1\oplus y_2\oplus 1\end{bmatrix}$	$C'_{2,17}(x,y)=\begin{bmatrix}x_1\oplus x_2\\ x_2\end{bmatrix}\oplus\begin{bmatrix}y_2\oplus 1\\ y_1\oplus y_2\end{bmatrix}$	$C'_{2,11}=\begin{bmatrix}x_1\oplus x_2\\ x_2\end{bmatrix}\oplus\begin{bmatrix}y_2\\ y_1\oplus y_2\oplus 1\end{bmatrix}$
Операції інверсії	$C_4(x)=\begin{bmatrix}x_2\\ x_1\end{bmatrix}$	$C_{2,4}(x,y)=\begin{bmatrix}x_1\oplus x_2\\ x_2\end{bmatrix}\oplus\begin{bmatrix}y_2\\ y_1\end{bmatrix}$	$C_{2,10}(x,y)=\begin{bmatrix}x_1\oplus x_2\\ x_2\end{bmatrix}\oplus\begin{bmatrix}y_2\\ y_1\oplus 1\end{bmatrix}$	$C_{2,16}(x,y)=\begin{bmatrix}x_1\oplus x_2\\ x_2\end{bmatrix}\oplus\begin{bmatrix}y_2\oplus 1\\ y_1\end{bmatrix}$	$C_{2,22}(x,y)=\begin{bmatrix}x_1\oplus x_2\\ x_2\end{bmatrix}\oplus\begin{bmatrix}y_2\oplus 1\\ y_1\oplus 1\end{bmatrix}$
		$C'_{2,6}(x,y)=\begin{bmatrix}x_1\oplus x_2\\ x_2\end{bmatrix}\oplus\begin{bmatrix}y_1\oplus y_2\\ y_1\end{bmatrix}$	$C'_{2,24}(x,y)=\begin{bmatrix}x_1\oplus x_2\\ x_2\end{bmatrix}\oplus\begin{bmatrix}y_1\oplus y_2\oplus 1\\ y_1\oplus 1\end{bmatrix}$	$C'_{2,18}(x,y)=\begin{bmatrix}x_1\oplus x_2\\ x_2\end{bmatrix}\oplus\begin{bmatrix}y_1\oplus y_2\oplus 1\\ y_1\end{bmatrix}$	$C'_{2,12}(x,y)=\begin{bmatrix}x_1\oplus x_2\\ x_2\end{bmatrix}\oplus\begin{bmatrix}y_1\oplus y_2\\ y_1\oplus 1\end{bmatrix}$
	$C_5(x)=\begin{bmatrix}x_2\\ x_1\oplus x_2\end{bmatrix}$	$C_{2,5}(x,y)=\begin{bmatrix}x_1\oplus x_2\\ x_2\end{bmatrix}\oplus\begin{bmatrix}k_2\\ k_1\oplus k_2\end{bmatrix}$	$C_{2,11}(x,y)=\begin{bmatrix}x_1\oplus x_2\\ x_2\end{bmatrix}\oplus\begin{bmatrix}y_2\\ y_1\oplus y_2\oplus 1\end{bmatrix}$	$C_{2,17}(x,y)=\begin{bmatrix}x_1\oplus x_2\\ x_2\end{bmatrix}\oplus\begin{bmatrix}y_2\oplus 1\\ y_1\oplus y_1\end{bmatrix}$	$C_{2,23}(x,y)=\begin{bmatrix}x_1\oplus x_2\\ x_2\end{bmatrix}\oplus\begin{bmatrix}y_2\oplus 1\\ y_1\oplus y_2\oplus 1\end{bmatrix}$
		$C'_{2,3}=\begin{bmatrix}x_1\oplus x_2\\ x_2\end{bmatrix}\oplus\begin{bmatrix}y_1\\ y_1\oplus y_2\end{bmatrix}$	$C'_{2,21}(x,y)=\begin{bmatrix}x_1\oplus x_2\\ x_2\end{bmatrix}\oplus\begin{bmatrix}y_1\oplus 1\\ y_1\oplus y_2\oplus 1\end{bmatrix}$	$C'_{2,15}(x,y)=\begin{bmatrix}x_1\oplus x_2\\ x_2\end{bmatrix}\oplus\begin{bmatrix}y_1\oplus 1\\ y_1\oplus y_2\end{bmatrix}$	$C'_{2,9}(x,y)=\begin{bmatrix}x_1\oplus x_2\\ x_2\end{bmatrix}\oplus\begin{bmatrix}y_1\\ y_1\oplus y_2\oplus 1\end{bmatrix}$
	$C_6(x)=\begin{bmatrix}x_1\oplus x_2\\ x_1\end{bmatrix}$	$C_{2,6}(x,y)=\begin{bmatrix}x_1\oplus x_2\\ x_2\end{bmatrix}\oplus\begin{bmatrix}y_1\oplus y_2\\ y_1\end{bmatrix}$	$C_{2,12}(x,y)=\begin{bmatrix}x_1\oplus x_2\\ x_2\end{bmatrix}\oplus\begin{bmatrix}y_1\oplus y_2\\ y_1\oplus 1\end{bmatrix}$	$C_{2,18}(x,y)=\begin{bmatrix}x_1\oplus x_2\\ x_2\end{bmatrix}\oplus\begin{bmatrix}y_1\oplus y_2\oplus 1\\ y_1\end{bmatrix}$	$C_{2,24}(x,y)=\begin{bmatrix}x_1\oplus x_2\\ x_2\end{bmatrix}\oplus\begin{bmatrix}y_1\oplus y_2\oplus 1\\ y_1\oplus 1\end{bmatrix}$
		$C'_{2,4}(x,y)=\begin{bmatrix}x_1\oplus x_2\\ x_2\end{bmatrix}\oplus\begin{bmatrix}y_2\\ y_1\end{bmatrix}$	$C'_{2,22}(x,y)=\begin{bmatrix}x_1\oplus x_2\\ x_2\end{bmatrix}\oplus\begin{bmatrix}y_2\oplus 1\\ y_1\oplus 1\end{bmatrix}$	$C'_{2,16}(x,y)=\begin{bmatrix}x_1\oplus x_2\\ x_2\end{bmatrix}\oplus\begin{bmatrix}y_2\oplus 1\\ y_1\end{bmatrix}$	$C'_{2,10}(x,y)=\begin{bmatrix}x_1\oplus x_2\\ x_2\end{bmatrix}\oplus\begin{bmatrix}y_2\\ y_1\oplus 1\end{bmatrix}$

При аналізі табл.4.3 були встановлені наступні залежності:

$$C_{2,1}(x,y)=C_2\begin{pmatrix}x_1\\x_2\end{pmatrix}\oplus C_1\begin{pmatrix}y_1\\y_2\end{pmatrix}\quad\Rightarrow\quad C'_{2,1}(x,y)=C_2\begin{pmatrix}x_1\\x_2\end{pmatrix}\oplus C_2\left(C_1\begin{pmatrix}y_1\\y_2\end{pmatrix}\right)$$

$$C_{2,2}(x,y)=C_2\begin{pmatrix}x_1\\x_2\end{pmatrix}\oplus C_2\begin{pmatrix}y_1\\y_2\end{pmatrix}\quad\Rightarrow\quad C'_{2,1}(x,y)=C_2\begin{pmatrix}x_1\\x_2\end{pmatrix}\oplus C_2\left(C_2\begin{pmatrix}y_1\\y_2\end{pmatrix}\right)$$

. . . . . .

$$C_{2,24}(x,y)=C_2\begin{pmatrix}x_1\\x_2\end{pmatrix}\oplus C_{24}\begin{pmatrix}y_1\\y_2\end{pmatrix}\quad\Rightarrow\quad C'_{2,24}(x,y)=C_2\begin{pmatrix}x_1\\x_2\end{pmatrix}\oplus C_2\left(C_{24}\begin{pmatrix}y_1\\y_2\end{pmatrix}\right)$$

Так як наведені залежності описують всі варіанти побудови двох розрядної двохоперандної операції шляхом об'єднання одноопераднних операцій на основі симетричної операції, тому можна допустити справедливість залежності [9]:

$$C_{i,j}(x,y)=C_i\begin{pmatrix}x_1\\x_2\end{pmatrix}\oplus C_j\begin{pmatrix}y_1\\y_2\end{pmatrix}\quad\Rightarrow\quad C'_{i,j}(x,y)=C_i\begin{pmatrix}x_1\\x_2\end{pmatrix}\oplus C_i\left(C_j\begin{pmatrix}y_1\\y_2\end{pmatrix}\right)\qquad(4.3)$$

за умови $C_i(x)=C'_i(x)$.

Результати побудови множини двохоперандних операцій на основі гіпотези (4.3) для операції $C_3(x)$. наведено в табл.. 4.4.

Перевіримо коректність побудованої множини моделей (табл. 4.4) наприклад на моделях операцій $C_{3,1}(x,y)$, $C_{3,16}(x,y)$, та $C_{3,23}(x,y)$.

Знайдемо обернену операцію для операції $C_{3,1}(x,y)$ [9].

$$C_{3,1}(x,y)=C_3\begin{pmatrix}x_1\\x_2\end{pmatrix}\oplus C_1\begin{pmatrix}y_1\\y_2\end{pmatrix}=\begin{bmatrix}x_1\\x_1\oplus x_2\end{bmatrix}\oplus\begin{bmatrix}y_1\\y_2\end{bmatrix};$$

$$C_{3,1}(x,y)=\begin{cases}\begin{bmatrix}x_1\\x_1\oplus x_2\end{bmatrix}\oplus\begin{bmatrix}y_1\\y_2\end{bmatrix},\ якщо\ y_1=0;\ y_2=0\\ \begin{bmatrix}x_1\\x_1\oplus x_2\end{bmatrix}\oplus\begin{bmatrix}y_1\\y_2\end{bmatrix},якщо\ y_1=0;\ y_2=1\\ \begin{bmatrix}x_1\\x_1\oplus x_2\end{bmatrix}\oplus\begin{bmatrix}y_1\\y_2\end{bmatrix},\ якщо\ y_1=1;\ y_2=0\\ \begin{bmatrix}x_1\\x_1\oplus x_2\end{bmatrix}\oplus\begin{bmatrix}y_1\\y_2\end{bmatrix},якщо\ y_1=1;\ y_2=1\end{cases}=\begin{cases}\begin{bmatrix}x_1\\x_1\oplus x_2\end{bmatrix},\ якщо\ y_1=0;\ y_2=0\\ \begin{bmatrix}x_1\\x_1\oplus x_2\oplus 1\end{bmatrix},якщо\ y_1=0;\ y_2=1\\ \begin{bmatrix}x_1\oplus 1\\x_1\oplus x_2\end{bmatrix},\ якщо\ y_1=1;\ y_2=0\\ \begin{bmatrix}x_1\oplus 1\\x_1\oplus x_2\oplus 1\end{bmatrix},якщо\ y_1=1;\ y_2=1\end{cases}=C_{3,9,15,21}(x,y)$$

Таблиця 4.4

Синтезована множина моделей двохоперандних двохрозрядних операцій на основі операції $C_3(x)$ [9]

$C_3(x)=\begin{bmatrix}x_1\\ x_1\oplus x_2\end{bmatrix}$		**Операції інверсії**			
Базові операції	$C_1(x)=\begin{bmatrix}x_1\\ x_2\end{bmatrix}$	$C_{3,1}(x,y)=\begin{bmatrix}x_1\\ x_1\oplus x_2\end{bmatrix}\oplus\begin{bmatrix}y_1\\ y_2\end{bmatrix}$	$C_{3,7}(x,y)=\begin{bmatrix}x_1\\ x_1\oplus x_2\end{bmatrix}\oplus\begin{bmatrix}y_1\\ y_2\oplus 1\end{bmatrix}$	$C_{3,13}(x,y)=\begin{bmatrix}x_1\\ x_1\oplus x_2\end{bmatrix}\oplus\begin{bmatrix}y_1\oplus 1\\ y_2\end{bmatrix}$	$C_{3,19}(x,y)=\begin{bmatrix}x_1\\ x_1\oplus x_2\end{bmatrix}\oplus\begin{bmatrix}y_1\oplus 1\\ y_2\oplus 1\end{bmatrix}$
		$C'_{3,1}(x,y)=\begin{bmatrix}x_1\\ x_1\oplus x_2\end{bmatrix}\oplus\begin{bmatrix}y_1\\ y_1\oplus y_2\end{bmatrix}$	$C'_{3,7}(x,y)=\begin{bmatrix}x_1\\ x_1\oplus x_2\end{bmatrix}\oplus\begin{bmatrix}y_1\\ y_1\oplus y_2\oplus 1\end{bmatrix}$	$C'_{3,13}(x,y)=\begin{bmatrix}x_1\\ x_1\oplus x_2\end{bmatrix}\oplus\begin{bmatrix}y_1\oplus 1\\ y_1\oplus y_2\oplus 1\end{bmatrix}$	$C'_{3,19}=\begin{bmatrix}x_1\\ x_1\oplus x_2\end{bmatrix}\oplus\begin{bmatrix}y_1\oplus 1\\ y_1\oplus y_2\end{bmatrix}$
	$C_2(x)=\begin{bmatrix}x_1\oplus x_2\\ x_2\end{bmatrix}$	$C_{3,2}(x,y)=\begin{bmatrix}x_1\\ x_1\oplus x_2\end{bmatrix}\oplus\begin{bmatrix}y_1\oplus y_2\\ y_2\end{bmatrix}$	$C_{3,8}(x,y)=\begin{bmatrix}x_1\\ x_1\oplus x_2\end{bmatrix}\oplus\begin{bmatrix}y_1\oplus y_2\\ y_2\oplus 1\end{bmatrix}$	$C_{3,14}(x,y)=\begin{bmatrix}x_1\\ x_1\oplus x_2\end{bmatrix}\oplus\begin{bmatrix}y_1\oplus y_2\oplus 1\\ y_2\end{bmatrix}$	$C_{3,20}(x,y)=\begin{bmatrix}x_1\\ x_1\oplus x_2\end{bmatrix}\oplus\begin{bmatrix}y_1\oplus y_2\oplus 1\\ y_2\oplus 1\end{bmatrix}$
		$C'_{3,2}(x,y)=\begin{bmatrix}x_1\\ x_1\oplus x_2\end{bmatrix}\oplus\begin{bmatrix}y_1\oplus y_2\\ y_1\end{bmatrix}$	$C'_{3,8}(x,y)=\begin{bmatrix}x_1\\ x_1\oplus x_2\end{bmatrix}\oplus\begin{bmatrix}y_1\oplus y_2\\ y_1\oplus 1\end{bmatrix}$	$C'_{3,14}(x,y)=\begin{bmatrix}x_1\\ x_1\oplus x_2\end{bmatrix}\oplus\begin{bmatrix}y_1\oplus y_2\oplus 1\\ y_1\oplus 1\end{bmatrix}$	$C'_{3,20}=\begin{bmatrix}x_1\\ x_1\oplus x_2\end{bmatrix}\oplus\begin{bmatrix}y_1\oplus y_2\oplus 1\\ y_1\end{bmatrix}$
	$C_3(x)=\begin{bmatrix}x_1\\ x_1\oplus x_2\end{bmatrix}$	$C_{3,3}(x,y)=\begin{bmatrix}x_1\\ x_1\oplus x_2\end{bmatrix}\oplus\begin{bmatrix}y_1\\ y_1\oplus y_2\end{bmatrix}$	$C_{3,9}(x,y)=\begin{bmatrix}x_1\\ x_1\oplus x_2\end{bmatrix}\oplus\begin{bmatrix}y_1\\ y_1\oplus y_2\oplus 1\end{bmatrix}$	$C_{3,15}(x,y)=\begin{bmatrix}x_1\\ x_1\oplus x_2\end{bmatrix}\oplus\begin{bmatrix}y_1\oplus 1\\ y_1\oplus y_2\end{bmatrix}$	$C_{3,21}(x,y)=\begin{bmatrix}x_1\\ x_1\oplus x_2\end{bmatrix}\oplus\begin{bmatrix}y_1\oplus 1\\ y_1\oplus y_2\oplus 1\end{bmatrix}$
		$C'_{3,3}(x,y)=\begin{bmatrix}x_1\\ x_1\oplus x_2\end{bmatrix}\oplus\begin{bmatrix}y_1\\ y_2\end{bmatrix}$	$C'_{3,9}(x,y)=\begin{bmatrix}x_1\\ x_1\oplus x_2\end{bmatrix}\oplus\begin{bmatrix}y_1\\ y_2\oplus 1\end{bmatrix}$	$C'_{3,15}(x,y)=\begin{bmatrix}x_1\\ x_1\oplus x_2\end{bmatrix}\oplus\begin{bmatrix}y_1\oplus 1\\ y_2\oplus 1\end{bmatrix}$	$C'_{3,21}(x,y)=\begin{bmatrix}x_1\\ x_1\oplus x_2\end{bmatrix}\oplus\begin{bmatrix}y_1\oplus 1\\ y_2\end{bmatrix}$
Операції інверсії	$C_4(x)=\begin{bmatrix}x_2\\ x_1\end{bmatrix}$	$C_{3,4}(x,y)=\begin{bmatrix}x_1\\ x_1\oplus x_2\end{bmatrix}\oplus\begin{bmatrix}y_2\\ y_1\end{bmatrix}$	$C_{3,10}(x,y)=\begin{bmatrix}x_1\\ x_1\oplus x_2\end{bmatrix}\oplus\begin{bmatrix}y_2\\ y_1\oplus 1\end{bmatrix}$	$C_{3,16}(x,y)=\begin{bmatrix}x_1\\ x_1\oplus x_2\end{bmatrix}\oplus\begin{bmatrix}y_2\oplus 1\\ y_1\end{bmatrix}$	$C_{3,22}(x,y)=\begin{bmatrix}x_1\\ x_1\oplus x_2\end{bmatrix}\oplus\begin{bmatrix}y_2\oplus 1\\ y_1\oplus 1\end{bmatrix}$
		$C'_{3,4}(x,y)=\begin{bmatrix}x_1\\ x_1\oplus x_2\end{bmatrix}\oplus\begin{bmatrix}y_2\\ y_1\oplus y_2\end{bmatrix}$	$C'_{3,10}(x,y)=\begin{bmatrix}x_1\\ x_1\oplus x_2\end{bmatrix}\oplus\begin{bmatrix}y_2\\ y_1\oplus y_2\oplus 1\end{bmatrix}$	$C'_{3,16}(x,y)=\begin{bmatrix}x_1\\ x_1\oplus x_2\end{bmatrix}\oplus\begin{bmatrix}y_2\oplus 1\\ y_1\oplus y_2\oplus 1\end{bmatrix}$	$C'_{3,22}(x,y)=\begin{bmatrix}x_1\\ x_1\oplus x_2\end{bmatrix}\oplus\begin{bmatrix}y_2\oplus 1\\ y_1\oplus y_2\end{bmatrix}$
	$C_5(x)=\begin{bmatrix}x_2\\ x_1\oplus x_2\end{bmatrix}$	$C_{3,5}(x,y)=\begin{bmatrix}x_1\\ x_1\oplus x_2\end{bmatrix}\oplus\begin{bmatrix}y_2\\ y_1\oplus y_2\end{bmatrix}$	$C_{3,11}(x,y)=\begin{bmatrix}x_1\\ x_1\oplus x_2\end{bmatrix}\oplus\begin{bmatrix}y_2\\ y_1\oplus y_2\oplus 1\end{bmatrix}$	$C_{3,17}(x,y)=\begin{bmatrix}x_1\\ x_1\oplus x_2\end{bmatrix}\oplus\begin{bmatrix}y_2\oplus 1\\ y_1\oplus y_2\end{bmatrix}$	$C_{3,23}(x,y)=\begin{bmatrix}x_1\\ x_1\oplus x_2\end{bmatrix}\oplus\begin{bmatrix}y_2\oplus 1\\ y_1\oplus y_2\oplus 1\end{bmatrix}$
		$C'_{3,5}=\begin{bmatrix}x_1\\ x_1\oplus x_2\end{bmatrix}\oplus\begin{bmatrix}y_2\\ y_1\end{bmatrix}$	$C'_{3,11}(x,y)=\begin{bmatrix}x_1\\ x_1\oplus x_2\end{bmatrix}\oplus\begin{bmatrix}y_2\\ y_1\oplus 1\end{bmatrix}$	$C'_{3,17}(x,y)=\begin{bmatrix}x_1\\ x_1\oplus x_2\end{bmatrix}\oplus\begin{bmatrix}y_2\oplus 1\\ y_1\oplus 1\end{bmatrix}$	$C'_{3,23}(x,y)=\begin{bmatrix}x_1\\ x_1\oplus x_2\end{bmatrix}\oplus\begin{bmatrix}y_2\oplus 1\\ y_1\oplus y_2\end{bmatrix}$
	$C_6(x)=\begin{bmatrix}x_1\oplus x_2\\ x_1\end{bmatrix}$	$C_{3,6}(x,y)=\begin{bmatrix}x_1\\ x_1\oplus x_2\end{bmatrix}\oplus\begin{bmatrix}y_1\oplus y_2\\ y_1\end{bmatrix}$	$C_{3,12}(x,y)=\begin{bmatrix}x_1\\ x_1\oplus x_2\end{bmatrix}\oplus\begin{bmatrix}y_1\oplus y_2\\ y_1\oplus 1\end{bmatrix}$	$C_{3,18}(x,y)=\begin{bmatrix}x_1\\ x_1\oplus x_2\end{bmatrix}\oplus\begin{bmatrix}y_1\oplus y_2\oplus 1\\ y_1\end{bmatrix}$	$C_{3,24}(x,y)=\begin{bmatrix}x_1\\ x_1\oplus x_2\end{bmatrix}\oplus\begin{bmatrix}y_1\oplus y_2\oplus 1\\ y_1\oplus 1\end{bmatrix}$
		$C'_{3,6}(x,y)=\begin{bmatrix}x_1\\ x_1\oplus x_2\end{bmatrix}\oplus\begin{bmatrix}y_1\oplus y_2\\ y_2\end{bmatrix}$	$C'_{3,12}(x,y)=\begin{bmatrix}x_1\\ x_1\oplus x_2\end{bmatrix}\oplus\begin{bmatrix}y_1\oplus y_2\\ y_2\oplus 1\end{bmatrix}$	$C'_{3,18}(x,y)=\begin{bmatrix}x_1\\ x_1\oplus x_2\end{bmatrix}\oplus\begin{bmatrix}y_1\oplus y_2\oplus 1\\ y_2\oplus 1\end{bmatrix}$	$C'_{3,24}(x,y)=\begin{bmatrix}x_1\\ x_1\oplus x_2\end{bmatrix}\oplus\begin{bmatrix}y_1\oplus y_2\oplus 1\\ y_2\end{bmatrix}$

$$C'_{3,1}(x,y)=\begin{cases}C'_3(x),\ якщо\ y_1=0;\ y_2=0\\ C'_9(x),якщо\ y_1=0;\ y_2=1\\ C'_{15}(x),\ якщо\ y_1=1;\ y_2=0\\ C'_{21}(x),якщо\ y_1=1;\ y_2=1\end{cases}=\begin{cases}C_3(x),\ якщо\ y_1=0;\ y_2=0\\ C_9(x),якщо\ y_1=0;\ y_2=1\\ C_{21}(x),\ якщо\ y_1=1;\ y_2=0\\ C_{15}(x),якщо\ y_1=1;\ y_2=1\end{cases}=$$

$$=\begin{cases}\begin{bmatrix}x_1\\ x_1\oplus x_2\end{bmatrix},\ якщо\ y_1=0;\ y_2=0\\ \begin{bmatrix}x_1\\ x_1\oplus x_2\oplus 1\end{bmatrix},якщо\ y_1=0;\ y_2=1\\ \begin{bmatrix}x_1\oplus 1\\ x_1\oplus x_2\oplus 1\end{bmatrix},\ якщо\ y_1=1;\ y_2=0\\ \begin{bmatrix}x_1\oplus 1\\ x_1\oplus x_2\end{bmatrix},якщо\ y_1=1;\ y_2=1\end{cases}=\begin{bmatrix}x_1\\ x_1\oplus x_2\end{bmatrix}\oplus\begin{bmatrix}y_1\\ y_1\oplus y_2\end{bmatrix}=C_{3,3}(x,y)$$

Результат побудови $C'_{3,1}(x,y)$ співпав з наведеним в табл.4.4.

Знайдемо обернену операцію для операції $C_{3,16}(x,y)$.

$$C_{3,16}(x,y)=C_3\begin{pmatrix}x_1\\ x_2\end{pmatrix}\oplus C_{16}\begin{pmatrix}y_1\\ y_2\end{pmatrix}=\begin{bmatrix}x_1\\ x_1\oplus x_2\end{bmatrix}\oplus\begin{bmatrix}y_2\oplus 1\\ y_1\end{bmatrix};$$

$$C_{3,16}(x,y)=\begin{cases}\begin{bmatrix}x_1\\ x_1\oplus x_2\end{bmatrix}\oplus\begin{bmatrix}y_2\oplus 1\\ y_1\end{bmatrix},\ якщо\ y_1=0;\ y_2=0\\ \begin{bmatrix}x_1\\ x_1\oplus x_2\end{bmatrix}\oplus\begin{bmatrix}y_2\oplus 1\\ y_1\end{bmatrix},якщо\ y_1=0;\ y_2=1\\ \begin{bmatrix}x_1\\ x_1\oplus x_2\end{bmatrix}\oplus\begin{bmatrix}y_2\oplus 1\\ y_1\end{bmatrix},\ якщо\ y_1=1;\ y_2=0\\ \begin{bmatrix}x_1\\ x_1\oplus x_2\end{bmatrix}\oplus\begin{bmatrix}y_2\oplus 1\\ y_1\end{bmatrix},якщо\ y_1=1;\ y_2=1\end{cases}=\begin{cases}\begin{bmatrix}x_1\oplus 1\\ x_1\oplus x_2\end{bmatrix},\ якщо\ y_1=0;\ y_2=0\\ \begin{bmatrix}x_1\\ x_1\oplus x_2\end{bmatrix},якщо\ y_1=0;\ y_2=1\\ \begin{bmatrix}x_1\oplus 1\\ x_1\oplus x_2\oplus 1\end{bmatrix},\ якщо\ y_1=1;\ y_2=0\\ \begin{bmatrix}x_1\\ x_1\oplus x_2\oplus 1\end{bmatrix},якщо\ y_1=1;\ y_2=1\end{cases}=C_{15,3,21,9}(x,y)$$

$$C'_{3,16}(x,y)=\begin{cases}C'_{15}(x),\ якщо\ y_1=0;\ y_2=0\\ C'_3(x),якщо\ y_1=0;\ y_2=1\\ C'_{21}(x),\ якщо\ y_1=1;\ y_2=0\\ C'_9(x),якщо\ y_1=1;\ y_2=1\end{cases}=\begin{cases}C_{21}(x),\ якщо\ y_1=0;\ y_2=0\\ C_3(x),якщо\ y_1=0;\ y_2=1\\ C_{13}(x),\ якщо\ y_1=1;\ y_2=0\\ C_9(x),якщо\ y_1=1;\ y_2=1\end{cases}=$$

$$=\begin{cases}\begin{bmatrix}x_1\oplus 1\\ x_1\oplus x_2\oplus 1\end{bmatrix},\ якщо\ y_1=0;\ y_2=0\\ \begin{bmatrix}x_1\\ x_1\oplus x_2\end{bmatrix},якщо\ y_1=0;\ y_2=1\\ \begin{bmatrix}x_1\oplus 1\\ x_1\oplus x_2\end{bmatrix},\ якщо\ y_1=1;\ y_2=0\\ \begin{bmatrix}x_1\\ x_1\oplus x_2\oplus 1\end{bmatrix},якщо\ y_1=1;\ y_2=1\end{cases}=\begin{bmatrix}x_1\\ x_1\oplus x_2\end{bmatrix}\oplus\begin{bmatrix}y_2\oplus 1\\ y_1\oplus y_2\oplus 1\end{bmatrix}=C_{3,23}(x,y)$$

Результат побудови $C'_{3,16}(x,y)$ співпав з наведеним в табл.4.4.

Коректність моделі синтезу обернених двохоперандних операції (4.3) до множини операцій криптографічного перетворення побудованих шляхом об'єднання одноопераднних операцій, перша з яких симетрична підтверджена на всіх можливих варіантах.

Порівняльний аналіз моделей синтезу (4.1) і (4.3) показав, що модель (4.1) є окремим випадком моделі (4.3).

Синтезувати множину симетричних двохоперандних операцій які допускають перестановку операндів місцями

$$C_{i,j}(x,y) = C_i\begin{pmatrix}x_1\\x_2\end{pmatrix} \oplus C_j\begin{pmatrix}y_1\\y_2\end{pmatrix} \quad \Rightarrow \quad C'_{i,j}(x,y) = C_i\begin{pmatrix}x_1\\x_2\end{pmatrix} \oplus C_j\begin{pmatrix}y_1\\y_2\end{pmatrix}$$

можна на основі моделі (4.13) за умови

$$C_i\left(C_j\begin{pmatrix}y_1\\y_2\end{pmatrix}\right) = C_j\begin{pmatrix}y_1\\y_2\end{pmatrix}. \qquad (4.4)$$

Умова (4.4) буде виконуватися якщо для симетричної одноопераднної операції, на основі якої будується множина симетричних двохоперандних операцій, існує група симетричних операцій інверсії.

Для двохрозрядних двохоперандних операцій можуть бути побудовані лише 4 множини симетричних операцій на основі одноопераднних операцій $C_1(x)$, $C_7(x)$, $C_{13}(x)$ і $C_{19}(x)$. Дані операції є симетричними і представляють групу операцій інверсії.

4.3. Синтез множини несиметричних двохоперандних двохрозрядних операцій шляхом поєднання одноопераднних операцій перша з яких є несиметричною.

Синтезуємо множину несиметричних двохоперандних двохрозрядних операцій шляхом поєднання одноопераднних операцій шляхом поєднання

несиметричної операції криптографічного перетворення $C_5(x)=\begin{bmatrix} x_2 \\ x_1 \oplus x_2 \end{bmatrix}$ з двохрозрядними одноопераднимиоперaціями. Оберненою операцією до операції $C_5(x)$ є операція $C_6(x)=\begin{bmatrix} x_1 \oplus x_2 \\ x_1 \end{bmatrix}$.

Побудуємо обернену операцію до $C_{5,1}(x,y)$

$$C_{5,1}(x,y)=C_5\begin{pmatrix} x_1 \\ x_2 \end{pmatrix}\oplus C_1\begin{pmatrix} y_1 \\ y_2 \end{pmatrix}=\begin{bmatrix} x_2 \\ x_1 \oplus x_2 \end{bmatrix}\oplus\begin{bmatrix} y_1 \\ y_2 \end{bmatrix};$$

$$C_{5,1}(x,y)=\begin{cases}\begin{bmatrix} x_2 \\ x_1 \oplus x_2 \end{bmatrix}\oplus\begin{bmatrix} y_1 \\ y_2 \end{bmatrix}, \text{ якщо } y_1=0;\ y_2=0 \\ \begin{bmatrix} x_2 \\ x_1 \oplus x_2 \end{bmatrix}\oplus\begin{bmatrix} y_1 \\ y_2 \end{bmatrix}, \text{якщо } y_1=0;\ y_2=1 \\ \begin{bmatrix} x_2 \\ x_1 \oplus x_2 \end{bmatrix}\oplus\begin{bmatrix} y_1 \\ y_2 \end{bmatrix}, \text{ якщо } y_1=1;\ y_2=0 \\ \begin{bmatrix} x_2 \\ x_1 \oplus x_2 \end{bmatrix}\oplus\begin{bmatrix} y_1 \\ y_2 \end{bmatrix}, \text{якщо } y_1=1;\ y_2=1\end{cases}=\begin{cases}\begin{bmatrix} x_2 \\ x_1 \oplus x_2 \end{bmatrix}, \text{ якщо } y_1=0;\ y_2=0 \\ \begin{bmatrix} x_2 \\ x_1 \oplus x_2 \oplus 1 \end{bmatrix}, \text{якщо } y_1=0;\ y_2=1 \\ \begin{bmatrix} x_2 \oplus 1 \\ x_1 \oplus x_2 \end{bmatrix}, \text{ якщо } y_1=1;\ y_2=0 \\ \begin{bmatrix} x_2 \oplus 1 \\ x_1 \oplus x_2 \oplus 1 \end{bmatrix}, \text{якщо } y_1=1;\ y_2=1\end{cases}=C_{5,11,17,23}(x,y)$$

$$C'_{3,16}(x,y)=\begin{cases}C'_5(x), \text{ якщо } y_1=0;\ y_2=0 \\ C'_{11}(x), \text{якщо } y_1=0;\ y_2=1 \\ C'_{17}(x), \text{ якщо } y_1=1;\ y_2=0 \\ C'_{23}(x), \text{якщо } y_1=1;\ y_2=1\end{cases}=\begin{cases}C_6(x), \text{ якщо } y_1=0;\ y_2=0 \\ C_{18}(x), \text{якщо } y_1=0;\ y_2=1 \\ C_{24}(x), \text{ якщо } y_1=1;\ y_2=0 \\ C_{12}(x), \text{якщо } y_1=1;\ y_2=1\end{cases}=$$

$$=\begin{cases}\begin{bmatrix} x_1 \oplus x_2 \\ x_1 \end{bmatrix}, \text{ якщо } y_1=0;\ y_2=0 \\ \begin{bmatrix} x_1 \oplus x_2 \oplus 1 \\ x_1 \end{bmatrix}, \text{якщо } y_1=0;\ y_2=1 \\ \begin{bmatrix} x_1 \oplus x_2 \oplus 1 \\ x_1 \oplus 1 \end{bmatrix}, \text{ якщо } y_1=1;\ y_2=0 \\ \begin{bmatrix} x_1 \oplus x_2 \\ x_1 \oplus 1 \end{bmatrix}, \text{якщо } y_1=1;\ y_2=1\end{cases}=\begin{bmatrix} x_1 \oplus x_2 \\ x_1 \end{bmatrix}\oplus\begin{bmatrix} y_1 \oplus y_2 \\ y_1 \end{bmatrix}=C_{6,6}(x,y)$$

Побудуємо обернену операцію до $C_{5,15}(x,y)$

$$C_{5,15}(x,y)=C_5\begin{pmatrix} x_1 \\ x_2 \end{pmatrix}\oplus C_1\begin{pmatrix} y_1 \\ y_2 \end{pmatrix}=\begin{bmatrix} x_2 \\ x_1 \oplus x_2 \end{bmatrix}\oplus\begin{bmatrix} y_1 \oplus 1 \\ y_1 \oplus y_2 \end{bmatrix};$$

$$C_{5,15}(x,y)=\begin{cases}\begin{bmatrix}x_2\\x_1\oplus x_2\end{bmatrix}\oplus\begin{bmatrix}y_1\oplus 1\\y_1\oplus y_2\end{bmatrix}, \text{ якщо } y_1=0;\ y_2=0\\ \begin{bmatrix}x_2\\x_1\oplus x_2\end{bmatrix}\oplus\begin{bmatrix}y_1\oplus 1\\y_1\oplus y_2\end{bmatrix}, \text{якщо } y_1=0;\ y_2=1\\ \begin{bmatrix}x_2\\x_1\oplus x_2\end{bmatrix}\oplus\begin{bmatrix}y_1\oplus 1\\y_1\oplus y_2\end{bmatrix}, \text{якщо } y_1=1;\ y_2=0\\ \begin{bmatrix}x_2\\x_1\oplus x_2\end{bmatrix}\oplus\begin{bmatrix}y_1\oplus 1\\y_1\oplus y_2\end{bmatrix}, \text{якщо } y_1=1;\ y_2=1\end{cases}=\begin{cases}\begin{bmatrix}x_2\oplus 1\\x_1\oplus x_2\end{bmatrix}, \text{ якщо } y_1=0;\ y_2=0\\ \begin{bmatrix}x_2\oplus 1\\x_1\oplus x_2\oplus 1\end{bmatrix}, \text{якщо } y_1=0;\ y_2=1\\ \begin{bmatrix}x_2\\x_1\oplus x_2\oplus 1\end{bmatrix}, \text{якщо } y_1=1;\ y_2=0\\ \begin{bmatrix}x_2\\x_1\oplus x_2\end{bmatrix}, \text{якщо } y_1=1;\ y_2=1\end{cases}=C_{17,23,11,5}(x,y)$$

$$C'_{5,15}(x,y)=\begin{cases}C'_{17}(x), \text{ якщо } y_1=0;\ y_2=0\\ C'_{23}(x), \text{якщо } y_1=0;\ y_2=1\\ C'_{11}(x), \text{ якщо } y_1=1;\ y_2=0\\ C'_5(x), \text{якщо } y_1=1;\ y_2=1\end{cases}=\begin{cases}C_{24}(x), \text{ якщо } y_1=0;\ y_2=0\\ C_{12}(x), \text{якщо } y_1=0;\ y_2=1\\ C_{18}(x), \text{ якщо } y_1=1;\ y_2=0\\ C_6(x), \text{якщо } y_1=1;\ y_2=1\end{cases}=$$

$$=\begin{cases}\begin{bmatrix}x_1\oplus x_2\oplus 1\\x_1\oplus 1\end{bmatrix}, \text{ якщо } y_1=0;\ y_2=0\\ \begin{bmatrix}x_1\oplus x_2\\x_1\oplus 1\end{bmatrix}, \text{якщо } y_1=0;\ y_2=1\\ \begin{bmatrix}x_1\oplus x_2\oplus 1\\x_1\end{bmatrix}, \text{ якщо } y_1=1;\ y_2=0\\ \begin{bmatrix}x_1\oplus x_2\\x_1\end{bmatrix}, \text{якщо } y_1=1;\ y_2=1\end{cases}=\begin{bmatrix}x_1\oplus x_2\\x_1\end{bmatrix}\oplus\begin{bmatrix}y_2\\y_1\oplus 1\end{bmatrix}=C_{6,10}(x,y)$$

По аналогії побудуємо всі прямі і обернені операції. Результати побудови наведені в табл.4.5

При аналізі табл.4.5 були встановлені наступні залежності:

$$C_{5,1}(x,y)=C_5\begin{pmatrix}x_1\\x_2\end{pmatrix}\oplus C_1\begin{pmatrix}y_1\\y_2\end{pmatrix}\quad\Rightarrow\quad C'_{5,1}(x,y)=C'_5\begin{pmatrix}x_1\\x_2\end{pmatrix}\oplus C'_5\left(C_1\begin{pmatrix}y_1\\y_2\end{pmatrix}\right)$$

$$C_{5,2}(x,y)=C_5\begin{pmatrix}x_1\\x_2\end{pmatrix}\oplus C_2\begin{pmatrix}y_1\\y_2\end{pmatrix}\quad\Rightarrow\quad C'_{5,1}(x,y)=C'_5\begin{pmatrix}x_1\\x_2\end{pmatrix}\oplus C'_5\left(C_2\begin{pmatrix}y_1\\y_2\end{pmatrix}\right)$$

. . . . . .

$$C_{5,24}(x,y)=C_5\begin{pmatrix}x_1\\x_2\end{pmatrix}\oplus C_{24}\begin{pmatrix}y_1\\y_2\end{pmatrix}\quad\Rightarrow\quad C'_{5,24}(x,y)=C'_5\begin{pmatrix}x_1\\x_2\end{pmatrix}\oplus C'_5\left(C_{24}\begin{pmatrix}y_1\\y_2\end{pmatrix}\right)$$

Таблиця 4.5

Синтезована множина моделей двохоперандних двохрозрядних операцій на основі операції $C_5(x)$ [8]

$C_5(x)=\begin{bmatrix}x_2\\x_1\oplus x_2\end{bmatrix}$		**Операції інверсії**			
Базові операції	$C_1(x)=\begin{bmatrix}x_1\\x_2\end{bmatrix}$	$C_{5,1}(x,y)=\begin{bmatrix}x_2\\x_1\oplus x_2\end{bmatrix}\oplus\begin{bmatrix}y_1\\y_2\end{bmatrix}$	$C_{5,7}(x,y)=\begin{bmatrix}x_2\\x_1\oplus x_2\end{bmatrix}\oplus\begin{bmatrix}y_1\\y_2\oplus 1\end{bmatrix}$	$C_{5,13}(x,y)=\begin{bmatrix}x_2\\x_1\oplus x_2\end{bmatrix}\oplus\begin{bmatrix}y_1\oplus 1\\y_2\end{bmatrix}$	$C_{5,19}(x,y)=\begin{bmatrix}x_2\\x_1\oplus x_2\end{bmatrix}\oplus\begin{bmatrix}y_1\oplus 1\\y_2\oplus 1\end{bmatrix}$
		$C'_{5,1}(x,y)=\begin{bmatrix}x_1\oplus x_2\\x_1\end{bmatrix}\oplus\begin{bmatrix}y_1\oplus y_2\\y_1\end{bmatrix}$	$C'_{5,7}(x,y)=\begin{bmatrix}x_1\oplus x_2\\x_1\end{bmatrix}\oplus\begin{bmatrix}y_1\oplus y_2\oplus 1\\y_1\end{bmatrix}$	$C'_{5,13}(x,y)=\begin{bmatrix}x_1\oplus x_2\\x_1\end{bmatrix}\oplus\begin{bmatrix}y_1\oplus y_2\oplus 1\\y_1\oplus 1\end{bmatrix}$	$C'_{5,19}(x,y)=\begin{bmatrix}x_1\oplus x_2\\x_1\end{bmatrix}\oplus\begin{bmatrix}y_1\oplus y_2\\y_1\oplus 1\end{bmatrix}$
	$C_2(x)=\begin{bmatrix}x_1\oplus x_2\\x_2\end{bmatrix}$	$C_{5,2}(x,y)=\begin{bmatrix}x_2\\x_1\oplus x_2\end{bmatrix}\oplus\begin{bmatrix}y_1\oplus y_2\\y_2\end{bmatrix}$	$C_{5,8}(x,y)=\begin{bmatrix}x_2\\x_1\oplus x_2\end{bmatrix}\oplus\begin{bmatrix}y_1\oplus y_2\\y_2\oplus 1\end{bmatrix}$	$C_{5,14}(x,y)=\begin{bmatrix}x_2\\x_1\oplus x_2\end{bmatrix}\oplus\begin{bmatrix}y_1\oplus y_2\oplus 1\\y_2\end{bmatrix}$	$C_{5,20}(x,y)=\begin{bmatrix}x_1\\x_1\oplus x_2\end{bmatrix}\oplus\begin{bmatrix}y_2\oplus 1\\y_1\oplus y_2\oplus 1\end{bmatrix}$
		$C'_{5,2}(x,y)=\begin{bmatrix}x_1\oplus x_2\\x_1\end{bmatrix}\oplus\begin{bmatrix}y_1\\y_1\oplus y_2\end{bmatrix}$	$C'_{5,8}(x,y)=\begin{bmatrix}x_1\oplus x_2\\x_1\end{bmatrix}\oplus\begin{bmatrix}y_1\oplus 1\\y_1\oplus y_2\end{bmatrix}$	$C'_{5,14}(x,y)=\begin{bmatrix}x_1\oplus x_2\\x_1\end{bmatrix}\oplus\begin{bmatrix}y_1\oplus 1\\y_1\oplus y_2\oplus 1\end{bmatrix}$	$C'_{5,20}(x,y)=\begin{bmatrix}x_1\oplus x_2\\x_1\end{bmatrix}\oplus\begin{bmatrix}y_1\\y_1\oplus y_2\oplus 1\end{bmatrix}$
	$C_3(x)=\begin{bmatrix}x_1\\x_1\oplus x_2\end{bmatrix}$	$C_{5,3}(x,y)=\begin{bmatrix}x_2\\x_1\oplus x_2\end{bmatrix}\oplus\begin{bmatrix}y_1\\y_1\oplus y_2\end{bmatrix}$	$C_{5,9}(x,y)=\begin{bmatrix}x_2\\x_1\oplus x_2\end{bmatrix}\oplus\begin{bmatrix}y_1\\y_1\oplus y_2\oplus 1\end{bmatrix}$	$C_{5,15}(x,y)=\begin{bmatrix}x_2\\x_1\oplus x_2\end{bmatrix}\oplus\begin{bmatrix}y_1\oplus 1\\y_1\oplus y_2\end{bmatrix}$	$C_{5,21}(x,y)=\begin{bmatrix}x_2\\x_1\oplus x_2\end{bmatrix}\oplus\begin{bmatrix}y_1\oplus 1\\y_1\oplus y_2\oplus 1\end{bmatrix}$
		$C'_{5,3}(x,y)=\begin{bmatrix}x_1\oplus x_2\\x_1\end{bmatrix}\oplus\begin{bmatrix}y_2\\y_1\end{bmatrix}$	$C'_{5,9}(x,y)=\begin{bmatrix}x_1\oplus x_2\\x_1\end{bmatrix}\oplus\begin{bmatrix}y_2\oplus 1\\y_1\end{bmatrix}$	$C'_{5,15}(x.y)=\begin{bmatrix}x_1\oplus x_2\\x_1\end{bmatrix}\oplus\begin{bmatrix}y_2\oplus 1\\y_1\oplus 1\end{bmatrix}$	$C'_{5,21}(x,y)=\begin{bmatrix}x_1\oplus x_2\\x_1\end{bmatrix}\oplus\begin{bmatrix}y_2\\y_1\oplus 1\end{bmatrix}$
Операції інверсії	$C_4(x)=\begin{bmatrix}x_2\\x_1\end{bmatrix}$	$C_{5,4}(x,y)=\begin{bmatrix}x_2\\x_1\oplus x_2\end{bmatrix}\oplus\begin{bmatrix}y_2\\y_1\end{bmatrix}$	$C_{5,10}(x,y)=\begin{bmatrix}x_2\\x_1\oplus x_2\end{bmatrix}\oplus\begin{bmatrix}y_2\\y_1\oplus 1\end{bmatrix}$	$C_{5,16}(x,y)=\begin{bmatrix}x_2\\x_1\oplus x_2\end{bmatrix}\oplus\begin{bmatrix}y_2\oplus 1\\y_1\end{bmatrix}$	$C_{5,22}(x,y)=\begin{bmatrix}x_2\\x_1\oplus x_2\end{bmatrix}\oplus\begin{bmatrix}y_2\oplus 1\\y_1\oplus 1\end{bmatrix}$
		$C'_{5,4}(x,y)=\begin{bmatrix}x_1\oplus x_2\\x_1\end{bmatrix}\oplus\begin{bmatrix}y_1\oplus y_2\\y_2\end{bmatrix}$	$C'_{5,10}(x,y)=\begin{bmatrix}x_1\oplus x_2\\x_1\end{bmatrix}\oplus\begin{bmatrix}y_1\oplus y_2\oplus 1\\y_1\end{bmatrix}$	$C'_{5,16}(x,y)=\begin{bmatrix}x_1\oplus x_2\\x_1\end{bmatrix}\oplus\begin{bmatrix}y_1\oplus y_2\oplus 1\\y_1\oplus 1\end{bmatrix}$	$C'_{5,22}(x,y)=\begin{bmatrix}x_1\oplus x_2\\x_1\end{bmatrix}\oplus\begin{bmatrix}y_1\oplus y_2\\y_1\oplus 1\end{bmatrix}$
	$C_5(x)=\begin{bmatrix}x_2\\x_1\oplus x_2\end{bmatrix}$	$C_{5,5}(x,y)=\begin{bmatrix}x_2\\x_1\oplus x_2\end{bmatrix}\oplus\begin{bmatrix}y_2\\y_1\oplus y_2\end{bmatrix}$	$C_{5,11}(x,y)=\begin{bmatrix}x_2\\x_1\oplus x_2\end{bmatrix}\oplus\begin{bmatrix}y_2\\y_1\oplus y_2\oplus 1\end{bmatrix}$	$C_{5,17}(x,y)=\begin{bmatrix}x_2\\x_1\oplus x_2\end{bmatrix}\oplus\begin{bmatrix}y_2\oplus 1\\y_1\oplus y_2\end{bmatrix}$	$C_{5,23}(x,y)=\begin{bmatrix}x_2\\x_1\oplus x_2\end{bmatrix}\oplus\begin{bmatrix}y_2\oplus 1\\y_1\oplus y_2\oplus 1\end{bmatrix}$
		$C'_{5,5}(x,y)=\begin{bmatrix}x_1\oplus x_2\\x_1\end{bmatrix}\oplus\begin{bmatrix}y_1\\y_2\end{bmatrix}$	$C'_{5,11}(x,y)=\begin{bmatrix}x_1\oplus x_2\\x_1\end{bmatrix}\oplus\begin{bmatrix}y_1\oplus 1\\y_2\end{bmatrix}$	$C'_{5,17}(x,y)=\begin{bmatrix}x_1\oplus x_2\\x_1\end{bmatrix}\oplus\begin{bmatrix}y_1\oplus 1\\y_2\oplus 1\end{bmatrix}$	$C'_{5,23}(x,y)=\begin{bmatrix}x_1\oplus x_2\\x_1\end{bmatrix}\oplus\begin{bmatrix}y_1\\y_2\oplus 1\end{bmatrix}$
	$C_6(x)=\begin{bmatrix}x_1\oplus x_2\\x_1\end{bmatrix}$	$C_{5,6}(x,y)=\begin{bmatrix}x_2\\x_1\oplus x_2\end{bmatrix}\oplus\begin{bmatrix}y_1\oplus y_2\\y_1\end{bmatrix}$	$C_{5,12}(x,y)=\begin{bmatrix}x_2\\x_1\oplus x_2\end{bmatrix}\oplus\begin{bmatrix}y_1\oplus y_2\\y_1\oplus 1\end{bmatrix}$	$C_{5,18}(x,y)=\begin{bmatrix}x_2\\x_1\oplus x_2\end{bmatrix}\oplus\begin{bmatrix}y_1\oplus y_2\oplus 1\\y_1\end{bmatrix}$	$C_{5,24}(x,y)=\begin{bmatrix}x_2\\x_1\oplus x_2\end{bmatrix}\oplus\begin{bmatrix}y_1\oplus y_2\oplus 1\\y_1\oplus 1\end{bmatrix}$
		$C'_{5,6}(x,y)=\begin{bmatrix}x_1\oplus x_2\\x_1\end{bmatrix}\oplus\begin{bmatrix}y_2\\y_1\oplus y_2\end{bmatrix}$	$C'_{5,12}(x,y)=\begin{bmatrix}x_1\oplus x_2\\x_1\end{bmatrix}\oplus\begin{bmatrix}y_2\oplus 1\\y_1\oplus y_2\end{bmatrix}$	$C'_{5,18}(x,y)=\begin{bmatrix}x_1\oplus x_2\\x_1\end{bmatrix}\oplus\begin{bmatrix}y_2\oplus 1\\y_1\oplus y_2\oplus 1\end{bmatrix}$	$C'_{5,24}(x,y)=\begin{bmatrix}x_1\oplus x_2\\x_1\end{bmatrix}\oplus\begin{bmatrix}y_2\\y_1\oplus y_2\oplus 1\end{bmatrix}$

Так як наведені залежності описують всі варіанти побудови двох розрядної двохоперандної операції шляхом об'єднання одноопераднних операцій на основі несиметричної операції, тому можна побудувати загальну залежність:

$$C_{i,j}(x,y) = C_i\begin{pmatrix} x_1 \\ x_2 \end{pmatrix} \oplus C_j\begin{pmatrix} y_1 \\ y_2 \end{pmatrix} \quad \Rightarrow \quad C'_{i,j}(x,y) = C'_i\begin{pmatrix} x_1 \\ x_2 \end{pmatrix} \oplus C'_i\left(C_j\begin{pmatrix} y_1 \\ y_2 \end{pmatrix}\right) \qquad (4.5)$$

Порівняльний аналіз моделей синтезу (4.3) і (4.5) показав, що модель (4.3) є окремим випадком моделі (4.5) при виконанні умови $C_i(x) = C'_i(x)$.

Синтезовані моделі двохоперандних двохрозрядних операцій отриманих шляхом поєднання одноопераднних двохрозрядних операцій допускають перестановку операндів. По аналогії можна будувати двохоперандні операції які допускають перестановку операндів більшої розрядності [3].

При перестановці операндів обернена операція також знаходиться на основі взаємозв'язків (4.5). Дане твердження ґрунтується на тому, перестановка операндів приводить до зміни послідовності поєднання одноопераднних операцій при синтезі двохоперандної операції.

Висновки до розділу 4

Удосконалено метод побудови двохрозрядних двохоперандних операцій які допускають перестановку операндів на основі об'єднання двохрозрядних одноопераднних операцій криптографічного перетворення, шляхом встановлення взаємозв'язків між прямими і оберненими операціями, що дозволило змоделювати всі двохрозрядні двохоперандні операцій, які допускають перестановку операндів.

1. Досліджено можливість синтезу множини симетричних двохрозрядних двохоперандних операцій на шляхом поєднання одноопераднних операцій.

2. Досліджено особливості синтезу прямих і обернених двохрозрядних двохоперандних СЕТ-операцій, які допускають перестановку операндів, шляхом поєднання одноопераднних операцій, перша з яких є симетричною.

3. Досліджено особливості синтезу прямих і обернених двохрозрядних двохоперандних СЕТ-операцій, які допускають перестановку операндів, шляхом поєднання одноопераднних операцій, перша з яких є несиметричною.

4. Встановлено взаємозв’язки і обмеження які відображають особливості синтезу двохрозрядних двохоперандних операцій криптографічного перетворення, які допускають перестановку операндів при різних моделях перетворення першого операнду.

5. Результати розділу опубліковані: [1] – [4], [9].

РОЗДІЛ 5 ІНФОРМАЦІЙНА ТЕХНОЛОГІЯ МОДЕЛЮВАННЯ КОМУТАТИВНИХ І НЕКОМУТАТИВНИХ ДВОХОПЕРАНДНИХ СЕТ-ОПЕРАЦІЙ ДЛЯ МАЛОРЕСУРСНИХ ПОТОКОВИХ ШИФРІВ

5.1. Генерації послідовності несиметричних СЕТ-операцій з точністю до перестановки другого операнда

Дослідемо можливость застосування методу генерації груп СЕТ-операцій з точністю до перестановки другого операнда для побудови псевдовипадкових послідовностей несиметричних СЕТ-операцій. При позитивному результаті дослідження, отримані моделі генераторів псевдовипадкового синтезу СЕТ-операцій стануть основою для побудови мало ресурсних несиметричних систем потокового шифрування [5, 15].

В процесі дослідження операцій строгого стійкого кодування було встановлено що генерувати групи операцій строгого стійкого кодування доцільно на основі модифікації СЕТ-операції строгого стійкого кодування з точністю до перестановки другого операнда [103].

Генерація груп прямих СЕТ-операцій строгого стійкого кодування з точністю до перестановки другого операнда може бути на основі моделі [33]:

$$C^*(x, y) = C(x, C_i(y)), \tag{5.1}$$

де $C(x, y)$ – двохоперандна СЕТ-операція строгого стійкого кодування, x – значення першого операнда, y –значення другого операнда, $C^*(x, y)$ – група двохоперандних СЕТ-операцій строгого стійкого кодування з точністю до перестановки другого операнда, $C_i(y)$ – одноопераднда СЕТ-операція для модифікації другого операнда, $i \in \{1; 2; ...; h\}$; h – кількість одноопераднда СЕТ-операцій для перетворення другого операнда, $h \le 2^m!$, m – кількість Сі-квантів інформації в другому операнді.

Генерація груп обернених двохоперандних СЕТ-операцій строгого стійкого кодування з точністю до перестановки другого операнда може бути задана виразом [33] :

$$C^{*/}(x, y) = C^{/}(x, C_i(y)), \tag{5.2}$$

де $C^{/}(x, y)$ – обернена двохоперандна СЕТ-операція строгого стійкого кодування $C^{*/}(x, y)$, – група обернених двохоперандних СЕТ-операцій строгого стійкого кодування з точністю до перестановки другого операнда.

Перевіримо коректність моделей (5.1) і (5.2) для синтезу груп прямих і обернених несиметричних двохоперандних СЕТ-операцій на прикладі.

Нехай модель несиметричної двохоперандної 2Сі-квантової СЕТ-операції [102] задана кортежем із чотирьох одноопераднних 2Сі-квантових СЕТ-операцій.

Якщо $C_1(x) = \begin{bmatrix} x_1 \oplus 1 \\ x_2 \end{bmatrix} = z$; $C_2(x) = \begin{bmatrix} x_1 \\ x_2 \oplus 1 \end{bmatrix} = z$; $C_3(x) = \begin{bmatrix} x_2 \oplus 1 \\ x_1 \end{bmatrix} = z$;

$C_4(x) = \begin{bmatrix} x_2 \\ x_1 \end{bmatrix} = z$, де $C_i(x)$ – i-та одноопераднда СЕТ-операція, x_1 і x_2 перший і других Сі-кванти першого операнда (вхідна інформація), z – результату криптографічного перетворення (2 Сі-кванти), тоді [5]:

$$C(x, y) = C(C_1(x), C_2(x), C_3(x), C_4(x)) = z \tag{5.3}$$

$$C(x, y) = \begin{cases} \begin{bmatrix} x_1 \oplus 1 \\ x_2 \end{bmatrix}, \text{ якщо } y_1 = 0; y_2 = 0 \\ \begin{bmatrix} x_1 \\ x_2 \oplus 1 \end{bmatrix}, \text{якщо } y_1 = 0; y_2 = 1 \\ \begin{bmatrix} x_2 \oplus 1 \\ x_1 \end{bmatrix}, \text{ якщо } y_1 = 1; y_2 = 0 \\ \begin{bmatrix} x_2 \\ x_1 \end{bmatrix}, \text{якщо } y_1 = 1; y_2 = 1 \end{cases} = z, \tag{5.4}$$

де $C(x, y)$ – двохоперандна СЕТ-операція, y_1 і y_2 перший і других Сі-кванти

другого операнда (інформація керування), z – результату криптографічного перетворення (2 Сі-кванти).

На основі моделі (1) отримаємо:

$$C(x, y) = \begin{bmatrix} x_1 \cdot \bar{y}_1 \oplus x_2 \cdot y_1 \oplus \bar{y}_2 \\ x_1 \cdot y_1 \oplus x_2 \cdot \bar{y}_1 \oplus \bar{y}_1 \cdot y_2 \end{bmatrix} = z \tag{5.5}$$

Слід відмітити, що для побудови систем потокового шифрування необхідно генерувати як псевдовипадкові послідовності СЕТ-операцій як для прямого так і для оберненого криптографічного перетворення. Взаємно відповідність даних послідовностей забезпечить як шифрування так і розшифрування інформацій [5].

Так як $C_1^{/}(z) = \begin{bmatrix} z_1 \oplus 1 \\ z_2 \end{bmatrix} = x$; $C_2^{/}(z) = \begin{bmatrix} z_1 \\ z_2 \oplus 1 \end{bmatrix} = x$; $C_3^{/}(z) = \begin{bmatrix} z_2 \\ z_1 \oplus 1 \end{bmatrix} = x$;

$C_4^{/}(z) = \begin{bmatrix} z_2 \\ z_1 \end{bmatrix} = x$, тоді:

$$C^{/}(z, y) = C(C_1^{/}(z), C_2^{/}(z), C_3^{/}(z), C_4^{/}(z)) = x \tag{5.6}$$

$$C^{/}(z, y) = \begin{cases} \begin{bmatrix} z_1 \oplus 1 \\ z_2 \end{bmatrix}, \text{ якщо } y_1 = 0;\ y_2 = 0 \\ \begin{bmatrix} z_1 \\ z_2 \oplus 1 \end{bmatrix}, \text{якщо } y_1 = 0;\ y_2 = 1 \\ \begin{bmatrix} z_2 \\ z_1 \oplus 1 \end{bmatrix}, \text{ якщо } y_1 = 1;\ y_2 = 0 \\ \begin{bmatrix} z_2 \\ z_1 \end{bmatrix}, \text{якщо } y_1 = 1;\ y_2 = 1 \end{cases} = x \tag{5.7}$$

На основі моделі (5.7) отримаємо

$$C^{/}(z, y) = \begin{bmatrix} z_1 \cdot \bar{y}_1 \oplus z_2 \cdot y_1 \oplus y_1 \cdot y_2 \\ z_1 \cdot y_1 \oplus z_2 \cdot \bar{y}_1 \oplus (y_1 \oplus y_2) \end{bmatrix} = z \tag{5.8}$$

Модифікуємо другий операнд моделі прямої СЕТ-операції (5.4) одноопераднною операцією $C_3(x)$. В результаті модифікації отримаємо:

$$C(x,\,y)=\begin{cases}\begin{bmatrix}x_1\oplus 1\\ x_2\end{bmatrix},\ якщо\ y_1=1;\ y_2=0\\ \begin{bmatrix}x_1\\ x_2\oplus 1\end{bmatrix},якщо\ y_1=0;\ y_2=0\\ \begin{bmatrix}x_2\oplus 1\\ x_1\end{bmatrix},\ якщо\ y_1=1;\ y_2=1\\ \begin{bmatrix}x_2\\ x_1\end{bmatrix},якщо\ y_1=0;\ y_2=1\end{cases}=\begin{cases}\begin{bmatrix}x_1\\ x_2\oplus 1\end{bmatrix},якщо\ y_1=0;\ y_2=0\\ \begin{bmatrix}x_2\\ x_1\end{bmatrix},якщо\ y_1=0;\ y_2=1\\ \begin{bmatrix}x_1\oplus 1\\ x_2\end{bmatrix},\ якщо\ y_1=1;\ y_2=0\\ \begin{bmatrix}x_2\oplus 1\\ x_1\end{bmatrix},\ якщо\ y_1=1;\ y_2=1\end{cases}=z$$

$$C(x,\,y)=\begin{bmatrix}x_1\cdot\bar{y}_1\oplus x_2\cdot y_1\oplus y_1\\ x_1\cdot y_1\oplus x_2\cdot\bar{y}_1\oplus\bar{y}_1\cdot\bar{y}_2\end{bmatrix}=z \tag{5.9}$$

$$C(x,\,y)=C(C_2(x),C_4(x),C_1(x),C_3(x))=z\,. \tag{5.10}$$

Модифікуємо другий операнд моделі оберненої СЕТ-операції (5.7) одноопераднною операцією $C_3(x)$. В результаті модифікації отримаємо [5]:

$$C'(z,\,y)=\begin{cases}\begin{bmatrix}z_1\oplus 1\\ z_2\end{bmatrix},\ якщо\ y_1=1;\ y_2=0\\ \begin{bmatrix}z_1\\ z_2\oplus 1\end{bmatrix},якщо\ y_1=0;\ y_2=0\\ \begin{bmatrix}z_2\\ z_1\oplus 1\end{bmatrix},\ якщо\ y_1=1;\ y_2=1\\ \begin{bmatrix}z_2\\ z_1\end{bmatrix},якщо\ y_1=0;\ y_2=1\end{cases}=\begin{cases}\begin{bmatrix}z_1\\ z_2\oplus 1\end{bmatrix},\ якщо\ y_1=0;\ y_2=0\\ \begin{bmatrix}z_2\\ z_1\end{bmatrix},якщо\ y_1=0;\ y_2=1\\ \begin{bmatrix}z_1\oplus 1\\ z_2\end{bmatrix},\ якщо\ y_1=1;\ y_2=0\\ \begin{bmatrix}z_2\\ z_1\oplus 1\end{bmatrix},якщо\ y_1=1;\ y_2=1\end{cases}=x$$

$$C'(z,\,y)=\begin{bmatrix}z_1\cdot\bar{y}_2\oplus z_2\cdot y_2\oplus y_1\cdot\bar{y}_2\\ z_1\cdot y_1\oplus z_2\cdot\bar{y}_1\oplus(y_1\oplus y_2\oplus 1)\end{bmatrix}=x \tag{5.11}$$

$$C'(z,\,y)=C(C_2'(z),C_4'(z),C_1'(z),C_3'(z))=x \tag{5.12}$$

За результатом моделювання можна зробити висновок про можливість генерації груп прямих і обернених несиметричних СЕТ-операцій з точністю до перестановки другого операнда на основі будь якої двохоперандної СЕТ-операції. Коректність даного висновку підтверджена результатами обчислювального експерименту для 2Сі-квантових несиметричних двохоперандних СЕТ-операцій.

Так як моделі прямих несиметричних двохоперандних 2Сі-квантових СЕТ-операції (5.5) і (5.8) відрізняються, то можна стверджувати що модифікація несиметричної СЕТ-операції з точністю до перестановки другого операнду приводить до зміни результату криптографічного перетворення [5].

Кортежі прямих несиметричних двохоперандних 2Сі-квантових СЕТ-операції (5.3) і (5.10) включають в себе переставлені місцями одні і ті самі одноопераднді СЕТ-операції. Тому можна стверджувати, що модифікація несиметричної двохоперандної СЕТ-операції не приводить до зміни таблиць підстановок на основі яких реалізується криптографічне перетворення.

Однакові послідовності прямих і обернених до них одноопераднді СЕТ-операцій в кортежах прямої (5.10) і оберненої (5.12) двохоперандних СЕТ-операцій продемонстрували коректність застосування моделей генерації псевдовипадкових послідовностей операцій (5.1) і (5.2) [5].

Так як в процесі модифікації двохоперандної СЕТ-операції набір одноопераднді операцій не змінюється, а міняється лише їх послідовність можна стверджувати, що всі отримані операції будуть мати однакові криптографічні властивості, тому що реалізують однакові таблиці підстановок.

Реалізація генераторів груп прямих обернених несиметричних двохоперандних СЕТ-операцій з точністю до перестановки другого операнда вимагає застосування прямої і оберненої несиметричної СЕТ-операції і набору лише прямих одноопераднді СЕТ-операцій. Відсутність в моделях синтезу генерацій (5.1) і (5.2) обернених одноопераднді СЕТ-операції забезпечує суттєве строщення алгоритмів СЕТ-шифрування [5].

Розглянемо інші методи генерації послідовності несиметричних сет-операцій з точністю до перестановки.

5.2. Генерації послідовності несиметричних СЕТ-операцій з точністю до перестановки першого операнда

Дослідимо можливість застосування методу генерації груп СЕТ-операцій з точністю до перестановки першого операнда для побудови мало ресурсних несиметричних систем потокового шифрування підвищеної криптостійкості [6].

При вдосконаленні і побудові систем потокового шифрування можна використовувати методи генерації псевдовипадкових послідовностей СЕТ-операцій з точністю до перестановки першого операнда, другого операнда, або результату криптографічного перетворення [33, 104]. При побудові несиметричних систем потокового шифрування на сьогоднішній день використовується генерації псевдовипадкових послідовностей СЕТ-операцій з точністю до перестановки другого операнда [103, 104]. Це пов’язано з простотою генерації груп прямих і обернених несиметричних СЕТ-операцій. Використання різних методів генерації синтезу груп операцій з точністю до перестановки приводить до генерації різних псевдовипадкових СЕТ операцій. При чому дані послідовності можуть відрізняються не тільки послідовностями операцій , але і різними їх наборами.

Дослідимо особливості застосування методу синтезу СЕТ-операцій з точністю до перестановки першого операнду а також визначимо переваги та недоліки їх застосування в несиметричних системах потокового шифрування.

Моделювання процесів прямого і оберненого криптографічного перетворення в групі несиметричних двохоперандних СЕТ-операцій з точністю до перестановки першого операнду проведемо на прикладі 2Сі-квантової СЕТ-операції [33]. Дане обмеження пов’язане з мінімальною кількістю СЕТ-операцій, на основі яких будуються несиметричні двохоперандні СЕТ-операції, а також простотою застосування математичного апарату для моделювання взаємних перетворень моделей операцій [43].

Коректність отриманих за результатами моделювання взаємозв'язків між прямими і оберненими модифікованими СЕТ-операціями з точністю до перестановки першого операнду перевіримо на основі обчислювального експерименту [6].

Задамо модель несиметричної двохоперандної 2Сі-квантової СЕТ-операції [33] кортежем із чотирьох однооперандних 2Сі-квантових СЕТ-операцій.

Якщо $C_1(x)=\begin{bmatrix} x_1 \oplus x_2 \\ x_2 \oplus 1 \end{bmatrix}=z$; $C_2(x)=\begin{bmatrix} x_1 \oplus 1 \\ x_1 \oplus x_2 \end{bmatrix}=z$; $C_3(x)=\begin{bmatrix} x_2 \\ x_1 \oplus 1 \end{bmatrix}=z$;

$C_4(x)=\begin{bmatrix} x_2 \oplus 1 \\ x_1 \end{bmatrix}=z$, де $C_i(x)$ – i-та однооперандна СЕТ-операція, x_1 і x_2 перший і других Сі-кванти першого операнда (вхідна інформація), z – результату криптографічного перетворення (2 Сі-кванти), тоді [6]:

$$C(x,\, y)=C(C_1(x),C_2(x),C_3(x),C_4(x))=z \tag{5.13}$$

$$C(x,\, y)=\begin{cases} \begin{bmatrix} x_1 \oplus x_2 \\ x_2 \oplus 1 \end{bmatrix}, \text{ якщо } y_1=0;\, y_2=0 \\ \begin{bmatrix} x_1 \oplus 1 \\ x_1 \oplus x_2 \end{bmatrix}, \text{якщо } y_1=0;\, y_2=1 \\ \begin{bmatrix} x_2 \\ x_1 \oplus 1 \end{bmatrix}, \text{ якщо } y_1=1;\, y_2=0 \\ \begin{bmatrix} x_2 \oplus 1 \\ x_1 \end{bmatrix}, \text{якщо } y_1=1;\, y_2=1 \end{cases} = z, \tag{5.14}$$

де $C(x,y)$ – двохоперандна СЕТ-операція, y_1 і y_2 перший і других Сі-кванти другого операнда (інформація керування), z – результату криптографічного перетворення (2 Сі-кванти).

На основі моделі (5.14) отримаємо удосконалену дискретну модель СЕТ-операції [6]:

$$C(x,\, y)=\begin{bmatrix} x_1 \cdot \bar{y}_1 \oplus x_2 \cdot (y_1 \vee \bar{y}_2) \oplus y_2 \\ x_1 \cdot (y_1 \vee y_2) \oplus x_2 \cdot \bar{y}_1 \oplus \bar{y}_2 \end{bmatrix}=z \tag{5.15}$$

При побудові насиметричних систем потокового СЕТ-шифрування

необхідно для кожної прямої СЕТ-операції знайти її обернену.

Для несиметричної двохоперандної СЕТ-операції заданої моделлю (5.13) модель оберненої операції модна представити [33]:

$$C'(z, y) = C(C_1'(z), C_2'(z), C_3'(z), C_4'(z)) = x \qquad (5.16)$$

Побудуємо дискретну модель оберненої удосконаленої СЕТ-операції. Для цього використаємо моделі обернених одноопераднних 2Сі-квантових СЕТ-операцій наведених в [96].

Так як $C_1'(z) = \begin{bmatrix} z_1 \oplus z_2 \oplus 1 \\ z_2 \oplus 1 \end{bmatrix} = x$; $C_2'(z) = \begin{bmatrix} z_1 \oplus 1 \\ z_1 \oplus z_2 \oplus 1 \end{bmatrix} = x$;

$C_3'(z) = \begin{bmatrix} z_2 \oplus 1 \\ z_1 \end{bmatrix} = x$; $C_4'(z) = \begin{bmatrix} z_2 \\ z_1 \oplus 1 \end{bmatrix} = x$, тоді:

$$C'(z, y) = \begin{cases} \begin{bmatrix} z_1 \oplus z_2 \oplus 1 \\ z_2 \oplus 1 \end{bmatrix}, \text{ якщо } y_1 = 0;\ y_2 = 0 \\ \begin{bmatrix} z_1 \oplus 1 \\ z_1 \oplus z_2 \oplus 1 \end{bmatrix}, \text{якщо } y_1 = 0;\ y_2 = 1 \\ \begin{bmatrix} z_2 \oplus 1 \\ z_1 \end{bmatrix}, \text{ якщо } y_1 = 1;\ y_2 = 0 \\ \begin{bmatrix} z_2 \\ z_1 \oplus 1 \end{bmatrix}, \text{якщо } y_1 = 1;\ y_2 = 1 \end{cases} = x \qquad (5.17)$$

На основі моделі (5.17) отримаємо [6]

$$C'(z, y) = \begin{bmatrix} z_1 \cdot \bar{y}_1 \oplus z_2 \cdot (y_1 \vee \bar{y}_2) \oplus (\bar{y}_1 \vee \bar{y}_2) \\ z_1 \cdot (y_1 \vee y_2) \oplus z_2 \cdot \bar{y}_1 \oplus (\bar{y}_1 \vee y_2) \end{bmatrix} = x \qquad (5.18)$$

Модифікація СЕТ-операції з точністю до перестановки першого операнда реалізується шляхом криптографічного перетворення одноопераднною СЕТ-операцією вхідних даних які поступають в перший операнд.

Модифікуємо моделі прямої СЕТ-операції (5.15) з точністю до перестановки першого операнду одноопераднною операцією $C_4(x)$ [6].

$$C_4(x, y) = C(C_4(x), y) = z_4 \qquad (5.19)$$

де $C_4(x, y)$ – несиметрична двохоперандна СЕТ-операція модифікована з

точністю до перестановки першого одноопераднною операцією $C_4(x)$, z_4 z – результату криптографічного перетворення даною модифікованою СЕТ-операцією.

Модифіковані одноопераднною СЕТ-операцією вхідні дані в просесі реалізації двохоперандної СЕТ-операції будуть перетворюватися однією із її одноопераднних операцій.

Відповідно до моделі (5.19), кортежну модель СЕТ-операції (5.13) можна представити [6]:

$$C_4(x,\, y) = C(C_1(C_4(x)), C_2(C_4(x)), C_3(C_4(x)), C_4(C_4(x))) = z_4 \qquad (5.20)$$

Модель модифікованої двохоперандної СЕТ-операції з точністю до перестановки першого операнду (5.19), на основі попереднього додаткового перетворення одноопераднної СЕТ-операцією $C_4(x)$ можна представити:

$$C_4(x,\, y) = \begin{cases} C_1(C_4(x)), \ \textit{якщо}\ y_1 = 0;\ y_2 = 0 \\ C_2(C_4(x)), \textit{якщо}\ y_1 = 0;\ y_2 = 1 \\ C_3(C_4(x)), \ \textit{якщо}\ y_1 = 1;\ y_2 = 0 \\ C_4(C_4(x)), \textit{якщо}\ y_1 = 1;\ y_2 = 1 \end{cases} = z_4 \qquad (5.21)$$

Модифікуємо одноопераднні операції $C_1(x)$ – $C_4(x)$ шляхом попереднього додаткового перетворення СЕТ-операцією $C_4(x)$ вхідних Сі-квантів інформації. Для цього в СЕТ-операції $C_1(x)$ – $C_4(x)$ замість першого і другого Сі-квантів першого операнда x_1 і x_2, підставимо першу і другу елементарні функції СЕТ-операції $C_4(x)$ $f_1(x) = x_2 \oplus 1$, $f_2(x) = x_1$ відповідно :

$$C_1(C_4(x)) = \begin{bmatrix} (x_2 \oplus 1) \oplus (x_1) \\ (x_1) \oplus 1 \end{bmatrix} = \begin{bmatrix} x_1 \oplus x_2 \oplus 1 \\ x_1 \oplus 1 \end{bmatrix} = C_5(x) = z_4 \qquad (5.22)$$

$$C_2(C_4(x)) = \begin{bmatrix} (x_2 \oplus 1) \oplus 1 \\ (x_2 \oplus 1) \oplus (x_1) \end{bmatrix} = \begin{bmatrix} x_2 \\ x_1 \oplus x_2 \oplus 1 \end{bmatrix} = C_6(x) = z_4 \qquad (5.23)$$

$$C_3(C_4(x)) = \begin{bmatrix} (x_1) \\ (x_2 \oplus 1) \oplus 1 \end{bmatrix} = \begin{bmatrix} x_1 \\ x_2 \end{bmatrix} = C_7(x) = z_4 \qquad (5.24)$$

$$C_4(C_4(x)) = \begin{bmatrix} (x_1) \oplus 1 \\ (x_2 \oplus 1) \end{bmatrix} = \begin{bmatrix} x_1 \oplus 1 \\ x_2 \oplus 1 \end{bmatrix} = C_8(x) = z_4 \qquad (5.25)$$

Підставивши результати модифікації одноопераднних СЕТ-операції (5.22) – (5.25) в модель модифікованої двохоперандної СЕТ-операції (5.21) отримаємо [6]:

$$C_4(x, y) = \begin{cases} \begin{bmatrix} x_1 \oplus x_2 \oplus 1 \\ x_1 \oplus 1 \end{bmatrix}, \text{ якщо } y_1 = 0;\ y_2 = 0 \\ \begin{bmatrix} x_2 \\ x_1 \oplus x_2 \oplus 1 \end{bmatrix}, \text{якщо } y_1 = 0;\ y_2 = 1 \\ \begin{bmatrix} x_1 \\ x_2 \end{bmatrix}, \text{ якщо } y_1 = 1;\ y_2 = 0 \\ \begin{bmatrix} x_1 \oplus 1 \\ x_2 \oplus 1 \end{bmatrix}, \text{якщо } y_1 = 1;\ y_2 = 1 \end{cases} = z_4 \qquad (5.26)$$

На основі моделі (5.26) отримаємо удосконалену модифіковану дискретну модель СЕТ-операції

$$C_4(x, y) = \begin{bmatrix} x_1 \cdot (y_1 \vee \bar{y}_2) \oplus x_2 \cdot \bar{y}_1) \oplus (y_1 \oplus y_2 \oplus 1) \\ x_1 \cdot \bar{y}_1 \oplus x_2 \cdot (y_1 \vee y_2) \oplus (\bar{y}_1 \vee y_2) \end{bmatrix} = z_4 \qquad (5.27)$$

Побудуємо обернену двохоперандну СЕТ-операції до модифікованої несиметричної двохоперандної СЕТ-операції заданої моделлю (5.20).

Представимо модель удосконалену модифіковану дискретну модель СЕТ-операції (5.27) її кортежною моделлю. Підставивши в (5.26) позначення прямих одноопераднних СЕТ-операцій отримаємо:

$$C_4(x, y) = \begin{cases} C_5(x), \text{ якщо } y_1 = 0;\ y_2 = 0 \\ C_6(x), \text{якщо } y_1 = 0;\ y_2 = 1 \\ C_7(x), \text{ якщо } y_1 = 1;\ y_2 = 0 \\ C_8(x), \text{якщо } y_1 = 1;\ y_2 = 1 \end{cases} = z_4 . \qquad (5.28)$$

Відповідно до (5.28) кортежну модель прямої модифікованої двохоперандуої СЕТ-операції можна представити [6]:

$$C_4(x, y) = C(C_5(x), C_6(x), C_7(x), C_8(x)) = z_4 \qquad (5.29)$$

Відповідно до (5.29) кортежну модель оберненої модифікованої двохоперандуої СЕТ-операції можна представити [6]:

$$C_4^{/}(z_4, y) = C(C_5^{/}(z_4), C_6^{/}(z_4), C_7^{/}(z_4), C_8^{/}(z_4)) = x . \qquad (5.30)$$

Побудуємо дискретну модель оберненої удосконаленої модифікованої

СЕТ-операції. Відповідно до [96] моделі обернених одноопераднних СЕТ-операцій до одноопераднних СЕТ-операцій $C_5(x)$ – $C_8(x)$ можна представити.

$$C_5^{/}(z_4)=\begin{bmatrix} z_{4.2}\oplus 1 \\ z_{4.1}\oplus z_{4.2}\end{bmatrix}=x; \tag{5.31}$$

$$C_6^{/}(z_4)=\begin{bmatrix} z_{4.1}\oplus z_{4.2}\oplus 1 \\ z_{4.1}\end{bmatrix}=x; \tag{5.32}$$

$$C_7^{/}(z_4)=\begin{bmatrix} z_{4.1} \\ z_{4.2}\end{bmatrix}=x; \tag{5.33}$$

$$C_8^{/}(z_4)=\begin{bmatrix} z_{4.1}\oplus 1 \\ z_{4.2}\oplus 1\end{bmatrix}=x, \tag{5.34}$$

де $z_{4.1}$, $z_{4.2}$ – перший і другий Сі-кванти результату криптографічного перетворення інформації модифікованою двохоперанднуої СЕТ-операції (15).

Підставивши моделі (5.31) – (5.34) в кортежну модель оберненої СЕТ-операції (5.30) отримаємо:

$$C_4^{/}(z_4,\, y)=\begin{cases} \begin{bmatrix} z_{4.2}\oplus 1 \\ z_{4.1}\oplus z_{4.2}\end{bmatrix}, \text{ якщо } y_1=0;\ y_2=0 \\ \begin{bmatrix} z_{4.1}\oplus z_{4.2}\oplus 1 \\ z_{4.1}\end{bmatrix}, \text{якщо } y_1=0;\ y_2=1 \\ \begin{bmatrix} z_{4.1} \\ z_{4.2}\end{bmatrix}, \text{ якщо } y_1=1;\ y_2=0 \\ \begin{bmatrix} z_{4.1}\oplus 1 \\ z_{4.2}\oplus 1\end{bmatrix}, \text{якщо } y_1=1;\ y_2=1 \end{cases} =x \tag{5.35}$$

На основі моделі (5.35)отримаємо:

$$C_4^{/}(z_4,\, y)=\begin{bmatrix} z_{4.1}\cdot(y_1\vee y_2)\oplus z_{4.2}\cdot\bar{y}_1\oplus(\bar{y}_1\vee y_2) \\ z_{4.1}\cdot\bar{y}_1\oplus z_{4.2}\cdot(y_1\vee\bar{y}_2)\oplus(y_1\cdot y_2)\end{bmatrix}=x \tag{5.36}$$

Побудована модель оберненої двох розрядної СЕТ-операції (5.36) дозволяє розшифровувати інформацію зашифровану прямою СЕТ-операції (15). Проте $C_4(x,\, y)=z_4$ лише одна із операцій, яка належить групі операцій з точністю до перестановки першого операнда. Групу двохоперандних СЕТ-

операцій з точністю до перестановки першого операнда модна представити як

$$C_i(x, y) = C(C_i(x), y) = z_i , \quad (5.37)$$

де i - індекс (номер) одноопераидної СЕТ-операції на основі якої була реалізована модифікація двохопаераидналї СЕТ-операції.

Побудова моделі (5.36) представляє собою побудову лише однієї оберненої СЕТ-операції з групи операцій (5.37). Тому на практиці використовувати даний підхід для реалізації оберненого перетворення складно і нераціонально [6].

Будь яку операції з групи операцій (5.37) можна представить як функцію від двохоперандної і одноопериндної СЕТ-операції

$$C_i(x, y) = f(C(x, y), C_i(x)) . \quad (5.38)$$

Обернену операцію для будь якої двохоперандної СЕТ-операції з групи СЕТ-операцій (5.38) можна представити як

$$C_i^{/}(x, y) = f(C^{/}(x, y), C_i^{/}(x)) , \quad (5.39)$$

На основі функції (27) можна представити три варіанти синтезу обернентї СЕТ-операції:

- з точністю до перестановки результату перетворення

$$C_i^{/}(x, y) = C_i^{/}(C^{/}(x, y)) ; \quad (5.40)$$

- з точністю до перестановки першого операнда

$$C_i^{/}(x, y) = C^{/}(C_i^{/}(x), y) ; \quad (5.41)$$

- з точністю до перестановки другого операнда

$$C_i^{/}(x, y) = C^{/}(x, C_i^{/}(y)) \quad (5.42)$$

Розглянемо можливість побудови оберненого СЕТ-операції (5.36) на основі моделі (5.40). Для цього підставимо в модель оберненої одноопераидної СЕТ-операції $C_4^{/}(z)$ обернену двохоперандну операцію (5.18):

$$C_4^{/}(z_4, y) = C_4^{/}(C^{/}(z_4, y)) = C(C_4^{/}(C_1^{/}(z_4)), C_4^{/}(C_2^{/}(z_4)), C_4^{/}(C_3^{/}(z_4)), C_4^{/}(C_4^{/}(z_4))) . \quad (5.43)$$

На основі кортежної моделі оберненої СЕТ-операції (5.43) отримаємо:

$$C_4^{/}(z_4, y) = \begin{cases} C_4^{/}(C_1^{/}(z_4)), \ якщо\ y_1 = 0;\ y_2 = 0 \\ C_4^{/}(C_2^{/}(z_4)), якщо\ y_1 = 0;\ y_2 = 1 \\ C_4^{/}(C_3^{/}(z_4)), \ якщо\ y_1 = 1;\ y_2 = 0 \\ C_4^{/}(C_4^{/}(z_4)), якщо\ y_1 = 1;\ y_2 = 1 \end{cases} = x. \quad (5.44)$$

Визначимо одноопераднді обернені СЕТ-оперпації, з яких побудовано кортеж оберненої двохоперандної СЕТ-операції (5.43):

$$C_4^{/}(C_1^{/}(z_4)) = \begin{bmatrix} (z_{4.2} \oplus 1) \\ (z_{4.1} \oplus z_{4.2} \oplus 1) \oplus 1 \end{bmatrix} = \begin{bmatrix} z_{4.2} \oplus 1 \\ z_{4.1} \oplus z_{4.2} \end{bmatrix} = x; \quad (5.45)$$

$$C_4^{/}(C_2^{/}(z_4)) = \begin{bmatrix} (z_{4.1} \oplus z_{4.2} \oplus 1) \\ (z_{4.1} \oplus 1) \oplus 1 \end{bmatrix} = \begin{bmatrix} z_{4.1} \oplus z_{4.2} \oplus 1 \\ z_{4.1} \end{bmatrix} = x; \quad (5.46)$$

$$C_4^{/}(C_3^{/}(z_4)) = \begin{bmatrix} (z_{4.1}) \\ (z_{4.2} \oplus 1) \oplus 1 \end{bmatrix} = \begin{bmatrix} z_{4.1} \\ z_{4.2} \end{bmatrix} = x; \quad (5.47)$$

$$C_4^{/}(C_4^{/}(z_4)) = \begin{bmatrix} (z_{4.1} \oplus 1) \\ (z_{4.2}) \oplus 1 \end{bmatrix} = \begin{bmatrix} z_{4.1} \oplus 1 \\ z_{4.2} \oplus 1 \end{bmatrix} = x. \quad (5.48)$$

Підставивши в модель оберненої двохоперандну СЕТ-операції (5.44) моделі обернених одноопераднних СЕТ-операцій (5.45) – (5.48) отримаємо:

$$C_4^{/}(z_4, y) = \begin{cases} \begin{bmatrix} z_{4.2} \oplus 1 \\ z_{4.1} \oplus z_{4.2} \end{bmatrix}, \ якщо\ y_1 = 0;\ y_2 = 0 \\ \begin{bmatrix} z_{4.1} \oplus z_{4.2} \oplus 1 \\ z_{4.1} \end{bmatrix}, якщо\ y_1 = 0;\ y_2 = 1 \\ \begin{bmatrix} z_{4.1} \\ z_{4.2} \end{bmatrix}, \ якщо\ y_1 = 1;\ y_2 = 0 \\ \begin{bmatrix} z_{4.1} \oplus 1 \\ z_{4.2} \oplus 1 \end{bmatrix}, якщо\ y_1 = 1;\ y_2 = 1 \end{cases} = x \quad (5.49)$$

Так як побудована модель оберненої двохоперандну СЕТ-операції (5.49) співпала з моделлю оберненої двохоперандну СЕТ-операції (5.35), то удосконалена модель оберненої двохоперандної СЕТ-операції буде описуватися моделлю (5.36).

Узагальнивши отриманий результат можна допустити, що при

модифікації прямої несиметричної двохоперандної СЕТ-операцій з точністю до перестановки першого операнда (5.37), тоді модифікація оберненої двохоперандної СЕТ-операцій оберненою одноопераднодної операцією з точністю до перестановки результату на основі моделі [6]

$$C_i^{/}(z_i, y) = C_i^{/}(C^{/}(z_i, y)) = x \qquad (5.50)$$

забезпечить обернене перетворення інформації.

Коректність наведених результатів моделювання підтверджена результатами обчислювального експерименту

В процесі модифікації несиметричної двохоперандної СЕТ-операцій з точністю до перестановки першого операнда змінюється математична модель СЕТ-операції. Про це свідчать побудовані моделі СЕТ-операції до її модифікації (5.13) і після модифікації (5.27). Необхідно відмітити, що в результаті модифікації СЕТ-операції буде змінюватися як сама модель операції, так і результат її реалізації [6].

Модифікації СЕТ-операцій з точність до перестановки другого операнда [94, 101] забезпечує зміну результату криптографічного перетворення за рахунок зміни послідовності одноопенандних СЕТ-операцій в кортежі двохоперандної операції. Модифікація СЕТ-операцій з точність до перестановки першого операнда приводить до модифікації не послідовності одноопераднодних операцій в кортежі, а модифікації самих одноопераднодних СЕТ-оперцій. Про це свідчать кортежні моделі операції до її модифікації (5.13) і після модифікації (5.29). Збільшення кількості одноопераднодних СЕТ-операцій при використанні групи модифікованих несиметричних СЕТ-операцій з точністю до перестановки першого операнду забезпечує збільшення кількості таблиць підстановки які реалізується в процесі шифрування. Збільшення кількості таблиць підстановки які реалізуються забезпечує збільшення криптостійкості алгоритму шифрування.

Якщо при шифруванні будо використано модифікацію СЕТ-операції з точністю до перестановки першого операнда відповідно до моделі (5.37), то при розшифруванні необхідно використовували модифікацію оберненої СЕТ-

операції точністю до перестановки результату перетворення відповідно до моделі (5.50). На основі моделей модифікації СЕТ-операцій реалізуються генератори псевдовипадкових послідовностей прямих і обернених модифікованих двохоперандних СЕТ-операцій [6]. Коректність наведених теоретичних результатів підтверджена результатами обчислювального експерименту

По аналогії можна дослідити генерацію послідовності несиметричних сет-операцій з точністю до перестановки результату криптографічного перетворення. Результати статистичної оцінки результатів застосування згенерованих псевдо випадкових послідовностей СЕТ-операцій наведені в [7].

5.3 Побудова інформаційної системи моделювання комутативних і некомутативних двохоперандних сет-операцій для малоресурсних систем потокового шифрування

Модель одноопераднної nCi-квантові СЕТ-операції можна представити [33]:

$$C(x) = C(f_1(x),\ f_2(x),\ f_3(x),\dots,\ f_n(x),),\ \text{або}\ C\begin{pmatrix} x_1 \\ x_2 \\ \dots \\ x_n \end{pmatrix} = \begin{bmatrix} f_1(x_1, x_2,..., x_n) \\ f_2(x_1, x_2,..., x_n) \\ ..... \\ f_n(x_1, x_2,..., x_n) \end{bmatrix} \quad (5.51)$$

де x_1, $x_2,\dots,x_n$ вхідні Сі-кванти інформації; $f_1(x_1, x_2,..., x_n)$, $f_2(x_1, x_2,..., x_n),\dots,$ $f_n(x_1, x_2,..., x_n)$ елементарні функції реалізації відповідних вихідних Сі-квантів інформації.

Якщо $C(C(x)) = x$ то одноопернадна СЕТ-операція буде симетричною, якщо $C(C(x)) \neq x$ – несиметричною. Для несиметричних СЕТ-операцій буде справедлива рівність $C'(C(x)) = x$ [33].

Модель двохоперандної СЕТ-операції можна представити [33]:

$$C(x, y) = C(C_1(x), C_2(x), C_3(x), \dots, C_k(x),), \tag{5.52}$$

де k – кількість одноопераднних операцій в кортежі двохоперандної СЕТ-операції.

Якщо $k = 2^m$, то двохоперандну СЕТ-операцію (5.51) можна представити [33]:

$$C(x, y) = \begin{cases} C_1(x), \ якщо\ y_1 = 0;\ y_2 = 0;\dots;\ y_m = 0 \\ C_2(x), \ якщо\ y_1 = 0;\ y_2 = 0;\dots;\ y_m = 1 \\ \dots\dots\dots \quad \dots\dots\dots \quad \dots\dots\dots \\ C_k x), \quad якщо\ y_1 = 1;\ y_2 = 1;\dots;\ y_m = 1; \end{cases} \tag{5.53}$$

Розглянемо перестановку операндів місцями в двохоперандній СЕТ-операції (5.53):

$$C(y, x) = \begin{cases} C_1(y), \ якщо\ x_1 = 0;\ x_2 = 0;\dots;\ x_m = 0 \\ C_2(y), \ якщо\ x_1 = 0;\ x_2 = 0;\dots;\ x_m = 1 \\ \dots\dots\dots \quad \dots\dots\dots \quad \dots\dots\dots \\ C_k(y), \quad якщо\ x_1 = 1;\ x_2 = 1;\dots;\ x_m = 1; \end{cases} \tag{5.54}$$

Для СЕТ-операції $C(x, y)$ існує обернена операція $C'(x, y)$, така що:

$$C'(C(x, y), y) = x. \tag{5.55}$$

Якщо в прямій і оберненій СЕТ-операціях переставити операнди місцями, по аналогії з (5.55) отримаємо:

$$C'(C(y, x), x) = y. \tag{5.56}$$

Так як $x \neq y$ то будуть справедливі нерівності:

$$\begin{cases} C'(C(x, y), y) \neq C'(C(y, x), x) \\ C(x, y) \neq C(y, x) \\ C'(x, y) \neq C'(y, x) \end{cases} \tag{5.57}$$

Для симетричних двохоперандних СЕТ-операції, які допускають перестановку операндів місцями будуть справедливі рівності [12]:

$$\begin{cases} C(x, y) = C(y, x) \\ C'(x, y) = C'(y, x) \\ C'(C(x, y), y) = C'(C(y, x), x) \end{cases} \tag{5.58}$$

Для дослідження СЕТ-операцій які відповідають вимогам (5.58) і була запропонована трьох рівнева ієрархічна інформаційна технологія моделювання і дослідження симетричних двохоперандних СЕТ-операцій [58].

Ієрархічний підхід до синтезу СЕТ-операцій передбачає поетапне формування та дослідження операцій різного рівня складності. На першому рівні ієрархії здійснюється синтез одноопераднних СЕТ-операцій, а також аналіз їхніх функціональних і структурних характеристик, що дозволяє визначити їхню придатність для подальшого використання. Другий рівень ієрархії базується на результатах попереднього етапу та передбачає синтез двохоперандних СЕТ-операцій на основі вже сформованої множини одноопераднних операцій, після чого виконується дослідження їхніх властивостей і закономірностей побудови. Формування та аналіз псевдовипадкових послідовностей двохоперандних СЕТ-операцій, що дає можливість оцінити їхній потенціал для застосування в криптографічних перетвореннях та системах захисту інформації відбувається з використанням синтезованих одноопераднних і двохоперандних СЕТ-операцій на третьому рівні ієрархії [13]. Оскільки симетричні двохоперандні СЕТ-операції допускають перестановку операндів з точністю до перестановки результатів, у процесі синтезу таких операцій і формування груп СЕТ-операцій результати їх виконання додатково обробляються за допомогою одноопераднних операцій.

Процес створення двохоперандних СЕТ-операцій у цій системі формалізовано таким чином:

$$C_i(x, y) = C_i(C(x, y)) \tag{5.59}$$

де i – це елемент множини лише тих одноопераднних СЕТ-операцій, які відповідають установленим вимогам і визначені для синтезу двохоперандних СЕТ-операцій.

Так як в симетричних двохоперандних СЕТ-операція прямі і обернені, а також з переставленими і не переставленими операндами співпадають відповідно до вимог (5.58) та їх означенням.

Відповідно до означення симетричних двохоперандних СЕТ-операція і вимог (5.58), прямі і обернені СЕТ-операція, до перестановки операндів і після перестановки співпадають. Тому в даній системі необхідно моделювати лише прямі СЕТ-операції [10].

Формалізований процес генерації псевдовипадкової послідовності двохоперандних СЕТ-операцій в даній системі можна представити:

$$C_{ji}(x, y) = C_j(C_i(C(x, y))) \tag{5.60}$$

де i – елемент множини одноопераднних СЕТ-операцій, які визначені для синтезу двохоперандних СЕТ-операцій; j – елемент множини одноопераднних СЕТ-операцій, які визначені для генерації псевдовипадкової послідовності двохоперандних СЕТ-операцій. Множини одноопераднних СЕТ-операцій для синтезу двохоперандних операцій і генерації псевдовипадкової послідовності двохоперандних операцій, як правило не співпадають, тому що формуються на основі різних вимог до синтезу.

Ієрархічний підхід до побудови інформаційної системи моделювання і дослідження СЕТ-операцій виявився універсальним. Але три рівні ієрархії системи достатні при побудові і дослідженні лише однієї класифікованої групи СЕТ-операцій. Побудова двохоперандних СЕТ-операцій однієї класифікованої групи пов’язана з використанням одних і тих самих моделей синтезу. Для розширення можливостей системи необхідно збільшити кількість класифікованих груп СЕТ-операцій, які синтезуються. Це приводить до збільшення кількості моделей які використовуються на кожному рівні ієрархії, і додатковому використанні моделей побудови двохоперандних СЕТ-операцій на основі одноопераднних. Тому між рівнями синтезу одноопераднних СЕТ-операцій і груп двохоперандних СЕТ-операцій, необхідно ввести рівень синтезу двохоперандних СЕТ-операцій.

Модель ієрархічної інформаційної систем для побудови і дослідження симетричних двохоперандних СЕТ-операцій які допускають перестановку операндів місцями, з урахуванням виразі (5.59) і (5.60), представлена на рис. 5.1 [11, 14].

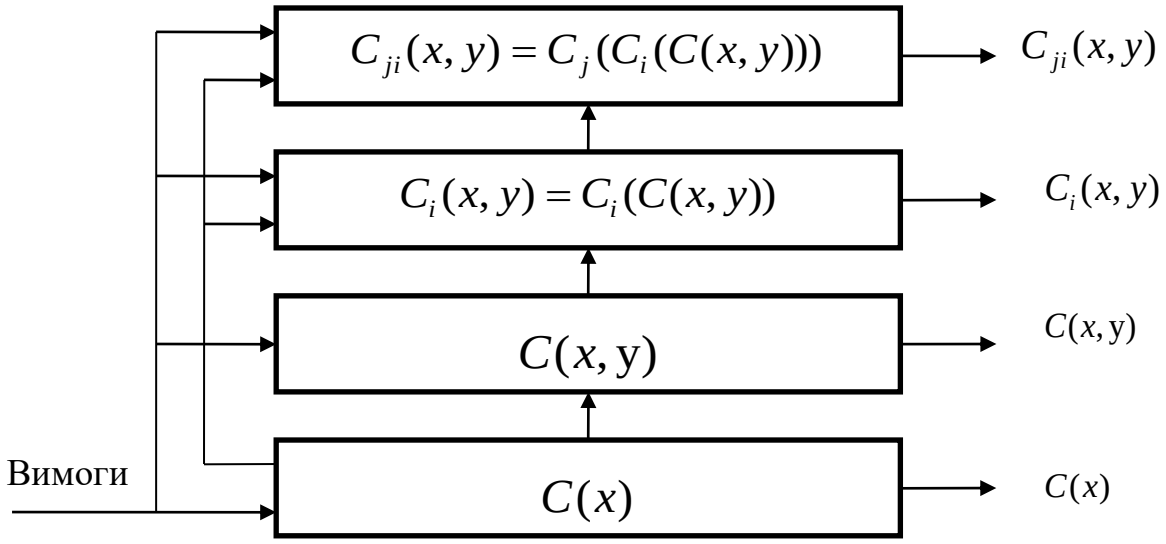

Рис. 5.1. Модель ієрархічної інформаційної систем для побудови і дослідження симетричних двохоперандних СЕТ-операцій які допускають перестановку операндів місцями

Розглянемо відмінності чотирьохрівневих ієрархічних систем для побудови і дослідження симетричних двохоперандних СЕТ-операцій які допускають перестановку операндів місцями і не допускають перестановки операндів місцями [12, 16].

На першому рівні ієрархії синтез і аналіз одноопераднних СЕТ-операцій для обох систем проводиться аналогічно.

На другому рівні ієрархії синтез двохоперандної операції проводиться на основі одноопераднних симетричних СЕТ-операцій ($C(x) = C^{/}(x)$). Синтез симетричних двохоперандних операцій які допускають перестановку операндів місцями вимагає виконання умови $C(x,y) = C(y,x)$. Для інших

симетричних двохоперандних операцій $C(y,x)$ може не існувати, або $C(x,y) \neq C(y,x))$.

На третьому рівні ієрархії синтез групи двохоперандних операції які допускають перестановку операндів проводиться з точністю до перестановки результату (5.59).

Так як можливість перестановки операндів не передбачається, тому відсутнє обмеження на комутативні властивості СЕТ-операції $C(x,y) \neq C(y,x)$.

Так як $C_i(C(x)) \neq C_i(C(y))$, і $C_i(C(x)) = C_j(x)$, де $C_j(C_j(x)) \neq x$, буде справедливий вираз:

$$C_i(C(x,y)) \neq C_i^{/}(C(x,y)). \qquad (5.61)$$

Модель (5.61) показує, що синтез несиметричних двохоперандних СЕТ-операції які не допускають перестановку операндів, з точністю до перестановки результатів, приводить до модифікації одноопераднних СЕТ-операцій. В результаті модифікації одннооперандних СЕТ-операцій вони можуть або залишитися симетричними, або стати несиметричними. Результати модифікації операцій [12].

Так як перестановка другого операнда змінює лише послідовність одноопераднних операцій в кортежі, без модифікації самих одноопераднних операцій тому доцільно її використати при побудові групи несиметричних двохоперандних СЕТ-операції з точністю до перестановки:

$$C_i(x,y) = C(x, C_i(y)); \qquad (5.62)$$

На четвертому рівні ієрархії відповідно до моделі (5.60) генерується псевдовипадкова послідовність операцій. Для генерації аналогічної послідовності симетричних операцій, в яких не обов'язково переставлять операнди місцями доцільно використати перетворення другого операнда з точністю до перестановки:

$$C_{ji}(x,y) = C(x, C_j(C_i(y))) \qquad (5.63)$$

Коректність моделі (5.63) базується на коректності моделі (5.62).

Для забезпечення можливості автоматизації синтезу побудови і дослідження симетричних двохоперандних СЕТ-операцій які допускають перестановку операндів місцями, необхідно в ієрархічній системі (рис.5.1) на третьому рівні ієрархії модель (5.59) замінити моделлю (5.62), а на четвертому рівні модель (5.60) замінити моделлю (5.63). Об'єднання моделей (5.59) і (5.62) і також (5.60) і (5.63) забезпечать можливість побудови і дослідження всіх симетричних двохоперандних СЕТ-операцій, які допускають, або не допускають перестановку операндів місцями.

Синтез і дослідження несиметричних двохоперандних СЕТ-операцій вимагає встановлення взаємозв'язків між прямими і оберненими операціями.

Розглянемо особливості моделі ієрархічної інформаційної систем для побудови і дослідження несиметричних двохоперандних СЕТ-операцій. Використання двохоперандних СЕТ-операцій можливе лише при наявності взаємозв'язків між прямими і оберненими операціями. Тому на першому рівні ієрархії необхідно будувати множину прямих і множину обернених СЕТ операцій. На другому рівні ієрархії при побудові прямої двохоперандної СЕТ-операції необхідно сформувати кортеж прямих одноопераднних СЕТ-операцій. Замінивши в побудованому кортежі прямі одноопераднді СЕТ-операції на обернені буде побудована обернена несиметрична двохоперандна операція.

Модифікація другого операнду не приводить до модифікації самих одноопераднних СЕТ-операції, а змінює лише їх послідовність в кортежі. Аналогічна модифікація другого операнда в оберненій двохоперандній СЕТ-операції забезпечить побудову кортежу обернених одноопераднних операцій, а значить і оберненої двохоперандної операції. Виходячи з цього на третьому рівні ієрархії побудова групи несиметричних двохоперандних СЕТ операцій з точністю до перестановки другого операнда буде описуватися моделями:

$$\begin{aligned} C_i(x,y) &= C(x, C_i(y)) \\ C_i^{/}(x,y) &= C^{/}(x, C_i(y)) \end{aligned}; \qquad (5.64)$$

де $C_i^{/}(x, C_i(y)) = x$.

Генерацію псевдовипадкової послідовності СЕТ-операцій можна також генерувати з точністю до перестановки другого операнда [10]:

$$\begin{aligned} C_{ji}(x,y) &= C(x, C_j(C_i(y))) \\ C'_{ji}(x,y) &= C'(x, C_j(C_i(y))) \end{aligned}; \qquad (5.65)$$

де $C'_{ji}(x, C_j(C_i(y))) = x$.

Модель ієрархічної інформаційної систем для побудови і дослідження несиметричних двохоперандних СЕТ-операцій, яка реалізує моделі (5.64) і (5.65) представлена на рис.5.2. [12].

Моделі ієрархічних інформаційних систем, представлених на рис.5.1, і рис.5.2 по суті відрізняються правилами побудови груп операцій і генерації псевдовипадкових послідовностей. Тому при програмній реалізації системи доцільно використати базу даних, і базу знань.

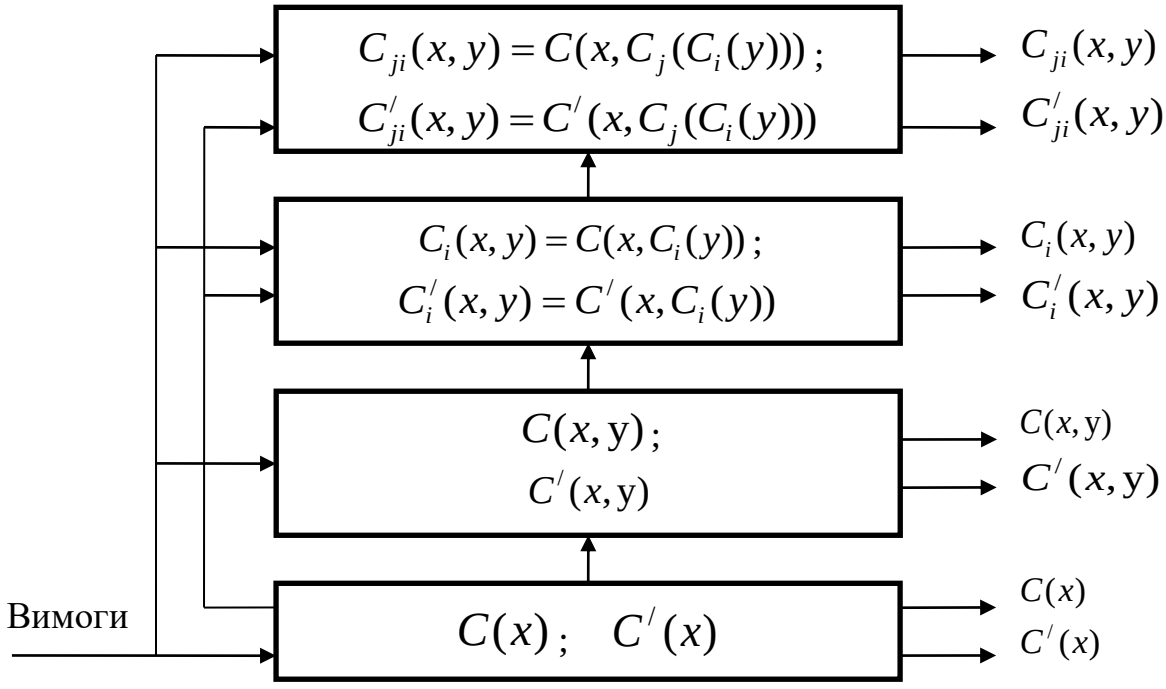

Рис. 5.2. Модель ієрархічної інформаційної систем для побудови і дослідження несиметричних двохоперандних СЕТ-операцій з точністю до перестановки другого операнда.

В базі даних необхідно зберігати синтезовані СЕТ-операції, їх властивості і параметри синтезу. База знань повинна включати моделі реалізації методів синтезу, моделі побудови груп операцій та моделі генерації псевдовипадкових послідовностей СЕТ-операцій. Наявність бази даних і бази знань забезпечать можливість оперативної перебудови системи для вирішення задач дослідження, а також вдосконалення самої системи шляхом розширення як бази даних так і бази знань [12].

Наявність в ієрархічній інформаційній системі бази даних і бази знань дозволяють частково зменшити наслідки комбінаторного зростання операцій і суттєво розширити можливості дослідження процесів практичного синтезу псевдовипадкових послідовностей СЕТ-операцій [12].

Проте на практиці використання бази знань даних і бази знань пов’язане з складністю їх реалізації. Традиційні підходи до побудови експертних систем напряму не дозволяють представляти дискретні моделі в якості даних. База знань, або правила виведення результату, по своїй сутності повинна представляти моделі перетворення моделей, або взаємного перетворення моделей. Результати принятого рішення повинні мати рекомендаційний характер для можливого використання і включати в себе відібрані синтезовані моделі на всиз рівнях. Тобто і дані і знання і оцінку якості за результатами статистичного тестування.

Розглянемо більш детально удосконалену модель ієрархічної інформаційної систем представлену на рис. 5.2.

На нижньому рівні ієрархії реалізується синтез прямих і обернених одноопераднних СЕТ-операцій. Відповідно до розробленої блок схеми (рис. 2.3). Для синтезу одноопераднних СЕТ-операцій необхідно отримати елементарні функції на основі яких вони будуть будуватися. Для синтезу елементарних функцій достатньо визначити кількість Сі-квантів інформації які вони перетворюють. Якщо синтезувати n Сі-квантові елементарні функції, то їх кількість буде визначатися як $C_n^{n/2}$ [41], тому що їх таблиця істинності має однакову кількість нулів і одиниць. Кількість 2Сі-квантових елементарних функцій буде 6, 3Сі-квантових елементарних функцій – 70, 4Сі-квантових елементарних функцій – 51480.

Для повного синтеза одноопераднних СЕТ-операцій, потрібно перебрати всі можливі варіанти поєднання елементарних функцій в кортежі, та перевірити наявність оберненого СЕТ-перетворення. Якщо, обернене перетворення ісрує необхідно знайти операцію оберненого перетворення. Для синтезу 2Сі-квантових одноопераднних СЕТ-операційц необхідно обьєднувати по дві 2Сі-квантові елементарні функції. Буде синтезовано 24 2Сі-квантові СЕТ-операції. Для синтезу 3Сі-квантових одноопераднних СЕТ-операційц необхідно обьєднувати по три 3Сі-квантові елементарні функції. Буде синтезовано 40320 3Сі-квантових СЕТ-операцій. Для синтезу 4Сі-квантових одноопераднних СЕТ-операційц необхідно обьєднувати по чотири 4Сі-квантові елементарні функції. Буде синтезовано 20922789888000 4Сі-квантові СЕТ-операції.

Серед синтезованих одноопераднних СЕТ-операцій необхідно виділити симетричні і несиметричні СЕТ-операції. Для несиметричних Сет-операцій необхідно виділити прямі ім обернені СЕТ-операції. Крім того Селекція синтезованих Одноопераднних СЕТ-операцій може проводитись по якості перетворення блоку інформації, наприклад мо максимальній невизначенні результату перетворення, яка забезпечується гарантованою зміною 50% біт вхідних данних. Можливі і інші вимоги до якості перетворення блоку інформації.

Крім того можливий синтез одноопераднних СЕТ-операцій на основі властивостей моделей і математичного апарату, яким описубться дані моделі. Наприклад СЕТ-операції на основі лінійних перетворень, такі як операції перестановки і матричні СЕТ-операції. Операції на основі нелінійних перетворень, такі як СЕТ-операції перестановок керованих інформацією, нелінійні матричні СЕТ-операції та інші. Проте автоматизація процесів синтезу відомих і тим більше невідомих множин елементарних Функцій і груп СЕТ-операцій побудованих на їх основі виходить за рамки даного дослідження.

Для даного рівня ієрархії базою даних є елементарні функції, а базою знань є правила побудови одноопераднних СЕТ-операцій. Результатом реалізації першого рівня ієрархії буде множина груп одноопераднних СЕТ-операцій з визначеними заданими властивостями кожної операції.

Для другого рівня ієрархії базою даних є множина груп одноопераднних СЕТ-операцій з визначеними заданими властивостями кожної операції.

Відповідно до властивостей двохоперандних СЕТ-операцій відбираються одноопераднді СЕТ-операції з аналогічними або наперед заданими властивостями і на основі їх використовуючи моделі об'єднання обноопераднних СЕТ-операцій будуються двохоперандні СЕТ-операції.

До проведення дисертаційних досліджень в інформаційний системі було реалізовано синтез симетричних двохоперандних СЕТ-операцій які допускають перестановку операндів на основі дублювання одноопераднних СЕТ-операцій базової групи [56], за умови що в СЕТ-операція базової групи відсутні додаткові інверсії результатів перетворення.

Дану модель синтезу СЕТ-операції в загальному вигляді можна представити:

$$C_i(x, \mathrm{y}) = C_i(x) \oplus C_i(\mathrm{y}) \tag{5.66}$$

де $i \in \{1,2,...,k\}$, k - кількість операцій базової групи n Сі-квантових СЕТ-операцій ($k << n!$).

Для синтезу повної групи двохоперандних СЕТ-операцій які допускають перестановку операндів необхідно використовувати узагальнену модель

$$C_{i.j.l}(x, \mathrm{y}) = C_i(x) \oplus C_j(\mathrm{y}) \oplus C_l(1) \tag{5.67}$$

де $i, j \in \{1,2,...,n!\}$, $C_l(1)$ - l-й вектор інвенсій n Сі-квантових СЕТ-операцій ($l \in \{1,2,...,2^n\}$.

Проте при побудові криптографічних систем не обов'язково використовувати двохоперандні СЕТ-операції які допускають перестановку операндів місцями. Синтез даних двохоперандних СЕТ-операцій полягає в об'єднанні одноопераднних СЕТ-операцій в кортежі двохоперандної операції.

$$C(x, \mathrm{y}) = C(C_i^1(x), C_j^2(x)...., C_l^{2^n}(x)) \qquad (5.68)$$

де $C_j^h(x)$ - j -та одноопераднда СЕТ-операція яка вибрана в якості h -ї операції в кортежі двохоперандної СЕТ-операції, n – кількість Сі-квонтів які перетворює двохоперандна СЕТ-операція.

Якщо $i, j, l \in \{1,2,...,n!\}$, то на основі моделі (5.68) будуть синтезуватися як симетричні так і несиметрисні двохоперандні СЕТ-операції

Якщо $i, j, l \in \{1,2,...,k\}$, де k - кількість операцій базової групи n Сі-квантових СЕТ-операцій то на основі моделі (5.68) будуть синтезуватися лише симетричні двохоперандні СЕТ-операції.

На основі моделей (5.66) – (5.68) будуть синтезуватися двохоперандні СЕТ-операції для реалізації яких кількість Сі-квантів псевдовипадкової послідовності співпадає з кількістю Сі-квантів інформації яка шифрується.

Проте, якщо кількість одноопераднних СЕТ-операцій в кортежі двохоперандної СЕТ-операції буде більшою, або меншою за 2^n то кількість Сі-квантів шифрограми не буде співпадати з кількістю Сі квантів гамуючої послідовності в потокових шифрах [33]. Дане неспівпадання суттєво ускладнює крипто аналіз шифрограм. Проте дослідження і прбудова даних двохоперандних СЕТ-операцій вимагає використання інших підходів до їх дослідження, а процес моделювання потребує використання нових додаткових вимог. Аналогічно побудова і дослідження взаємообернених СЕТ-операцій [96], в яких перестановка операндів забезпечує перетворення операції кодування в операцію декодування, і навпаки.

Розглянемо алгоритми синтезу двохоперандних СЕТ-операцій на основі одноопераднихСЕТ операцій.

Алгоритм синтезу групи симетричних двохоперандних СЕТ-операцій які допускають перестановку операндів на на основі одноопераднихСЕТ-операцій базової групи представлено на рис. 5.3.

Рис 5.3. Алгоритм синтезу групи симетричних двохоперандних СЕТ-операцій які допускають перестановку операндів на основі одноопераднихСЕТ-операцій базової групи

Алгоритм синтезу групи несиметричних двохоперандних СЕТ-операцій які допускають перестановку операндів на основі одноопераднихСЕТ-операцій базової групи представлено на рис. 5.4.

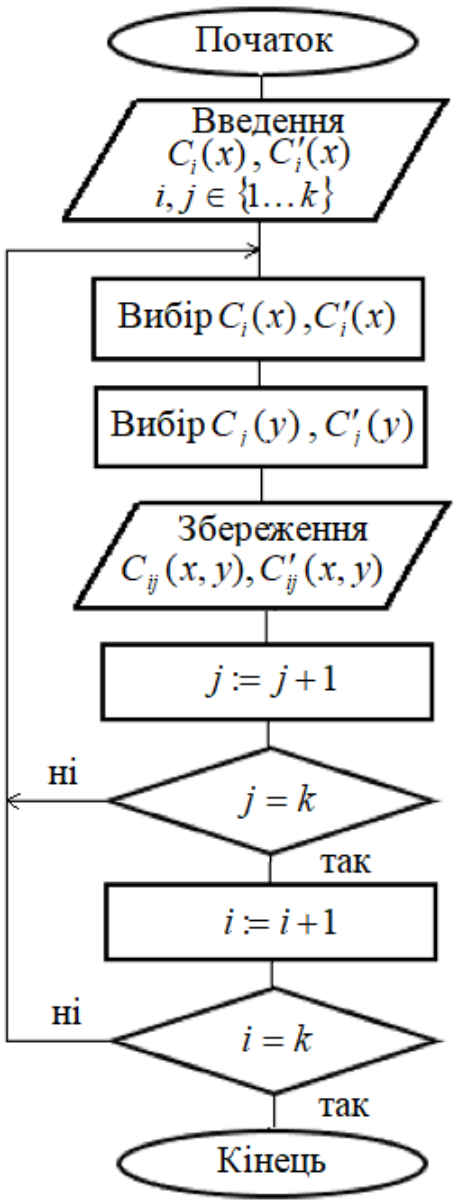

Рис 5.4. Алгоритм синтезу групи несиметричних двохоперандних СЕТ-операцій які допускають перестановку операндів на основі одноопераднних СЕТ-операцій базової групи

Як видно їх рис. 5.3 і рпис. 5.4 алгоритм синтезу повної групи симетричних двохоперандних СЕТ-операцій які допускають перестановку операндів на основі одноопераднних СЕТ-операцій базової групи представлено є спрощеним варіантом алгоритму синтезу групи несиметричних двохоперандних СЕТ-операцій які допускають перестановку операндів. Проте дані алгоритми синтезують лише частину Двогоперандних операцій.

Алгоритм синтез групи двохоперандних СЕТ-операцій які допускають перестановку операндів шляхом одноопераднння СЕТ-операцій на основі об’єднання одноопераднних СЕТ-операцій з додатковим гамуванням відповідно до моделі (5.67) представлено на рис. 5.5.

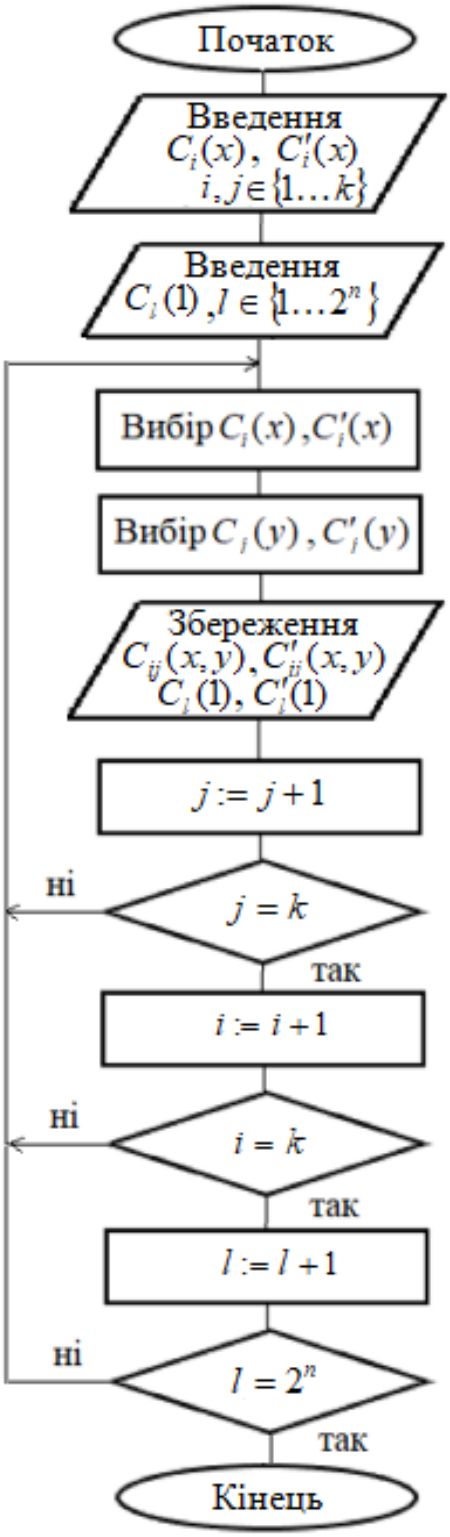

Рис 5.5. Алгоритм синтезу групи двохоперандних СЕТ-операцій які допускають перестановку операндів на основі моделі (5.67)

Наведені алгоритми синтезу хвозоперандних операцій відображають наявні знання про матоди і моделі синтезу двохоперандних СЕТ-операцій. Вони вони структурують і впроваджують наявні знанняБ та дозволяють об’єднати їх в одну систему. Це суттево відрізняє представлення знань для синтезу нових моделей на основі взаємоперетворення моделей. Адже взаємоперетворення матемотичних моделей значно складніше за перетворення вхідних нанних на основі формального виведення в експертних системах.

Необхідно відмітити, що отримані на першому рівні ієрархії, відповідно до заданих нових вимог, отримані нові моделі розглядаються як як основа для виводу нових знань. Проте результати використання нових знань (отримані нові моделі) є вхідними даними для другого рівня ієрархії системи. На другому рівні ієрархії вхідні дані (нові моделі першого рівня) на основі знань другого рівня перетворюються в нові моделі двохоперандних операцій, які в свою чергі розглядаються як для виводу нових знань другого рівня і як вхідні дані для третього рівня ієрархії системи. Аналогічні взаємозв’язки мають другий і третій рівні ієрархії, а також третій і четвертих рівень. Тому в даній системі знання забезпечують зв'язок між вхідними моделями і алгоритмами взаємоперетворення моделей для синтезу моделей наступного рівня інтеграції. В класичному вигляді правила формального виведення можуть знайти лише обмежене застосування для узгодження вимог між рівнями ієрархії.

Обмеження на використання запропонованою ієрархічної системи не залежно від потужності засобів обчислювальної техніки пов’язані з комбінаторним зростанням кількості СЕТ-операцій при збільшенні кількості Сі-квантів інформації. Кількість одноопераднних nСі-квантових СЕТ-операції визначається як $2^n!$ [41]. При побудові двохоперандних nСі-квантових СЕТ-операції на основі кортежів з k одноопераднних СЕТ-операції їх кількість буде визначатися як $C_{2^n}^{k} = \frac{2^n!}{k!(2^n!-k)!}$. На основі кожної

синтезованої двохоперандної СЕТ-операції буде синтезуватися група модифікованих операцій з точністю до перестановки. Кількість модифікованих операцій в групі визначається як $k!$. За умови $k = 2^m$, реалізувати побудову групи операцій можливо на основі використання групи mCi-квантових одноопераднних СЕТ-операції [12].

Висновки по розділу 5

Вперше побудована модель ієрархічної інформаційної системи моделювання і дослідження симетричних і несиметричних СЕТ-операцій, на основі методів синтезу СЕТ-операцій і груп СЕТ-операцій, шляхом вдосконалення моделей, методів і технології побудови комутативних і некомутативних СЕТ-операції, а також генераторів псевдовипадкових наборів СЕТ-операцій, що дозволило встановлювати нові залежності між моделями синтезу симетричних і несиметричних операцій, які приводять до розширення взаємозв'язків між моделями ієрархічних рівнів інформаційної системи, реалізація якої забезпечить експериментальну підтримку для побудову перспективних стійких мало ресурсних алгоритмів потокового шифрування.

1. Основним елементом малоресурсної системи потокового СЕТ-шифрування е генератор псевдовипадкової послідовності СЕТ-операцій з точністю до перестановки. Тому будувати високоефективні малорксурсні потокові шифри без результатів дослідження генераторів псевдовипадкових послідовностей СЕТ-операцій не представляється можливим.

2. В процесі дослідження генераторів послідовності несиметричних СЕТ-операцій з точністю до перестановки другого операнда було встановлено наступне:

– в процесі модифікації двохоперандної СЕТ-операції набір одноопераднних операцій не змінюється, а міняється лише їх послідовність,

отримані модифіковані СЕТ-операції будуть мати однакові криптографічні властивості, тому що реалізують однакові набори таблиць підстановок;

– застосування лише однієї пари (прямої та оберненої) несиметричних двохоперандних СЕТ-операцій разом із набором прямих одноопераднних дозволяє реалізувати всі генератори з точністю до перестановки операнда, що суттєво спрощує алгоритми СЕТ-шифрування [7].

3. В процесі дослідження генераторів послідовності несиметричних СЕТ-операцій з точністю до перестановки першого операнда було встановлено наступне:

– в процесі модифікації несиметричної двохоперандної СЕТ-операцій з змінюється математична модель двохоперандної СЕТ-операції за рахунок модифікації моделей одноопераднних СЕТ-операцій, що приводить до модифікації таблиць підстановки;

– якщо при шифруванні інформації генератор реалізує модифікацію СЕТ-операції з точністю до перестановки першого операнда, то для розшифрування необхідно використовувати генератор обернених СЕТ-операції точністю до перестановки результату криптографічного перетворення;

– збільшення кількості одноопераднних СЕТ-операцій при використанні групи модифікованих несиметричних СЕТ-операцій з точністю до перестановки першого операнду забезпечує збільшення кількості таблиць підстановки які реалізується в процесі шифрування і як наслідок збільшення криптостійкості алгоритму шифрування.

3. Отримані результати досліджень стали теоретичною основою для побудови моделі ієрархічної інформаційної системи моделювання і дослідження симетричних і несиметричних СЕТ-операцій.

– реалізація моделі даної інформаційної системи забезпечує розширення спектру аналізуємих операцій з 96 симетричних 2Сі-квантових

СЕТ-операцій які допускають перестановку операндів до 576 симетричних та несимньричних 2Сі-квантових СЕТ-опрерацій які допускають перестановку операндів і до 10623 2Сі-квантових СЕТ-опрерацій які недопускають перестановку операндів. Дана інформаційна система забезпечить дослідження систем потокового шифрування в яких може бути використано $65 \cdot 10^{35}$ 3Сі-квантових несиметричних двохоперандних СЕТ-операцій, з яких 1 625 702 400 операцій, що допускають перестановку операндів.

– практичне застосування даної інформаційної системи створить необхідні інформаційну базу для дослідження можливості побудови малоресурсних систем потокового шифрування на основі застосування не комутативних взаємно обернених СЕТ-операцій.

Результати розділу опубліковані: [5], [6], [7], [12], [13], [15], [16].

ВИСНОВКИ

У дисертаційному дослідженні вирішено важливу науково-технічну задачу підвищення продуктивності наукових досліджень СЕТ-операцій при побудові перспективних стійких алгоритмів потокового шифрування на основі розширення можливостей ієрархічної інформаційної системи моделювання і дослідження СЕТ-операцій за рахунок встановлення нових і уточнення існуючих взаємозв'язків між моделями ієрархічних рівнів, які в сукупності забезпечать автоматизований синтез і аналіз симетричних та несиметричних одноопераднних і багатоопераднних СЕТ-операцій, а також генераторів їх псевдовипадкових послідовностей для потокового СЕТ-шифрування.

1. Удосконалено технологію побудови удосконалених моделей некомутативних двохрозрядних двохоперандних СЕТ-операції за результатами експерименту. За результатами аналізу сценаріїв потокового шифрування які базуються на використанні комутативних і не комутативних двохоперандних СЕТ-операцій, а також особливостей застосування симетричних і несиметричних двохоперандних СЕТ-операцій які допускають перестановку операндів визначено необхідність розширення можливості технології побудови симетричних двохоперандних СЕТ-операцій до симетричних і несиметричних двохоперандних СЕТ-операцій. В процесі дослідження послідовності дискретних перетворень на основі яких, за результатами експерименту, будуються удосконалені моделі двохоперандних СЕТ-операцій до і після перестановки операндів були встановлені взаємозв'язки між даними операціями. Отримані взаємозв'язки забезпечили можливість удосконалення технології побудови удосконалених моделей комутативних двохоперандних СЕТ-операцій до синтезу комутативних і некомутативних двохоперандних СЕТ-операцій. Крім того отримані взаємозв'язки забезпечили можливість зменшення складності моделювання некомутативних СЕТ-операцій на основі реалізації прямого переході від

побудованої моделі СЕТ-операції до моделі СЕТ-операції з переставленими операндами. Сутність удосконалення полягає в заміні повторного використання технології для знаходження удосконаленої моделі після перестановки операндів на зміну змінних в удосконаленій моделі СЕТ-операції до перестановки операндів, що суттєво спрощує побудову удосконаленої моделі двохоперандної операції після перестановки операндів.

2. Удосконалено метод синтезу двохоперандних двохрозрядних операцій криптографічного перетворення. За результатами побудови моделей двох розрядних двохоперандних СЕТ-операцій, які допускають перестановку операндів і належать до однієї групи з точністю до результату перетворення інформації, було встановлено взаємозв'язки між моделями СЕТ-операцій в групі, що дозволило адаптувати метод синтезу моделей симетричних комутативних СЕТ-операцій для синтезу прямих несиметричних не комутативних СЕТ-операцій. Моделі обернених несиметричних не комутативних СЕТ-операцій необхідно будувати за результатами обчислювального експерименту, або реалізацією запропонованої послідовності дискретних перетворень. Удосконалено метод синтезу двохоперандних двохрозрядних операцій криптографічного перетворення забезпечив синтез груп несиметричних операцій подвійного циклу на основі заданих несиметричних не комутативних СЕТ-операцій.

3. Удосконалено метод побудови двохрозрядних двохоперандних операцій які допускають перестановку операндів. В процесі моделювання множини несиметричних двохоперандних двохрозрядних операцій подвійного циклу на основі дублювання операцій для різних сценаріїв шифрування було встановлено можливість синтезу двохоперандних операцій, яка допускають перестановку операндів шляхом поєднання одноопераднних операцій. В процесі синтезу прямих і обернених двохоперандних СЕТ-операцій, які допускають перестановку операндів встановлено встановлено взаємозв'язки і обмеження які відображають особливості синтезу СЕТ-операцій криптографічного перетворення, при

різних моделях перетворення першого операнду. Отримані взаємозв'язки і обмеження дозволили удосконалити метод побудови двохрозрядних двохоперандних операцій і забезпечити моделювання повної множини двохоперандних операцій, які допускають перестановку операндів.

4. Вперше побудована модель ієрархічної інформаційної системи моделювання і дослідження симетричних і несиметричних СЕТ-операцій, реалізація якої забезпечить побудову перспективних стійких мало ресурсних алгоритмів потокового шифрування. В процесі функціонування інформаційна система повинна забезпечити комплексну задачу моделювання генераторів псевдовипадкових послідовностей на основі яких будуються потокові алгоритми СЕТ-шифрування. Досліджено особливості побудови генераторів псевдовипадкових послідовностей несиметричних СЕТ-операцій з точністю до перестановки першого та другого операндів. Отримані результати стали основою четвертого рівня ієрархії ієрархічної інформаційної системи моделювання і дослідження СЕТ-операцій.

5. Практична цінність дисертаційної роботи полягає в тому, що отримані наукові результати доведено здобувачем до конкретних моделей, інженерних методик розрахунку, та отриманих варіантів застосування моделей генераторів псевдовипадкових послідовностей СЕТ-операцій. На підставі проведених досліджень побудовано програмний макет ієрархічної інформаційної системи моделювання і дослідження алгоритмів потокового СЕТ-шифрування. Дана інформаційна система забезпечує розширення спектру 2Сі-квантових СЕТ-операцій, що аналізуються, та які допускають перестановку операндів з 96 симетричних до 576 симетричних та несиметричних 2Сі-квантових СЕТ-операцій які допускають перестановку операндів, а також до 10623 2Сі-квантових СЕТ-операцій які не допускають перестановку операндів. Дана інформаційна система забезпечить дослідження систем потокового шифрування в яких може бути використано до $65 \cdot 10^{35}$ несиметричних двохоперандних СЕТ-операцій, з

яких 1 625 702 400 3Сі-квантові СЕТ-операції що допускають перестановку операндів.

Результати дисертаційного дослідження впроваджено в навчальний процес Черкаського державного технологічного університету на кафедрі інформаційних технологій проектування при підготовці бакалаврів за спеціальністю 126 «Інформаційні системи та технології» в курсі лекцій з дисциплін «Системи інформаційної безпеки», а також при виконанні курсових і кваліфікаційних робіт; на кафедрі інформаційної безпеки та комп'ютерної інженерії при підготовці бакалаврів за спеціальністю 123 «Комп'ютерна інженерія» в курсі лекцій з дисциплін «Безпека програмного забезпечення», «Арифметичні та логічні структури комп'ютерів», а також при виконанні кваліфікаційних робіт магістрів за спеціальністю 123 «Комп'ютерна інженерія» освітньої програми «Системне програмування».

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. В. Рудницький, Н. Лада, В.Бабенко, В. Ларін, Т. Короткий (2025) Модель побудови множини симетричних двохоперандних СЕТ-операцій, які допускають перестановку операндів шляхом поєднання одноопераднихопераций. Innovative Technologies and Scientific Solutions for Industries. Харківський національний університет радіоелектроніки та ДП «Південний національний конструкторсько-дослідний інститут аерокосмічної промисловості» №3. 2025. – с .126-136. (SCOPUS, у фаховому виданні)

DOI: https://doi.org/10.30837/2522-9818.2025.3.126

2. Rudnytskyi, V., Lada, N., Herashchenko, M., Korotkyi, T. & Stebetska, T. (2024) Modeling relationships in non-commutative two-operand two-bit cet-operations of a double cycle when permuting the operands. Technology audit and production reserves. Scientific journal. Vol. 3 No 2 (77), 2024. p.30-35.
(SCOPUS, у фаховому виданні)
URL: https://journals.uran.ua/tarp/article/view/306980

DOI: 10.15587/2706-5448.2024.306980

3. Ларін В. Моделювання множин двохоперандних трьохрозрядних операцій криптоперетворення шляхом поєднання одноопераднихСЕТ-операцій. / В.В. Ларін, М.Ю. Гусак, Т.К. Короткий, О.М. Гук, О.Л. Кащишин // Збірник наукових праць Харківського національного університету Повітряних Сил. – Х.: ХНУПС, 1 (83), 2025. DOI: https://doi.org/10.30748/zhups.2025.83.06 – С. 56 – 62. (У фаховому виданні)

4. Рудницький С.В., Ларін В.В., Підласий Д.А., Короткий Т.К. Синтез двохоперандних двохрозрядних СЕТ-операцій шляхом поєднання одноопераднихдвохрозрядних СЕТ-операцій. Наука і техніка Повітряних Сил України. Щоквартальний науково-технічний журнал. Вип. 4(57) 2024. с.71-79 (У фаховому виданні) DOI: 10.30748/nitps.2024.57.09

5. В. Рудницький, В. Бабенко, С. Рудницький, Т. Короткий Генерація послідовності несиметричних СЕТ-операцій з точністю до перестановки

другого операнда Інформаційні технології та суспільство / [головний редактор О. Попов]. – Київ : Міжрегіональна Академія управління персоналом, 2025. – Випуск 1 (16). – С/221-226. (У фаховому виданні)

6. Рудницький В.М., Бабенко В.Г., Рудницький С.В., Короткий Т.К., Ковтюх В.А. Особливості груп несиметричних сет-операцій синтезованих з точністю до перестановки першого операнда. Вчені записки ТНУ імені В.І. Вернадського. Серія: Технічні науки. Том 36 (75) № 4 2025 – С. 265-271. (У фаховому виданні)
URL:https://www.tech.vernadskyjournals.in.ua/journals/2025/4_2025/part_2/37.pf

7. Semenov, S.; Rudnytskyi, V.; Lada, N.; Krivtsun, V.; Korotkyi, T.; Zazhoma, V.; Wasiuta, O. Stream Encryption Cryptographic Systems Based on Asymmetric Cet Operations with an Accuracy of Permutation. *Appl. Sci.* 2026, *16*, 4987. https://doi.org/10.3390/app16104987 (SCOPUS)

8. Рудницький В. М., Лада Н. В., Рудницька Ю. В., Короткий Т. К. Моделювання симетричних двохоперандних операцій криптографічного кодування на основі об'єднання одноопераднних операцій. Сучасна спеціальна техніка, 2021. №4 с. 32-38. (У фаховому виданні)

9. Короткий Т. К. Дослідження і синтез некомутативних двохрозрядних двохоперандних СЕТ-операцій які допускають перестановку операндів. Технології розвитку безпілотних систем. Том 1. Малоресурсний захист інформації в безпілотних системах. Монографія / під ред. В.М. Рудницького. – Черкаси : видавець Вовчок О.Ю., 2025. –с165-205. ISBN 978-617-7508-50-1

10. V. Rudnytskyi, N. Lada , V. Larin, O. Melnyk, T. Stabetska, T. Korotkyi, D. Pidlasyi Usage of non-commutative two-operand CET-operations in limited resources stream ciphers Journal of Xidian University Volume 18 – Issue 5 – May 2024 Page No: 1105-1120.
URL: https://doi.org/10.5281/Zenodo.11253625

11. Rudnytskyi, V., Lada, N., Larin, V., Tkachenko, V., Korotkyi, T., Pidlasyi, D. & Tarasenko, D. (2024). Information system for modeling and research of pseudorandom sequences of CET-operations for post quantum stream

encryption systems. Journal of Xidian University. Vol. 18, Issue 7, July 24, 1284 – 1298. (SCOPUS) URL: https://xadzkjdx.cn/index.php/volume-18-issue-7-july-24/ DOI:https://doi.org/10.5281/Zenodo.13096683

12. Рудницька Ю. В. Короткий Т. К. Інформаційна технологія моделювання та дослідження симетричних СЕТ-операцій. Проблеми інформатизації : Десята міжнар. наук.-техн. конф.: тези доп. Черкаси – Баку – Бельсько-Бяла – Харків, 24 – 25 листоп. 2022 р. Черкаси: ЧДТУ; Баку: ВА ЗС АР, Бельсько-Бяла: УТіГН, Харків: НТУ «ХПІ», 2022. Т. 1. С. 40.

13. Рудницький В.М., Ларін В.В., Лада Н.В, Короткий Т.К. Сучасний стан та перспективи розвитку СЕТ-шифрування / Воєнні інновації в сучасних війнах: Збірник тез Міжнародного академічного форуму/Центральний науково-дослідний інститут Збройних Сил України – К.: 7БЦ, 2024. – с.39-40.

14. Короткий Т.К, Ковтюх В.А. Моделювання і дослідження генераторів двохоперандних СЕТ-операцій для мало ресурсної криптографії. Актуальні проблеми розвитку сучасної науки: виклики та перспективи : збірник тез Міжнародної науково-практичної конференції здобувачів вищої освіти і молодих вчених (м. Запоріжжя, 29 квіт.). Запоріжжя : ЗНУ, 2025. с.472.

URL: https://dspace.znu.edu.ua/jspui/handle/12345/25952

15. Рудницький В. М., Лада Н. В., Короткий Т. К. Вдосконалення технології побудови некомутативних СЕТ-операцій. Сучасні напрямки розвитку інформаційно-комунікаційних технологій та засобів управління. Тези доповідей 15 міжнародної науково-технічної конференції 24-25 квітня 2025 р. Том 1: секції 1, 5. Баку-Харків-Жиліна-2025. С.41.

URL: https://doi.org/10.32620/ICT.25.t1

16. Рудницький В.М., Ларін В.В., Нікорчук А.І., Короткий Т.К. Особливості застосування малоресурсної криптографії в безпілотних комплексах. Проблемні питання щодо експлуатації та відновлення автобронетанкової техніки в Національній гвардії України:. Тези доповіді науково-практичної конференції 27 травня 2025р. м.Золочів. Харків НАНГУ 2025. с. 35–37.

17. Yalamuri, G., Honnavalli, P. & Eswaran, S.(2022). A Review of the Present Cryptographic Arsenal to Deal with Post-Quantum Threats. Procedia Comput. Sci. 215, 834–845. https://doi.org/10.1016/j.procs.2022.12.086.

18. Zeadallya, S., Das, A.K., & Sklavos, N. (2019). Cryptographic technologies and protocol standards for Internet of Things. Internet Things. Elsevier, 14. URL: https://doi.org/10.1016/j.iot.2019.100075

19. Aboshosha, B., Dessouky, M. & El-Sayed, A. (2019). Energy Efficient Encryption Algorithm for Low Resources DevicesPDF. The Academic Research Community publication. ISSN 2663-4023(EBQL), 3(3), 26–37.
URL: https://doi.org/10.21625/archive.v3i3.520.

20. Thakor, V., Razzaque, A. & Khandaker, M. (2021). Lightweight Cryptography Algorithms for Resource-Constrained IoT Devices: A Review, Comparison and Research Opportunities.IEEE Access, 9,28177–28193. URL: https://doi.org/10.1109/ACCESS.2021.3052867.

21. Kumar, C., Prajapati, S. & Verma, R. (2022). A Survey of Various Lightweight Cryptography Block ciphers for IoT devices.IEEE International Conference on Current Development in Engineering and Technology (CCET),1–6. https://doi.org/10.1109/CCET56606.2022.10080556.

22. Zakaria, A., et al. (2023). Systematic literature review: Trend analysis on the design of lightweight block cipher. Journal of King Saud University - Computer and Information Sciences, 35(5), 101550. URL: https://doi.org/10.1016/j.jksuci.2023.04.003

23. Suomalainen, J., et al. (2018). Evaluating the Efficiency of Physical and Cryptographic Security Solutions for Quantum Immune IoT. Cryptography, 2(1):5. URL: https://doi.org/10.3390/cryptography2010005

24. Manifavas, C., Hatzivasilis, G., Fysarakis, K. & Rantos, K. (2012). Lightweight cryptography for embedded systems a comparative analysis. In: 6th International Workshop on Autonomous and Spontaneous Security SETOP 2012, Springer, LNCS, 8247, 333–349. URL: https://doi.org/10.1007/978-3-642-54568-9_21.

25. Yasmin, N., Gupta, R. (2023). Modified lightweight cryptography scheme and its applications in IoT environment. Int. j. inf. tecnol. 15, 4403–4414 URL: https://doi.org/10.1007/s41870-023-01486-2.

26. Thabit, F., Can, O., Aljahdali, A.O., Al-Gaphari, G.H. & Alkhzaimi, H.A. (2023). Cryptography algorithms for enhancing IoT security. Internet of Things, 22, 100759. ISSN 2542-6605. URL: https://doi.org/10.1016/j.iot.2023.100759.

27. Khudoykulov, Z. (2024). A Comparison of Lightweight Cryptographic Algorithms. In: Aliev, R.A., et al. 12th World Conference “Intelligent System for Industrial Automation” (WCIS-2022). WCIS 2022. Lecture Notes in Networks and Systems, vol 912. Springer, Cham. URL: https://doi.org/10.1007/978-3-031-53488-1_36

28. McKay, K.A., Bassham, L.,Turan,M.S., & Mouha,N. (2017). Report on lightweight cryptography. URL: https://doi.org/10.6028/nist.ir.8114

29. ISO/IEC 29192-2:2012. (2012). Information technology Security techniques Lightweight cryptography Part 2: Block ciphers. Retrieved from URL: https://www.iso.org/obp/ui#iso:std:iso-iec:29192:-2:ed-2:v1:en.

30. Banik, S., Bogdanov, A., Isobe, T., Shibutani, K., Hiwatari, H., Akishita, T., & Regazzoni, F. (2015). Midori: A Block Cipher for Low Energy.Advances in Cryptology –ASIACRYPT 2015, 411–436. URL: https://doi.org/10.1007/978-3-662-48800-3_17

31. Eisenbarth, T., Gong, Z., Güneysu, T., Heyse, S., Indesteege, S., Kerckhof, S., Koeune, F., Nad, T., Plos, T., Regazzoni, F.,Standaert, F.-X., & van Oldeneel tot Oldenzeel, L. (2012). Compact Implementation and Performance Evaluation of Block Ci-phers in ATtiny Devices.Progress in Cryptology - AFRICACRYPT 2012, 172–187. URL: https://doi.org/10.1007/978-3-642-31410-0_11

32. Архітектура CET-операцій і технології потокового шифрування. Architecture of CET-operations and stream encryption technologies: монографія / В. М. Рудницький, Н. В. Лада, Г. А. Кучук, Д. А. Підласий. – Черкаси: видавець Пономаренко Р.В., 2024. – 374 с.

33. Rudnytskyi, V., Lada, N., Pochebut, M., Melnyk, O. & Tarasenko, Ya. (2023) Increasing the cryptographic strength of CET-encryption by ensuring the transformation quality of the information block. The 13th IEEE International Conference on Dependable Systems, Services and Technologies, DESSERT'2023 13-15 October, 2023, Athens, Greece

34. Рудницький В.М. Моделювання логічного пристрою для систем захисту інформації / В.М. Рудницький, Н.М. Пантелєєва, В.Г. Бабенко // Проблеми і перспективи розвитку банківської системи України: Зб. наук. пр. - Суми. – 2006. - Т. 18. – С. 185-190.

35. Бабенко В.Г. Технологія визначення спеціальних логічних функцій для систем захисту інформації / В.Г. Бабенко, В.М. Рудницький, Т.В. Дахно // Вісник інженерної академії України. – 2007. – Вип. 3-4. – С.64-67.

36. Рудницький В.М. Визначення множини логічних функцій для синтезу цифрових пристроїв систем захисту інформації / В.М. Рудницький, Н.М. Пантелєєва, В.Г. Бабенко // Системи управління, навігації та зв'язку: Зб. наук. пр. – Київ. - 2008. – Вип. 4(8). – С. 155-157

37. Рудницький В.М. Модель уніфікованого пристрою криптографічного перетворення інформації / В.М. Рудницький, В.Г. Бабенко // Системи обробки інформації: Зб. наук. пр. – Харків. – 2009. – Випуск . – С. 173-177.

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

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

40. Криптографическое кодирование: методы и средства реализации (часть 2): монография / В.Н. Рудницкий, В.Я. Мильчевич, В.Г. Бабенко, Р.П. Мельник, С.В. Рудницкий, О. Г. Мельник. – Х. : Изд-во «Щедрая усадьба плюс», 2014. – 224 с.

41. Бабенко Віра. Класифікація трирозрядних елементарних функцій для криптографічного перетворення інформації / Віра Бабенко, Ольга Мельник, Руслан Мельник // Безпека інформації: наук. журнал. – Київ : НАУ, 2013. – Том 19. – № 1. – С. 56–59.

URL: https://jrnl.nau.edu.ua/index.php/Infosecurity/issue/view/220.

42. Бабенко В. Г. Дослідження способів запису трьохрозрядних криптографічних операцій / В. Г. Бабенко, Р. П. Мельник, С. В. Рудницький // Системи управління, навігації та зв'язку : зб. наук. праць. – Вип. 1 (21), т. 2. – К. : Центр. наук.-досл. ін-т навігації і управл., 2012. – С. 170–173.

43. Рудницький В. М., Бабенко В. Г., Рудницький С. В. Метод синтезу матричних моделей операцій криптографічного перекодування інформації. Захист інформації : наук.-практ. журн. 2012. № 3 (56). С. 50–56.

44. Голуб С. В., Бабенко В. Г., Рудницький С. В. Метод синтезу операцій криптографічного перетворення на основі додавання за модулем два Системи обробки інформації: зб. наук. пр. Харків: ХУПС ім. І. Кожедуба, 2012. Вип. 3 (101), т. 1. С. 119–122.

45. 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 : зб. наук. праць. Київ: Центр. наук.-досл. ін-т навігації і управл., 2012. Вип. 2 (22). С. 163–168.

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

47. Рудницький В. М., Бабенко В. Г., Стабецька Т. А. Узагальнений метод синтезу обернених нелінійних операцій розширеного матричного криптографічного перетворення. Системи обробки інформації: зб. наук. пр. Харків: ХУПС ім. І. Кожедуба, 2014. Вип. 6 (122). С. 118–121.

48. Миронюк Т. В. Визначення елементарних операцій базової групи перестановок, керованих інформацією / Т. В. Миронюк // Вісник Черкаського державного технологічного університету. – 2016. – № 2. - С. 100–105.

49. Миронюк Т. В. Дискретна модель базових груп операцій перестановок, керованих інформацією, для криптоперетворення / Т. В. Миронюк, Є. В. Ланських // Smart and Young : щомісячний наук. журн. – Вип. 11-12. – Київ, 2016. – С. 58–65.

50. Рудницький В.М., Ларін В.В., Мельник О. Г, Підласий Д. А. Дискретно-казуальне представлення моделей елементарних функцій і СЕТ-операцій. Системи управління, навігації та зв'язку №4 ст.96-101.

51. Рудницкий В. Н., Мильчевич В. Я., Бабенко В. Г., Мельник Р. П., Рудницкий С.В., Мельник О. Г.: Криптографическое кодирование: методы и средства реализации (часть 2): монография Щедрая усадьба плюс, 224с. (2014).

52. Шнайер Б. Прикладная криптография. Протоколы, алгоритмы, исходные тексты на языке Си / Б. Шнайер. – М. : Изд-во ТРИУМФ, 2002. – 816 с.

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

54. Rudnytskyi, V., Lada, N. & Kozlovska, S. (2018). Technology of two operand operations construction of information cryptographic transformation by modeling results. Advanced Information Systems, 2 (4), C.26-30.

URL: http://ais.khpi.edu.ua/article/viewFile/2522-9052.2018.4.04/151747

55. Rudnytskyi, V., Babenko, V., Lada, N., Tarasenko, Ya. & Rudnytska, Yu. (2022). Constructing symmetric operations of cryptographic information encoding. Workshop on Cybersecurity Providing in Information and Telecommunication

Systems (CPITS II 2021), Oct. 26, 2021. Kyiv, Ukraine: CEUR Workshop Proceedings, 2022, 182–194. ISSN 1613-0073

56. Бабенко В.Г. Алгоритми синтезу логічних функцій для систем захисту інформації / В.Г. Бабенко, Т.В. Дахно, В.М. Рудницький // Інтегровані інформаційні технології та системи (ІІТС-2007): матеріали наук.-практ. конф. молодих учених та аспірантів, 29-31 жовт. 2007 р. – К.: НАУ, 2007. – С. 46–48.

57. Прокопенко Т. О, Рудницька Ю. В. Автоматизація проектування криптопримітивів. Проблеми інформатизації: матеріали Дев'ятої міжнар. наук.-техн. конф.: тези доп., Черкаси – Харків – Баку – Бельсько-Бяла, 16–18 листоп. 2021 р. Черкаси: ЧДТУ; Баку: ВА ЗС АР, Бельсько-Бяла: УТіГН, Харків: НТУ «ХПІ», 2021. Т. 1. С. 85

58. Daniel Jancarczyk, Volodymyr Rudnytskyi, Roksolana Breus, Mykhailo Pustovit, Olga Veselska and Ruslana Ziubina. Two-Operand Operations of Strict Stable Cryptographic Coding With Different Operands' Bits. The 5-th IEEE International Symposium on Smart and Wireless Systems within the International Conferences on Intelligent Data Acquisition and Advanced Computing Systems, 17-18 September, 2020, Dortmund, Germany.

59. J. L. Massey. An introduction to contemporary cryptology. In Proceedings of the IEEE, vol. 76, no. 5, pp. 533-549, May 1988.

60. Schneier B. Applied cryptography. Protocols, algorithms, source texts in C language. - M.: Тріумф, 2002. – 816.

61. Singh S. The Code Book: The Secret History of Codes and Code-Breaking. – HarperCollins Publishers, Jan. 1, 2011. — 402.

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

63. 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.

64. Бабенко В. Г., Лада Н. В. Синтез і аналіз операцій криптографічного додавання за модулем два. *Системи обробки інформації:* зб. наук. пр. Харків: ХУПС ім. І. Кожедуба, 2014. Вип. 2 (118). С. 116–118.

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

66. Лада Н. В. Аналіз коректності взаємозв'язків між прямими та оберненими матричними моделями операцій криптографічного перетворення інформації. *Системи управління, навігації та зв'язку: Полтава : ПНТУ, 2015. - Вип. 4 (36). - С. 73-78.*

67. 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 берез. –1 квіт. 2016 р.). С. 17.

68. Лада Н. В. Використання графічного представлення операцій для виявлення їх взаємозв'язків в моделях операцій криптографічного перетворення. *Проблеми інформатизації*: матеріали Четвертої міжнар. наук.-техн. конф.: тези доп., (Черкаси – Баку – Бельсько-Бяла – Полтава, 3–4 листоп. 2016 р.). Черкаси: ЧДТУ, 2016. С. 9–10.

69. Бабенко В. Г., Лада Н. В. Технологія дослідження операцій за модулем два. *Smart and Young*: щомісячний наук. журн. 2016. № 11–12. Ч. 1. С. 49–54.

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

71. 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*: proceedings of the Internat. sci. conf., (St. Andrews, Scotland, UK, December, 1, 2016) / ed. N. P. Kazmyna. NGO «European Scientific Platform». Vinnytsia: PE Rogalska I. O., 2016. С. 108–111. (Шотландия, Логос)

72. 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.

73. 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.

74. Лада Н. В., Козловська С. Г., Рудницький С. В. Побудова математичної групи симетричних операцій на основі додавання за модулем два. *Сучасна спеціальна техніка*: наук.-практ. журн. Київ, 2019. № 4 (59). С. 33–41.

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

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

77. Козловська С. Г. Синтез груп двохоперандних операцій криптоперетворення на основі перестановлюваних схем. *Сучасна спеціальна техніка*: наук.-практ. журн. Київ, 2018. № 4 (55). С. 47–56.

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

79. Лада Н. В., Козловська С. Г., Рудницька Ю. В. Дослідження і синтез групи симетричних модифікованих операцій додавання за модулем чотири. *Центральноукраїнський науковий вісник. Технічні науки*: зб. наук. пр. Кропивницький: КНТУ, 2019. Вип. 2 (33). С. 181–189. DOI: https://*doi*.org/10.32515/2664-262X.2019.2(33).181-189

80. Лада Н. В., Рудницький С. В., Зажома В. М., Рудницька Ю. В. Дослідження і синтез групи симетричних модифікованих операцій правостороннього додавання за модулем чотири. *Системи управління, навігації та зв'язку*: зб. наук. пр. Полтава: ПНТУ, 2020. № 1 (59). С. 93–96. DOI: https://*doi*.org/10.26906/SUNZ.2020.1.093

81. Рудницька Ю. В. Рудницький С. В. Моделювання симетричних операцій криптографічного кодування. *Проблеми інформатизації : Десята міжнар. наук.-техн. конф.:* тези доп. Черкаси – Баку – Бельсько-Бяла – Харків, 24 – 25 листоп. 2022 р. Черкаси: ЧДТУ; Баку: ВА ЗС АР, Бельсько-Бяла: УТіГН, Харків: НТУ «ХПІ», 2022. Т. 2. С. 10.

82. Рудницька Ю.В. Інформаційна технологія моделювання симетричних операцій криптографічного кодування для захищених інформаційних систем критичної інфраструктури. Дисертація на здобуття наукового ступеня доктора філософії за спеціальністю 126 «Інформаційні системи та технології» – Черкаський державний технологічний університет, Черкаси, 2023. 162с

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

84. Пристрій для виконання логічних операцій криптографічного перетворення: деклара. пат. на корисну модель 46617 Україна, МПК H03M 13/00 / Рудницький В. М., Паціра Є. В., Миронець І. В., Бабенко В. Г. № u200908000; заявл. 29.07.2009; опубл. 25.12.2009, Бюл. № 24. 3 с.

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

86. Бабенко В. Г., Лада Н. В., Лада С. В. Розширення множини двоопераднних 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.

87. Лада Н.В., Лада С.В., Шувалова Л.А., Гушлевський О.В. Дослідження результатів комп'ютерного моделювання несиметричних операцій криптоперетворення Сучасна спеціальна техніка: науково-практичний журнал. Київ, 2020. № 4 (63). С. 33-47. (У фаховому виданні)

88. Рудницький В.М., Лада Н. В., Лада С.В. Дослідження множин несиметричних вохоперандних операцій з подвійним циклом криптоперетворення. Збірник праць матеріалів дев'ятої між нар. Наук.-техн. конф. «Датчики, прилади та системи -2021», Черкаси-Херсон-Лазурне, вересень 2021.С. 78-80.

89. Lada N., Dzyuba V., Breus R., Lada S. Synthesis of sets of non-symmetric two-operand two-bit crypto operations within the permutation accuracy Technology audit and production reserves, 2020, № 2/2 (52), С. 28-31. - DOI: 10.15587/2312-8372.2020.202099

90. Рудницький В.М., Лада Н. В., Лада С.В. Аналіз методів синтезу операцій криптографічного кодування для побудови груп несиметричних двохоперандних операцій подвійного циклу. Проблеми інформатизації: матеріали Дев'ятої міжнар. наук.-техн. конф.: тези доп., (Черкаси – Харків Баку – Бельсько-Бяла, 18–19 листоп. 2021 р.). Черкаси: ЧДТУ; Баку: ВА ЗС АР, Бельсько-Бяла: УТіГН, Харків: НТУ «ХПІ», 2021. Т.1 С. 80.

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

92. V. Rudnytskyi, I. Opirskyy, O. Melnyk, M. Pustovit The implementation of strict stable cryptographic coding operations Сучасні інформаційні системи Щоквартальний науково-технічнийй журнал – Х.: НТУ «ХПІ» 2019, Т 3, №4 С. 109-114

93. Синтез групи операцій строгого стійкого криптографічного кодування для побудови потокових шифрів / Рудницький В. М., Опірський І.Р., Мельник О.Г, Пустовіт М. О.// Науковий журнал «Безпека інформації» Том 24, № 3 (2018) – с. 195-200

94. Лада Н. В., Бреус Р. В., Рудницька Ю. В., Висоцький С. В. Аналіз групи двохоперандних симетричних операцій криптоперетворення. *Проблеми інформатизації: матеріали Сьомої міжнар. наук.-техн. конф.*: тези доп., Черкаси – Харків – Баку – Бельсько-Бяла, 13–15 листоп. 2019 р. Черкаси: ЧДТУ; Баку: ВА ЗС АР, Бельсько-Бяла: УТіГН, Харків: НТУ «ХПІ», 2019. Т. 1. С. 85.

95. V. Rudnytskyi, N. Lada, V. Babenko, H. Kuchuk, D. Pidlasyi, D. Kamak and Ye. Ivashchenko Modeling of groups of dual-cycle non-commutative two-operand CET-operations. Journal of Xidian University Volume 18 – Issue 10 – October 2024 Page No: 916-958.
Doi.10.37896/jxu18.10/069
URL: https://xadzkjdx.cn/index.php/volume-18-issue-10-october-24/

96. Рудницький В.М., Лада Н.В., Федотова-Півень І.М., Пустовіт М.А., Нестеренко О.Б. Синтез обернених двохрозрядних двохоперандних операцій строгого стійкого криптографічного кодування *Сучасна спеціальна техніка, науково-практичний журнал: Київ 2018. 4(55)* С. 76-82.

97. Федотова-Пивень И. М., Лада Н. В., Канашевич Г. В., Пустовіт М. А. Технологія побудови двохоперандної чотирьохрозрядної операції мінімальної складності для строгого стійкого криптографічного кодування Системы управления, навигации и связи, Полтава: ПНТУ, 2019, выпуск 4 (56). С. 95-99.

98. Рудницький В.М., Лада Н.В., Федотова-Півень І.М., Пустовіт М.А., Нестеренко О.Б. Побудова двохрозрядних двохоперандних операцій строгого

стійкого криптографічного кодування *Системи управління, навігації та зв'язку: Полтава : ПНТУ* 2018, выпуск 6 (52). С. 113-115.

99. І.М. Федотова-Півень, Н.В. Лада, О.Г. Мельник, М.О. Пустовіт Технологія побудови оберненої двохоперандної чотирьохрозрядної операції мінімальної складності для строгого стійкого криптографічного кодування *Системи обробки інформації: зб. наук. пр. – Х.: Харк. ун-т Повітряних Сил ім. Івана Кожедуба, 2019.– Вип. 1(156)–С.101-105.*

100. V. Rudnitsky, R. Berdybaev, R. Breus, N. Lada, M.Pustovit Synthesis of reverse two-bit dual-operated strictly straight cryptographic coding on the basis of another operation Сучасні інформаційні системи Щоквартальний науково-технічнийй журнал – Х.: НТУ «ХПІ» 2019, Т 3, №4 С. 109-114

101. Rudnytskyi V., Lada N., Pochebut M., Melnyk O., Tarasenko Ya. Increasing the cryptographic strength of CETencryption by ensuring the transformation quality of the information block. 13th International Conference on Dependable Systems, Services and Technologies (DESSERT), October 13-15, 2023, Athens, Greece. 2023. P. 1-6.
DOI: 10.1109/DESSERT61349.2023.10416546.

102. Лада Н. В., Бреус Р. В., Лада С. В. Генерація моделей прямих і обернених двохрозрядних двохоперандних операцій строгого стійкого криптографічного кодування. Science and Education a New Dimension Natural and Technical science: Budapest, 2020. V. 224, p. 31-37

103. Лада Н. В., Головняк Д. В., Сапожніков С. К. Механізми практичної реалізації несиметричних двохоперандних СЕТ-операцій. Проблеми інформатизації Тези доповідей одинадцятої міжнародної науково-технічної конференції (16-17 листопада 2023 року) Том 2: секції 3, 6 Баку – Харків – Бельсько-Бяла. 2023 с.34.

Додаток 1

Результати обчислювального експерименту по синтезу несиметричних двохоперандних двохрозрядних операцій криптоперетворення на основі кортежів одноопераднних операцій

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

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

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

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

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

ДОДАТОК 2

Список публікацій, в яких опубліковані основні наукові результати дисертації

Список публікацій здобувача:

1. Rudnytskyi V., Semenov S., Lada N., Babenko V., Larin V., Korotkyi T. The model for constructing a set of symmetric two-operand set operations that allow perversion of operands by combining one-operand operations. *Innovative Technologies and Scientific Solutions for Industries*. 2025. № 3(33). P. 126–136. DOI: https://doi.org/10.30837/2522-9818.2025.3.126. URL: https://journals.uran.ua/itssi/article/view/340558 (Scopus, фахове видання)

2. Rudnytskyi V., Lada N., Herashchenko M., Korotkyi T., Stabetska T. Modeling relationships in non-commutative two-operand two-bit CET-operations of a double cycle when permuting the operands. *Technology Audit and Production Reserves*. 2024. Vol. 3, No. 2(77). P. 30–35. DOI: https://doi.org/10.15587/2706-5448.2024.306980. URL: https://journals.uran.ua/tarp/article/view/306980 (Scopus, фахове видання)

3. Ларін В. В., Гусак М. Ю., Короткий Т. К., Гук О. М., Кащишин О. Л. Моделювання множин двохоперандних трьохрозрядних операцій криптоперетворення шляхом поєднання одноопераднних СЕТ-операцій. *Збірник наукових праць Харківського національного університету Повітряних Сил*. 2025. № 1(83). С. 56–62. DOI: https://doi.org/10.30748/zhups.2025.83.06. Режим доступу: https://journal-hnups.com.ua/index.php/zhups/article/view/1922 (фахове видання)

4. Рудницький С. В., Ларін В. В., Підласий Д. А., Короткий Т. К. Синтез двохоперандних двохрозрядних СЕТ-операцій шляхом поєднання одноопераднних двохрозрядних СЕТ-операцій. *Наука і техніка Повітряних* Сил України. 2024. № 4(57). С. 71–79. DOI: https://doi.org/10.30748/nitps.2024.57.09. Режим доступу: https://journal-hnups.com.ua/index.php/nitps/article/view/1868 (фахове видання)

5. Рудницький В., Бабенко В., Рудницький С., Короткий Т. Генерація послідовності несиметричних СЕТ-операцій з точністю до перестановки другого операнда. *Інформаційні технології та суспільство*. 2025. Вип. 1(16). С. 221–226. DOI: https://doi.org/10.32689/maup.it.2025.1.28. Режим доступу: https://journals.maup.com.ua/index.php/it/article/view/4827 (фахове видання)

6. Рудницький В. М., Бабенко В. Г., Рудницький С. В., Короткий Т. К., Ковтюх В. А. Особливості груп несиметричних СЕТ-операцій синтезованих з точністю до перестановки першого операнда. *Вчені записки ТНУ імені В. І. Вернадського. Серія: Технічні науки*. 2025. Т. 36(75), № 4. С. 265–271. DOI: https://doi.org/10.32782/2663-5941/2025.4.2/35. Режим доступу: https://www.tech.vernadskyjournals.in.ua/journals/2025/4_2025/part_2/37.pdf (фахове видання)

7. Semenov S., Rudnytskyi V., Lada N., Krivtsun V., Korotkyi T., Zazhoma V., Wasiuta O. Stream Encryption Cryptographic Systems Based on Asymmetric CET Operations with an Accuracy of Permutation. *Applied Sciences*. 2026. Vol. 16. Article 4987. DOI: https://doi.org/10.3390/app16104987. URL: https://www.mdpi.com/2076-3417/16/10/4987 (Scopus, WoS)

8. Рудницький В. М., Лада Н. В., Рудницька Ю. В., Короткий Т. К. Моделювання симетричних двохоперандних операцій криптографічного кодування на основі об'єднання одноопераднних операцій. *Сучасна спеціальна техніка*. 2021. № 4. С. 32–38. (фахове видання)

9. Короткий Т. К. Дослідження і синтез некомутативних двохрозрядних двохоперандних СЕТ-операцій які допускають перестановку операндів. *Технології розвитку безпілотних систем. Том 1. Малоресурсний захист інформації в безпілотних системах : монографія* / за ред. В. М. Рудницького. Черкаси : Видавець Вовчок О. Ю., 2025. С. 165–205. (розділ монографії)

10. Rudnytskyi V., Lada N., Larin V., Melnyk O., Stebetska T., Korotkyi T., Pidlasyi D. Usage of non-commutative two-operand CET-operations in limited resources stream ciphers. *Journal of Xidian University*. 2024. Vol. 18, Issue 5.

P. 1105–1120. DOI: https://doi.org/10.5281/Zenodo.11253625. URL: https://repositsc.nuczu.edu.ua/bitstream/123456789/21303/1/110-May-10807.pdf

11. Rudnytskyi V., Lada N., Larin V., Tkachenko V., Korotkyi T., Pidlasyi D., Tarasenko D. Information system for modeling and research of pseudorandom sequences of CET-operations for post quantum stream encryption systems. *Journal of Xidian University*. 2024. Vol. 18, Issue 7. P. 1284–1298. DOI: https://doi.org/10.5281/Zenodo.13096683. URL: https://xadzkjdx.cn/index.php/volume-18-issue-7-july-24/.

Список публікацій, які засвідчують апробацію матеріалів дисертації:

12. Рудницька Ю. В., Короткий Т. К. Інформаційна технологія моделювання та дослідження симетричних СЕТ-операцій. *Проблеми інформатизації : тези доп. Десятої міжнар. наук.-техн. конф.* Черкаси – Баку – Бельсько-Бяла – Харків, 24–25 листопада 2022 р. Черкаси : ЧДТУ, 2022. Т. 1. С. 40.

13. Рудницький В. М., Ларін В. В., Лада Н. В., Короткий Т. К. Сучасний стан та перспективи розвитку СЕТ-шифрування. *Воєнні інновації в сучасних війнах : збірник тез Міжнародного академічного форуму*. Київ : Центральний науково-дослідний інститут Збройних Сил України, 2024. С. 39–40.

14. Короткий Т. К., Ковтюх В. А. Моделювання і дослідження генераторів двохоперандних СЕТ-операцій для малоресурсної криптографії. *Актуальні проблеми розвитку сучасної науки: виклики та перспективи : збірник тез Міжнародної науково-практичної конференції здобувачів вищої освіти і молодих вчених*. Запоріжжя, 29 квітня 2025 р. Запоріжжя : ЗНУ, 2025. С. 472. URL: https://dspace.znu.edu.ua/jspui/handle/12345/25952.

15. Рудницький В. М., Лада Н. В., Короткий Т. К. Вдосконалення технології побудови некомутативних СЕТ-операцій. *Сучасні напрямки розвитку інформаційно-комунікаційних технологій та засобів управління : тези доповідей 15-ї міжнародної науково-технічної конференції*. Баку–

Харків–Жиліна, 24–25 квітня 2025 р. Т. 1. Харків, 2025. С. 41. DOI: https://doi.org/10.32620/ICT.25.t1.

16. Рудницький В. М., Ларін В. В., Нікорчук А. І., Короткий Т. К. Особливості застосування малоресурсної криптографії в безпілотних комплексах. *Проблемні питання щодо експлуатації та відновлення автобронетанкової техніки в Національній гвардії України : матеріали наук.-практ. конф.*. Золочів, 27 травня 2025 р. Харків : НАНГУ, 2025.

ДОДАТОК 3

Документи про впровадження результатів дисертаційної роботи

«ЗАТВЕРДЖУЮ»

Перший проректор Черкаського державного технологічного університету

_____ Артем ГОНЧАРОВ

«___» _____ 2025р.

АКТ
впровадження результатів дисертаційної роботи
Короткого Тимофія Костянтиновича в навчальний процес кафедри інформаційної безпеки та комп'ютерної інженерії
Черкаського державного технологічного університету

Комісія у складі: професора кафедри інформаційної безпеки та комп'ютерної інженерії д.т.н., професора Бабенко В.Г., доцента кафедри інформаційної безпеки та комп'ютерної інженерії к.т.н., доцента Тазетдінова В.А., доцента кафедри інформаційної безпеки та комп'ютерної інженерії к.т.н., доцента Миронюк Т.В., розглянувши матеріали дисертаційного дослідження Короткого Тимофія Костянтиновича, встановила наступне:

При підготовці бакалаврів за спеціальністю 123 «Комп'ютерна інженерія» в курсі лекцій з дисциплін «Безпека програмного забезпечення» та «Арифметичні та логічні структури комп'ютерів» використовуються результати дисертаційного дослідження, а саме:

– метод побудови двохрозрядних двохоперандних СЕТ-операцій які допускають перестановку операндів на основі об'єднання двохрозрядних одноопераднних операцій криптографічного перетворення;

– моделі синтезу груп несиметричних двохоперандних СЕТ-операцій на основі які допускають перестановку операндів на основі об'єднання двохрозрядних одноопераднних операцій.

Наведені наукові результати використовуються при виконанні кваліфікаційних робіт магістрів за спеціальністю 123 «Комп'ютерна інженерія» освітньої програми «Системне програмування».

Професор кафедри ІБ та КІ, д.т.н., проф. Віра БАБЕНКО

Доцент кафедри ІБ та КІ, к.т.н., доц. Валерій ТАЗЕТДІНОВ

Доцент кафедри ІБ та КІ, к.т.н., доц. Тетяна МИРОНЮК

«ЗАТВЕРДЖУЮ»
Ректор Черкаського
державного технологічного
університету

_____ Олег ГРИГОР
_____ 2025р.

АКТ
впровадження результатів дисертаційної роботи
Короткого Тимофія Костянтиновича в навчальний процес кафедри
інформаційних технологій проектування
Черкаського державного технологічного університету

Комісія у складі: завідувача кафедри інформаційних технологій проектування д.т.н., професора Прокопенко Т.О., доцента кафедри інформаційних технологій проектування к.т.н., доцента Лавданської О.В., доцента кафедри інформаційних технологій проектування к.т.н., доцента Рудницького С.В., розглянувши матеріали дисертаційного дослідження Короткого Тимофія Костянтиновича, встановила наступне:

1. При підготовці бакалаврів за спеціальністю 126 «Інформаційні системи та технології» в курсі лекцій з дисциплін «Системи інформаційної безпеки» використовуються результати дисертаційного дослідження, а саме:

– удосконалена технологія побудови моделей некомутативних двохрозрядних двохоперандних СЕТ-операції;

– модель ієрархічної інформаційної системи моделювання і дослідження симетричних і несиметричних СЕТ-операцій, на основі методів синтезу СЕТ-операцій і груп СЕТ-операцій.

2. При виконанні курсових і кваліфікаційних робіт використовуються запропоновані методики синтезу симетричних і несиметричних СЕТ-операцій для моделювання псевдовипадкових процесів з заданими характеристиками.

Завідувач кафедри ІТП, д.т.н., професор Т.О. Прокопенко

Доцент кафедри ІТП, к.т.н., доц. О.В.Лавданська

Доцент кафедри ІТП, к.т.н., доц.. С.В. Рудницький