**ЧЕРКАСЬКИЙ ДЕРЖАВНИЙ ТЕХНОЛОГІЧНИЙ УНІВЕРСИТЕТ**
**МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ**

Кваліфікаційна наукова
праця на правах рукопису

**Рудницька Юлія Володимирівна**

**УДК 004.421.5:004.056.55**

# ДИСЕРТАЦІЯ

# ІНФОРМАЦІЙНА ТЕХНОЛОГІЯ МОДЕЛЮВАННЯ СИМЕТРИЧНИХ ОПЕРАЦІЙ КРИПТОГРАФІЧНОГО КОДУВАННЯ ДЛЯ ЗАХИЩЕНИХ ІНФОРМАЦІЙНИХ СИСТЕМ КРИТИЧНОЇ ІНФРАСТРУКТУРИ

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.

_____Ю.В. Рудницька

Науковий керівник:
**Прокопенко Тетяна Олександрівна,**
доктор технічних наук, професор

Черкаси – 2023

## *АНОТАЦІЯ*

*Рудницька Ю.В.* Інформаційна технологія моделювання симетричних операцій криптографічного кодування для захищених інформаційних систем критичної інфраструктури. – 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, 2023.

Дисертаційна робота присвячена підвищенню продуктивності наукових досліджень процесів покращення захищеності інформаційних систем критичної інфраструктури шляхом створення нових методів моделювання та аналізу симетричних операцій криптографічного кодування.

У першому розділі визначено, що одним із перспективних напрямів розвитку інформаційних систем і технологіїй є їх удосконалення для забезпечення можливості автоматизації проведення наукових досліджень направлених на підвищення захищеності інформаційних систем критичної інфраструктури. Проведено аналітичний огляду захищених інформаційних систем критичної інфраструктури який показав необхідність її постійного вдосконалення. Аналіз моделей і методів захисту інформації в інформаційних системах критичної інфраструктури показав, що вони як правило аналогічні методіам захисту інформації в інформаційних та телекомунікаційних системах, і не враховують особливості практичного застосування. Наведено результати сучасного стану наукових досліджень пов’язаних із синтезом та аналізом операцій криптографічного кодування. Дані результати показали можливість адаптації систем захисту інформації до особливостей представлення інформації, яка використовується в інформаційних систем управління об’єктами критичної інфраструктури.

Встановлено що симетричні двохоперандні операції використовуються при побудові практично всіх криптоалгоритмів, проте процесам автоматизації їх моделювання та дослідження не приділялося достатньої уваги. Формулюється мета і задачі наукового дослідження.

Другий розділ присвячений побудові методу синтезу моделей симетричних двохоперандних операцій криптографічного кодування на основі кортежів симетричних одноопераднних операцій. Для цього досліджено можливість синтезу моделей симетричних двохоперандних операцій криптографічного кодування на основі об'єднання за модулем моделей симетричних одноопераднних операцій. Досліджено можливість синтезу симетричних двохоперандних операцій криптографічного кодування на основі дублювання та об'єднання за модулем моделей симетричних одноопераднних операцій. Досліджено можливість синтезу моделей симетричних двохрозрядних двохоперандних операцій криптографічного кодування на основі кортежів симетричних одноопераднних операцій перетворення інформації. Під час проведення досліджень було встановлено якісні і кількісні характеристики різних підходів до синтезу симетричних двохоперандних операцій. На основі отриманих результатів побудовано методу синтезу моделей симетричних двохоперандних операцій криптографічного кодування на основі кортежів симетричних одноопераднних операцій та розроблено алгоритм його реалізації.

Третій розділ присвячений розробленню методу синтезу груп моделей симетричних двохоперандних операцій криптографічного кодування для блокового шифрування на основі заданої симетричної двохоперандної операції. Для цього на основі узагальнення відомих методів аналізу результатів синтезу груп симетричних модифікованих запропоновано концепцію синтезу, яка дозволяє об'єднати методи синтезу груп симетричних двохрозрядних двохоперандних операцій, які досліджувався. На основі запропонованої концепції синтезовано дві нові групи симетричних

двохоперандних операцій. Побудовані групи операцій підтвердили коректність запропонованої концепції синтезу модифікованих двохоперандних операцій. На основі запропонованої концепции синтезу та аналізу синтезованих груп симетричних двохоперандних операцій розроблено метод синтезу моделей симетричних двохоперандних операцій криптографічного кодування, та алгоритм його реалізації.

Четвертий розділ присвячено удосконаленню методів побудови інформаційних систем і інформаційних технологій моделювання і дослідження операцій криптографічного кодування. Для цього досліджено особливості реалізації методу синтезу моделей симетричних двохоперандних операцій криптографічного кодування на основі кортежів симетричних одноопераднних операцій для систем блокового шифрування. На основі отриманих практичних результатів запропоновано алгоритм пошуку симетричних комутативних двохоперандних операцій. Досліджено особливості реалізації методу синтезу груп симетричних двохоперандних операцій криптографічного кодування на основі вибраної симетричної комутативної операції. На основі отриманих результатів удосконаленно методи побудови інформаційних систем і інформаційних технологій моделювання і дослідження операцій криптографічного кодування. Розроблено структуру інформаційної системи яка забезпечує реалізацію ієрархічної інформаційної технології моделювання симетричних двохоперандних операцій криптографічного кодування. Наведено алгоритми функціонування інформаційної технології на різних рівнях ієрархії. Вертикальні і горизонтальні зв’язки в даній технології реалізовано за допомогою бази даних та бази знань. Побудована інформаційна технологія порівняно з іншими дозволила автоматизувати процес синтезу та дослідження моделей симетричних двохоперандних операцій криптографічного кодування.

**Наукова новизна отриманих результатів:**

- вперше побудовано метод синтезу моделей симетричних двохоперандних операцій криптографічного кодування на основі кортежів симетричних одноопераднних операцій шляхом встановлення взаємозв'язків та моделювання коефіцієнтів наявності розрядів першого операнда в елементарних функціях операції, що забезпечує практичну побудову раніше невідомих симетричних двохоперандних операцій, та забезпечується можливість автоматизації створення бази знань для автоматизації досліджень операцій криптографічного захисту інформації;
- вперше розроблено метод синтезу груп моделей симетричних двохоперандних операцій криптографічного кодування для блокового шифрування на основі заданої симетричної двохоперандних операцій шляхом виконання над нею одноопераднних операцій криптографічного перетворення за умови однакової розрядності, що забезпечує побудову моделей раніше невідомих симетричних двохоперандних операцій, які забезпечують можливість перестановки інформації між операндами, необхідної для розширення можливостей застосування в захищених інформаційних системах критичної інфраструктури при реалізації блокового шифрування;
- удосконалено методи побудови інформаційних систем і інформаційних технологій моделювання і дослідження операцій криптографічного кодування, на основі розроблених методів синтезу моделей та математичних груп моделей симетричних двохоперандних операцій криптографічного кодування, шляхом їх використання як надбудови над методами побудови одноопераднних операцій, що забезпечило можливість автоматизації генерації та дослідження симетричних двохоперандних операцій і послідовностей симетричних двохоперандних операцій для застосування в захищених інформаційних системах критичної інфраструктури.

**Практичне значення отриманих результатів.** Практична цінність дисертаційного дослідження полягає в застосуванні отриманих результатів для побудови інформаційної технології моделювання і дослідження симетричних операцій криптографічного кодування та оцінки ефективності їх застосування. Основною метою застосування розробленої технології є визначення наборів багато розрядних симетричних двохоперандних операцій, які, ставши багатоваріантною альтернативою додавання за модулем, забезпечать підвищення якості блокових шифрів для захищених інформаційних систем критичної інфраструктури.

Побудовані автором алгоритми реалізації розроблених методів використані при створенні елементів програмного забезпечення запропонованої інформаційної технології.

Отримані результати дослідження дозволили синтезувати 96 симетричних дворозрядних двохоперандних операцій, які становлять 4 групи по 24 операції в кожній. Лише на основі трьохрозрядних однооперандних матричних операцій було синтезовано і досліджено 18816 симетричних трьохрозрядних двохоперандних операцій, які становлять 14 груп по 1344 операції в кожній.

**Реалізація.** Результати дисертаційного дослідження впроваджено:

1) в навчальний процес Черкаського державного технологічного університету:

- на кафедрі інформаційних технологій проектування у матеріалах курсу лекцій «Системи інформаційної безпеки», при курсовому та дипломному проектуванні;
- на кафедрі інформаційної безпеки та комп'ютерної інженерії у матеріалах лекційних курсів «Комплексні системи захисту інформації», «Програмний захист інформації в інформаційно-комунікаційних системах»;

2) у виробничу діяльність ПАТ «Черкасиавтотранс» для забезпечення конфіденційності поточної інформації, яка зберігається на електронних носіях.

**Ключові слова:** ієрархічна інформаційна технологія, криптографічне кодування, симетричні двохоперандні операції, синтез груп симетричних операцій, генерація послідовностей операцій.

# ABSTRACT

*Rudnytska Yu.V.* The information technology for modeling symmetric operations of cryptographic encoding for protected information systems of critical infrastructure. – Qualifying scientific work on the rights of manuscripts.

Thesis for the level of higher education – Doctor of Philosophy on Specialty 126 – "Information Systems and Technologies". – Cherkasy State Technological University, Cherkasy, 2023.

The thesis is devoted to increasing the scientific research productivity of the security improving processes in the information systems of critical infrastructure by creating new methods of symmetric cryptographic coding operations' modeling and analysis.

In the first section, it is determined that one of the promising directions of information systems and technologies development is their improvement to ensure the possibility of automating the scientific research conduction aimed at increasing the security of information systems of critical infrastructure. An analytical review of protected information systems of critical infrastructure was conducted, which showed the need for its constant improvement. As a result of analysizing the models and methods of information protection in information systems of critical infrastructure it was found that they are generally similar to the information protection methods in information and telecommunication systems, and do not take into account the peculiarities of practical application. The results of the current state of scientific research related to the synthesis and analysis of cryptographic coding operations are presented. The results have shown the possibility of information protection systems adaptation to the features of information representation, which is used in information systems of critical infrastructure objects management. It has been established that symmetric two-operand operations are used in the construction of almost all cryptographic algorithms, but not enough attention was paid to the automating processes of their modeling and research. The aim and objectives of the study are formulated.

The second section is devoted to constructing a method for synthesizing the models of symmetric two-operand operations of cryptographic encoding based on tuples of symmetric one-operand operations. For this purpose, the possibility of synthesizing the models of symmetric two-operand operations of cryptographic encoding based on modulo union of symmetric one-operand operations models was investigated. The possibility of synthesizing symmetric two-operand operations of cryptographic encoding based on modulo duplication and modulo union of symmetric one-operand operations models has been studied. The possibility of synthesizing the models of symmetric two-bit two-operand operations of cryptographic encoding based on the tuples of symmetric one-operand operations of information transformation has been investigated. At the research, the qualitative and quantitative characteristics of various approaches to synthyzing symmetric two-operand operations were established. Basing on the obtained results, a method for synthesizing the models of symmetric two-operand operations of cryptographic encoding through the tuples of symmetric one-operand operations was proposed and an algorithm for its implementation was developed.

The third section is devoted to developing a method of synthesizing the models' groups of symmetric two-operand operations of cryptographic encoding for block cypher based on a given symmetric two-operand operation. For this purpose, based on the generalization of the known methods of analyzing the results of the groups of symmetric modified operations synthesis, it was proposed a concept of synthesis, which allows combining the methods of synthesizing the groups of symmetric two-bit two-operand operations that were studied. Based on the proposed concept, two new groups of symmetric two-operand operations are synthesized. The constructed groups of operations confirmed the correctness of the proposed concept of modified two-operand operations synthesis. On the basis of the proposed concept of the synthesized groups of symmetric two-operand operations synthesis and analysis, a method of synthesizing models of symmetric two-operand operations of cryptographic encoding was constructed and an algorithm for its implementation has been developed.

The fourth section is devoted to the improvement of the methods for building information systems and information technologies of cryptographic encoding operations modeling and research. For this purpose, the implementation features of the method for synthesizing the models of symmetric two-operand operations of cryptographic encoding based on tuples of symmetric one-operand operations for the block cipher systems were investigated. Based on the obtained practical results, a search algorithm of symmetric commutative two-operand operations is proposed. The implementation peculiarities of the method for synthesizing the groups of symmetric two-operand operations of cryptographic encoding on the basis of the selected symmetric commutative operation are studied. Basing on the obtained results, the methods for building information systems and information technologies of cryptographic encoding operations modeling and research have been improved. It has been developed the structure of the information system, which ensures the implementation of the hierarchical information technology of modeling symmetric two-operand operations of cryptographic encoding. The information technology function algorithms at different levels of the hierarchy are given. Vertical and horizontal connections in the technology are implemented using a database and a knowledge base. Compared to others, the constructed information technology made it possible to automate the process of synthesizing and researching the models of symmetric two-operand operations of cryptographic encoding.

**Scientific novelty of the obtained results:**

- for the first time, a method for synthesizing the models of symmetric two-operand operations of cryptographic encoding based on tuples of symmetric one-operand operations was constructed by the relationships establishment and modeling the presence coefficients of the first operand's digits in the operation's elementary functions, which ensures the practical construction of previously unknown symmetric two-operand operations, and ensures the possibility of

automating the process of a knowledge base creation for automating studies of cryptographic information protection operations;

- for the first time, a method of synthesizing the models' groups of symmetric two-operand operations of cryptographic encoding for block cypher was developed based on a given symmetric two-operand operation by performing on it one-operand operations of cryptographic transformation under the condition of the same bit depth, which ensures constructing the models of previously unknown symmetric two-operand operations that provide the possibility of information permutation between operands, which is necessary for expanding the possibilities of application in protected information systems of critical infrastructure when implementing block cypher;
- the methods for building information systems and information technologies of cryptographic encoding operations modeling and research have been improved, based on the developed methods for synthesizing models and models' mathematical groups of symmetric two-operand operations of cryptographic encoding, by using them as a superstructure over the methods of building one-operand operations, which made it possible to automate the process of generating and researching symmetric two-operand operations and sequences of symmetric two-operand operations for the use in protected information systems of critical infrastructure.

**The practical value of the obtained results.** The practical value of research held in thesis is in applying the obtained results for the construction of information technology for symmetric operations of cryptographic encoding modeling and research and the evaluation of their application effectiveness. The main purpose of using the developed technology is to define collections of multi-bit symmetric two-operand operations, which, in becoming a multivariant alternative to modulo-2 addition, will ensure an increase in the quality of block ciphers for protected information systems of critical infrastructure.

The author's built algorithms for the implementation of the developed methods were used in creating the software elements of the proposed information technology.

The obtained research results made it possible to synthesize 96 symmetric two-bit two-operand operations, which make up 4 groups, 24 operations per each group. Only on the basis of three-bit one-operand matrix operations, 18816 symmetrical three-bit two-operand operations were synthesized and studied, which make up 14 groups, 1344 operations per each group.

**Implementation.** The results obtained in the thesis are implemented to:

1) the educational process of Cherkasy State Technological University:

- at the Department of Information Technology Design in lecture course materials of «Information security systems», as well as in the tasks for the coursework and graduate work;
- at the Department of Information Security and Computer Engineering in lecture course materials of «Complex information protection systems» and «Software information protection in information and communication systems»;

2) in the production activity of PJSC "Cherkasyavtotrans" to ensure the confidentiality of current information stored on electronic carriers.

**Keywords:** hierarchical information technology, cryptographic encoding, symmetric two-operand operations, groups of symmetric operations synthesis, operations sequences generation.

***Список публікацій здобувача:***

1. 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

2. 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

3. Прокопенко Т. О., Можаєв М. О., Рудницький С. В., Рудницька Ю. В. Програмування режиму ненавантаженого резервування у комп'ютерних системах критичного застосування. *Вісник Черкаського державного технологічного університету*. Черкаси: ЧДТУ, 2020. № 4. С. 77–83. DOI: https://doi.org/10.24025/2306-4412.4.2020.221845

4. 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.

5. Lada N., Rudnytska Yu. Implementation of a method for synthesizing groups of symmetric double-operand operations of cryptographic information coding for block encryption systems. *Innovative Technologies and Scientific Solutions for Industries / Information Technology*. 2022. No. 2 (20). DOI: https://doi.org/10.30837/ITSSI.2022.20.035

6. Rudnytskyi V., Babenko V., Lada N., Tarasenko Ya., Rudnytska Yu. 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. P. 182–194. ISSN 1613-0073 **(Scopus)**

7. Prokopenko T., Tarasenko Ya., Lavdanska O., Rudnytskyi S., Rudnytska Yu. Developing the comprehensive technology for alternative management of complex organizational and technological objects in the conditions of cyber threats. *Workshop on Cybersecurity Providing in Information and Telecommunication Systems (CPITS II 2021)*, Oct. 26, 2021. Kyiv, Ukraine: CEUR Workshop Proceedings, 2022. P. 170–181. ISSN 1613-0073 **(Scopus)**

8. Лада Н. В., Рудницька Ю. В. Класифікація груп несиметричних двохоперандних операцій криптоперетворення інформації на основі перестановочних схем їх синтезу. *Проблеми інформатизації: матеріали Шостої міжнар. наук.-техн. конф.*: тези доп., Черкаси – Баку – Бельсько-Бяла – Харків, 14–16 листоп. 2018 р. Черкаси: ЧДТУ; Баку: ВА ЗС АР, Бельсько-Бяла: УТіГН, Харків: НТУ «ХПІ», 2018. С. 11.

9. 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.

10. 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.

11. 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.

12. 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.

# ЗМІСТ

# ВСТУП

**Актуальність теми.** В умовах сучасних інформаційних протистоянь, руйнівних впливів інформації, розмежування національних інформаційних інтересів, поширення інформаційної агресії важливим постає питання захисту національного інформаційного простору та забезпечення інформаційної безпеки об’єктів критичної інфраструктури. Особливо актуальним це завдання стало в цьому році, адже війна з росією відбувається як на територіальному, так і на кібернетичному фронті.

За даними Державної служби спеціального зв’язку та захисту інформації України, лише протягом перших 1,5 місяців війни було здійснено понад 360 кібератак на критичну інфраструктуру нашої держави.

На сьогоднішній день надзвичайно актуальним стає питання створення та впровадження захищених інформаційних систем і технологій, особливо для інформаційного забезпечення надійного функціонування об’єктів критичної інфраструктури. Теоретичним і практичним аспектам розвитку інформаційних систем присвячено результати дослідження вітчизняних і зарубіжних науковців: Д. А. Поспєлова, М. Д. Месаровича, Е. В. Попова, В. Н. Вагіна, Н. Д. Панкратової, А. П. Еремєєва, О. Г. Івахненка, Г. С. Плесневича, П. М. Брусиловського, В. Є. Степаненка, Е. Г. Петрова, С. В. Голуба, І. В. Шостака, J. Allen, P. van Beek, L. Vila, A. Galton, E. Schwalb, P. Ladkin, D. McDermott, Y. Shoham, G. Ferguson та ін. Великий внесок у розвиток інформаційно-аналітичних систем з питань цивільного захисту, пожежної безпеки та критичної інфраструктури України зробили такі науковці, як: О. Г. Додонов, О. В. Коваль, О. Ю. Петропавловський та ін. Значний внесок у розвиток інформаційної безпеки та захисту інформації зробили І. Д. Горбенко, П. В. Дорошкевич, В. А. Хорошко, О. А. Логачов, Р. А. Хаді, Ю. В. Кузнецов, В. В. Ященко, С. О. Шестаков, А. Н. Фіонов, О. Г. Корченко, Б. Я. Рябко, Г. Ф. Конахович, 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 існує низка інформаційних систем для оцінки якості систем захисту інформації. Проте автоматизації технологій проектування захищених інформаційних систем критичної інфраструктури не приділялось достатньої уваги. Не вирішена задача автоматизованого моделювання та дослідження груп симетричних операцій криптографічного кодування для забезпечення підвищення захищеності інформаційних систем критичної інфраструктури.

Таким чином, можна стверджувати, що тема дисертаційного дослідження «Інформаційна технологія моделювання симетричних операцій криптографічного кодування для захищених інформаційних систем критичної інфраструктури» є актуальною.

**Зв'язок роботи з науковими програмами, планами, темами.** Дисертаційна робота виконана відповідно до Постанови Президії НАНУ від 30.01.19 № 30 «Основні наукові напрями та найважливіші проблеми фундаментальних досліджень у галузі природничих, технічних і гуманітарних наук Національної академії наук України на 2019–2023 рр.», а саме – пп 1.2.3.4 Розроблення обчислювальних алгоритмів і процедур з метою вирішення практичних задач міждисциплінарного характеру для застосувань, що належать до науково-технічної та соціально-економічної сфер діяльності людини; пп 1.2.4.9 Розроблення теоретико-методологічних засад створення комп'ютерних інформаційно-аналітичних систем та засобів комп'ютерного моделювання сценаріїв аналітичної діяльності; пп 1.2.8.5 Дослідження та розроблення методів інформаційної безпеки комп'ютерних систем і мереж. Результати дисертаційної роботи включені в НДР Черкаського державного технологічного університету: «Дослідження шляхів розвитку потокового шифрування на основі криптографічного кодування» (ДР № 0121U114389), у яких автор брала участь як виконавець.

**Мета і задачі дослідження.** Основною метою дослідження є підвищення продуктивності наукових досліджень процесів покращення захищеності інформаційних систем критичної інфраструктури шляхом створення нових методів моделювання та аналізу симетричних операцій криптографічного кодування.

Для досягнення поставленої мети сформульовано і вирішено такі задачі:

- розроблення методу синтезу моделей симетричних двохоперандних операцій криптографічного кодування на основі кортежів симетричних одноопераднних операцій;
- розроблення методу синтезу груп моделей симетричних двохоперандних операцій криптографічного кодування для блокового шифрування на основі заданих симетричних двохоперандних операцій;
- удосконалення методів побудови інформаційних технологій моделювання і дослідження операцій криптографічного кодування на основі застосування розроблених методів синтезу моделей симетричних двохоперандних операцій криптографічного кодування.

**Об’єкт дослідження** – процеси автоматизації моделювання і дослідження.

**Предмет дослідження** – методи і засоби моделювання та дослідження симетричних операцій криптографічного кодування для захищених інформаційних систем критичної інфраструктури.

**Методи дослідження.** У процесі розробки методу синтезу моделей симетричних двохоперандних операцій криптографічного кодування використовувався математичний апарат теорії інформації, теорії алгоритмів, криптографії, логіки, методів дискретної математики.

Для розробки методу синтезу груп моделей симетричних двохоперандних операцій криптографічного кодування використовувалися: теорія алгоритмів, теорії інформації, криптографія, методи комп’ютерного моделювання та дискретної математики.

Для удосконалення методів побудови інформаційних технологій моделювання і дослідження симетричних операцій криптографічного кодування та оцінки ефективності їх застосування 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 побудовано метод синтезу моделей симетричних двохоперандних операцій криптографічного кодування на основі кортежів симетричних одноопераднних операцій шляхом встановлення взаємозв'язків та моделювання коефіцієнтів наявності розрядів першого операнда в елементарних функціях операції, що забезпечує практичну побудову раніше не відомих симетричних двохоперандних операцій, та забезпечується можливість автоматизації створення бази знань для автоматизації досліджень операцій криптографічного захисту інформації;

2) вперше розроблено метод синтезу груп моделей симетричних двохоперандних операцій криптографічного кодування для блокового шифрування на основі заданої симетричної двохоперандної операції шляхом виконання над нею одноопераднних операцій криптографічного перетворення за умови однакової розрядності, що забезпечує побудову моделей раніше не відомих симетричних двохоперандних операцій, які забезпечують можливість перестановки інформації між операндами, необхідної для розширення можливостей застосування в захищених інформаційних системах критичної інфраструктури при реалізації блокового шифрування;

3) удосконалено методи побудови інформаційних систем та інформаційних технологій моделювання і дослідження операцій криптографічного кодування на основі розроблених методів синтезу моделей та математичних груп моделей симетричних двохоперандних операцій

криптографічного кодування шляхом їх використання як надбудови над методами побудови одноопераднних операцій, що забезпечило можливість автоматизації генерації та дослідження симетричних двохоперандних операцій і послідовностей симетричних двохоперандних операцій для застосування в захищених інформаційних системах критичної інфраструктури.

**Практичне значення отриманих результатів.** Практична цінність дисертаційного дослідження полягає в застосуванні отриманих результатів для побудови інформаційної технології моделювання і дослідження симетричних операцій криптографічного кодування та оцінки ефективності їх застосування. Основною метою застосування розробленої технології є визначення наборів багаторозрядних симетричних двохоперандних операцій, які, ставши багатоваріантною альтернативою додавання за модулем, забезпечать підвищення якості блокових шифрів для захищених інформаційних систем критичної інфраструктури.

Побудовані автором алгоритми реалізації розроблених методів використані при створенні елементів програмного забезпечення запропонованої інформаційної технології.

Отримані результати дослідження дозволили синтезувати 96 симетричних дворозрядних двохоперандних операцій, які становлять 4 групи по 24 операції в кожній. Лише на основі трьохрозрядних одноопераднних матричних операцій було синтезовано і досліджено 18816 симетричних трьохрозрядних двохоперандних операцій, які становлять 14 груп по 1344 операції в кожній.

**Реалізація.** Результати дисертаційного дослідження впроваджено:

1) у навчальний процес Черкаського державного технологічного університету:

- на кафедрі інформаційних технологій проектування у матеріалах курсу лекцій «Системи інформаційної безпеки», при курсовому та дипломному проектуванні;

- на кафедрі інформаційної безпеки та комп'ютерної інженерії у матеріалах лекційних курсів «Комплексні системи захисту інформації», «Програмний захист інформації в інформаційно-комунікаційних системах»;

2) у виробничу діяльність ПАТ «Черкасиавтотранс» для забезпечення конфіденційності поточної інформації, яка зберігається на електронних носіях.

**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: моделі симетричних модифікованих операцій додавання за модулем чотири [1, 2]; результати статистичного дослідження коректної реалізації операцій криптографічного перетворення для порівняльного аналізу моделей оцінки ненавантажених систем [3]; синтез моделей симетричних двохоперандних операцій криптографічного кодування на основі об'єднання кортежів симетричних одноопераднних операцій [4, 9, 12] та на основі об'єднання моделей одноопераднних операцій [5, 10]; метод синтезу груп моделей симетричних двохоперандних операцій криптографічного кодування [6]; запропоновано використання симетричних двохоперандних операцій криптографічного кодування у стеганографічному методі захисту секретних службових даних від загроз інсайдерських атак [7]; особливості класифікації моделей операцій криптоперетворення кодування [8]; структура технології моделювання та дослідження симетричних операцій [11].

**Апробація результатів дисертації.** Результати дисертаційної роботи доповідалися й обговорювалися на Шостій міжнародній науково-технічній конференції «Проблеми інформатизації» (Черкаси – Баку – Бельсько-Бяла – Полтава, 2018), Сьомій міжнародній науково-технічній конференції «Проблеми інформатизації» (Черкаси – Баку – Бельсько-Бяла – Полтава, 2019), Дев'ятій міжнародній науково-технічній конференції «Проблеми інформатизації» (Черкаси – Баку – Бельсько-Бяла – Полтава, 2021), Десятій

міжнародній науково-технічній конференції «Проблеми інформатизації» (Черкаси – Баку – Бельсько-Бяла – Харків, 2022), Workshop on Cybersecurity Providing in Information and Telecommunication Systems CPITS II 2021 26 October 2021 Kyiv, Ukraine.

**Публікації.** Основні положення дисертації опубліковано у 12 друкованих працях, зокрема: у 5 статтях у фахових виданнях України, 2 статтях у збірнику матеріалів «CPITS-II-1 2021 Забезпечення кібербезпеки в інформаційно-телекомунікаційних системах II 2021», проіндексованому в Scopus, і в матеріалах чотирьох міжнародних науково-технічних конференцій.

**Структура і обсяг дисертації**. Робота складається зі вступу, чотирьох розділів, висновків, списку використаних джерел, додатків. Загальний обсяг дисертації – 162 сторінок. Основний зміст викладений на 155 сторінках, у тому числі – 17 таблиць, 7 рисунків. Список використаних джерел містить 121 найменування. Робота містить 2 додатки.

# РОЗДІЛ 1 АНАЛІЗ МОДЕЛЕЙ І МЕТОДІВ ПОБУДОВИ ЗАХИЩЕНИХ ІНФОРМАЦІЙНИХ СИСТЕМ КРИТИЧНОЇ ІНФРАСТРУКТУРИ

## 1.1 Аналітичний огляд захищених інформаційних систем критичної інфраструктури

Аналіз розвитку світових держав свідчить, що періодично перед кожним суспільством постають небезпеки як зовнішнього, так і внутрішнього характеру. З часом, залежно від економічного, соціального та технологічного рівня розвитку, змінюються лише форми прояву таких загроз та об’єкти на які вони направлені. Виведення з ладу чи пошкодження даних об’єктів повинно приводити до найбільш серйозних наслідків успішної життєдіяльності суспільства, соціально-економічного розвитку держави, територіальної цілісності та національної безпеки [13, 14].

Еволюція форм та засобів ведення гібридної війни прямо залежить від об’єктів спрямувань, що теж еволюціонують. Серед найбільш резонансних фактів кібератак на об’єкти критичної інфраструктури варто згадати кібератаки на об’єкти ядерної галузі Ірану в 2010 р. за допомогою комп’ютерного вірусу «Stuxnet». Українські оператори теж ставали об’єктами деструктивного впливу [15]. Зокрема, в 2015 р. троянською програмою «BlackEnergy» було виведено з ладу енергосистему «Прикарпаттяобленерго». Тоді було вимкнено близько 30 підстанцій, понад 230 тисяч мешканців залишились без світла [16]. Тому провідні світові держави, поряд з фізичною інфраструктурою, виділяють та здійснюють захист кіберкритичної інфраструктури [16].

В Україні цю наукову проблему хоч і розпочали розглядати з початку 2000-х рр., однак можна стверджувати, що нового рівня вона досягла, починаючи з 2015 р. Поштовхом цьому слугували результати досліджень

науковців Національного інституту стратегічних досліджень [17–19]. Саме вони визначили термін «критична інфраструктура України».

Загалом автори дослідження намагалися сформулювати стратегічні цілі державної політики у сфері захисту критичної інфраструктури в Україні, принципи побудови системи захисту критичної інфраструктури та завдання такої системи. Наразі в продовження порушених питань фахівцями у зазначеній галузі в державі назріла актуальність здійснити подальші кроки стосовно аргументації вибору моделі функціонування при безпосередній побудові цієї системи, визначенні ролі та місця учасників процесу. Звісно, що для вирішення такого завдання правильним шляхом буде розгляд еволюційних процесів та апробованого досвіду у сфері захисту критичної інфраструктури провідних держав Європи [15]. Як уже зазначалось, зміст поняття «критична інфраструктура» постійно коригується та удосконалюється. Так, у 2002 р. в рамках роботи Євроатлантичної ради НАТО закріплено, що «критична інфраструктура включає в себе фізичні та кібернетичні системи забезпечення важливих і необхідних видів діяльності економіки та державного управління». До таких галузей, в першу чергу, включені: телекомунікаційні, енергетичні, банківські, фінансові, водногосподарські системи та аварійні служби державної і недержавної власності та інші. Досить активно дослідження з безпеки почали проводитися з 2003 р. в рамках програм ЄС  З 2007 р. з метою підготовки заходів на випадок війни чи надзвичайних подій розпочалась робота над ініціативою «Research for Secure Europe» (Дослідження для безпеки Європи). Поряд із зазначеним, починаючи з 2004 р., на рівні ЄС та Європейської комісії почалося створення проекту захисту критичної інфраструктури «European Programme for Critical Infrastructure Protection». У ньому важливу увагу було приділено захисту від терористичних загроз [15, 19].

В нашій державі інформаційна безпека є невід’ємною складовою частиною національної безпеки [20]. Тому саме держава визначає політику

інформаційної безпеки [21], систему управління інформаційною безпекою [22], а також перспективи та шляхи розвитку [23, 24].

Для забезпечення якісної розбудови систем інформаційної безпеки, в тому числі і інформаційної безпеки об’єктів критичної інфраструктури приймаються закони України [25, 26] та державні стандарти [27–29]. Регулює проведення робіт в сфері захисту інформації [30–31], та проводить державну експертизу у сфері технічного захисту [32].

Не дивлячись на всі зусилля по забезпеченню інформаційної безпеки, інформаційний простір і кіберпростір постійно міняється, адаптуючись до нових реалій технічного прогресу. Це вимагає постійних значних зусиль по вдосконалення кіберзахищеності об’єктів критичної інфраструктури. Адже змінюються системи, об’єкти та методи кібератак, змінюється навіть термінологія необхідна для їх коректного опису [33].

Для забезпечення якісної оцінки захищених об’єктів критичної інфростректури необхідно системно підходити до їх інформаційної безпеки [34, 35]. І це дає можливість науковцям вносити свій вагомий вклад в вирішення нагальних науково-технічних завдань. Необхідно оцінювати ризики і загрози на рівень захищеності об’єктів [36–38]. Для забезпечення оперативності проведення досліджень та прийняття необхідних рішень потрібно розширювати використання інформаційних технологій [39]. Інформаційні технології забезпечують можливість вдосконалення систем захисту інформації об’єктів критичної інфроструктури [40–42]. Крім того інформаційні технології дають можливість моделювати і прогнозувати вдосконалення та розвиток захисту інформації на об’єктах критичної інфраструктури [24, 43, 44].

Як видно з наведеного обзору інформаційній безпеці захищених інформаційних систем критичної інфраструктури приділяється надзвичайно велика увага. Впроваджені системи захисту відповідають сучасним вимогам і стандартам України. Проте існуючі системи інформаційної безпеки контролюють конфіденціальність інформації в основному між об’єктами

критичної інфраструктури. Захисту інформації в самих об’єктах, особливо при реалізації технологічних процесів на жаль не приділяється достатньо уваги.

## 1.2. Криптографічний захист інформації в інформаційних системах критичної інфраструктури

На сьогоднішній день криптографічний захист інформації вважається самим ефективним. Ефективність його реалізації ґрунтується на контролі якості шифрування. Реалізацію контролю виконує Державна служба спеціального зв’язку та захисту інформації України.

Реалізація криптографічного захисту регулюється стандартами України. Наприклад блокове шифрування повинно відповідати вимогам ДСТУ 7624:2014 [45], ДСТУ ISO/IEC 18033:2015 [46], ДСТУ ГОСТ 28147:2009 [47]. Потокове шифрування необхідно реалізовувати згідно вимог ДСТУ 8845:2019 [48], ДСТУ ISO/IEC 18033:2015 (ISO/IEC 18033-3:2010, ILD) [49]. Реалізація цифрового підпису повинна відповідати вимогам ДСТУ 4145-2002 [50]. Хешування повинно відповідати вимогам стандарту ДСТУ 7564:2014 [51].

Наведені криптографічні алгоритми як правило використовуються при забезпеченні зв’язку між об’єктами критичної інфраструктури, а при необхідності лише між деякими структурно-організаційними елементами об’єкту. Це в першу чергу пов’язано з тим що на практиці недоцільно використовувати блокові шифри, наприклад «Калину» [52], для захисту інформаційних каналів управління технічними виробничими системами. Проте несанкціоноване втручання в сигнали управління, особливо перехоплення управління може мати значні негативні наслідки. Тому необхідно для захисту каналів внутрішнього управління об’єктами критичної інфраструктури використовувати легку криптографію.

На сьогоднішній день увага до легкої, або інколи вона розглядається як мало ресурсна криптографія надзвичайно велика. Увага до легкої криптографії пояснюється надзвичайно широкими можливостями її впровадження та комерційною привабливістю. Про це свідчать аналітичні огляди напрямків розвитку криптографії наведені в [53–56].

Наявність запиту на нові наукові дослідження завжди базуються на наявних наукових результатах та існуванні перспектив їх покращення. Якщо ці дослідження стосуються кібербезпеки то до них завжди існує підвищена зацікавленість. Постійно проводиться аналіз сучасного стану легкої криптографії [57, 58].

Необхідно відмітити, що принципи побудови легких криптографічних систем і криптографічних систем повністю співпадають і теоперично обґрунтовані Клодом Шенноном в 1949 році [59].

На сьогоднішній день в ряді країн на рівні стандартів реалізуються можливості управління розробкою систем мало ресурсної криптографії, приймаються стандарти (наприклад ISO/IEC 29192:2012) [60 – 62].

Наукові дослідження в сфері легкої криптографії сконцентровані на побудові мало ресурсних блокових і потокових шифрів.

Побудові легких блокових шифрів присвячено роботи [63–67]. Наукові дослідження [68-70] присвячені легкому і ультра легкому потоковому шифруванню. Крім побудови легких шифрів проводяться наукові розробки по їх використонню [71–74]. Особливо слід відмітити використання легкої криптографії в сенсорних мережах [75–77].

Проводяться наукові дослідження по побудові легких шифрів пост квантової криптографії [78, 79]. Публікується цілий ряд результатів наукових досліджень технічній реалізації легких шифрів [80, 84].

Специфіка області застосування легких шифрів приводить виникнення специфічних атак. Дослідження якості легких шифрів та їх оцінки наведені в роботах [85–88].

Підводячи підсумки короткого огляду наукових розробок стосовно легкої криптографії, можна зробити висновок, що майже всі наукові розробки направлені на спрощення існуючих шифрів та їх адаптацію для можливості застосування при обмежених програмно-апаратних ресурсах. При розробці даних шифрів враховується можливість протидії специфічним загрозам, але не враховуються специфічні особливості їх використання (за виключенням обмежень на складність реалізації).

Враховувати особливості використання легких криптографічних систем можна на основі впровадження. Операції криптографічного кодування представляють собою поєднання елементарних дискретних функцій, які в сукупності реалізують таблицю підстановок [89, 90]. Дані операції забезпечать взаємозв’язок між алгоритмом шифрування та областю застосування. Даний зв'язок забезпечується шляхом визначення набору операцій, які забезпечать максимальну ефективність крипто алгоритму при заданих умовах його використання.

## 1.3 Основні результати досліджень операцій криптографічного кодування

Операції криптографічного перетворення інформації забезпечують збільшення стійкості крипто перетворень [84, 88, 91]. Крім того, аналіз цих операцій дозволяє виокремити нові підходи для побудови систем комп’ютерної криптографії [92, 93]. Перші дослідження операцій криптографічного кодування були спрямовані на побудову, аналіз та пошук варіантів застосування одноопераднних двохрозрядних операцій криптографічного перетворення інформації [89, 90, 94–97]. Основним результатом цієї роботи в теоретичному плані є синтез математичної групи одноопераднних двохрозрядних операцій криптографічного кодування та їх

класифікація. Основними практичними результатами можна вважати отримані моделі операцій, схемотехнічні варіанти їх реалізації та рекомендації по використанню.

У табл. 1.1 наведені двохрозрядні одноопераднді операції криптографічного кодування ($F_1$, $F_2$, $F_3$ – базові операції, $F_3$, $F_4$, $F_5$ – операції перестановки, $\begin{bmatrix}0\\0\end{bmatrix}$, $\begin{bmatrix}0\\1\end{bmatrix}$, $\begin{bmatrix}1\\0\end{bmatrix}$, $\begin{bmatrix}1\\1\end{bmatrix}$ – операції інверсії). В математичних моделях операцій криптографічного кодування позначено: $x_1$ – $x_2$ – значення першого і другого розрядів операнда.

В алгоритмах комп'ютерної криптографії особливе місце займають операції додавання за модулем, а також модифікації цих операцій з точністю до перестановки [98, 99]. Збільшення кількості операцій додавання за модулем дозволяє збільшити варіативність алгоритмів, стійкість результатів шифрування та надійність криптосистем [100].

Проте для ефективного проведення наукових досліджень у цьому напрямі було недостатньо наявних фактичних даних по двохоперандних операціях криптографічного кодування.

В основу експерименту було взято групу одноопераднді операцій криптоперетворення, наведених у табл. 1.1 [101]. Під час проведення обчислювального експерименту одноопераднді двохрозрядні операції об'єднувалися в кортежі по чотири операції. Експериментально синтезованою (вибраною) вважалася операція, яка забезпечувала пряме і обернене перетворення без зміни операцій у кортежі або порядку їх розміщення.

В роботах [101, 102] наведено результати обчислювального експерименту, на основі якого отримано 96 симетричних двохрозрядних двохоперандних симетричних операцій, представлених поєднанням одноопераднді операцій та їх таблицями підстановки.

Таблиця 1.1

**Одноопернадні двохрозрядні операції криптографічного кодування [101]**

| **Класифікатор операцій** | **Операції інверсії** | | | |
|---|---|---|---|---|
| | $\begin{bmatrix}0\\0\end{bmatrix}$ | $\begin{bmatrix}0\\1\end{bmatrix}$ | $\begin{bmatrix}1\\0\end{bmatrix}$ | $\begin{bmatrix}1\\1\end{bmatrix}$ |
| **Базові операції** | $F_1=\begin{bmatrix}x_1\\x_2\end{bmatrix}$ | $F_7=\begin{bmatrix}x_1\\x_2\oplus 1\end{bmatrix}$ | $F_{13}=\begin{bmatrix}x_1\oplus 1\\x_2\end{bmatrix}$ | $F_{19}=\begin{bmatrix}x_1\oplus 1\\x_2\oplus 1\end{bmatrix}$ |
| | $F_2=\begin{bmatrix}x_1\oplus x_2\\x_2\end{bmatrix}$ | $F_8=\begin{bmatrix}x_1\oplus x_2\\x_2\oplus 1\end{bmatrix}$ | $F_{14}=\begin{bmatrix}x_1\oplus x_2\oplus 1\\x_2\end{bmatrix}$ | $F_{20}=\begin{bmatrix}x_1\oplus x_2\oplus 1\\x_2\oplus 1\end{bmatrix}$ |
| | $F_3=\begin{bmatrix}x_1\\x_1\oplus x_2\end{bmatrix}$ | $F_9=\begin{bmatrix}x_1\\x_1\oplus x_2\oplus 1\end{bmatrix}$ | $F_{15}=\begin{bmatrix}x_1\oplus 1\\x_1\oplus x_2\end{bmatrix}$ | $F_{21}=\begin{bmatrix}x_1\oplus 1\\x_1\oplus x_2\oplus 1\end{bmatrix}$ |
| **Операції перестановок** | $F_4=\begin{bmatrix}x_2\\x_1\end{bmatrix}$ | $F_{10}=\begin{bmatrix}x_2\\x_1\oplus 1\end{bmatrix}$ | $F_{16}=\begin{bmatrix}x_2\oplus 1\\x_1\end{bmatrix}$ | $F_{22}=\begin{bmatrix}x_2\oplus 1\\x_1\oplus 1\end{bmatrix}$ |
| | $F_5=\begin{bmatrix}x_2\\x_1\oplus x_2\end{bmatrix}$ | $F_{11}=\begin{bmatrix}x_2\\x_1\oplus x_2\oplus 1\end{bmatrix}$ | $F_{17}=\begin{bmatrix}x_2\oplus 1\\x_1\oplus x_2\end{bmatrix}$ | $F_{23}=\begin{bmatrix}x_2\oplus 1\\x_1\oplus x_2\oplus 1\end{bmatrix}$ |
| | $F_6=\begin{bmatrix}x_1\oplus x_2\\x_1\end{bmatrix}$ | $F_{12}=\begin{bmatrix}x_1\oplus x_2\\x_1\oplus 1\end{bmatrix}$ | $F_{18}=\begin{bmatrix}x_1\oplus x_2\oplus 1\\x_1\end{bmatrix}$ | $F_{24}=\begin{bmatrix}x_1\oplus x_2\oplus 1\\x_1\oplus 1\end{bmatrix}$ |

Експериментально отримані операції було поділено на 4 математичні групи по 24 операції в кожній, що дало змогу досліджувати кожну групу операцій окремо. При поділі операцій на групи було використано множини таблиць істинності операцій. Результати поділу операцій на групи наведено в табл. 1.2 [103]. У цій таблиці група нижніх індексів двохоперандної операції відображає кортеж одноопернадних операцій, з яких її синтезовано. Нумерація одноопернадних операцій відповідає нумерації одноопернадних операцій, наведених в табл. 1.1.

В таблицях істинності першої групи операцій присутня таблиця істинності порозрядного додавання за модулем два ($O_1^{\text{mod}2}$). Таблицю істиннності операції порозрядного додавання за модулем два та узагальненої операції з точністю до перестановки ($O_i^{\text{mod}2}$) наведено в табл. 1.3.

В роботі [104] досліджено можливість побудови повної групи двохоперандних операцій криптоперетворення на основі відомої, за рахунок встановлення і застосування перестановочних взаємозв'язків між таблицями істинності. Встановлено, що застосування повної групи перестановочних схем забезпечить побудову повної групи наборів модифікованих двохоперандних операцій криптоперетворення невідомої групи на основі однієї відомої операції [105]. Отримані результати співпали з результатами обчислювального експерименту.

Робота [106] присвячена розробці технології побудови двохоперандних операцій криптографічного перетворення інформації за результатами моделювання, придатних для практичного застосування в комп'ютерній криптографії. Застосувавши цю технологію, було побудовано групу двохрозрядних двохоперандних операцій криптографічного кодування, синтезовану на основі порозрядного додавання по модулю два. Цю групу операцій наведено в табл. 1.4 [106].

Аналіз другої класифікованої групи двохрозрядних двохоперандних операцій криптографічного кодування встановив, що в цю групу входить двохрозрядна двохоперандна операція криптографічного кодування за модулем чотири ($O_1^{\mathrm{mod}4}$).

Таблицю істинності двохрозрядної двохоперандної операції криптографічного кодування за модулем чотири та узагальненої двохрозрядної двохоперандної операції криптографічного кодування за модулем чотири з точністю до перестановки ($O_i^{\mathrm{mod}4}$) наведено в табл. 1.5.

За аналогією з групою двохрозрядних двохоперандних операцій криптографічного кодування, синтезованою на основі порозрядного додавання за модулем два, було синтезовано групу двохрозрядних двохоперандних операцій криптографічного кодування на основі додавання за модулем чотири.

Таблиця 1.2

**Результати моделювання двохоперандних операцій криптографічного перетворення**

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

Таблиця 1.3

**Таблиця істинності операцій $O_1^{\mathrm{mod}\,2}$ и $O_i^{\mathrm{mod}\,2}$**

| **Операція** | $O_1^{\mathrm{mod}\,2}$ | | | | $O_i^{\mathrm{mod}\,2}$ | | | |
|---|---|---|---|---|---|---|---|---|
| **Значення операндів** | **00** | **01** | **10** | **11** | **00** | **01** | **10** | **11** |
| **00** | **00** | **01** | **10** | **11** | **a** | **b** | **c** | **d** |
| **01** | **01** | **00** | **11** | **10** | **b** | **d** | **a** | **c** |
| **10** | **10** | **11** | **00** | **01** | **c** | **a** | **d** | **b** |
| **11** | **11** | **10** | **01** | **00** | **d** | **c** | **b** | **a** |
| $a \neq b \neq c \neq d \in \{00; 01; 10; 11\}$, $i \in \{1; 2; ...; 24\}$ | | | | | | | | |

Таблиця 1.4

**Двохрозрядні двохоперандні операції криптографічного кодування, синтезовані на основі порозрядного додавання за модулем два**

| 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 | $F_1=\begin{bmatrix}x_1\\x_2\end{bmatrix}$ | $O_1^{\text{mod}2}=\begin{bmatrix}x_1\oplus k_1\\x_2\oplus k_2\end{bmatrix}$ | $O_7^{\text{mod}2}=\begin{bmatrix}x_1\oplus k_1\\x_2\oplus k_2\oplus 1\end{bmatrix}$ |
| | | $O_{13}^{\text{mod}2}=\begin{bmatrix}x_1\oplus k_1\oplus 1\\x_2\oplus k_2\end{bmatrix}$ | $O_{19}^{\text{mod}2}=\begin{bmatrix}x_1\oplus k_1\oplus 1\\x_2\oplus k_2\oplus 1\end{bmatrix}$ |
| | $F_2=\begin{bmatrix}x_1\oplus x_2\\x_2\end{bmatrix}$ | $O_2^{\text{mod}2}=\begin{bmatrix}x_1\oplus x_2\oplus k_1\oplus k_2\\x_2\oplus k_2\end{bmatrix}$ | $O_8^{\text{mod}2}=\begin{bmatrix}x_1\oplus x_2\oplus k_1\oplus k_2\\x_2\oplus k_2\oplus 1\end{bmatrix}$ |
| | | $O_{14}^{\text{mod}2}=\begin{bmatrix}x_1\oplus x_2\oplus k_1\oplus k_2\oplus 1\\x_2\oplus k_2\end{bmatrix}$ | $O_{20}^{\text{mod}2}=\begin{bmatrix}x_1\oplus x_2\oplus k_1\oplus k_2\oplus 1\\x_2\oplus k_2\oplus 1\end{bmatrix}$ |
| | $F_3=\begin{bmatrix}x_1\\x_1\oplus x_2\end{bmatrix}$ | $O_3^{\text{mod}2}=\begin{bmatrix}x_1\oplus k_1\\x_1\oplus x_2\oplus k_1\oplus k_2\end{bmatrix}$ | $O_9^{\text{mod}2}=\begin{bmatrix}x_1\oplus k_1\\x_1\oplus x_2\oplus k_1\oplus k_2\oplus 1\end{bmatrix}$ |
| | | $O_{15}^{\text{mod}2}=\begin{bmatrix}x_1\oplus k_1\oplus 1\\x_1\oplus x_2\oplus k_1\oplus k_2\end{bmatrix}$ | $O_{21}^{\text{mod}2}=\begin{bmatrix}x_1\oplus k_1\oplus 1\\x_1\oplus x_2\oplus k_1\oplus k_2\oplus 1\end{bmatrix}$ |
| 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 1.5

**Таблиця істинності операцій $O_1^{\mathrm{mod}\,4}$ і $O_i^{\mathrm{mod}\,4}$**

| **Операція** | $O_1^{\mathrm{mod}\,4}$ | | | | $O_i^{\mathrm{mod}\,4}$ | | | |
|---|---|---|---|---|---|---|---|---|
| **Значення операндів** | **00** | **01** | **10** | **11** | **00** | **01** | **10** | **11** |
| **00** | **00** | **01** | **10** | **11** | **a** | **b** | **c** | **d** |
| **01** | **01** | **10** | **11** | **00** | **b** | **c** | **d** | **a** |
| **10** | **10** | **11** | **00** | **01** | **c** | **d** | **a** | **b** |
| **11** | **11** | **00** | **01** | **10** | **d** | **a** | **b** | **c** |
| $a \neq b \neq c \neq d \in \{00; 01; 10; 11\}$, $i \in \{1; 2; ...; 24\}$ | | | | | | | | |

Надалі було встановлено [1], що групу двохрозрядних двохоперандних операцій криптографічного кодування на основі додавання за модулем чотири слід називати як групу двохрозрядних двохоперандних операцій криптографічного кодування на основі лівостороннього додавання за модулем чотири. Синтезовану групу двохрозрядних двохоперандних операцій криптографічного кодування на основі лівостороннього додавання за модулем чотири наведено в табл. 1.6 [1].

Дослідження третьої і четвертої груп двохрозрядних двохоперандних операцій криптографічного кодування не проводилися.

Основна перевага симетричних двохрозрядних двохоперандних операцій криптографічного кодування, порівняно з групами одноопераднних операцій, – це простота їх реалізації як на апаратному, так і на програмному рівнях. На підтвердження цієї гіпотези свідчать результати дослідження двохрозрядних двохоперандних операцій строгого стійкого криптографічного кодування, наведені в [107].

На сьогоднішній день в доступних літературних джерелах відсутня інформація про результати дослідження групи симетричних двохоперандних операцій криптографічного кодування, які перетворюють більше двох біт інформації.

Таблиця 1.6

**Двохрозрядні двохоперандні операції криптографічного кодування, синтезовані на основі лівостороннього додавання за модулем чотири**

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

Спираючись на результати проведеного аналізу захищених інформаційних систем критичної інфраструктури, моделей і методів захисту

інформації в інформаційних системах критичної інфраструктури та результати дослідження операцій криптографічного кодування, можна перейти до визначення та формулювання мети і завдань дисертаційного дослідження.

## 1.4 Мета та завдання дисертаційної роботи

Результати аналітичного огляду захищених інформаційних систем критичної інфраструктури показали, що захисту систем критичної інфраструктури в Україні, як і в усьому світі завжди приділялась особлива увага, адже від безпеки систем критичної інфраструктури напряму залежить національна безпека держави. На початку 2000-х років у низці країн почалося створення проектів захисту критичної інфраструктури, в рамках яких розглядалися аспекти інформаційної безпеки критичної інфраструктури. За результатами проведених робіт почали створюватися захищені інформаційні системи для критичної інфраструктури. При побудові цих систем використовувались методи захисту інформації в інформаційних і телекомунікаційних системах. Розглянуті методи, на жаль, не враховують специфіку й особливості інформації, яка використовується для забезпечення надійного функціонування об’єктів критичної інфраструктури. Вирішення цієї задачі можливо на основі застосування операцій криптографічного кодування. Застосування цих операцій дозволяє розробляти криптоалгоритми, адаптовані до захисту специфічної однотипної інформації, а також забезпечить вдосконалення існуючих алгоритмів для досягнення аналогічних цілей. Проведений огляд результатів дослідження операцій криптографічного кодування показав, що синтезу симетричних двохоперандних багаторозрядних операцій приділялося недостатньо уваги. Це пояснюється комбінаторним зростанням кількості двохоперандних операцій при збільшенні розрядності, навіть порівняно з одноопераднимі.

Симетричні двохоперандні операції використовуються при побудові практично всіх криптоалгоритмів, тому необхідно проводити дослідження симетричних двохоперандних операцій криптографічного кодування. Єдиним шляхом вирішення задачі синтезу й аналізу симетричних двохоперандних операцій криптографічного кодування є побудова спеціалізованої інформаційної технології.

Таким чином, мету дисертаційної роботи можна сформулювати як підвищення продуктивності наукових досліджень процесів покращення захищеності інформаційних систем критичної інфраструктури шляхом створення нових методів моделювання та аналізу симетричних операцій криптографічного кодування.

Для досягнення цієї мети необхідно провести низку досліджень, які можна умовно розбити на три етапи (рис. 1.1).

На першому етапі на прикладі двохрозрядних операцій необхідно перевірити всі можливі варіанти побудови симетричних двохоперандних операцій на основі об’єднання одноопераднних операцій. За реальними результатами побудови визначитися з концепцією синтезу симетричних двохрозрядних двохоперандних операцій. На основі результатів дослідження та концепції синтезу операцій розробити метод синтезу моделей симетричних двохоперандних операцій криптографічного кодування на основі кортежів симетричних одноопераднних операцій.

На другому етапі, узагальнивши результати відомих та вперше побудованих груп симетричних двохрозрядних двохоперандних операцій, розробити метод синтезу симетричних двохрозрядних двохоперандних операцій криптографічного кодування інформації для блокового шифрування. На основі розробленого методу вдосконалити концепцію синтезу для забезпечення можливості побудови симетричних багаторозрядних двохоперандних операцій. Розробити метод синтезу груп моделей симетричних двохоперандних операцій криптографічного кодування для блокового шифрування.

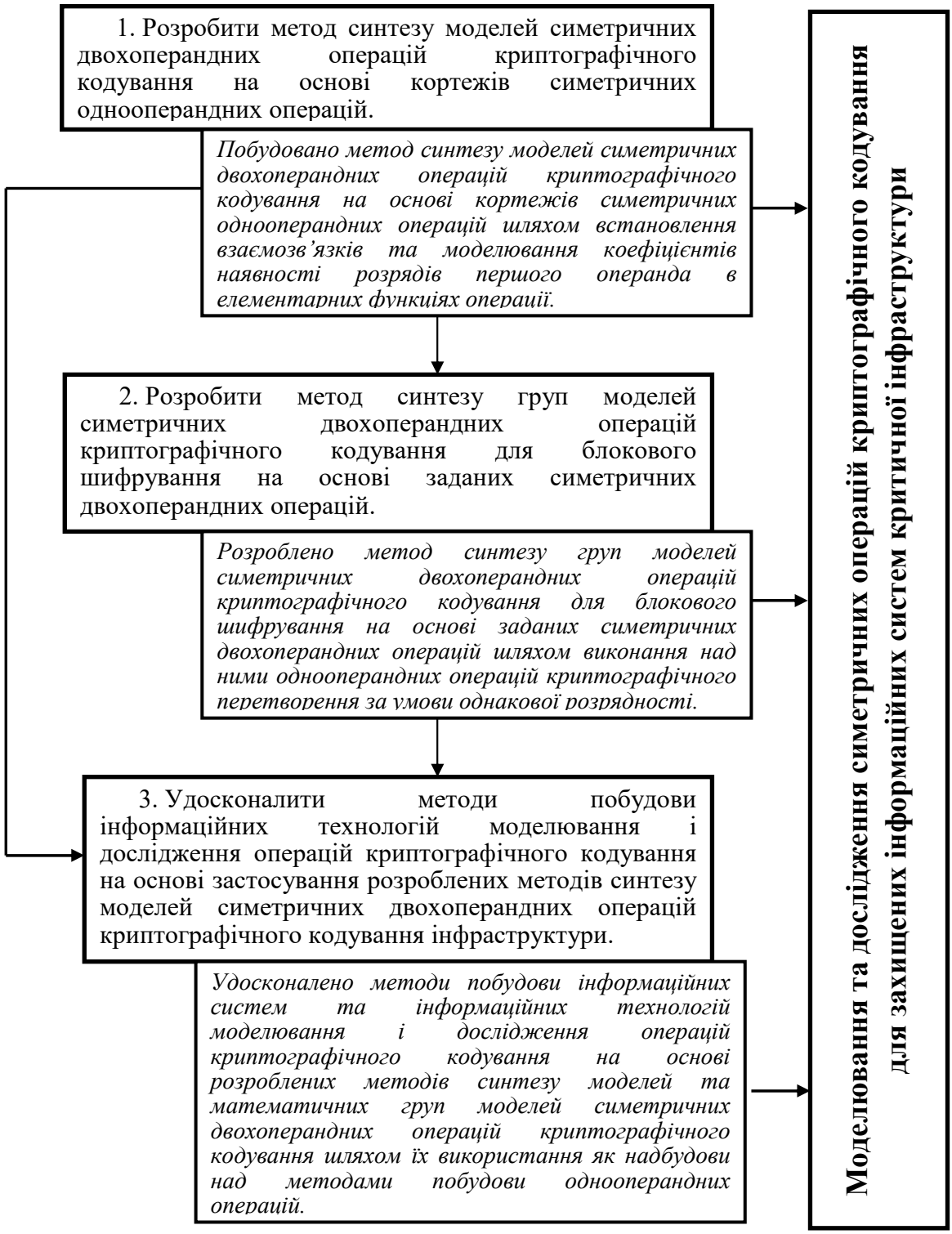


Рис. 1.1. Етапи виконання наукових досліджень

На третьому етапі дослідити особливості реалізації методу синтезу моделей симетричних двохоперандних операцій та груп симетричних двохоперандних операцій криптографічного кодування інформації. На основі

отриманих результатів запропонувати інформаційну технологію моделювання та дослідження симетричних операцій криптографічного кодування та оцінити її ефективність.

Відповідно до мети та намічених етапів досліджень необхідно вирішити такі завдання дисертаційної роботи:

1. Розробити метод синтезу моделей симетричних двохоперандних операцій криптографічного кодування на основі кортежів симетричних одноопераднних операцій.

2. Розробити метод синтезу груп моделей симетричних двохоперандних операцій криптографічного кодування для блокового шифрування на основі заданих симетричних двохоперандних операцій.

3. Удосконалити методи побудови інформаційних технологій моделювання і дослідження операцій криптографічного кодування на основі застосування розроблених методів синтезу моделей симетричних двохоперандних операцій криптографічного кодування.

**Висновки по розділу 1**

1. Результати аналітичного огляду захищених інформаційних систем критичної інфраструктури показали нагальну необхідність їх вдосконалення.

2. Інформаційна безпека захищених інформаційних систем для критичної інфраструктури, як правило, базується на використанні методів захисту інформації в інформаційних і телекомунікаційних системах, які не враховують особливості області застосування.

3. Огляд основних результатів досліджень операцій криптографічного кодування показав можливість адаптації захисту інформаційних систем управління об’єктами критичної інфраструктури до особливостей представлення інформації, яка використовується.

4. Встановлено, що синтезу симетричних двохоперандних багаторозрядних операцій приділялося недостатньо уваги. Ці операції використовуються при побудові практично всіх криптоалгоритмів.

5. Сформульовано мету та завдання дисертаційної роботи.

# РОЗДІЛ 2 МЕТОД СИНТЕЗУ МОДЕЛЕЙ СИМЕТРИЧНИХ ДВОХОПЕРАНДНИХ ОПЕРАЦІЙ КРИПТОГРАФІЧНОГО КОДУВАННЯ НА ОСНОВІ ОДНООПЕРАНДНИХ ОПЕРАЦІЙ

## 2.1 Синтез моделей симетричних двохоперандних операцій криптографічного кодування на основі об'єднання за модулем моделей симетричних одноопераднних операцій перетворення операндів

### 2.1.1 Синтез моделей симетричних двохоперандних операцій криптографічного кодування на основі дублювання та об'єднання за модулем моделей симетричних одноопераднних операцій

Серед операцій криптографічного перетворення інформації в комп'ютерній криптографії особливе місце займає операція додавання за модулем два. Ця операція є основною операцією в алгоритмах потокового шифрування, а також важливою для алгоритмів блокового шифрування [63, 67, 90].

Двохрозрядну двохоперандну операцію додавання за модулем два можна представити [108]:

$$O_{\oplus}^{*} = \begin{bmatrix} x_1 \oplus y_1 \\ x_2 \oplus y_2 \end{bmatrix}, \tag{2.1}$$

де $x_1$ – $x_2$ – значення першого і другого розрядів першого операнда, $y_1$ – $y_2$ – значення першого і другого розрядів другого операнда.

Використавши представлення одноопераднних двохрозрядних операцій, операцію (2.1) можна представити:

$$O_{\oplus}^{*} = \begin{bmatrix} x_1 \oplus y_1 \\ x_2 \oplus y_2 \end{bmatrix} = \begin{bmatrix} x_1 \\ x_2 \end{bmatrix} \oplus \begin{bmatrix} y_1 \\ y_2 \end{bmatrix} = F_1\begin{pmatrix} x_1 \\ x_2 \end{pmatrix} \oplus F_1\begin{pmatrix} y_1 \\ y_2 \end{pmatrix}. \tag{2.2}$$

Двохрозрядну двохоперандну операцію додавання за модулем два можна представити як набір операцій перетворення першого операнда залежно від значень другого операнда або набір операцій перетворення другого операнда залежно від значень першого операнда [8, 9]:

$$O_{\oplus}^{*}=\begin{bmatrix}x_1\oplus y_1\\ x_2\oplus y_2\end{bmatrix}=\begin{cases}\begin{bmatrix}x_1\\ x_2\end{bmatrix}, \text{ якщо } y_1=0;\ y_2=0\\ \begin{bmatrix}x_1\\ x_2\oplus 1\end{bmatrix}, \text{ якщо } y_1=0;\ y_2=1\\ \begin{bmatrix}x_1\oplus 1\\ x_2\end{bmatrix}, \text{ якщо } y_1=1;\ y_2=0\\ \begin{bmatrix}x_1\oplus 1\\ x_2\oplus 1\end{bmatrix}, \text{ якщо } y_1=1;\ y_2=1\end{cases}=\begin{cases}\begin{bmatrix}y_1\\ y_2\end{bmatrix}, \text{ якщо } x_1=0;\ x_2=0\\ \begin{bmatrix}y_1\\ y_2\oplus 1\end{bmatrix}, \text{ якщо } x_1=0;\ x_2=1\\ \begin{bmatrix}y_1\oplus 1\\ y_2\end{bmatrix}, \text{ якщо } x_1=1;\ x_2=0\\ \begin{bmatrix}y_1\oplus 1\\ y_2\oplus 1\end{bmatrix}, \text{ якщо } x_1=1;\ x_2=1\end{cases}. \quad (2.3)$$

Встановимо, чи симетрична операція $O_{\oplus}^{*}$. Представимо операцію (2.3) поєднанням функцій моделей одноопераднних операцій.

$$O_{\oplus}^{*}=\begin{cases}F_1\begin{pmatrix}x_1\\ x_2\end{pmatrix}, \text{ якщо } y_1=0;\ y_2=0\\ F_7\begin{pmatrix}x_1\\ x_2\end{pmatrix}, \text{ якщо } y_1=0;\ y_2=1\\ F_{13}\begin{pmatrix}x_1\\ x_2\end{pmatrix}, \text{ якщо } y_1=1;\ y_2=0\\ F_{19}\begin{pmatrix}x_1\\ x_2\end{pmatrix}, \text{ якщо } y_1=1;\ y_2=1\end{cases}=\begin{cases}F_1\begin{pmatrix}y_1\\ y_2\end{pmatrix}, \text{ якщо } x_1=0;\ x_2=0\\ F_7\begin{pmatrix}y_1\\ y_2\end{pmatrix}, \text{ якщо } x_1=0;\ x_2=1\\ F_{13}\begin{pmatrix}y_1\\ y_2\end{pmatrix}, \text{ якщо } x_1=1;\ x_2=0\\ F_{19}\begin{pmatrix}y_1\\ y_2\end{pmatrix}, \text{ якщо } x_1=1;\ x_2=1\end{cases}.$$

Серед наведених у табл. 1.1 двохрозрядних одноопераднних операцій відповідно до [99] симетричними операціями є такі: $F_1$, $F_2$, $F_3$, $F_4$, $F_7$, $F_9$, $F_{13}$, $F_{14}$, $F_{19}$, $F_{22}$. Виходячи з цього, можна стверджувати, що операція $O_{\oplus}^{*}$ є симетричною.

Як видно з (2.2), двохрозрядна двохоперандна операція додавання за модулем два складається з двох однакових двохрозрядних одноопераднних операцій. При цьому слід зауважити, що $F_1$ є симетричною одноопераднною операцією. Виходячи з зазначеного, можна допустити, що симетрична

двохрозрядна двохоперандна операція може бути побудована з однакових симетричних двохрозрядних одноопераднних операцій.

Побудуємо шляхом поєднання однакових двохрозрядних одноопераднних операцій двохрозрядні двохоперандні операції та перевіримо їх на симетричність.

Оскільки $F_2 = \begin{bmatrix} x_1 \oplus x_2 \\ x_2 \end{bmatrix}$, то

$$O_2^* = F_2\begin{pmatrix} x_1 \\ x_2 \end{pmatrix} \oplus F_2\begin{pmatrix} y_1 \\ y_2 \end{pmatrix} = \begin{bmatrix} x_1 \oplus x_2 \\ x_2 \end{bmatrix} \oplus \begin{bmatrix} y_1 \oplus y_2 \\ y_2 \end{bmatrix} = \begin{bmatrix} x_1 \oplus x_2 \oplus y_1 \oplus y_2 \\ x_2 \oplus y_2 \end{bmatrix}; \quad (2.4)$$

$$O_2^* = \begin{cases} \begin{bmatrix} x_1 \oplus x_2 \\ x_2 \end{bmatrix}, \ якщо\ y_1 = 0;\ y_2 = 0 \\ \begin{bmatrix} x_1 \oplus x_2 \oplus 1 \\ x_2 \oplus 1 \end{bmatrix}, якщо\ y_1 = 0;\ y_2 = 1 \\ \begin{bmatrix} x_1 \oplus x_2 \oplus 1 \\ x_2 \end{bmatrix}, якщо\ y_1 = 1;\ y_2 = 0 \\ \begin{bmatrix} x_1 \oplus x_2 \\ x_2 \oplus 1 \end{bmatrix}, якщо\ y_1 = 1;\ y_2 = 1 \end{cases} = \begin{cases} F_2\begin{pmatrix} x_1 \\ x_2 \end{pmatrix}, \ якщо\ y_1 = 0;\ y_2 = 0 \\ F_{20}\begin{pmatrix} x_1 \\ x_2 \end{pmatrix}, якщо\ y_1 = 0;\ y_2 = 1 \\ F_{14}\begin{pmatrix} x_1 \\ x_2 \end{pmatrix}, якщо\ y_1 = 1;\ y_2 = 0 \\ F_8\begin{pmatrix} x_1 \\ x_2 \end{pmatrix}, якщо\ y_1 = 1;\ y_2 = 1 \end{cases};$$

$$O_2^* = \begin{cases} \begin{bmatrix} y_1 \oplus y_2 \\ y_2 \end{bmatrix}, \ якщо\ x_1 = 0;\ x_2 = 0 \\ \begin{bmatrix} y_1 \oplus y_2 \oplus 1 \\ y_2 \oplus 1 \end{bmatrix}, якщо\ x_1 = 0;\ x_2 = 1 \\ \begin{bmatrix} y_1 \oplus y_2 \oplus 1 \\ y_2 \end{bmatrix}, якщо\ x_1 = 1;\ x_2 = 0 \\ \begin{bmatrix} y_1 \oplus y_2 \\ y_2 \oplus 1 \end{bmatrix}, якщо\ x_1 = 1;\ x_2 = 1 \end{cases} = \begin{cases} F_2\begin{pmatrix} y_1 \\ y_2 \end{pmatrix}, \ якщо\ x_1 = 0;\ x_2 = 0 \\ F_{20}\begin{pmatrix} y_1 \\ y_2 \end{pmatrix}, якщо\ x_1 = 0;\ x_2 = 1 \\ F_{14}\begin{pmatrix} y_1 \\ y_2 \end{pmatrix}, якщо\ x_1 = 1;\ x_2 = 0 \\ F_8\begin{pmatrix} y_1 \\ y_2 \end{pmatrix}, якщо\ x_1 = 1;\ x_2 = 1 \end{cases}.$$

Операція $O_2^*$ не буде симетричною операцією, тому що $F_8$ і $F_{20}$ – несиметричні одноопераднні операції.

Оскільки $F_3 = \begin{bmatrix} x_1 \\ x_1 \oplus x_2 \end{bmatrix}$, то

$$O_3^* = F_3\begin{pmatrix} x_1 \\ x_2 \end{pmatrix} \oplus F_3\begin{pmatrix} y_1 \\ y_2 \end{pmatrix} = \begin{bmatrix} x_1 \\ x_1 \oplus x_2 \end{bmatrix} \oplus \begin{bmatrix} y_1 \\ y_1 \oplus y_2 \end{bmatrix} = \begin{bmatrix} x_1 \oplus y_1 \\ x_1 \oplus x_2 \oplus y_1 \oplus y_2 \end{bmatrix}; \qquad (2.5)$$

$$O_3^* = \begin{cases} \begin{bmatrix} x_1 \\ x_1 \oplus x_2 \end{bmatrix}, \text{ якщо } y_1 = 0;\ y_2 = 0 \\ \begin{bmatrix} x_1 \\ x_1 \oplus x_2 \oplus 1 \end{bmatrix}, \text{ якщо } y_1 = 0;\ y_2 = 1 \\ \begin{bmatrix} x_1 \oplus 1 \\ x_1 \oplus x_2 \oplus 1 \end{bmatrix}, \text{ якщо } y_1 = 1;\ y_2 = 0 \\ \begin{bmatrix} x_1 \oplus 1 \\ x_1 \oplus x_2 \end{bmatrix}, \text{ якщо } y_1 = 1;\ y_2 = 1 \end{cases} = \begin{cases} F_3\begin{pmatrix} x_1 \\ x_2 \end{pmatrix}, \text{ якщо } y_1 = 0;\ y_2 = 0 \\ F_9\begin{pmatrix} x_1 \\ x_2 \end{pmatrix}, \text{ якщо } y_1 = 0;\ y_2 = 1 \\ F_{21}\begin{pmatrix} x_1 \\ x_2 \end{pmatrix}, \text{ якщо } y_1 = 1;\ y_2 = 0 \\ F_{15}\begin{pmatrix} x_1 \\ x_2 \end{pmatrix}, \text{ якщо } y_1 = 1;\ y_2 = 1 \end{cases}.$$

$F_{15}$ і $F_{21}$ – несиметричні одноопераднді операції, тоді двохоперандна операція $O_3^*$ буде несиметричною.

Оскільки $F_4 = \begin{bmatrix} x_2 \\ x_1 \end{bmatrix}$, то

$$O_4^* = F_4\begin{pmatrix} x_1 \\ x_2 \end{pmatrix} \oplus F_4\begin{pmatrix} y_1 \\ y_2 \end{pmatrix} = \begin{bmatrix} x_2 \\ x_1 \end{bmatrix} \oplus \begin{bmatrix} y_2 \\ y_1 \end{bmatrix} = \begin{bmatrix} x_2 \oplus y_2 \\ x_1 \oplus y_1 \end{bmatrix}; \qquad (2.6)$$

$$O_4^* = \begin{cases} \begin{bmatrix} x_2 \\ x_1 \end{bmatrix}, \text{ якщо } y_1 = 0;\ y_2 = 0 \\ \begin{bmatrix} x_2 \oplus 1 \\ x_1 \end{bmatrix}, \text{ якщо } y_1 = 0;\ y_2 = 1 \\ \begin{bmatrix} x_2 \\ x_1 \oplus 1 \end{bmatrix}, \text{ якщо } y_1 = 1;\ y_2 = 0 \\ \begin{bmatrix} x_2 \oplus 1 \\ x_1 \oplus 1 \end{bmatrix}, \text{ якщо } y_1 = 1;\ y_2 = 1 \end{cases} = \begin{cases} F_4\begin{pmatrix} x_1 \\ x_2 \end{pmatrix}, \text{ якщо } y_1 = 0;\ y_2 = 0 \\ F_{16}\begin{pmatrix} x_1 \\ x_2 \end{pmatrix}, \text{ якщо } y_1 = 0;\ y_2 = 1 \\ F_{10}\begin{pmatrix} x_1 \\ x_2 \end{pmatrix}, \text{ якщо } y_1 = 1;\ y_2 = 0 \\ F_{22}\begin{pmatrix} x_1 \\ x_2 \end{pmatrix}, \text{ якщо } y_1 = 1;\ y_2 = 1 \end{cases}.$$

$F_{10}$ і $F_{16}$ – несиметричні одноопераднді операції, тоді двохоперандна операція $O_3^*$ буде несиметричною.

Оскільки $F_7 = \begin{bmatrix} x_1 \\ x_2 \oplus 1 \end{bmatrix}$, то

$$O_7^* = F_7\begin{pmatrix} x_1 \\ x_2 \end{pmatrix} \oplus F_7\begin{pmatrix} y_1 \\ y_2 \end{pmatrix} = \begin{bmatrix} x_1 \\ x_2 \oplus 1 \end{bmatrix} \oplus \begin{bmatrix} y_1 \\ y_2 \oplus 1 \end{bmatrix} = \begin{bmatrix} x_1 \oplus y_1 \\ x_2 \oplus y_2 \end{bmatrix} = O_1^* = O_\oplus^*. \qquad (2.7)$$

Двохоперандна операція $O_{\oplus}^{*}$ симетрична, тоді і двохоперандна операція $O_{7}^{*}$ буде симетричною.

Оскільки $F_9 = \begin{bmatrix} x_1 \\ x_1 \oplus x_2 \oplus 1 \end{bmatrix}$, то

$$O_9^* = F_9\begin{pmatrix} x_1 \\ x_2 \end{pmatrix} \oplus F_9\begin{pmatrix} y_1 \\ y_2 \end{pmatrix} = \begin{bmatrix} x_1 \\ x_1 \oplus x_2 \oplus 1 \end{bmatrix} \oplus \begin{bmatrix} y_1 \\ y_1 \oplus y_2 \oplus 1 \end{bmatrix} = \begin{bmatrix} x_1 \oplus y_1 \\ x_1 \oplus x_2 \oplus y_1 \oplus y_2 \end{bmatrix} = O_3^*. \quad (2.8)$$

Двохоперандна операція $O_{3}^{*}$ несиметрична, тоді й операція $O_{9}^{*}$ буде несиметричною.

Оскільки $F_{13} = \begin{bmatrix} x_1 \oplus 1 \\ x_2 \end{bmatrix}$, то

$$O_{13}^* = F_{13}\begin{pmatrix} x_1 \\ x_2 \end{pmatrix} \oplus F_{13}\begin{pmatrix} y_1 \\ y_2 \end{pmatrix} = \begin{bmatrix} x_1 \oplus 1 \\ x_2 \end{bmatrix} \oplus \begin{bmatrix} y_1 \oplus 1 \\ y_2 \end{bmatrix} = \begin{bmatrix} x_1 \oplus y_1 \\ x_2 \oplus y_2 \end{bmatrix} = O_1^* = O_7^* = O_{\oplus}^*. \quad (2.9)$$

Двохоперандна операція $O_{7}^{*}$ симетрична, тоді й операція $O_{13}^{*}$ буде симетричною.

Оскільки $F_{14} = \begin{bmatrix} x_1 \oplus x_2 \oplus 1 \\ x_2 \end{bmatrix}$, то

$$O_{14}^* = F_{14}\begin{pmatrix} x_1 \\ x_2 \end{pmatrix} \oplus F_{14}\begin{pmatrix} y_1 \\ y_2 \end{pmatrix} = \begin{bmatrix} x_1 \oplus x_2 \oplus 1 \\ x_2 \end{bmatrix} \oplus \begin{bmatrix} y_1 \oplus y_2 \oplus 1 \\ y_2 \end{bmatrix} = \begin{bmatrix} x_1 \oplus x_2 \oplus y_1 \oplus y_2 \\ x_2 \oplus y_2 \end{bmatrix} = O_2^*. \quad (2.10)$$

Двохоперандна операція $O_{2}^{*}$ несиметрична, тоді й операція $O_{14}^{*}$ буде несиметричною.

Оскільки $F_{19} = \begin{bmatrix} x_1 \oplus 1 \\ x_2 \oplus 1 \end{bmatrix}$, то

$$O_{19}^* = F_{19}\begin{pmatrix} x_1 \\ x_2 \end{pmatrix} \oplus F_{19}\begin{pmatrix} y_1 \\ y_2 \end{pmatrix} = \begin{bmatrix} x_1 \oplus 1 \\ x_2 \oplus 1 \end{bmatrix} \oplus \begin{bmatrix} y_1 \oplus 1 \\ y_2 \oplus 1 \end{bmatrix} = \begin{bmatrix} x_1 \oplus y_1 \\ x_2 \oplus y_2 \end{bmatrix} = O_1^* = O_7^* = O_{\oplus}^*. \quad (2.11)$$

Двохоперандна операція $O_{7}^{*}$ симетрична, тоді й операція $O_{19}^{*}$ буде симетричною.

Оскільки $F_{22} = \begin{bmatrix} x_2 \oplus 1 \\ x_1 \oplus 1 \end{bmatrix}$, то

$$O_{22}^{*} = F_{22}\begin{pmatrix} x_1 \\ x_2 \end{pmatrix} \oplus F_{22}\begin{pmatrix} y_1 \\ y_2 \end{pmatrix} = \begin{bmatrix} x_2 \oplus 1 \\ x_1 \oplus 1 \end{bmatrix} \oplus \begin{bmatrix} y_2 \oplus 1 \\ y_1 \oplus 1 \end{bmatrix} = \begin{bmatrix} x_2 \oplus y_2 \\ x_1 \oplus y_1 \end{bmatrix} = O_4^{*}. \qquad (2.12)$$

Двохоперандна операція $O_4^{*}$ несиметрична, тоді й операція $O_{22}^{*}$ буде несиметричною.

Результати аналізу моделей двохрозрядних двохоперандних операцій (2.1), (2.4) – (2.12) показали, що синтезовані операції $O_1^{*}$, $O_7^{*}$, $O_{13}^{*}$ і $O_{19}^{*}$ будуть симетричними, а операції $O_2^{*}$, $O_3^{*}$, $O_4^{*}$, $O_9^{*}$, $O_{14}^{*}$ і $O_{22}^{*}$ будуть несиметричними. За результатами дослідження встановлено, що синтезувати моделі двохоперандних операцій симетричного криптографічного кодування на основі додавання за модулем однойменних моделей симетричних одноопераднних операцій перетворення операндів не видається можливим [8, 9].

### 2.1.2 Синтез моделей симетричних двохоперандних операцій криптографічного кодування на основі об'єднання за модулем моделей симетричних і несиметричних одноопераднних операцій

За аналогією з синтезом двохоперандних операцій симетричного криптографічного кодування на основі додавання за модулем однойменних моделей симетричних одноопераднних операцій перетворення операндів можна синтезувати операції поєднанням різнойменних одноопераднних операцій. Розглянемо це на деяких прикладах.

Поєднаємо моделі $F_1 = \begin{bmatrix} x_1 \\ x_2 \end{bmatrix}$ і $F_2 = \begin{bmatrix} x_1 \oplus x_2 \\ x_2 \end{bmatrix}$.

$$O_{1,2}^{*} = F_1\begin{pmatrix} x_1 \\ x_2 \end{pmatrix} \oplus F_2\begin{pmatrix} y_1 \\ y_2 \end{pmatrix} = \begin{bmatrix} x_1 \\ x_2 \end{bmatrix} \oplus \begin{bmatrix} y_1 \oplus y_2 \\ y_2 \end{bmatrix} = \begin{bmatrix} x_1 \oplus y_1 \oplus y_2 \\ x_2 \oplus y_2 \end{bmatrix}; \qquad (2.13)$$

$$O^*_{1,2}=\begin{cases}\begin{bmatrix}x_1\\x_2\end{bmatrix}, \text{ якщо } y_1=0;\ y_2=0\\ \begin{bmatrix}x_1\oplus 1\\x_2\oplus 1\end{bmatrix}, \text{ якщо } y_1=0;\ y_2=1\\ \begin{bmatrix}x_1\oplus 1\\x_2\end{bmatrix}, \text{ якщо } y_1=1;\ y_2=0\\ \begin{bmatrix}x_1\\x_2\oplus 1\end{bmatrix}, \text{ якщо } y_1=1;\ y_2=1\end{cases}=\begin{cases}F_1\begin{pmatrix}x_1\\x_2\end{pmatrix}, \text{ якщо } y_1=0;\ y_2=0\\ F_{19}\begin{pmatrix}x_1\\x_2\end{pmatrix}, \text{ якщо } y_1=0;\ y_2=1\\ F_{13}\begin{pmatrix}x_1\\x_2\end{pmatrix}, \text{ якщо } y_1=1;\ y_2=0\\ F_7\begin{pmatrix}x_1\\x_2\end{pmatrix}, \text{ якщо } y_1=1;\ y_2=1\end{cases}.$$

Двохоперандна операція $O^*_{1,2}$ буде симетричною, тому що всі одноопераднi операції $F_1$, $F_{19}$, $F_{13}$ і $F_7$ симетричні.

Поєднаємо моделі $F_2=\begin{bmatrix}x_1\oplus x_2\\x_2\end{bmatrix}$ і $F_1=\begin{bmatrix}x_1\\x_2\end{bmatrix}$.

$$O^*_{2,1}=F_2\begin{pmatrix}x_1\\x_2\end{pmatrix}\oplus F_1\begin{pmatrix}y_1\\y_2\end{pmatrix}=\begin{bmatrix}x_1\oplus x_2\\x_2\end{bmatrix}\oplus\begin{bmatrix}y_1\\y_2\end{bmatrix}=\begin{bmatrix}x_1\oplus x_2\oplus y_1\\x_2\oplus y_2\end{bmatrix};$$

$$O^*_{2,1}=\begin{cases}\begin{bmatrix}x_1\oplus x_2\\x_2\end{bmatrix}, \text{ якщо } y_1=0;\ y_2=0\\ \begin{bmatrix}x_1\oplus x_2\\x_2\oplus 1\end{bmatrix}, \text{ якщо } y_1=0;\ y_2=1\\ \begin{bmatrix}x_1\oplus x_2\oplus 1\\x_2\end{bmatrix}, \text{ якщо } y_1=1;\ y_2=0\\ \begin{bmatrix}x_1\oplus x_2\oplus 1\\x_2\oplus 1\end{bmatrix}, \text{ якщо } y_1=1;\ y_2=1\end{cases}=\begin{cases}F_2\begin{pmatrix}x_1\\x_2\end{pmatrix}, \text{ якщо } y_1=0;\ y_2=0\\ F_8\begin{pmatrix}x_1\\x_2\end{pmatrix}, \text{ якщо } y_1=0;\ y_2=1\\ F_{14}\begin{pmatrix}x_1\\x_2\end{pmatrix}, \text{ якщо } y_1=1;\ y_2=0\\ F_{20}\begin{pmatrix}x_1\\x_2\end{pmatrix}, \text{ якщо } y_1=1;\ y_2=1\end{cases}.$$

Оскільки $F_8$ і $F_{20}$ – несиметричні одноопераднi операції, то двохоперандна операція $O^*_{2,1}$ буде несиметричною.

Поєднаємо моделі $F_1=\begin{bmatrix}x_1\\x_2\end{bmatrix}$ і $F_3=\begin{bmatrix}x_1\\x_1\oplus x_2\end{bmatrix}$.

$$O^*_{1,3}=F_1\begin{pmatrix}x_1\\x_2\end{pmatrix}\oplus F_3\begin{pmatrix}y_1\\y_2\end{pmatrix}=\begin{bmatrix}x_1\\x_2\end{bmatrix}\oplus\begin{bmatrix}y_1\\y_1\oplus y_2\end{bmatrix}=\begin{bmatrix}x_1\oplus y_1\\x_2\oplus y_1\oplus y_2\end{bmatrix};\qquad(2.14)$$

$$O^*_{1,3}=\begin{cases}\begin{bmatrix}x_1\\x_2\end{bmatrix}, \text{ якщо } y_1=0;\ y_2=0\\ \begin{bmatrix}x_1\\x_2\oplus 1\end{bmatrix}, \text{ якщо } y_1=0;\ y_2=1\\ \begin{bmatrix}x_1\oplus 1\\x_2\oplus 1\end{bmatrix}, \text{ якщо } y_1=1;\ y_2=0\\ \begin{bmatrix}x_1\oplus 1\\x_2\end{bmatrix}, \text{ якщо } y_1=1;\ y_2=1\end{cases}=\begin{cases}F_1\begin{pmatrix}x_1\\x_2\end{pmatrix}, \text{ якщо } y_1=0;\ y_2=0\\ F_7\begin{pmatrix}x_1\\x_2\end{pmatrix}, \text{ якщо } y_1=0;\ y_2=1\\ F_{19}\begin{pmatrix}x_1\\x_2\end{pmatrix}, \text{ якщо } y_1=1;\ y_2=0\\ F_3\begin{pmatrix}x_1\\x_2\end{pmatrix}, \text{ якщо } y_1=1;\ y_2=1\end{cases}.$$

Двохоперандна операція $O^*_{1,3}$ буде симетричною, тому що всі одноопераднi операції симетричні.

Поєднаємо моделі $F_3=\begin{bmatrix}x_1\\x_1\oplus x_2\end{bmatrix}$ і $F_1=\begin{bmatrix}x_1\\x_2\end{bmatrix}$.

$$O^*_{3,1}=F_3\begin{pmatrix}x_1\\x_2\end{pmatrix}\oplus F_1\begin{pmatrix}y_1\\y_2\end{pmatrix}=\begin{bmatrix}x_1\\x_1\oplus x_2\end{bmatrix}\oplus\begin{bmatrix}y_1\\y_2\end{bmatrix}=\begin{bmatrix}x_1\oplus y_1\\x_1\oplus x_2\oplus y_2\end{bmatrix};$$

$$O^*_{3,1}=\begin{cases}\begin{bmatrix}x_1\\x_1\oplus x_2\end{bmatrix}, \text{ якщо } y_1=0;\ y_2=0\\ \begin{bmatrix}x_1\\x_1\oplus x_2\oplus 1\end{bmatrix}, \text{ якщо } y_1=0;\ y_2=1\\ \begin{bmatrix}x_1\oplus 1\\x_1\oplus x_2\end{bmatrix}, \text{ якщо } y_1=1;\ y_2=0\\ \begin{bmatrix}x_1\oplus 1\\x_1\oplus x_2\oplus 1\end{bmatrix}, \text{ якщо } y_1=1;\ y_2=1\end{cases}=\begin{cases}F_3\begin{pmatrix}x_1\\x_2\end{pmatrix}, \text{ якщо } y_1=0;\ y_2=0\\ F_9\begin{pmatrix}x_1\\x_2\end{pmatrix}, \text{ якщо } y_1=0;\ y_2=1\\ F_{15}\begin{pmatrix}x_1\\x_2\end{pmatrix}, \text{ якщо } y_1=1;\ y_2=0\\ F_{21}\begin{pmatrix}x_1\\x_2\end{pmatrix}, \text{ якщо } y_1=1;\ y_2=1\end{cases}.$$

Оскільки $F_{15}$ і $F_{21}$ – несиметричні одноопераднi операції, то двохоперандна операція $O^*_{3,1}$ буде несиметричною.

Поєднаємо моделі $F_4=\begin{bmatrix}x_2\\x_1\end{bmatrix}$ і $F_3=\begin{bmatrix}x_1\\x_1\oplus x_2\end{bmatrix}$.

$$O^*_{4,3}=F_4\begin{pmatrix}x_1\\x_2\end{pmatrix}\oplus F_3\begin{pmatrix}y_1\\y_2\end{pmatrix}=\begin{bmatrix}x_2\\x_1\end{bmatrix}\oplus\begin{bmatrix}y_1\\y_1\oplus y_2\end{bmatrix}=\begin{bmatrix}x_2\oplus y_1\\x_1\oplus y_1\oplus y_2\end{bmatrix};$$

$$O^*_{4,3}=\begin{cases}\begin{bmatrix}x_2\\x_1\end{bmatrix}, \text{ якщо } y_1=0;\ y_2=0\\ \begin{bmatrix}x_2\\x_1\oplus 1\end{bmatrix}, \text{ якщо } y_1=0;\ y_2=1\\ \begin{bmatrix}x_2\oplus 1\\x_1\oplus 1\end{bmatrix}, \text{ якщо } y_1=1;\ y_2=0\\ \begin{bmatrix}x_2\oplus 1\\x_1\end{bmatrix}, \text{ якщо } y_1=1;\ y_2=1\end{cases}=\begin{cases}F_4\begin{pmatrix}x_1\\x_2\end{pmatrix}, \text{ якщо } y_1=0;\ y_2=0\\ F_{10}\begin{pmatrix}x_1\\x_2\end{pmatrix}, \text{ якщо } y_1=0;\ y_2=1\\ F_{22}\begin{pmatrix}x_1\\x_2\end{pmatrix}, \text{ якщо } y_1=1;\ y_2=0\\ F_{16}\begin{pmatrix}x_1\\x_2\end{pmatrix}, \text{ якщо } y_1=1;\ y_2=1\end{cases}.$$

Оскільки $F_{10}$ і $F_{16}$ – несиметричні одноопераднді операції, то двохоперандна операція $O^*_{4,3}$ буде несиметричною.

Поєднаємо моделі $F_3=\begin{bmatrix}x_1\\x_1\oplus x_2\end{bmatrix}$ і $F_4=\begin{bmatrix}x_2\\x_1\end{bmatrix}$.

$$O^*_{3,4}=F_4\begin{pmatrix}x_1\\x_2\end{pmatrix}\oplus F_3\begin{pmatrix}y_1\\y_2\end{pmatrix}=\begin{bmatrix}x_1\\x_1\oplus x_2\end{bmatrix}\oplus\begin{bmatrix}y_2\\y_1\end{bmatrix}=\begin{bmatrix}x_1\oplus y_2\\x_1\oplus x_2\oplus y_1\end{bmatrix}; \qquad (2.15)$$

$$O^*_{3,4}=\begin{cases}\begin{bmatrix}x_1\\x_1\oplus x_2\end{bmatrix}, \text{ якщо } y_1=0;\ y_2=0\\ \begin{bmatrix}x_1\oplus 1\\x_1\oplus x_2\end{bmatrix}, \text{ якщо } y_1=0;\ y_2=1\\ \begin{bmatrix}x_1\\x_1\oplus x_2\oplus 1\end{bmatrix}, \text{ якщо } y_1=1;\ y_2=0\\ \begin{bmatrix}x_1\oplus 1\\x_1\oplus x_2\oplus 1\end{bmatrix}, \text{ якщо } y_1=1;\ y_2=1\end{cases}=\begin{cases}F_3\begin{pmatrix}x_1\\x_2\end{pmatrix}, \text{ якщо } y_1=0;\ y_2=0\\ F_{15}\begin{pmatrix}x_1\\x_2\end{pmatrix}, \text{ якщо } y_1=0;\ y_2=1\\ F_9\begin{pmatrix}x_1\\x_2\end{pmatrix}, \text{ якщо } y_1=1;\ y_2=0\\ F_{21}\begin{pmatrix}x_1\\x_2\end{pmatrix}, \text{ якщо } y_1=1;\ y_2=1\end{cases}.$$

Оскільки $F_{15}$ і $F_{21}$ – несиметричні одноопераднді операції, то двохоперандна операція $O^*_{3,4}$ буде несиметричною.

Поєднаємо моделі $F_6=\begin{bmatrix}x_1\oplus x_2\\x_1\end{bmatrix}$ і $F_3=\begin{bmatrix}x_1\\x_1\oplus x_2\end{bmatrix}$.

$$O^*_{6,3}=F_4\begin{pmatrix}x_1\\x_2\end{pmatrix}\oplus F_3\begin{pmatrix}y_1\\y_2\end{pmatrix}=\begin{bmatrix}x_1\oplus x_2\\x_1\end{bmatrix}\oplus\begin{bmatrix}y_1\\y_1\oplus y_2\end{bmatrix}=\begin{bmatrix}x_1\oplus x_2\oplus y_1\\x_1\oplus y_1\oplus y_2\end{bmatrix};$$

$$O^*_{6,3}=\begin{cases}\begin{bmatrix}x_1\oplus x_2\\ x_1\end{bmatrix}, \text{ якщо } y_1=0;\ y_2=0\\ \begin{bmatrix}x_1\oplus x_2\\ x_1\oplus 1\end{bmatrix}, \text{ якщо } y_1=0;\ y_2=1\\ \begin{bmatrix}x_1\oplus x_2\oplus 1\\ x_1\oplus 1\end{bmatrix}, \text{ якщо } y_1=1;\ y_2=0\\ \begin{bmatrix}x_1\oplus x_2\oplus 1\\ x_1\end{bmatrix}, \text{ якщо } y_1=1;\ y_2=1\end{cases}=\begin{cases}F_6\begin{pmatrix}x_1\\ x_2\end{pmatrix}, \text{ якщо } y_1=0;\ y_2=0\\ F_{12}\begin{pmatrix}x_1\\ x_2\end{pmatrix}, \text{ якщо } y_1=0;\ y_2=1\\ F_{24}\begin{pmatrix}x_1\\ x_2\end{pmatrix}, \text{ якщо } y_1=1;\ y_2=0\\ F_{18}\begin{pmatrix}x_1\\ x_2\end{pmatrix}, \text{ якщо } y_1=1;\ y_2=1\end{cases}.$$

Двохоперандна операція $O^*_{6,3}$ буде несиметричною, тому що всі одноопернадні операції несиметричні.

Як видно з наведених прикладів, двохрозрядна двохоперандна операція криптоперетворення буде симетричною лише тоді, коли при об'єднанні операцій операцією обробки першого операнда буде операція повтору (2.13, 2.14).

Цей підхід до синтезу симетричних двохрозрядних двохоперандних операцій криптографічного перетворення є недостатньо ефективним, тому що він дозволяє отримати лише 10 операцій, а саме: $O^*_{1,1}$, $O^*_{1,2}$, $O^*_{1,3}$, $O^*_{1,4}$, $O^*_{1,7}$, $O^*_{1,9}$, $O^*_{1,13}$, $O^*_{1,14}$, $O^*_{1,19}$, $O^*_{1,22}$.

Сутність отриманого результату полягає в наступному:

- операція обробки першого операнда повторює вхідну інформацію як при прямому, так і при оберненому перетворенні;
- операція перетворення другого операнда формує гаму, яка при однакових значеннях другого операнда буде однаковою;
- об'єднана операція виконує гамування вхідної інформації і забезпечує при однакових гамах як пряме, так і обернене перетворення;
- ця операція криптоперетворення буде симетричною.

Слід зауважити, що для синтезу симетричної операції не обов'язково використовувати симетричну операцію обробки другого операнда, як операція обробки другого операнда може використовуватися будь-яка двохрозрядна одноопернадна операція криптоперетворення.

Продемонструємо це на прикладах.

Поєднаємо моделі $F_1 = \begin{bmatrix} x_1 \oplus x_2 \\ x_2 \end{bmatrix}$ і $F_{15} = \begin{bmatrix} x_1 \oplus 1 \\ x_1 \oplus x_2 \end{bmatrix}$.

$$O^*_{1,15} = F_1\begin{pmatrix} x_1 \\ x_2 \end{pmatrix} \oplus F_{15}\begin{pmatrix} y_1 \\ y_2 \end{pmatrix} = \begin{bmatrix} x_1 \\ x_2 \end{bmatrix} \oplus \begin{bmatrix} y_1 \oplus 1 \\ y_1 \oplus y_2 \end{bmatrix} = \begin{bmatrix} x_1 \oplus y_1 \oplus 1 \\ x_2 \oplus y_1 \oplus y_2 \end{bmatrix};$$

$$O^*_{1,15} = \begin{cases} \begin{bmatrix} x_1 \oplus 1 \\ x_2 \end{bmatrix}, \text{ якщо } y_1 = 0;\ y_2 = 0 \\ \begin{bmatrix} x_1 \oplus 1 \\ x_2 \oplus 1 \end{bmatrix}, \text{ якщо } y_1 = 0;\ y_2 = 1 \\ \begin{bmatrix} x_1 \\ x_2 \oplus 1 \end{bmatrix}, \text{ якщо } y_1 = 1;\ y_2 = 0 \\ \begin{bmatrix} x_1 \\ x_2 \end{bmatrix}, \text{ якщо } y_1 = 1;\ y_2 = 1 \end{cases} = \begin{cases} F_{13}\begin{pmatrix} x_1 \\ x_2 \end{pmatrix}, \text{ якщо } y_1 = 0;\ y_2 = 0 \\ F_{19}\begin{pmatrix} x_1 \\ x_2 \end{pmatrix}, \text{ якщо } y_1 = 0;\ y_2 = 1 \\ F_7\begin{pmatrix} x_1 \\ x_2 \end{pmatrix}, \text{ якщо } y_1 = 1;\ y_2 = 0 \\ F_1\begin{pmatrix} x_1 \\ x_2 \end{pmatrix}, \text{ якщо } y_1 = 1;\ y_2 = 1 \end{cases}.$$

Двохоперандна операція $O^*_{1,15}$ буде симетричною, тому що всі одноопераднідні операції симетричні.

Поєднаємо моделі $F_1 = \begin{bmatrix} x_1 \\ x_2 \end{bmatrix}$ і $F_{17} = \begin{bmatrix} x_2 \oplus 1 \\ x_1 \oplus x_2 \end{bmatrix}$.

$$O^*_{1,17} = F_1\begin{pmatrix} x_1 \\ x_2 \end{pmatrix} \oplus F_{17}\begin{pmatrix} y_1 \\ y_2 \end{pmatrix} = \begin{bmatrix} x_1 \\ x_2 \end{bmatrix} \oplus \begin{bmatrix} y_2 \oplus 1 \\ y_1 \oplus y_2 \end{bmatrix} = \begin{bmatrix} x_1 \oplus y_2 \oplus 1 \\ x_2 \oplus y_1 \oplus y_2 \end{bmatrix};$$

$$O^*_{1,17} = \begin{cases} \begin{bmatrix} x_1 \oplus 1 \\ x_2 \end{bmatrix}, \text{ якщо } y_1 = 0;\ y_2 = 0 \\ \begin{bmatrix} x_1 \\ x_2 \oplus 1 \end{bmatrix}, \text{ якщо } y_1 = 0;\ y_2 = 1 \\ \begin{bmatrix} x_1 \oplus 1 \\ x_2 \oplus 1 \end{bmatrix}, \text{ якщо } y_1 = 1;\ y_2 = 0 \\ \begin{bmatrix} x_1 \\ x_2 \end{bmatrix}, \text{ якщо } y_1 = 1;\ y_2 = 1 \end{cases} = \begin{cases} F_{13}\begin{pmatrix} x_1 \\ x_2 \end{pmatrix}, \text{ якщо } y_1 = 0;\ y_2 = 0 \\ F_7\begin{pmatrix} x_1 \\ x_2 \end{pmatrix}, \text{ якщо } y_1 = 0;\ y_2 = 1 \\ F_{19}\begin{pmatrix} x_1 \\ x_2 \end{pmatrix}, \text{ якщо } y_1 = 1;\ y_2 = 0 \\ F_1\begin{pmatrix} x_1 \\ x_2 \end{pmatrix}, \text{ якщо } y_1 = 1;\ y_2 = 1 \end{cases}.$$

Двохоперандна операція $O^*_{1,17}$ буде симетричною, тому що всі одноопераднідні операції симетричні.

Перевірка гіпотези на повній множині двохрозрядних одноопераднних операцій криптоперетворення показала, що синтезувати симетричну операцію можна шляхом поєднання операції повтору для обробки першого операнда (інформації, яка перетворюється) та будь-якої одноопераднної операції для обробки другого операнда (операції, якою шифрують, або псевдовипадкової послідовності).

## 2.2 Синтез моделей симетричних двохрозрядних двохоперандних операцій криптографічного кодування на основі кортежів симетричних одноопераднних операцій перетворення інформації

В процесі проведення досліджень було встановлено, що всі симетричні операції криптоперетворення складаються з кортежів симетричних одноопераднних операцій.

Серед наведених раніше прикладів найчастіше траплялися кортежі, які включали одноопераднні операції $F_1$, $F_7$, $F_{13}$, $F_{19}$.

Розглянемо варіанти цього кортежу детально.

$$O_{1,7,13,19}=\begin{cases} F_1\begin{pmatrix}x_1\\x_2\end{pmatrix}, \text{ якщо } y_1=0;\ y_2=0 \\ F_7\begin{pmatrix}x_1\\x_2\end{pmatrix}, \text{ якщо } y_1=0;\ y_2=1 \\ F_{13}\begin{pmatrix}x_1\\x_2\end{pmatrix}, \text{ якщо } y_1=1;\ y_2=0 \\ F_{19}\begin{pmatrix}x_1\\x_2\end{pmatrix}, \text{ якщо } y_1=1;\ y_2=1 \end{cases} = \begin{cases} \begin{bmatrix}x_1\\x_2\end{bmatrix}, \text{ якщо } y_1=0;\ y_2=0 \\ \begin{bmatrix}x_1\\x_2\oplus 1\end{bmatrix}, \text{ якщо } y_1=0;\ y_2=1 \\ \begin{bmatrix}x_1\oplus 1\\x_2\end{bmatrix}, \text{ якщо } y_1=1;\ y_2=0 \\ \begin{bmatrix}x_1\oplus 1\\x_2\oplus 1\end{bmatrix}, \text{ якщо } y_1=1;\ y_2=1 \end{cases} = \begin{bmatrix}x_1\oplus y_1\\x_2\oplus y_2\end{bmatrix} = O^*_{1,1}.$$

Узагальнена модель цієї симетричної двохрозрядної двохоперандної операції відповідає (2.3).

Розглянемо інший порядок одноопераднних операцій у кортежі (2.13):

$$O_{1,19,13,7}=\begin{cases} F_1\begin{pmatrix}x_1\\x_2\end{pmatrix},\ якщо\, y_1=0;\ y_2=0 \\ F_{19}\begin{pmatrix}x_1\\x_2\end{pmatrix},\ якщо\, y_1=0;\ y_2=1 \\ F_{13}\begin{pmatrix}x_1\\x_2\end{pmatrix},\ якщо\, y_1=1;\ y_2=0 \\ F_7\begin{pmatrix}x_1\\x_2\end{pmatrix},\ якщо\, y_1=1;\ y_2=1 \end{cases}=\begin{cases} \begin{bmatrix}x_1\\x_2\end{bmatrix},\ якщо\, y_1=0;\ y_2=0 \\ \begin{bmatrix}x_1\oplus 1\\x_2\oplus 1\end{bmatrix},\ якщо\, y_1=0;\ y_2=1 \\ \begin{bmatrix}x_1\oplus 1\\x_2\end{bmatrix},\ якщо\, y_1=1;\ y_2=0 \\ \begin{bmatrix}x_1\\x_2\oplus 1\end{bmatrix},\ якщо\, y_1=1;\ y_2=1 \end{cases}=\begin{bmatrix}x_1\oplus y_1\oplus y_2\\x_2\oplus y_2\end{bmatrix}=O^*_{1,2}.$$

Модель операції (2.14) забезпечує наступний порядок розміщення одноопераднних операцій у кортежі:

$$O_{1,7,19,13}=\begin{cases} F_1\begin{pmatrix}x_1\\x_2\end{pmatrix},\ якщо\, y_1=0;\ y_2=0 \\ F_7\begin{pmatrix}x_1\\x_2\end{pmatrix},\ якщо\, y_1=0;\ y_2=1 \\ F_{19}\begin{pmatrix}x_1\\x_2\end{pmatrix},\ якщо\, y_1=1;\ y_2=0 \\ F_{13}\begin{pmatrix}x_1\\x_2\end{pmatrix},\ якщо\, y_1=1;\ y_2=1 \end{cases}=\begin{cases} \begin{bmatrix}x_1\\x_2\end{bmatrix},\ якщо\, y_1=0;\ y_2=0 \\ \begin{bmatrix}x_1\\x_2\oplus 1\end{bmatrix},\ якщо\, y_1=0;\ y_2=1 \\ \begin{bmatrix}x_1\oplus 1\\x_2\oplus 1\end{bmatrix},\ якщо\, y_1=1;\ y_2=0 \\ \begin{bmatrix}x_1\oplus 1\\x_2\end{bmatrix},\ якщо\, y_1=1;\ y_2=1 \end{cases}=\begin{bmatrix}x_1\oplus y_1\\x_2\oplus y_1\oplus y_2\end{bmatrix}=O^*_{1,3}.$$

Ці моделі двохрозрядних двохоперандних операцій було взято з раніше розглянутих прикладів. Побудувати моделі аналогічних симетричних операцій на основі інших перестановок можна, базуючись на застосуванні технології побудови двохрозрядних двохоперандних операцій строгого стійкого криптографічного кодування [107].

Наприклад:

$$O_{7,1,19,13}=\begin{cases} F_7\begin{pmatrix}x_1\\x_2\end{pmatrix},\ якщо\, y_1=0;\ y_2=0 \\ F_1\begin{pmatrix}x_1\\x_2\end{pmatrix},\ якщо\, y_1=0;\ y_2=1 \\ F_{19}\begin{pmatrix}x_1\\x_2\end{pmatrix},\ якщо\, y_1=1;\ y_2=0 \\ F_{13}\begin{pmatrix}x_1\\x_2\end{pmatrix},\ якщо\, y_1=1;\ y_2=1 \end{cases}=\begin{cases} \begin{bmatrix}x_1\\x_2\oplus 1\end{bmatrix},\ якщо\, y_1=0;\ y_2=0 \\ \begin{bmatrix}x_1\\x_2\end{bmatrix},\ якщо\, y_1=0;\ y_2=1 \\ \begin{bmatrix}x_1\oplus 1\\x_2\oplus 1\end{bmatrix},\ якщо\, y_1=1;\ y_2=0 \\ \begin{bmatrix}x_1\oplus 1\\x_2\end{bmatrix},\ якщо\, y_1=1;\ y_2=1 \end{cases}=\begin{cases} \begin{bmatrix}x_1\\x_2\end{bmatrix}\oplus\begin{bmatrix}0\\1\end{bmatrix},\ якщо\, y_1=0;\ y_2=0 \\ \begin{bmatrix}x_1\\x_2\end{bmatrix}\oplus\begin{bmatrix}0\\0\end{bmatrix},\ якщо\, y_1=0;\ y_2=1 \\ \begin{bmatrix}x_1\\x_2\end{bmatrix}\oplus\begin{bmatrix}1\\1\end{bmatrix},\ якщо\, y_1=1;\ y_2=0 \\ \begin{bmatrix}x_1\\x_2\end{bmatrix}\oplus\begin{bmatrix}1\\0\end{bmatrix},\ якщо\, y_1=1;\ y_2=1 \end{cases}.$$

Побудувавши таблиці істинності операндів та інверсій і виконавши мінімізацію таблиць істинності, отримаємо:

$$O_{7,1,19,13}=\begin{bmatrix}x_1\oplus y_1\\x_2\oplus y_2\oplus 1\end{bmatrix}=O^*_{1,7}.$$

При викладенні подальших результатів будемо опускати побудову таблиць істинності та їх мінімізацію.

$$O_{7,1,13,19}=\begin{cases} F_7\begin{pmatrix}x_1\\x_2\end{pmatrix}, \text{ якщо } y_1=0;\ y_2=0 \\ F_1\begin{pmatrix}x_1\\x_2\end{pmatrix}, \text{ якщо } y_1=0;\ y_2=1 \\ F_{13}\begin{pmatrix}x_1\\x_2\end{pmatrix}, \text{ якщо } y_1=1;\ y_2=0 \\ F_{19}\begin{pmatrix}x_1\\x_2\end{pmatrix}, \text{ якщо } y_1=1;\ y_2=1 \end{cases} = \begin{cases} \begin{bmatrix}x_1\\x_2\oplus 1\end{bmatrix}, \text{ якщо } y_1=0;\ y_2=0 \\ \begin{bmatrix}x_1\\x_2\end{bmatrix}, \text{ якщо } y_1=0;\ y_2=1 \\ \begin{bmatrix}x_1\oplus 1\\x_2\end{bmatrix}, \text{ якщо } y_1=1;\ y_2=0 \\ \begin{bmatrix}x_1\oplus 1\\x_2\oplus 1\end{bmatrix}, \text{ якщо } y_1=1;\ y_2=1 \end{cases} = \begin{bmatrix}x_1\oplus y_1\\x_2\oplus y_1\oplus y_2\oplus 1\end{bmatrix} = O^*_{1,9};$$

$$O_{7,13,19,1}=\begin{cases} F_7\begin{pmatrix}x_1\\x_2\end{pmatrix}, \text{ якщо } y_1=0;\ y_2=0 \\ F_{13}\begin{pmatrix}x_1\\x_2\end{pmatrix}, \text{ якщо } y_1=0;\ y_2=1 \\ F_{19}\begin{pmatrix}x_1\\x_2\end{pmatrix}, \text{ якщо } y_1=1;\ y_2=0 \\ F_1\begin{pmatrix}x_1\\x_2\end{pmatrix}, \text{ якщо } y_1=1;\ y_2=1 \end{cases} = \begin{cases} \begin{bmatrix}x_1\\x_2\oplus 1\end{bmatrix}, \text{ якщо } y_1=0;\ y_2=0 \\ \begin{bmatrix}x_1\oplus 1\\x_2\end{bmatrix}, \text{ якщо } y_1=0;\ y_2=1 \\ \begin{bmatrix}x_1\oplus 1\\x_2\oplus 1\end{bmatrix}, \text{ якщо } y_1=1;\ y_2=0 \\ \begin{bmatrix}x_1\\x_2\end{bmatrix}, \text{ якщо } y_1=1;\ y_2=1 \end{cases} = \begin{bmatrix}x_1\oplus y_1\oplus y_2\\x_2\oplus y_2\oplus 1\end{bmatrix} = O^*_{1,8};$$

$$O_{7,19,1,13}=\begin{cases} F_7\begin{pmatrix}x_1\\x_2\end{pmatrix}, \text{ якщо } y_1=0;\ y_2=0 \\ F_{19}\begin{pmatrix}x_1\\x_2\end{pmatrix}, \text{ якщо } y_1=0;\ y_2=1 \\ F_1\begin{pmatrix}x_1\\x_2\end{pmatrix}, \text{ якщо } y_1=1;\ y_2=0 \\ F_{13}\begin{pmatrix}x_1\\x_2\end{pmatrix}, \text{ якщо } y_1=1;\ y_2=1 \end{cases} = \begin{cases} \begin{bmatrix}x_1\\x_2\oplus 1\end{bmatrix}, \text{ якщо } y_1=0;\ y_2=0 \\ \begin{bmatrix}x_1\oplus 1\\x_2\oplus 1\end{bmatrix}, \text{ якщо } y_1=0;\ y_2=1 \\ \begin{bmatrix}x_1\\x_2\end{bmatrix}, \text{ якщо } y_1=1;\ y_2=0 \\ \begin{bmatrix}x_1\oplus 1\\x_2\end{bmatrix}, \text{ якщо } y_1=1;\ y_2=1 \end{cases} = \begin{bmatrix}x_1\oplus y_2\\x_2\oplus y_1\oplus 1\end{bmatrix} = O^*_{1,10};$$

$$O_{19,7,1,13}=\begin{cases} F_{19}\begin{pmatrix}x_1\\x_2\end{pmatrix}, \text{ якщо } y_1=0;\ y_2=0 \\ F_7\begin{pmatrix}x_1\\x_2\end{pmatrix}, \text{ якщо } y_1=0;\ y_2=1 \\ F_1\begin{pmatrix}x_1\\x_2\end{pmatrix}, \text{ якщо } y_1=1;\ y_2=0 \\ F_{13}\begin{pmatrix}x_1\\x_2\end{pmatrix}, \text{ якщо } y_1=1;\ y_2=1 \end{cases} = \begin{cases} \begin{bmatrix}x_1\oplus 1\\x_2\oplus 1\end{bmatrix}, \text{ якщо } y_1=0;\ y_2=0 \\ \begin{bmatrix}x_1\\x_2\oplus 1\end{bmatrix}, \text{ якщо } y_1=0;\ y_2=1 \\ \begin{bmatrix}x_1\\x_2\end{bmatrix}, \text{ якщо } y_1=1;\ y_2=0 \\ \begin{bmatrix}x_1\oplus 1\\x_2\end{bmatrix}, \text{ якщо } y_1=1;\ y_2=1 \end{cases} = \begin{bmatrix}x_1\oplus y_1\oplus y_2\oplus 1\\x_2\oplus y_1\oplus 1\end{bmatrix} = O^*_{1,24}.$$

Результати побудови всієї групи операцій з точністю до перестановки наведено в табл. 2.1.

Таблиця 2.1

**Двохоперандні двохрозрядні операції криптографічного кодування на основі кортежу $F_1$, $F_7$, $F_{13}$, $F_{19}$**

| | **Операції інверсії** | | | |
|---|---|---|---|---|
| | $\begin{bmatrix}0\\0\end{bmatrix}$ | $\begin{bmatrix}0\\1\end{bmatrix}$ | $\begin{bmatrix}1\\0\end{bmatrix}$ | $\begin{bmatrix}1\\1\end{bmatrix}$ |
| **Базові операції** | $O_{1,7,13,19}=\begin{bmatrix}x_1\oplus y_1\\x_2\oplus y_2\end{bmatrix}$ | $O_{7,1,19,13}=\begin{bmatrix}x_1\oplus y_1\\x_2\oplus y_2\oplus 1\end{bmatrix}$ | $O_{13,19,1,7}=\begin{bmatrix}x_1\oplus y_1\oplus 1\\x_2\oplus y_2\end{bmatrix}$ | $O_{19,13,7,1}=\begin{bmatrix}x_1\oplus y_1\oplus 1\\x_2\oplus y_2\oplus 1\end{bmatrix}$ |
| | $O_{1,19,13,7}=\begin{bmatrix}x_1\oplus y_1\oplus y_2\\x_2\oplus y_2\end{bmatrix}$ | $O_{7,13,19,1}=\begin{bmatrix}x_1\oplus y_1\oplus y_2\\x_2\oplus y_2\oplus 1\end{bmatrix}$ | $O_{13,7,1,19}=\begin{bmatrix}x_1\oplus y_1\oplus y_2\oplus 1\\x_2\oplus y_2\end{bmatrix}$ | $O_{19,1,7,13}=\begin{bmatrix}x_1\oplus y_1\oplus y_2\\x_2\oplus y_2\end{bmatrix}$ |
| | $O_{1,7,19,13}=\begin{bmatrix}x_1\oplus y_1\\x_2\oplus y_1\oplus y_2\end{bmatrix}$ | $O_{7,1,13,19}=\begin{bmatrix}x_1\oplus y_1\\x_2\oplus y_1\oplus y_2\oplus 1\end{bmatrix}$ | $O_{13,19,7,1}=\begin{bmatrix}x_1\oplus y_1\oplus 1\\x_2\oplus y_1\oplus y_2\end{bmatrix}$ | $O_{19,13,1,7}=\begin{bmatrix}x_1\oplus y_1\oplus 1\\x_2\oplus y_1\oplus y_2\oplus 1\end{bmatrix}$ |
| **Операції перестановок** | $O_{1,13,7,19}=\begin{bmatrix}x_1\oplus y_2\\x_2\oplus y_1\end{bmatrix}$ | $O_{7,19,1,13}=\begin{bmatrix}x_1\oplus y_2\\x_2\oplus y_1\oplus 1\end{bmatrix}$ | $O_{13,1,19,7}=\begin{bmatrix}x_1\oplus y_2\oplus 1\\x_2\oplus y_1\end{bmatrix}$ | $O_{19,7,13,1}=\begin{bmatrix}x_1\oplus y_2\oplus 1\\x_2\oplus y_1\oplus 1\end{bmatrix}$ |
| | $O_{1,19,7,13}=\begin{bmatrix}x_1\oplus y_2\\x_2\oplus y_1\oplus y_2\end{bmatrix}$ | $O_{7,13,1,19}=\begin{bmatrix}x_1\oplus y_2\\x_2\oplus y_1\oplus y_2\oplus 1\end{bmatrix}$ | $O_{13,7,19,1}=\begin{bmatrix}x_1\oplus y_2\oplus 1\\x_2\oplus y_1\oplus y_2\end{bmatrix}$ | $O_{19,1,13,7}=\begin{bmatrix}x_1\oplus y_2\oplus 1\\x_2\oplus y_1\oplus y_2\oplus 1\end{bmatrix}$ |
| | $O_{1,19,7,13}=\begin{bmatrix}x_1\oplus y_1\oplus y_2\\x_2\oplus y_1\end{bmatrix}$ | $O_{7,19,13,1}=\begin{bmatrix}x_1\oplus y_1\oplus y_2\\x_2\oplus y_1\oplus 1\end{bmatrix}$ | $O_{13,1,7,19}=\begin{bmatrix}x_1\oplus y_1\oplus y_2\oplus 1\\x_2\oplus y_1\end{bmatrix}$ | $O_{19,7,1,13}=\begin{bmatrix}x_1\oplus y_1\oplus y_2\oplus 1\\x_2\oplus y_1\oplus 1\end{bmatrix}$ |

Як видно з табл. 2.1, з одного кортежу, який включає одноопераднді операції $F_1$, $F_7$, $F_{13}$, $F_{19}$ (двохоперандна операція $O_{1,7,13,19}$), шляхом перестановок елементів кортежу отримано 24 двохоперандні операції.

Візьмемо ще чотири симетричні двохрозрядні двохоперандні операції.

Розглянемо кортеж $F_2$, $F_7$, $F_{13}$, $F_{14}$.

Побудову узагальненої моделі операції виконаємо шляхом побудови таблиць істинності наявності операндів та таблиць істинності інверсій розрядів з подальшою мінімізацією відповідно до [12, 107].

$$O_{2,7,13,14}=\begin{cases} F_2\begin{pmatrix}x_1\\x_2\end{pmatrix}, \text{ якщо } y_1=0;\ y_2=0 \\ F_7\begin{pmatrix}x_1\\x_2\end{pmatrix}, \text{ якщо } y_1=0;\ y_2=1 \\ F_{13}\begin{pmatrix}x_1\\x_2\end{pmatrix}, \text{ якщо } y_1=1;\ y_2=0 \\ F_{14}\begin{pmatrix}x_1\\x_2\end{pmatrix}, \text{ якщо } y_1=1;\ y_2=1 \end{cases} = \begin{cases} \begin{bmatrix}x_1\oplus x_2\\x_2\end{bmatrix}, \text{ якщо } y_1=0;\ y_2=0 \\ \begin{bmatrix}x_1\\x_2\oplus 1\end{bmatrix}, \text{ якщо } y_1=0;\ y_2=1 \\ \begin{bmatrix}x_1\oplus 1\\x_2\end{bmatrix}, \text{ якщо } y_1=1;\ y_2=0 \\ \begin{bmatrix}x_1\oplus x_2\oplus 1\\x_2\end{bmatrix}, \text{ якщо } y_1=1;\ y_2=1 \end{cases} = \begin{bmatrix}x_1\oplus(y_1\oplus y_2)\cdot x_2\oplus y_1\\x_2\oplus\bar{y}_1\cdot y_2\end{bmatrix};$$

$$O_{2,7,14,13}=\begin{cases} F_2\begin{pmatrix}x_1\\x_2\end{pmatrix}, \text{ якщо } y_1=0;\ y_2=0 \\ F_7\begin{pmatrix}x_1\\x_2\end{pmatrix}, \text{ якщо } y_1=0;\ y_2=1 \\ F_{14}\begin{pmatrix}x_1\\x_2\end{pmatrix}, \text{ якщо } y_1=1;\ y_2=0 \\ F_{13}\begin{pmatrix}x_1\\x_2\end{pmatrix}, \text{ якщо } y_1=1;\ y_2=1 \end{cases} = \begin{cases} \begin{bmatrix}x_1\oplus x_2\\x_2\end{bmatrix}, \text{ якщо } y_1=0;\ y_2=0 \\ \begin{bmatrix}x_1\\x_2\oplus 1\end{bmatrix}, \text{ якщо } y_1=0;\ y_2=1 \\ \begin{bmatrix}x_1\oplus x_2\oplus 1\\x_2\end{bmatrix}, \text{ якщо } y_1=1;\ y_2=0 \\ \begin{bmatrix}x_1\oplus 1\\x_2\end{bmatrix}, \text{ якщо } y_1=1;\ y_2=1 \end{cases} = \begin{bmatrix}x_1\oplus\bar{y}_2\cdot x_2\oplus y_1\\x_2\oplus\bar{y}_1\cdot y_2\end{bmatrix};$$

$$O_{2,13,7,14}=\begin{cases} F_2\begin{pmatrix}x_1\\x_2\end{pmatrix}, \text{ якщо } y_1=0;\ y_2=0 \\ F_{13}\begin{pmatrix}x_1\\x_2\end{pmatrix}, \text{ якщо } y_1=0;\ y_2=1 \\ F_7\begin{pmatrix}x_1\\x_2\end{pmatrix}, \text{ якщо } y_1=1;\ y_2=0 \\ F_{14}\begin{pmatrix}x_1\\x_2\end{pmatrix}, \text{ якщо } y_1=1;\ y_2=1 \end{cases} = \begin{cases} \begin{bmatrix}x_1\oplus x_2\\x_2\end{bmatrix}, \text{ якщо } y_1=0;\ y_2=0 \\ \begin{bmatrix}x_1\oplus 1\\x_2\end{bmatrix}, \text{ якщо } y_1=0;\ y_2=1 \\ \begin{bmatrix}x_1\\x_2\oplus 1\end{bmatrix}, \text{ якщо } y_1=1;\ y_2=0 \\ \begin{bmatrix}x_1\oplus x_2\oplus 1\\x_2\end{bmatrix}, \text{ якщо } y_1=1;\ y_2=1 \end{cases} = \begin{bmatrix}x_1\oplus(y_1\oplus y_2)\cdot x_2\oplus y_2\\x_2\oplus y_1\cdot\bar{y}_2\end{bmatrix};$$

$$O_{2,13,14,7}=\begin{cases}F_2\begin{pmatrix}x_1\\x_2\end{pmatrix}, \text{ якщо } y_1=0;\ y_2=0\\ F_{13}\begin{pmatrix}x_1\\x_2\end{pmatrix}, \text{ якщо } y_1=0;\ y_2=1\\ F_{14}\begin{pmatrix}x_1\\x_2\end{pmatrix}, \text{ якщо } y_1=1;\ y_2=0\\ F_7\begin{pmatrix}x_1\\x_2\end{pmatrix}, \text{ якщо } y_1=1;\ y_2=1\end{cases}=\begin{cases}\begin{bmatrix}x_1\oplus x_2\\x_2\end{bmatrix}, \text{ якщо } y_1=0;\ y_2=0\\ \begin{bmatrix}x_1\oplus 1\\x_2\end{bmatrix}, \text{ якщо } y_1=0;\ y_2=1\\ \begin{bmatrix}x_1\oplus x_2\oplus 1\\x_2\end{bmatrix}, \text{ якщо } y_1=1;\ y_2=0\\ \begin{bmatrix}x_1\\x_2\oplus 1\end{bmatrix}, \text{ якщо } y_1=1;\ y_2=1\end{cases}=\begin{bmatrix}x_1\oplus \bar{y}_2\cdot x_2\oplus y_1\oplus y_2\\x_2\oplus y_1\cdot y_2\end{bmatrix};$$

$$O_{2,14,13,7}=\begin{cases}F_2\begin{pmatrix}x_1\\x_2\end{pmatrix}, \text{ якщо } y_1=0;\ y_2=0\\ F_{14}\begin{pmatrix}x_1\\x_2\end{pmatrix}, \text{ якщо } y_1=0;\ y_2=1\\ F_{13}\begin{pmatrix}x_1\\x_2\end{pmatrix}, \text{ якщо } y_1=1;\ y_2=0\\ F_7\begin{pmatrix}x_1\\x_2\end{pmatrix}, \text{ якщо } y_1=1;\ y_2=1\end{cases}=\begin{cases}\begin{bmatrix}x_1\oplus x_2\\x_2\end{bmatrix}, \text{ якщо } y_1=0;\ y_2=0\\ \begin{bmatrix}x_1\oplus x_2\oplus 1\\x_2\end{bmatrix}, \text{ якщо } y_1=0;\ y_2=1\\ \begin{bmatrix}x_1\oplus 1\\x_2\end{bmatrix}, \text{ якщо } y_1=1;\ y_2=0\\ \begin{bmatrix}x_1\\x_2\oplus 1\end{bmatrix}, \text{ якщо } y_1=1;\ y_2=1\end{cases}=\begin{bmatrix}x_1\oplus \bar{y}_1\cdot x_2\oplus y_1\oplus y_2\\x_2\oplus \bar{y}_1\cdot y_2\end{bmatrix};$$

$$O_{2,14,7,13}=\begin{cases}F_2\begin{pmatrix}x_1\\x_2\end{pmatrix}, \text{ якщо } y_1=0;\ y_2=0\\ F_{14}\begin{pmatrix}x_1\\x_2\end{pmatrix}, \text{ якщо } y_1=0;\ y_2=1\\ F_{17}\begin{pmatrix}x_1\\x_2\end{pmatrix}, \text{ якщо } y_1=1;\ y_2=0\\ F_{13}\begin{pmatrix}x_1\\x_2\end{pmatrix}, \text{ якщо } y_1=1;\ y_2=1\end{cases}=\begin{cases}\begin{bmatrix}x_1\oplus x_2\\x_2\end{bmatrix}, \text{ якщо } y_1=0;\ y_2=0\\ \begin{bmatrix}x_1\oplus x_2\oplus 1\\x_2\end{bmatrix}, \text{ якщо } y_1=0;\ y_2=1\\ \begin{bmatrix}x_1\\x_2\oplus 1\end{bmatrix}, \text{ якщо } y_1=1;\ y_2=0\\ \begin{bmatrix}x_1\oplus 1\\x_2\end{bmatrix}, \text{ якщо } y_1=1;\ y_2=1\end{cases}=\begin{bmatrix}x_1\oplus \bar{y}_1\cdot x_2\oplus y_2\\x_2\oplus y_1\cdot \bar{y}_2\end{bmatrix};$$

$$O_{7,2,13,14}=\begin{cases}F_7\begin{pmatrix}x_1\\x_2\end{pmatrix}, \text{ якщо } y_1=0;\ y_2=0\\ F_2\begin{pmatrix}x_1\\x_2\end{pmatrix}, \text{ якщо } y_1=0;\ y_2=1\\ F_{13}\begin{pmatrix}x_1\\x_2\end{pmatrix}, \text{ якщо } y_1=1;\ y_2=0\\ F_{14}\begin{pmatrix}x_1\\x_2\end{pmatrix}, \text{ якщо } y_1=1;\ y_2=1\end{cases}=\begin{cases}\begin{bmatrix}x_1\\x_2\oplus 1\end{bmatrix}, \text{ якщо } y_1=0;\ y_2=0\\ \begin{bmatrix}x_1\oplus x_2\\x_2\end{bmatrix}, \text{ якщо } y_1=0;\ y_2=1\\ \begin{bmatrix}x_1\oplus 1\\x_2\end{bmatrix}, \text{ якщо } y_1=1;\ y_2=0\\ \begin{bmatrix}x_1\oplus x_2\oplus 1\\x_2\end{bmatrix}, \text{ якщо } y_1=1;\ y_2=1\end{cases}=\begin{bmatrix}x_1\oplus y_2\cdot x_2\oplus y_1\\x_2\oplus \bar{y}_1\cdot \bar{y}_2\end{bmatrix};$$

$$O_{7,2,14,13}=\begin{cases}F_7\begin{pmatrix}x_1\\x_2\end{pmatrix}, \text{ якщо } y_1=0;\ y_2=0\\ F_2\begin{pmatrix}x_1\\x_2\end{pmatrix}, \text{ якщо } y_1=0;\ y_2=1\\ F_{14}\begin{pmatrix}x_1\\x_2\end{pmatrix}, \text{ якщо } y_1=1;\ y_2=0\\ F_{13}\begin{pmatrix}x_1\\x_2\end{pmatrix}, \text{ якщо } y_1=1;\ y_2=1\end{cases}=\begin{cases}\begin{bmatrix}x_1\\x_2\oplus 1\end{bmatrix}, \text{ якщо } y_1=0;\ y_2=0\\ \begin{bmatrix}x_1\oplus x_2\\x_2\end{bmatrix}, \text{ якщо } y_1=0;\ y_2=1\\ \begin{bmatrix}x_1\oplus x_2\oplus 1\\x_2\end{bmatrix}, \text{ якщо } y_1=1;\ y_2=0\\ \begin{bmatrix}x_1\oplus 1\\x_2\end{bmatrix}, \text{ якщо } y_1=1;\ y_2=1\end{cases}=\begin{bmatrix}x_1\oplus (y_1\oplus y_2)\cdot x_2\oplus y_1\\x_2\oplus \bar{y}_1\cdot \bar{y}_2\end{bmatrix};$$

$$O_{7,13,2,14}=\begin{cases} F_7\begin{pmatrix}x_1\\x_2\end{pmatrix},\ якщо y_1=0;\ y_2=0 \\ F_{13}\begin{pmatrix}x_1\\x_2\end{pmatrix},\ якщо y_1=0;\ y_2=1 \\ F_2\begin{pmatrix}x_1\\x_2\end{pmatrix},\ якщо y_1=1;\ y_2=0 \\ F_{14}\begin{pmatrix}x_1\\x_2\end{pmatrix},\ якщо y_1=1;\ y_2=1 \end{cases}=\begin{cases} \begin{bmatrix}x_1\\x_2\oplus 1\end{bmatrix},\ якщо y_1=0;\ y_2=0 \\ \begin{bmatrix}x_1\oplus 1\\x_2\end{bmatrix},\ якщо y_1=0;\ y_2=1 \\ \begin{bmatrix}x_1\oplus x_2\\x_2\end{bmatrix},\ якщо y_1=1;\ y_2=0 \\ \begin{bmatrix}x_1\oplus x_2\oplus 1\\x_2\end{bmatrix},\ якщо y_1=1;\ y_2=1 \end{cases}=\begin{bmatrix}x_1\oplus y_1\cdot x_2\oplus y_2\\x_2\oplus \bar{y}_1\cdot \bar{y}_2\end{bmatrix};$$

$$O_{7,13,14,2}=\begin{cases} F_7\begin{pmatrix}x_1\\x_2\end{pmatrix},\ якщо y_1=0;\ y_2=0 \\ F_{13}\begin{pmatrix}x_1\\x_2\end{pmatrix},\ якщо y_1=0;\ y_2=1 \\ F_{14}\begin{pmatrix}x_1\\x_2\end{pmatrix},\ якщо y_1=1;\ y_2=0 \\ F_2\begin{pmatrix}x_1\\x_2\end{pmatrix},\ якщо y_1=1;\ y_2=1 \end{cases}=\begin{cases} \begin{bmatrix}x_1\\x_2\oplus 1\end{bmatrix},\ якщо y_1=0;\ y_2=0 \\ \begin{bmatrix}x_1\oplus 1\\x_2\end{bmatrix},\ якщо y_1=0;\ y_2=1 \\ \begin{bmatrix}x_1\oplus x_2\oplus 1\\x_2\end{bmatrix},\ якщо y_1=1;\ y_2=0 \\ \begin{bmatrix}x_1\oplus x_2\\x_2\end{bmatrix},\ якщо y_1=1;\ y_2=1 \end{cases}=\begin{bmatrix}x_1\oplus (y_1\oplus y_2)\cdot x_2\oplus y_2\\x_2\oplus \bar{y}_1\cdot \bar{y}_2\end{bmatrix};$$

$$O_{7,14,13,2}=\begin{cases} F_7\begin{pmatrix}x_1\\x_2\end{pmatrix},\ якщо y_1=0;\ y_2=0 \\ F_{14}\begin{pmatrix}x_1\\x_2\end{pmatrix},\ якщо y_1=0;\ y_2=1 \\ F_{13}\begin{pmatrix}x_1\\x_2\end{pmatrix},\ якщо y_1=1;\ y_2=0 \\ F_2\begin{pmatrix}x_1\\x_2\end{pmatrix},\ якщо y_1=1;\ y_2=1 \end{cases}=\begin{cases} \begin{bmatrix}x_1\\x_2\oplus 1\end{bmatrix},\ якщо y_1=0;\ y_2=0 \\ \begin{bmatrix}x_1\oplus x_2\oplus 1\\x_2\end{bmatrix},\ якщо y_1=0;\ y_2=1 \\ \begin{bmatrix}x_1\oplus 1\\x_2\end{bmatrix},\ якщо y_1=1;\ y_2=0 \\ \begin{bmatrix}x_1\oplus x_2\\x_2\end{bmatrix},\ якщо y_1=1;\ y_2=1 \end{cases}=\begin{bmatrix}x_1\oplus y_2\cdot x_2\oplus y_1\oplus y_2\\x_2\oplus \bar{y}_1\cdot \bar{y}_2\end{bmatrix};$$

$$O_{7,14,2,13}=\begin{cases} F_7\begin{pmatrix}x_1\\x_2\end{pmatrix},\ якщо y_1=0;\ y_2=0 \\ F_{14}\begin{pmatrix}x_1\\x_2\end{pmatrix},\ якщо y_1=0;\ y_2=1 \\ F_2\begin{pmatrix}x_1\\x_2\end{pmatrix},\ якщо y_1=1;\ y_2=0 \\ F_{13}\begin{pmatrix}x_1\\x_2\end{pmatrix},\ якщо y_1=1;\ y_2=1 \end{cases}=\begin{cases} \begin{bmatrix}x_1\\x_2\oplus 1\end{bmatrix},\ якщо y_1=0;\ y_2=0 \\ \begin{bmatrix}x_1\oplus x_2\oplus 1\\x_2\end{bmatrix},\ якщо y_1=0;\ y_2=1 \\ \begin{bmatrix}x_1\oplus x_2\\x_2\end{bmatrix},\ якщо y_1=1;\ y_2=0 \\ \begin{bmatrix}x_1\oplus 1\\x_2\end{bmatrix},\ якщо y_1=1;\ y_2=1 \end{cases}=\begin{bmatrix}x_1\oplus (y_1\oplus y_2)\cdot x_2\oplus y_2\\x_2\oplus \bar{y}_1\cdot \bar{y}_2\end{bmatrix};$$

$$O_{13,2,7,14}=\begin{cases} F_{13}\begin{pmatrix}x_1\\x_2\end{pmatrix}, \text{ якщо } y_1=0;\ y_2=0 \\ F_{2}\begin{pmatrix}x_1\\x_2\end{pmatrix}, \text{ якщо } y_1=0;\ y_2=1 \\ F_{7}\begin{pmatrix}x_1\\x_2\end{pmatrix}, \text{ якщо } y_1=1;\ y_2=0 \\ F_{14}\begin{pmatrix}x_1\\x_2\end{pmatrix}, \text{ якщо } y_1=1;\ y_2=1 \end{cases} = \begin{cases} \begin{bmatrix}x_1\oplus 1\\ x_2\end{bmatrix}, \text{ якщо } y_1=0;\ y_2=0 \\ \begin{bmatrix}x_1\oplus x_2\\ x_2\end{bmatrix}, \text{ якщо } y_1=0;\ y_2=1 \\ \begin{bmatrix}x_1\\ x_2\oplus 1\end{bmatrix}, \text{ якщо } y_1=1;\ y_2=0 \\ \begin{bmatrix}x_1\oplus x_2\oplus 1\\ x_2\end{bmatrix}, \text{ якщо } y_1=1;\ y_2=1 \end{cases} = \begin{bmatrix}x_1\oplus y_2\cdot x_2\oplus y_1\oplus y_2\oplus 1\\ x_2\oplus y_1\cdot \bar{y}_2\end{bmatrix};$$

$$O_{13,2,14,7}=\begin{cases} F_{13}\begin{pmatrix}x_1\\x_2\end{pmatrix}, \text{ якщо } y_1=0;\ y_2=0 \\ F_{2}\begin{pmatrix}x_1\\x_2\end{pmatrix}, \text{ якщо } y_1=0;\ y_2=1 \\ F_{14}\begin{pmatrix}x_1\\x_2\end{pmatrix}, \text{ якщо } y_1=1;\ y_2=0 \\ F_{7}\begin{pmatrix}x_1\\x_2\end{pmatrix}, \text{ якщо } y_1=1;\ y_2=1 \end{cases} = \begin{cases} \begin{bmatrix}x_1\oplus 1\\ x_2\end{bmatrix}, \text{ якщо } y_1=0;\ y_2=0 \\ \begin{bmatrix}x_1\oplus x_2\\ x_2\end{bmatrix}, \text{ якщо } y_1=0;\ y_2=1 \\ \begin{bmatrix}x_1\oplus x_2\oplus 1\\ x_2\end{bmatrix}, \text{ якщо } y_1=1;\ y_2=0 \\ \begin{bmatrix}x_1\\ x_2\oplus 1\end{bmatrix}, \text{ якщо } y_1=1;\ y_2=1 \end{cases} = \begin{bmatrix}x_1\oplus (y_1\oplus y_2)\cdot x_2\oplus y_2\oplus 1\\ x_2\oplus y_1\cdot y_2\end{bmatrix};$$

$$O_{13,7,2,14}=\begin{cases} F_{13}\begin{pmatrix}x_1\\x_2\end{pmatrix}, \text{ якщо } y_1=0;\ y_2=0 \\ F_{7}\begin{pmatrix}x_1\\x_2\end{pmatrix}, \text{ якщо } y_1=0;\ y_2=1 \\ F_{2}\begin{pmatrix}x_1\\x_2\end{pmatrix}, \text{ якщо } y_1=1;\ y_2=0 \\ F_{14}\begin{pmatrix}x_1\\x_2\end{pmatrix}, \text{ якщо } y_1=1;\ y_2=1 \end{cases} = \begin{cases} \begin{bmatrix}x_1\oplus 1\\ x_2\end{bmatrix}, \text{ якщо } y_1=0;\ y_2=0 \\ \begin{bmatrix}x_1\\ x_2\oplus 1\end{bmatrix}, \text{ якщо } y_1=0;\ y_2=1 \\ \begin{bmatrix}x_1\oplus x_2\\ x_2\end{bmatrix}, \text{ якщо } y_1=1;\ y_2=0 \\ \begin{bmatrix}x_1\oplus x_2\oplus 1\\ x_2\end{bmatrix}, \text{ якщо } y_1=1;\ y_2=1 \end{cases} = \begin{bmatrix}x_1\oplus y_1\cdot x_2\oplus y_1\oplus y_2\oplus 1\\ x_2\oplus \bar{y}_1\cdot y_2\end{bmatrix};$$

$$O_{13,7,14,2}=\begin{cases} F_{13}\begin{pmatrix}x_1\\x_2\end{pmatrix}, \text{ якщо } y_1=0;\ y_2=0 \\ F_{7}\begin{pmatrix}x_1\\x_2\end{pmatrix}, \text{ якщо } y_1=0;\ y_2=1 \\ F_{14}\begin{pmatrix}x_1\\x_2\end{pmatrix}, \text{ якщо } y_1=1;\ y_2=0 \\ F_{2}\begin{pmatrix}x_1\\x_2\end{pmatrix}, \text{ якщо } y_1=1;\ y_2=1 \end{cases} = \begin{cases} \begin{bmatrix}x_1\oplus 1\\ x_2\end{bmatrix}, \text{ якщо } y_1=0;\ y_2=0 \\ \begin{bmatrix}x_1\\ x_2\oplus 1\end{bmatrix}, \text{ якщо } y_1=0;\ y_2=1 \\ \begin{bmatrix}x_1\oplus x_2\oplus 1\\ x_2\end{bmatrix}, \text{ якщо } y_1=1;\ y_2=0 \\ \begin{bmatrix}x_1\oplus x_2\\ x_2\end{bmatrix}, \text{ якщо } y_1=1;\ y_2=1 \end{cases} = \begin{bmatrix}x_1\oplus y_1\cdot x_2\oplus y_2\oplus 1\\ x_2\oplus \bar{y}_1\cdot y_2\end{bmatrix};$$

$$O_{13,14,2,7}=\begin{cases} F_{13}\begin{pmatrix}x_1\\x_2\end{pmatrix}, \text{ якщо } y_1=0;\ y_2=0 \\ F_{14}\begin{pmatrix}x_1\\x_2\end{pmatrix}, \text{ якщо } y_1=0;\ y_2=1 \\ F_{2}\begin{pmatrix}x_1\\x_2\end{pmatrix}, \text{ якщо } y_1=1;\ y_2=0 \\ F_{7}\begin{pmatrix}x_1\\x_2\end{pmatrix}, \text{ якщо } y_1=1;\ y_2=1 \end{cases} = \begin{cases} \begin{bmatrix}x_1\oplus 1\\ x_2\end{bmatrix}, \text{ якщо } y_1=0;\ y_2=0 \\ \begin{bmatrix}x_1\oplus x_2\oplus 1\\ x_2\end{bmatrix}, \text{ якщо } y_1=0;\ y_2=1 \\ \begin{bmatrix}x_1\oplus x_2\\ x_2\end{bmatrix}, \text{ якщо } y_1=1;\ y_2=0 \\ \begin{bmatrix}x_1\\ x_2\oplus 1\end{bmatrix}, \text{ якщо } y_1=1;\ y_2=1 \end{cases} = \begin{bmatrix}x_1\oplus(y_1\oplus y_2)\cdot x_2\oplus y_1\oplus 1\\ x_2\oplus y_1\cdot y_2\end{bmatrix};$$

$$O_{13,14,7,2}=\begin{cases} F_{13}\begin{pmatrix}x_1\\x_2\end{pmatrix}, \text{ якщо } y_1=0;\ y_2=0 \\ F_{14}\begin{pmatrix}x_1\\x_2\end{pmatrix}, \text{ якщо } y_1=0;\ y_2=1 \\ F_{7}\begin{pmatrix}x_1\\x_2\end{pmatrix}, \text{ якщо } y_1=1;\ y_2=0 \\ F_{2}\begin{pmatrix}x_1\\x_2\end{pmatrix}, \text{ якщо } y_1=1;\ y_2=1 \end{cases} = \begin{cases} \begin{bmatrix}x_1\oplus 1\\ x_2\end{bmatrix}, \text{ якщо } y_1=0;\ y_2=0 \\ \begin{bmatrix}x_1\oplus x_2\oplus 1\\ x_2\end{bmatrix}, \text{ якщо } y_1=0;\ y_2=1 \\ \begin{bmatrix}x_1\\ x_2\oplus 1\end{bmatrix}, \text{ якщо } y_1=1;\ y_2=0 \\ \begin{bmatrix}x_1\oplus x_2\\ x_2\end{bmatrix}, \text{ якщо } y_1=1;\ y_2=1 \end{cases} = \begin{bmatrix}x_1\oplus y_2\cdot x_2\oplus y_1\oplus 1\\ x_2\oplus y_1\cdot \bar{y}_2\end{bmatrix};$$

$$O_{14,2,7,13}=\begin{cases} F_{14}\begin{pmatrix}x_1\\x_2\end{pmatrix}, \text{ якщо } y_1=0;\ y_2=0 \\ F_{2}\begin{pmatrix}x_1\\x_2\end{pmatrix}, \text{ якщо } y_1=0;\ y_2=1 \\ F_{7}\begin{pmatrix}x_1\\x_2\end{pmatrix}, \text{ якщо } y_1=1;\ y_2=0 \\ F_{13}\begin{pmatrix}x_1\\x_2\end{pmatrix}, \text{ якщо } y_1=1;\ y_2=1 \end{cases} = \begin{cases} \begin{bmatrix}x_1\oplus x_2\oplus 1\\ x_2\end{bmatrix}, \text{ якщо } y_1=0;\ y_2=0 \\ \begin{bmatrix}x_1\oplus x_2\\ x_2\end{bmatrix}, \text{ якщо } y_1=0;\ y_2=1 \\ \begin{bmatrix}x_1\\ x_2\oplus 1\end{bmatrix}, \text{ якщо } y_1=1;\ y_2=0 \\ \begin{bmatrix}x_1\oplus 1\\ x_2\end{bmatrix}, \text{ якщо } y_1=1;\ y_2=1 \end{cases} = \begin{bmatrix}x_1\oplus \bar{y}_1\cdot x_2\oplus y_1\oplus y_2\oplus 1\\ x_2\oplus y_1\cdot \bar{y}_2\end{bmatrix};$$

$$O_{14,2,13,7}=\begin{cases} F_{14}\begin{pmatrix}x_1\\x_2\end{pmatrix}, \text{ якщо } y_1=0;\ y_2=0 \\ F_{2}\begin{pmatrix}x_1\\x_2\end{pmatrix}, \text{ якщо } y_1=0;\ y_2=1 \\ F_{13}\begin{pmatrix}x_1\\x_2\end{pmatrix}, \text{ якщо } y_1=1;\ y_2=0 \\ F_{7}\begin{pmatrix}x_1\\x_2\end{pmatrix}, \text{ якщо } y_1=1;\ y_2=1 \end{cases} = \begin{cases} \begin{bmatrix}x_1\oplus x_2\oplus 1\\ x_2\end{bmatrix}, \text{ якщо } y_1=0;\ y_2=0 \\ \begin{bmatrix}x_1\oplus x_2\\ x_2\end{bmatrix}, \text{ якщо } y_1=0;\ y_2=1 \\ \begin{bmatrix}x_1\oplus 1\\ x_2\end{bmatrix}, \text{ якщо } y_1=1;\ y_2=0 \\ \begin{bmatrix}x_1\\ x_2\oplus 1\end{bmatrix}, \text{ якщо } y_1=1;\ y_2=1 \end{cases} = \begin{bmatrix}x_1\oplus \bar{y}_1\cdot x_2\oplus y_2\oplus 1\\ x_2\oplus y_1\cdot y_2\end{bmatrix};$$

$$O_{14,7,2,13}=\begin{cases} F_{14}\begin{pmatrix}x_1\\x_2\end{pmatrix}, \text{ якщо } y_1=0;\ y_2=0 \\ F_{7}\begin{pmatrix}x_1\\x_2\end{pmatrix}, \text{ якщо } y_1=0;\ y_2=1 \\ F_{2}\begin{pmatrix}x_1\\x_2\end{pmatrix}, \text{ якщо } y_1=1;\ y_2=0 \\ F_{13}\begin{pmatrix}x_1\\x_2\end{pmatrix}, \text{ якщо } y_1=1;\ y_2=1 \end{cases} = \begin{cases} \begin{bmatrix}x_1\oplus x_2\oplus 1\\ x_2\end{bmatrix}, \text{ якщо } y_1=0;\ y_2=0 \\ \begin{bmatrix}x_1\\ x_2\oplus 1\end{bmatrix}, \text{ якщо } y_1=0;\ y_2=1 \\ \begin{bmatrix}x_1\oplus x_2\\ x_2\end{bmatrix}, \text{ якщо } y_1=1;\ y_2=0 \\ \begin{bmatrix}x_1\oplus 1\\ x_2\end{bmatrix}, \text{ якщо } y_1=1;\ y_2=1 \end{cases} = \begin{bmatrix}x_1\oplus \bar{y}_2\cdot x_2\oplus y_1\oplus y_2\oplus 1\\ x_2\oplus \bar{y}_1\cdot y_2\end{bmatrix};$$

$$O_{14,7,13,2}=\begin{cases} F_{14}\begin{pmatrix}x_1\\x_2\end{pmatrix}, \text{ якщо } y_1=0;\ y_2=0 \\ F_{7}\begin{pmatrix}x_1\\x_2\end{pmatrix}, \text{ якщо } y_1=0;\ y_2=1 \\ F_{13}\begin{pmatrix}x_1\\x_2\end{pmatrix}, \text{ якщо } y_1=1;\ y_2=0 \\ F_{2}\begin{pmatrix}x_1\\x_2\end{pmatrix}, \text{ якщо } y_1=1;\ y_2=1 \end{cases} = \begin{cases} \begin{bmatrix}x_1\oplus x_2\oplus 1\\ x_2\end{bmatrix}, \text{ якщо } y_1=0;\ y_2=0 \\ \begin{bmatrix}x_1\\ x_2\oplus 1\end{bmatrix}, \text{ якщо } y_1=0;\ y_2=1 \\ \begin{bmatrix}x_1\oplus 1\\ x_2\end{bmatrix}, \text{ якщо } y_1=1;\ y_2=0 \\ \begin{bmatrix}x_1\oplus x_2\\ x_2\end{bmatrix}, \text{ якщо } y_1=1;\ y_2=1 \end{cases} = \begin{bmatrix}x_1\oplus (\overline{y_1\oplus y_2})\cdot x_2\oplus y_2\oplus 1\\ x_2\oplus \bar{y}_1\cdot y_2\end{bmatrix};$$

$$O_{14,13,2,7}=\begin{cases} F_{14}\begin{pmatrix}x_1\\x_2\end{pmatrix}, \text{ якщо } y_1=0;\ y_2=0 \\ F_{13}\begin{pmatrix}x_1\\x_2\end{pmatrix}, \text{ якщо } y_1=0;\ y_2=1 \\ F_{2}\begin{pmatrix}x_1\\x_2\end{pmatrix}, \text{ якщо } y_1=1;\ y_2=0 \\ F_{7}\begin{pmatrix}x_1\\x_2\end{pmatrix}, \text{ якщо } y_1=1;\ y_2=1 \end{cases} = \begin{cases} \begin{bmatrix}x_1\oplus x_2\oplus 1\\ x_2\end{bmatrix}, \text{ якщо } y_1=0;\ y_2=0 \\ \begin{bmatrix}x_1\oplus 1\\ x_2\end{bmatrix}, \text{ якщо } y_1=0;\ y_2=1 \\ \begin{bmatrix}x_1\oplus x_2\\ x_2\end{bmatrix}, \text{ якщо } y_1=1;\ y_2=0 \\ \begin{bmatrix}x_1\\ x_2\oplus 1\end{bmatrix}, \text{ якщо } y_1=1;\ y_2=1 \end{cases} = \begin{bmatrix}x_1\oplus \bar{y}_2\cdot x_2\oplus y_1\oplus 1\\ x_2\oplus y_1\cdot y_2\end{bmatrix};$$

$$O_{14,13,7,2}=\begin{cases} F_{14}\begin{pmatrix}x_1\\x_2\end{pmatrix}, \text{ якщо } y_1=0;\ y_2=0 \\ F_{13}\begin{pmatrix}x_1\\x_2\end{pmatrix}, \text{ якщо } y_1=0;\ y_2=1 \\ F_{7}\begin{pmatrix}x_1\\x_2\end{pmatrix}, \text{ якщо } y_1=1;\ y_2=0 \\ F_{2}\begin{pmatrix}x_1\\x_2\end{pmatrix}, \text{ якщо } y_1=1;\ y_2=1 \end{cases} = \begin{cases} \begin{bmatrix}x_1\oplus x_2\oplus 1\\ x_2\end{bmatrix}, \text{ якщо } y_1=0;\ y_2=0 \\ \begin{bmatrix}x_1\oplus 1\\ x_2\end{bmatrix}, \text{ якщо } y_1=0;\ y_2=1 \\ \begin{bmatrix}x_1\\ x_2\oplus 1\end{bmatrix}, \text{ якщо } y_1=1;\ y_2=0 \\ \begin{bmatrix}x_1\oplus x_2\\ x_2\end{bmatrix}, \text{ якщо } y_1=1;\ y_2=1 \end{cases} = \begin{bmatrix}x_1\oplus (\overline{y_1\oplus y_2})\cdot x_2\oplus y_1\oplus 1\\ x_2\oplus y_1\cdot \bar{y}_2\end{bmatrix}.$$

Результати побудови групи двохоперандних двохрозрядних операцій криптографічного кодування на основі кортежу $F_2$, $F_7$, $F_{13}$, $F_{14}$ наведено в табл. 2.2.

Таблиця 2.2

**Двохоперандні двохрозрядні операції криптографічного кодування на основі кортежу $F_2$, $F_7, F_{13}$, $F_{14}$**

| | | | |
|---|---|---|---|
| $O_{2,7,14,13} = \begin{bmatrix} x_1 \oplus \bar{y}_2 \cdot x_2 \oplus y_1 \\ x_2 \oplus \bar{y}_1 \cdot y_2 \end{bmatrix}$ | $O_{7,2,13,14} = \begin{bmatrix} x_1 \oplus y_2 \cdot x_2 \oplus y_1 \\ x_2 \oplus \bar{y}_1 \cdot \bar{y}_2 \end{bmatrix}$ | $O_{13,2,7,14} = \begin{bmatrix} x_1 \oplus y_2 \cdot x_2 \oplus y_1 \oplus y_2 \oplus 1 \\ x_2 \oplus y_1 \cdot \bar{y}_2 \end{bmatrix}$ | $O_{14,2,7,13} = \begin{bmatrix} x_1 \oplus \bar{y}_1 \cdot x_2 \oplus y_1 \oplus y_2 \oplus 1 \\ x_2 \oplus y_1 \cdot \bar{y}_2 \end{bmatrix}$ |
| $O_{2,14,7,13} = \begin{bmatrix} x_1 \oplus \bar{y}_1 \cdot x_2 \oplus y_2 \\ x_2 \oplus y_1 \cdot \bar{y}_2 \end{bmatrix}$ | $O_{7,13,2,14} = \begin{bmatrix} x_1 \oplus y_1 \cdot x_2 \oplus y_2 \\ x_2 \oplus \bar{y}_1 \cdot \bar{y}_2 \end{bmatrix}$ | $O_{13,7,2,14} = \begin{bmatrix} x_1 \oplus y_1 \cdot x_2 \oplus y_1 \oplus y_2 \oplus 1 \\ x_2 \oplus \bar{y}_1 \cdot y_2 \end{bmatrix}$ | $O_{14,2,13,7} = \begin{bmatrix} x_1 \oplus \bar{y}_1 \cdot x_2 \oplus y_2 \oplus 1 \\ x_2 \oplus \bar{y}_1 \cdot \bar{y}_2 \end{bmatrix}$ |
| $O_{2,13,14,7} = \begin{bmatrix} x_1 \oplus \bar{y}_2 \cdot x_2 \oplus y_1 \oplus y_2 \\ x_2 \oplus y_1 \cdot y_2 \end{bmatrix}$ | $O_{7,14,13,2} = \begin{bmatrix} x_1 \oplus y_2 \cdot x_2 \oplus y_1 \oplus y_2 \\ x_2 \oplus \bar{y}_1 \cdot \bar{y}_2 \end{bmatrix}$ | $O_{13,7,14,2} = \begin{bmatrix} x_1 \oplus y_1 \cdot x_2 \oplus y_2 \oplus 1 \\ x_2 \oplus \bar{y}_1 \cdot y_2 \end{bmatrix}$ | $O_{14,7,2,13} = \begin{bmatrix} x_1 \oplus \bar{y}_2 \cdot x_2 \oplus y_1 \oplus y_2 \oplus 1 \\ x_2 \oplus \bar{y}_1 \cdot y_2 \end{bmatrix}$ |
| $O_{2,14,13,7} = \begin{bmatrix} x_1 \oplus \bar{y}_1 \cdot x_2 \oplus y_1 \oplus y_2 \\ x_2 \oplus \bar{y}_1 \cdot y_2 \end{bmatrix}$ | $O_{7,14,2,13} = \begin{bmatrix} x_1 \oplus (y_1 \oplus y_2) \cdot x_2 \oplus y_2 \\ x_2 \oplus \bar{y}_1 \cdot \bar{y}_2 \end{bmatrix}$ | $O_{13,14,2,7} = \begin{bmatrix} x_1 \oplus (y_1 \oplus y_2) \cdot x_2 \oplus y_1 \oplus 1 \\ x_2 \oplus y_1 \cdot y_2 \end{bmatrix}$ | $O_{14,7,13,2} = \begin{bmatrix} x_1 \oplus (\overline{y_1 \oplus y_2}) \cdot x_2 \oplus y_2 \oplus 1 \\ x_2 \oplus \bar{y}_1 \cdot y_2 \end{bmatrix}$ |
| $O_{2,7,13,14} = \begin{bmatrix} x_1 \oplus (y_1 \oplus y_2) \cdot x_2 \oplus y_1 \\ x_2 \oplus \bar{y}_1 \cdot y_2 \end{bmatrix}$ | $O_{7,2,14,13} = \begin{bmatrix} x_1 \oplus (y_1 \oplus y_2) \cdot x_2 \oplus y_1 \\ x_2 \oplus \bar{y}_1 \cdot \bar{y}_2 \end{bmatrix}$ | $O_{13,14,7,2} = \begin{bmatrix} x_1 \oplus y_2 \cdot x_2 \oplus y_1 \oplus 1 \\ x_2 \oplus y_1 \cdot \bar{y}_2 \end{bmatrix}$ | $O_{14,13,2,7} = \begin{bmatrix} x_1 \oplus \bar{y}_2 \cdot x_2 \oplus y_1 \oplus 1 \\ x_2 \oplus y_1 \cdot y_2 \end{bmatrix}$ |
| $O_{2,13,7,14} = \begin{bmatrix} x_1 \oplus (y_1 \oplus y_2) \cdot x_2 \oplus y_2 \\ x_2 \oplus y_1 \cdot \bar{y}_2 \end{bmatrix}$ | $O_{7,13,14,2} = \begin{bmatrix} x_1 \oplus (y_1 \oplus y_2) \cdot x_2 \oplus y_2 \\ x_2 \oplus \bar{y}_1 \cdot \bar{y}_2 \end{bmatrix}$ | $O_{13,2,14,7} = \begin{bmatrix} x_1 \oplus (y_1 \oplus y_2) \cdot x_2 \oplus y_2 \oplus 1 \\ x_2 \oplus y_1 \cdot y_2 \end{bmatrix}$ | $O_{14,13,7,2} = \begin{bmatrix} x_1 \oplus (\overline{y_1 \oplus y_2}) \cdot x_2 \oplus y_1 \oplus 1 \\ x_2 \oplus y_1 \cdot \bar{y}_2 \end{bmatrix}$ |

Розглянемо варіанти побудови двохрозрядних двохоперандних операцій криптоперетворення на основі кортежу $F_1,\ F_2,\ F_3,\ F_4$.

$$O_{1,2,3,4}=\begin{cases} F_1\begin{pmatrix}x_1\\x_2\end{pmatrix}, \text{ якщо } y_1=0;\ y_2=0 \\ F_2\begin{pmatrix}x_1\\x_2\end{pmatrix}, \text{ якщо } y_1=0;\ y_2=1 \\ F_3\begin{pmatrix}x_1\\x_2\end{pmatrix}, \text{ якщо } y_1=1;\ y_2=0 \\ F_4\begin{pmatrix}x_1\\x_2\end{pmatrix}, \text{ якщо } y_1=1;\ y_2=1 \end{cases} = \begin{cases} \begin{bmatrix}x_1\\x_2\end{bmatrix}, \text{ якщо } y_1=0;\ y_2=0 \\ \begin{bmatrix}x_1\oplus x_2\\x_2\end{bmatrix}, \text{ якщо } y_1=0;\ y_2=1 \\ \begin{bmatrix}x_1\\x_1\oplus x_2\end{bmatrix}, \text{ якщо } y_1=1;\ y_2=0 \\ \begin{bmatrix}x_2\\x_1\end{bmatrix}, \text{ якщо } y_1=1;\ y_2=1 \end{cases} = \begin{bmatrix} y_1\cdot y_2\cdot x_1\oplus y_2\cdot x_2 \\ y_1\cdot x_1\oplus \bar{y}_1\cdot \bar{y}_2\cdot x_2 \end{bmatrix};$$

$$O_{1,2,4,3}=\begin{cases} F_1\begin{pmatrix}x_1\\x_2\end{pmatrix}, \text{ якщо } y_1=0;\ y_2=0 \\ F_2\begin{pmatrix}x_1\\x_2\end{pmatrix}, \text{ якщо } y_1=0;\ y_2=1 \\ F_4\begin{pmatrix}x_1\\x_2\end{pmatrix}, \text{ якщо } y_1=1;\ y_2=0 \\ F_3\begin{pmatrix}x_1\\x_2\end{pmatrix}, \text{ якщо } y_1=1;\ y_2=1 \end{cases} = \begin{cases} \begin{bmatrix}x_1\\x_2\end{bmatrix}, \text{ якщо } y_1=0;\ y_2=0 \\ \begin{bmatrix}x_1\oplus x_2\\x_2\end{bmatrix}, \text{ якщо } y_1=0;\ y_2=1 \\ \begin{bmatrix}x_2\\x_1\end{bmatrix}, \text{ якщо } y_1=1;\ y_2=0 \\ \begin{bmatrix}x_1\\x_1\oplus x_2\end{bmatrix}, \text{ якщо } y_1=1;\ y_2=1 \end{cases} = \begin{bmatrix} y_1\cdot \bar{y}_2\cdot x_1\oplus (y_1\oplus y_2)\cdot x_2 \\ y_1\cdot x_1\oplus (y_1\vee \bar{y}_2)\cdot x_2 \end{bmatrix};$$

$$O_{1,3,2,4}=\begin{cases} F_1\begin{pmatrix}x_1\\x_2\end{pmatrix}, \text{ якщо } y_1=0;\ y_2=0 \\ F_3\begin{pmatrix}x_1\\x_2\end{pmatrix}, \text{ якщо } y_1=0;\ y_2=1 \\ F_2\begin{pmatrix}x_1\\x_2\end{pmatrix}, \text{ якщо } y_1=1;\ y_2=0 \\ F_4\begin{pmatrix}x_1\\x_2\end{pmatrix}, \text{ якщо } y_1=1;\ y_2=1 \end{cases} = \begin{cases} \begin{bmatrix}x_1\\x_2\end{bmatrix}, \text{ якщо } y_1=0;\ y_2=0 \\ \begin{bmatrix}x_1\\x_1\oplus x_2\end{bmatrix}, \text{ якщо } y_1=0;\ y_2=1 \\ \begin{bmatrix}x_1\oplus x_2\\x_2\end{bmatrix}, \text{ якщо } y_1=1;\ y_2=0 \\ \begin{bmatrix}x_2\\x_1\end{bmatrix}, \text{ якщо } y_1=1;\ y_2=1 \end{cases} = \begin{bmatrix} (\bar{y}_1\vee \bar{y}_2)\cdot x_1\oplus y_1\cdot x_2 \\ y_2\cdot x_1\oplus (\bar{y}_1\vee \bar{y}_2)\cdot x_2 \end{bmatrix};$$

$$O_{1,3,4,2}=\begin{cases} F_1\begin{pmatrix}x_1\\x_2\end{pmatrix}, \text{ якщо } y_1=0;\ y_2=0 \\ F_3\begin{pmatrix}x_1\\x_2\end{pmatrix}, \text{ якщо } y_1=0;\ y_2=1 \\ F_4\begin{pmatrix}x_1\\x_2\end{pmatrix}, \text{ якщо } y_1=1;\ y_2=0 \\ F_2\begin{pmatrix}x_1\\x_2\end{pmatrix}, \text{ якщо } y_1=1;\ y_2=1 \end{cases} = \begin{cases} \begin{bmatrix}x_1\\x_2\end{bmatrix}, \text{ якщо } y_1=0;\ y_2=0 \\ \begin{bmatrix}x_1\\x_1\oplus x_2\end{bmatrix}, \text{ якщо } y_1=0;\ y_2=1 \\ \begin{bmatrix}x_2\\x_1\end{bmatrix}, \text{ якщо } y_1=1;\ y_2=0 \\ \begin{bmatrix}x_1\oplus x_2\\x_2\end{bmatrix}, \text{ якщо } y_1=1;\ y_2=1 \end{cases} = \begin{bmatrix} (y_1\vee \bar{y}_2)\cdot x_1\oplus y_1\cdot x_2 \\ (y_1\oplus y_2)\cdot x_1\oplus (y_1\vee \bar{y}_2)\cdot x_2 \end{bmatrix};$$

$$O_{1,4,2,3}=\begin{cases} F_1\begin{pmatrix}x_1\\x_2\end{pmatrix}, \text{ якщо } y_1=0;\ y_2=0 \\ F_4\begin{pmatrix}x_1\\x_2\end{pmatrix}, \text{ якщо } y_1=0;\ y_2=1 \\ F_2\begin{pmatrix}x_1\\x_2\end{pmatrix}, \text{ якщо } y_1=1;\ y_2=0 \\ F_3\begin{pmatrix}x_1\\x_2\end{pmatrix}, \text{ якщо } y_1=1;\ y_2=1 \end{cases} = \begin{cases} \begin{bmatrix}x_1\\x_2\end{bmatrix}, \text{ якщо } y_1=0;\ y_2=0 \\ \begin{bmatrix}x_2\\x_1\end{bmatrix}, \text{ якщо } y_1=0;\ y_2=1 \\ \begin{bmatrix}x_1\oplus x_2\\x_2\end{bmatrix}, \text{ якщо } y_1=1;\ y_2=0 \\ \begin{bmatrix}x_1\\x_1\oplus x_2\end{bmatrix}, \text{ якщо } y_1=1;\ y_2=1 \end{cases} = \begin{bmatrix} (\bar{y}_1\vee y_2)\cdot x_1\oplus (y_1\oplus y_2)\cdot x_2 \\ y_2\cdot x_1\oplus (\bar{y}_1\vee y_2)\cdot x_2 \end{bmatrix};$$

$$O_{1,4,3,2}=\begin{cases} F_1\begin{pmatrix}x_1\\x_2\end{pmatrix}, \text{ якщо } y_1=0;\ y_2=0 \\ F_4\begin{pmatrix}x_1\\x_2\end{pmatrix}, \text{ якщо } y_1=0;\ y_2=1 \\ F_3\begin{pmatrix}x_1\\x_2\end{pmatrix}, \text{ якщо } y_1=1;\ y_2=0 \\ F_2\begin{pmatrix}x_1\\x_2\end{pmatrix}, \text{ якщо } y_1=1;\ y_2=1 \end{cases} = \begin{cases} \begin{bmatrix}x_1\\x_2\end{bmatrix}, \text{ якщо } y_1=0;\ y_2=0 \\ \begin{bmatrix}x_2\\x_1\end{bmatrix}, \text{ якщо } y_1=0;\ y_2=1 \\ \begin{bmatrix}x_1\\x_1\oplus x_2\end{bmatrix}, \text{ якщо } y_1=1;\ y_2=0 \\ \begin{bmatrix}x_1\oplus x_2\\x_1\end{bmatrix}, \text{ якщо } y_1=1;\ y_2=1 \end{cases} = \begin{bmatrix}(\bar{y}_1\vee y_2)\cdot x_1\oplus y_2\cdot x_2\\(\bar{y}_1\vee \bar{y}_2)\cdot x_1\oplus \bar{y}_2\cdot x_2\end{bmatrix};$$

$$O_{2,1,3,4}=\begin{cases} F_2\begin{pmatrix}x_1\\x_2\end{pmatrix}, \text{ якщо } y_1=0;\ y_2=0 \\ F_1\begin{pmatrix}x_1\\x_2\end{pmatrix}, \text{ якщо } y_1=0;\ y_2=1 \\ F_3\begin{pmatrix}x_1\\x_2\end{pmatrix}, \text{ якщо } y_1=1;\ y_2=0 \\ F_4\begin{pmatrix}x_1\\x_2\end{pmatrix}, \text{ якщо } y_1=1;\ y_2=1 \end{cases} = \begin{cases} \begin{bmatrix}x_1\oplus x_2\\x_2\end{bmatrix}, \text{ якщо } y_1=0;\ y_2=0 \\ \begin{bmatrix}x_1\\x_2\end{bmatrix}, \text{ якщо } y_1=0;\ y_2=1 \\ \begin{bmatrix}x_1\\x_1\oplus x_2\end{bmatrix}, \text{ якщо } y_1=1;\ y_2=0 \\ \begin{bmatrix}x_2\\x_1\end{bmatrix}, \text{ якщо } y_1=1;\ y_2=1 \end{cases} = \begin{bmatrix}(\bar{y}_1\vee \bar{y}_2)\cdot x_1\oplus \overline{(y_1\oplus y_2)}\cdot x_2\\y_1\cdot x_1\oplus(\bar{y}_1\vee \bar{y}_2)\cdot x_2\end{bmatrix};$$

$$O_{2,1,4,3}=\begin{cases} F_2\begin{pmatrix}x_1\\x_2\end{pmatrix}, \text{ якщо } y_1=0;\ y_2=0 \\ F_1\begin{pmatrix}x_1\\x_2\end{pmatrix}, \text{ якщо } y_1=0;\ y_2=1 \\ F_4\begin{pmatrix}x_1\\x_2\end{pmatrix}, \text{ якщо } y_1=1;\ y_2=0 \\ F_3\begin{pmatrix}x_1\\x_2\end{pmatrix}, \text{ якщо } y_1=1;\ y_2=1 \end{cases} = \begin{cases} \begin{bmatrix}x_1\oplus x_2\\x_2\end{bmatrix}, \text{ якщо } y_1=0;\ y_2=0 \\ \begin{bmatrix}x_1\\x_2\end{bmatrix}, \text{ якщо } y_1=0;\ y_2=1 \\ \begin{bmatrix}x_2\\x_1\end{bmatrix}, \text{ якщо } y_1=1;\ y_2=0 \\ \begin{bmatrix}x_1\\x_1\oplus x_2\end{bmatrix}, \text{ якщо } y_1=1;\ y_2=1 \end{cases} = \begin{bmatrix}(y_1\vee \bar{y}_2)\cdot x_1\oplus \bar{y}_2\cdot x_2\\y_1\cdot x_1\oplus(y_1\vee \bar{y}_2)\cdot x_2\end{bmatrix};$$

$$O_{2,3,1,4}=\begin{cases} F_2\begin{pmatrix}x_1\\x_2\end{pmatrix}, \text{ якщо } y_1=0;\ y_2=0 \\ F_3\begin{pmatrix}x_1\\x_2\end{pmatrix}, \text{ якщо } y_1=0;\ y_2=1 \\ F_1\begin{pmatrix}x_1\\x_2\end{pmatrix}, \text{ якщо } y_1=1;\ y_2=0 \\ F_4\begin{pmatrix}x_1\\x_2\end{pmatrix}, \text{ якщо } y_1=1;\ y_2=1 \end{cases} = \begin{cases} \begin{bmatrix}x_1\oplus x_2\\x_2\end{bmatrix}, \text{ якщо } y_1=0;\ y_2=0 \\ \begin{bmatrix}x_1\\x_1\oplus x_2\end{bmatrix}, \text{ якщо } y_1=0;\ y_2=1 \\ \begin{bmatrix}x_1\\x_2\end{bmatrix}, \text{ якщо } y_1=1;\ y_2=0 \\ \begin{bmatrix}x_2\\x_1\end{bmatrix}, \text{ якщо } y_1=1;\ y_2=1 \end{cases} = \begin{bmatrix}(\bar{y}_1\vee \bar{y}_2)\cdot x_1\oplus \overline{(y_1\oplus y_2)}\cdot x_2\\y_2\cdot x_1\oplus(\bar{y}_1\vee \bar{y}_2)\cdot x_2\end{bmatrix};$$

$$O_{2,3,4,1}=\begin{cases} F_2\begin{pmatrix}x_1\\x_2\end{pmatrix}, \text{ якщо } y_1=0;\ y_2=0 \\ F_3\begin{pmatrix}x_1\\x_2\end{pmatrix}, \text{ якщо } y_1=0;\ y_2=1 \\ F_4\begin{pmatrix}x_1\\x_2\end{pmatrix}, \text{ якщо } y_1=1;\ y_2=0 \\ F_1\begin{pmatrix}x_1\\x_2\end{pmatrix}, \text{ якщо } y_1=1;\ y_2=1 \end{cases} = \begin{cases} \begin{bmatrix}x_1\oplus x_2\\x_2\end{bmatrix}, \text{ якщо } y_1=0;\ y_2=0 \\ \begin{bmatrix}x_1\\x_1\oplus x_2\end{bmatrix}, \text{ якщо } y_1=0;\ y_2=1 \\ \begin{bmatrix}x_2\\x_1\end{bmatrix}, \text{ якщо } y_1=1;\ y_2=0 \\ \begin{bmatrix}x_1\\x_2\end{bmatrix}, \text{ якщо } y_1=1;\ y_2=1 \end{cases} = \begin{bmatrix}(y_1\vee \bar{y}_2)\cdot x_1\oplus y_2\cdot x_2\\(y_1\oplus y_2)\cdot x_1\oplus(y_1\vee \bar{y}_2)\cdot x_2\end{bmatrix};$$

$$O_{2,4,1,3}=\begin{cases} F_2\begin{pmatrix}x_1\\x_2\end{pmatrix}, & якщо\ y_1=0;\ y_2=0 \\ F_4\begin{pmatrix}x_1\\x_2\end{pmatrix}, & якщо\ y_1=0;\ y_2=1 \\ F_1\begin{pmatrix}x_1\\x_2\end{pmatrix}, & якщо\ y_1=1;\ y_2=0 \\ F_3\begin{pmatrix}x_1\\x_2\end{pmatrix}, & якщо\ y_1=1;\ y_2=1 \end{cases}=\begin{cases} \begin{bmatrix}x_1\oplus x_2\\x_2\end{bmatrix}, & якщо\ y_1=0;\ y_2=0 \\ \begin{bmatrix}x_2\\x_1\end{bmatrix}, & якщо\ y_1=0;\ y_2=1 \\ \begin{bmatrix}x_1\\x_2\end{bmatrix}, & якщо\ y_1=1;\ y_2=0 \\ \begin{bmatrix}x_1\\x_1\oplus x_2\end{bmatrix}, & якщо\ y_1=1;\ y_2=1 \end{cases}=\begin{bmatrix}(y_1\vee\bar{y}_2)\cdot x_1\oplus\bar{y}_1\cdot x_2\\ y_2\cdot x_1\oplus(y_1\vee\bar{y}_2)\cdot x_2\end{bmatrix};$$

$$O_{2,4,3,1}=\begin{cases} F_2\begin{pmatrix}x_1\\x_2\end{pmatrix}, & якщо\ y_1=0;\ y_2=0 \\ F_4\begin{pmatrix}x_1\\x_2\end{pmatrix}, & якщо\ y_1=0;\ y_2=1 \\ F_3\begin{pmatrix}x_1\\x_2\end{pmatrix}, & якщо\ y_1=1;\ y_2=0 \\ F_1\begin{pmatrix}x_1\\x_2\end{pmatrix}, & якщо\ y_1=1;\ y_2=1 \end{cases}=\begin{cases} \begin{bmatrix}x_1\oplus x_2\\x_2\end{bmatrix}, & якщо\ y_1=0;\ y_2=0 \\ \begin{bmatrix}x_2\\x_1\end{bmatrix}, & якщо\ y_1=0;\ y_2=1 \\ \begin{bmatrix}x_1\\x_1\oplus x_2\end{bmatrix}, & якщо\ y_1=1;\ y_2=0 \\ \begin{bmatrix}x_1\\x_2\end{bmatrix}, & якщо\ y_1=1;\ y_2=1 \end{cases}=\begin{bmatrix}(y_1\vee\bar{y}_2)\cdot x_1\oplus\bar{y}_1\cdot x_2\\ (y_1\oplus y_2)\cdot x_1\oplus(y_1\vee\bar{y}_2)\cdot x_2\end{bmatrix};$$

$$O_{3,1,2,4}=\begin{cases} F_3\begin{pmatrix}x_1\\x_2\end{pmatrix}, & якщо\ y_1=0;\ y_2=0 \\ F_1\begin{pmatrix}x_1\\x_2\end{pmatrix}, & якщо\ y_1=0;\ y_2=1 \\ F_2\begin{pmatrix}x_1\\x_2\end{pmatrix}, & якщо\ y_1=1;\ y_2=0 \\ F_4\begin{pmatrix}x_1\\x_2\end{pmatrix}, & якщо\ y_1=1;\ y_2=1 \end{cases}=\begin{cases} \begin{bmatrix}x_1\\x_1\oplus x_2\end{bmatrix}, & якщо\ y_1=0;\ y_2=0 \\ \begin{bmatrix}x_1\\x_2\end{bmatrix}, & якщо\ y_1=0;\ y_2=1 \\ \begin{bmatrix}x_1\oplus x_2\\x_2\end{bmatrix}, & якщо\ y_1=1;\ y_2=0 \\ \begin{bmatrix}x_2\\x_1\end{bmatrix}, & якщо\ y_1=1;\ y_2=1 \end{cases}=\begin{bmatrix}(y_1\vee y_2)\cdot x_1\oplus y_1\cdot x_2\\ \overline{(y_1\oplus y_2)}\cdot x_1\oplus(y_1\vee y_2)\cdot x_2\end{bmatrix};$$

$$O_{3,1,4,2}=\begin{cases} F_3\begin{pmatrix}x_1\\x_2\end{pmatrix}, & якщо\ y_1=0;\ y_2=0 \\ F_1\begin{pmatrix}x_1\\x_2\end{pmatrix}, & якщо\ y_1=0;\ y_2=1 \\ F_4\begin{pmatrix}x_1\\x_2\end{pmatrix}, & якщо\ y_1=1;\ y_2=0 \\ F_2\begin{pmatrix}x_1\\x_2\end{pmatrix}, & якщо\ y_1=1;\ y_2=1 \end{cases}=\begin{cases} \begin{bmatrix}x_1\\x_1\oplus x_2\end{bmatrix}, & якщо\ y_1=0;\ y_2=0 \\ \begin{bmatrix}x_1\\x_2\end{bmatrix}, & якщо\ y_1=0;\ y_2=1 \\ \begin{bmatrix}x_2\\x_1\end{bmatrix}, & якщо\ y_1=1;\ y_2=0 \\ \begin{bmatrix}x_1\oplus x_2\\x_2\end{bmatrix}, & якщо\ y_1=1;\ y_2=1 \end{cases}=\begin{bmatrix}(y_1\vee\bar{y}_2)\cdot x_1\oplus y_1\cdot x_2\\ \bar{y}_2\cdot x_1\oplus(\bar{y}_1\vee y_2)\cdot x_2\end{bmatrix};$$

$$O_{3,2,1,4}=\begin{cases} F_3\begin{pmatrix}x_1\\x_2\end{pmatrix}, & якщо\ y_1=0;\ y_2=0 \\ F_2\begin{pmatrix}x_1\\x_2\end{pmatrix}, & якщо\ y_1=0;\ y_2=1 \\ F_1\begin{pmatrix}x_1\\x_2\end{pmatrix}, & якщо\ y_1=1;\ y_2=0 \\ F_4\begin{pmatrix}x_1\\x_2\end{pmatrix}, & якщо\ y_1=1;\ y_2=1 \end{cases}=\begin{cases} \begin{bmatrix}x_1\\x_1\oplus x_2\end{bmatrix}, & якщо\ y_1=0;\ y_2=0 \\ \begin{bmatrix}x_1\oplus x_2\\x_2\end{bmatrix}, & якщо\ y_1=0;\ y_2=1 \\ \begin{bmatrix}x_1\\x_2\end{bmatrix}, & якщо\ y_1=1;\ y_2=0 \\ \begin{bmatrix}x_2\\x_1\end{bmatrix}, & якщо\ y_1=1;\ y_2=1 \end{cases}=\begin{bmatrix}(y_1\vee y_2)\cdot x_1\oplus y_2\cdot x_2\\ (y_1\oplus y_2)\cdot x_1\oplus(y_1\vee y_2)\cdot x_2\end{bmatrix};$$

$$O_{3,2,4,1}=\begin{cases} F_3\begin{pmatrix}x_1\\x_2\end{pmatrix}, \text{ якщо } y_1=0;\ y_2=0 \\ F_2\begin{pmatrix}x_1\\x_2\end{pmatrix}, \text{ якщо } y_1=0;\ y_2=1 \\ F_4\begin{pmatrix}x_1\\x_2\end{pmatrix}, \text{ якщо } y_1=1;\ y_2=0 \\ F_1\begin{pmatrix}x_1\\x_2\end{pmatrix}, \text{ якщо } y_1=1;\ y_2=1 \end{cases} = \begin{cases} \begin{bmatrix}x_1\\x_1\oplus x_2\end{bmatrix}, \text{ якщо } y_1=0;\ y_2=0 \\ \begin{bmatrix}x_1\oplus x_2\\x_2\end{bmatrix}, \text{ якщо } y_1=0;\ y_2=1 \\ \begin{bmatrix}x_2\\x_1\end{bmatrix}, \text{ якщо } y_1=1;\ y_2=0 \\ \begin{bmatrix}x_1\\x_2\end{bmatrix}, \text{ якщо } y_1=1;\ y_2=1 \end{cases} = \begin{bmatrix}(y_1\vee\bar{y}_2)\cdot x_1\oplus(\overline{y_1\oplus y_2})\cdot x_2\\ \bar{y}_2\cdot x_1\oplus(y_1\vee\bar{y}_2)\cdot x_2\end{bmatrix};$$

$$O_{3,4,1,2}=\begin{cases} F_3\begin{pmatrix}x_1\\x_2\end{pmatrix}, \text{ якщо } y_1=0;\ y_2=0 \\ F_4\begin{pmatrix}x_1\\x_2\end{pmatrix}, \text{ якщо } y_1=0;\ y_2=1 \\ F_1\begin{pmatrix}x_1\\x_2\end{pmatrix}, \text{ якщо } y_1=1;\ y_2=0 \\ F_2\begin{pmatrix}x_1\\x_2\end{pmatrix}, \text{ якщо } y_1=1;\ y_2=1 \end{cases} = \begin{cases} \begin{bmatrix}x_1\\x_1\oplus x_2\end{bmatrix}, \text{ якщо } y_1=0;\ y_2=0 \\ \begin{bmatrix}x_2\\x_1\end{bmatrix}, \text{ якщо } y_1=0;\ y_2=1 \\ \begin{bmatrix}x_1\\x_2\end{bmatrix}, \text{ якщо } y_1=1;\ y_2=0 \\ \begin{bmatrix}x_1\oplus x_2\\x_2\end{bmatrix}, \text{ якщо } y_1=1;\ y_2=1 \end{cases} = \begin{bmatrix}(\bar{y}_1\vee y_2)\cdot x_1\oplus y_2\cdot x_2\\ \bar{y}_1\cdot x_1\oplus(\bar{y}_1\vee y_2)\cdot x_2\end{bmatrix};$$

$$O_{3,4,2,1}=\begin{cases} F_3\begin{pmatrix}x_1\\x_2\end{pmatrix}, \text{ якщо } y_1=0;\ y_2=0 \\ F_4\begin{pmatrix}x_1\\x_2\end{pmatrix}, \text{ якщо } y_1=0;\ y_2=1 \\ F_2\begin{pmatrix}x_1\\x_2\end{pmatrix}, \text{ якщо } y_1=1;\ y_2=0 \\ F_1\begin{pmatrix}x_1\\x_2\end{pmatrix}, \text{ якщо } y_1=1;\ y_2=1 \end{cases} = \begin{cases} \begin{bmatrix}x_1\\x_1\oplus x_2\end{bmatrix}, \text{ якщо } y_1=0;\ y_2=0 \\ \begin{bmatrix}x_2\\x_1\end{bmatrix}, \text{ якщо } y_1=0;\ y_2=1 \\ \begin{bmatrix}x_1\oplus x_2\\x_2\end{bmatrix}, \text{ якщо } y_1=1;\ y_2=0 \\ \begin{bmatrix}x_1\\x_2\end{bmatrix}, \text{ якщо } y_1=1;\ y_2=1 \end{cases} = \begin{bmatrix}(y_1\vee\bar{y}_2)\cdot x_1\oplus(y_1\oplus y_2)\cdot x_2\\ \bar{y}_1\cdot x_1\oplus(y_1\vee\bar{y}_2)\cdot x_2\end{bmatrix};$$

$$O_{4,1,2,3}=\begin{cases} F_4\begin{pmatrix}x_1\\x_2\end{pmatrix}, \text{ якщо } y_1=0;\ y_2=0 \\ F_1\begin{pmatrix}x_1\\x_2\end{pmatrix}, \text{ якщо } y_1=0;\ y_2=1 \\ F_2\begin{pmatrix}x_1\\x_2\end{pmatrix}, \text{ якщо } y_1=1;\ y_2=0 \\ F_3\begin{pmatrix}x_1\\x_2\end{pmatrix}, \text{ якщо } y_1=1;\ y_2=1 \end{cases} = \begin{cases} \begin{bmatrix}x_2\\x_1\end{bmatrix}, \text{ якщо } y_1=0;\ y_2=0 \\ \begin{bmatrix}x_1\\x_2\end{bmatrix}, \text{ якщо } y_1=0;\ y_2=1 \\ \begin{bmatrix}x_1\oplus x_2\\x_2\end{bmatrix}, \text{ якщо } y_1=1;\ y_2=0 \\ \begin{bmatrix}x_1\\x_1\oplus x_2\end{bmatrix}, \text{ якщо } y_1=1;\ y_2=1 \end{cases} = \begin{bmatrix}(y_1\vee y_2)\cdot x_1\oplus\bar{y}_2\cdot x_2\\ (\overline{y_1\oplus y_2})\cdot x_1\oplus(y_1\vee y_2)\cdot x_2\end{bmatrix};$$

$$O_{4,1,3,2}=\begin{cases} F_4\begin{pmatrix}x_1\\x_2\end{pmatrix}, \text{ якщо } y_1=0;\ y_2=0 \\ F_1\begin{pmatrix}x_1\\x_2\end{pmatrix}, \text{ якщо } y_1=0;\ y_2=1 \\ F_3\begin{pmatrix}x_1\\x_2\end{pmatrix}, \text{ якщо } y_1=1;\ y_2=0 \\ F_2\begin{pmatrix}x_1\\x_2\end{pmatrix}, \text{ якщо } y_1=1;\ y_2=1 \end{cases} = \begin{cases} \begin{bmatrix}x_2\\x_1\end{bmatrix}, \text{ якщо } y_1=0;\ y_2=0 \\ \begin{bmatrix}x_1\\x_2\end{bmatrix}, \text{ якщо } y_1=0;\ y_2=1 \\ \begin{bmatrix}x_1\\x_1\oplus x_2\end{bmatrix}, \text{ якщо } y_1=1;\ y_2=0 \\ \begin{bmatrix}x_1\oplus x_2\\x_2\end{bmatrix}, \text{ якщо } y_1=1;\ y_2=1 \end{cases} = \begin{bmatrix}(y_1\vee y_2)\cdot x_1\oplus(\overline{y_1\oplus y_2})\cdot x_2\\ \bar{y}_2\cdot x_1\oplus(y_1\vee y_2)\cdot x_2\end{bmatrix};$$

$$O_{4,2,1,3}=\begin{cases} F_4\begin{pmatrix}x_1\\x_2\end{pmatrix}, \text{ якщо } y_1=0;\ y_2=0 \\ F_2\begin{pmatrix}x_1\\x_2\end{pmatrix}, \text{ якщо } y_1=0;\ y_2=1 \\ F_1\begin{pmatrix}x_1\\x_2\end{pmatrix}, \text{ якщо } y_1=1;\ y_2=0 \\ F_3\begin{pmatrix}x_1\\x_2\end{pmatrix}, \text{ якщо } y_1=1;\ y_2=1 \end{cases} = \begin{cases} \begin{bmatrix}x_2\\x_1\end{bmatrix}, \text{ якщо } y_1=0;\ y_2=0 \\ \begin{bmatrix}x_1\oplus x_2\\x_2\end{bmatrix}, \text{ якщо } y_1=0;\ y_2=1 \\ \begin{bmatrix}x_1\\x_2\end{bmatrix}, \text{ якщо } y_1=1;\ y_2=0 \\ \begin{bmatrix}x_1\\x_1\oplus x_2\end{bmatrix}, \text{ якщо } y_1=1;\ y_2=1 \end{cases} = \begin{bmatrix}(y_1\vee y_2)\cdot x_1\oplus \bar{y}_1\cdot x_2\\ \overline{(y_1\oplus y_2)}\cdot x_1\oplus (y_1\vee y_2)\cdot x_2\end{bmatrix};$$

$$O_{4,2,3,1}=\begin{cases} F_4\begin{pmatrix}x_1\\x_2\end{pmatrix}, \text{ якщо } y_1=0;\ y_2=0 \\ F_2\begin{pmatrix}x_1\\x_2\end{pmatrix}, \text{ якщо } y_1=0;\ y_2=1 \\ F_3\begin{pmatrix}x_1\\x_2\end{pmatrix}, \text{ якщо } y_1=1;\ y_2=0 \\ F_1\begin{pmatrix}x_1\\x_2\end{pmatrix}, \text{ якщо } y_1=1;\ y_2=1 \end{cases} = \begin{cases} \begin{bmatrix}x_2\\x_1\end{bmatrix}, \text{ якщо } y_1=0;\ y_2=0 \\ \begin{bmatrix}x_1\oplus x_2\\x_2\end{bmatrix}, \text{ якщо } y_1=0;\ y_2=1 \\ \begin{bmatrix}x_1\\x_1\oplus x_2\end{bmatrix}, \text{ якщо } y_1=1;\ y_2=0 \\ \begin{bmatrix}x_1\\x_2\end{bmatrix}, \text{ якщо } y_1=1;\ y_2=1 \end{cases} = \begin{bmatrix}(y_1\vee y_2)\cdot x_1\oplus \bar{y}_1\cdot x_2\\ \bar{y}_2\cdot x_1\oplus (y_1\vee y_2)\cdot x_2\end{bmatrix};$$

$$O_{4,3,1,2}=\begin{cases} F_4\begin{pmatrix}x_1\\x_2\end{pmatrix}, \text{ якщо } y_1=0;\ y_2=0 \\ F_2\begin{pmatrix}x_1\\x_2\end{pmatrix}, \text{ якщо } y_1=0;\ y_2=1 \\ F_1\begin{pmatrix}x_1\\x_2\end{pmatrix}, \text{ якщо } y_1=1;\ y_2=0 \\ F_2\begin{pmatrix}x_1\\x_2\end{pmatrix}, \text{ якщо } y_1=1;\ y_2=1 \end{cases} = \begin{cases} \begin{bmatrix}x_2\\x_1\end{bmatrix}, \text{ якщо } y_1=0;\ y_2=0 \\ \begin{bmatrix}x_1\\x_1\oplus x_2\end{bmatrix}, \text{ якщо } y_1=0;\ y_2=1 \\ \begin{bmatrix}x_1\\x_2\end{bmatrix}, \text{ якщо } y_1=1;\ y_2=0 \\ \begin{bmatrix}x_1\oplus x_2\\x_2\end{bmatrix}, \text{ якщо } y_1=1;\ y_2=1 \end{cases} = \begin{bmatrix}(y_1\vee y_2)\cdot x_1\oplus \overline{(y_1\oplus y_2)}\cdot x_2\\ \bar{y}_1\cdot x_1\oplus (y_1\vee y_2)\cdot x_2\end{bmatrix};$$

$$O_{4,3,2,1}=\begin{cases} F_4\begin{pmatrix}x_1\\x_2\end{pmatrix}, \text{ якщо } y_1=0;\ y_2=0 \\ F_2\begin{pmatrix}x_1\\x_2\end{pmatrix}, \text{ якщо } y_1=0;\ y_2=1 \\ F_2\begin{pmatrix}x_1\\x_2\end{pmatrix}, \text{ якщо } y_1=1;\ y_2=0 \\ F_1\begin{pmatrix}x_1\\x_2\end{pmatrix}, \text{ якщо } y_1=1;\ y_2=1 \end{cases} = \begin{cases} \begin{bmatrix}x_2\\x_1\end{bmatrix}, \text{ якщо } y_1=0;\ y_2=0 \\ \begin{bmatrix}x_1\\x_1\oplus x_2\end{bmatrix}, \text{ якщо } y_1=0;\ y_2=1 \\ \begin{bmatrix}x_1\oplus x_2\\x_2\end{bmatrix}, \text{ якщо } y_1=1;\ y_2=0 \\ \begin{bmatrix}x_1\\x_2\end{bmatrix}, \text{ якщо } y_1=1;\ y_2=1 \end{cases} = \begin{bmatrix}(y_1\vee y_2)\cdot x_1\oplus \bar{y}_2\cdot x_2\\ \bar{y}_1\cdot x_1\oplus (y_1\vee y_2)\cdot x_2\end{bmatrix}.$$

Результати побудови групи двохоперандних двохрозрядних операцій криптографічного кодування з точністю до перестановки на основі кортежу $F_1,\ F_2, F_3,\ F_4$ наведено в табл. 2.3.

За аналогією можна синтезувати групи двохрозрядних двохоперандних операцій криптоперетворення на основі інших кортежів.

Таблиця 2.3

**Двохоперандні двохрозрядні операції криптографічного кодування на основі кортежу $F_1,\ F_2, F_3,\ F_4$**

| | | | |
|---|---|---|---|
| $O_{1,2,3,4}=\begin{bmatrix} y_1\cdot y_2\cdot x_1 \oplus y_2\cdot x_2 \\ y_1\cdot x_1 \oplus \bar{y}_1\cdot \bar{y}_2\cdot x_2 \end{bmatrix}$ | $O_{2,1,3,4}=\begin{bmatrix} (\bar{y}_1 \vee \bar{y}_2)\cdot x_1 \oplus \overline{(y_1 \oplus y_2)}\cdot x_2 \\ y_1\cdot x_1 \oplus (\bar{y}_1 \vee \bar{y}_2)\cdot x_2 \end{bmatrix}$ | $O_{3,1,2,4}=\begin{bmatrix} (y_1 \vee y_2)\cdot x_1 \oplus y_1\cdot x_2 \\ \overline{(y_1 \oplus y_2)}\cdot x_1 \oplus (y_1 \vee y_2)\cdot x_2 \end{bmatrix}$ | $O_{4,1,2,3}=\begin{bmatrix} (y_1 \vee y_2)\cdot x_1 \oplus \bar{y}_2\cdot x_2 \\ \overline{(y_1 \oplus y_2)}\cdot x_1 \oplus (y_1 \vee y_2)\cdot x_2 \end{bmatrix}$ |
| $O_{1,2,4,3}=\begin{bmatrix} y_1\cdot \bar{y}_2\cdot x_1 \oplus (y_1 \oplus y_2)\cdot x_2 \\ y_1\cdot x_1 \oplus (y_1 \vee \bar{y}_2)\cdot x_2 \end{bmatrix}$ | $O_{2,1,4,3}=\begin{bmatrix} (y_1 \vee \bar{y}_2)\cdot x_1 \oplus \bar{y}_2\cdot x_2 \\ y_1\cdot x_1 \oplus (y_1 \vee \bar{y}_2)\cdot x_2 \end{bmatrix}$ | $O_{3,1,4,2}=\begin{bmatrix} (y_1 \vee \bar{y}_2)\cdot x_1 \oplus y_1\cdot x_2 \\ \bar{y}_2\cdot x_1 \oplus (\bar{y}_1 \vee y_2)\cdot x_2 \end{bmatrix}$ | $O_{4,1,3,2}=\begin{bmatrix} (y_1 \vee y_2)\cdot x_1 \oplus \overline{(y_1 \oplus y_2)}\cdot x_2 \\ \bar{y}_2\cdot x_1 \oplus (y_1 \vee y_2)\cdot x_2 \end{bmatrix}$ |
| $O_{1,3,2,4}=\begin{bmatrix} (\bar{y}_1 \vee \bar{y}_2)\cdot x_1 \oplus y_1\cdot x_2 \\ y_2\cdot x_1 \oplus (\bar{y}_1 \vee \bar{y}_2)\cdot x_2 \end{bmatrix}$ | $O_{2,3,1,4}=\begin{bmatrix} (\bar{y}_1 \vee \bar{y}_2)\cdot x_1 \oplus \overline{(y_1 \oplus y_2)}\cdot x_2 \\ y_2\cdot x_1 \oplus (\bar{y}_1 \vee \bar{y}_2)\cdot x_2 \end{bmatrix}$ | $O_{3,2,1,4}=\begin{bmatrix} (y_1 \vee y_2)\cdot x_1 \oplus y_2\cdot x_2 \\ (y_1 \oplus y_2)\cdot x_1 \oplus (y_1 \vee y_2)\cdot x_2 \end{bmatrix}$ | $O_{4,2,1,3}=\begin{bmatrix} (y_1 \vee y_2)\cdot x_1 \oplus \bar{y}_1\cdot x_2 \\ \overline{(y_1 \oplus y_2)}\cdot x_1 \oplus (y_1 \vee y_2)\cdot x_2 \end{bmatrix}$ |
| $O_{1,3,4,2}=\begin{bmatrix} (y_1 \vee \bar{y}_2)\cdot x_1 \oplus y_1\cdot x_2 \\ (y_1 \oplus y_2)\cdot x_1 \oplus (y_1 \vee \bar{y}_2)\cdot x_2 \end{bmatrix}$ | $O_{2,3,4,1}=\begin{bmatrix} (y_1 \vee \bar{y}_2)\cdot x_1 \oplus y_2\cdot x_2 \\ (y_1 \oplus y_2)\cdot x_1 \oplus (y_1 \vee \bar{y}_2)\cdot x_2 \end{bmatrix}$ | $O_{3,2,4,1}=\begin{bmatrix} (y_1 \vee \bar{y}_2)\cdot x_1 \oplus \overline{(y_1 \oplus y_2)}\cdot x_2 \\ \bar{y}_2\cdot x_1 \oplus (y_1 \vee \bar{y}_2)\cdot x_2 \end{bmatrix}$ | $O_{4,2,3,1}=\begin{bmatrix} (y_1 \vee y_2)\cdot x_1 \oplus \bar{y}_1\cdot x_2 \\ \bar{y}_2\cdot x_1 \oplus (y_1 \vee y_2)\cdot x_2 \end{bmatrix}$ |
| $O_{1,4,2,3}=\begin{bmatrix} (\bar{y}_1 \vee y_2)\cdot x_1 \oplus (y_1 \oplus y_2)\cdot x_2 \\ y_2\cdot x_1 \oplus (\bar{y}_1 \vee y_2)\cdot x_2 \end{bmatrix}$ | $O_{2,4,1,3}=\begin{bmatrix} (y_1 \vee \bar{y}_2)\cdot x_1 \oplus \bar{y}_1\cdot x_2 \\ y_2\cdot x_1 \oplus (y_1 \vee \bar{y}_2)\cdot x_2 \end{bmatrix}$ | $O_{3,4,1,2}=\begin{bmatrix} (\bar{y}_1 \vee y_2)\cdot x_1 \oplus y_2\cdot x_2 \\ \bar{y}_1\cdot x_1 \oplus (\bar{y}_1 \vee y_2)\cdot x_2 \end{bmatrix}$ | $O_{4,3,1,2}=\begin{bmatrix} (y_1 \vee y_2)\cdot x_1 \oplus \overline{(y_1 \oplus y_2)}\cdot x_2 \\ \bar{y}_1\cdot x_1 \oplus (y_1 \vee y_2)\cdot x_2 \end{bmatrix}$ |
| $O_{1,4,3,2}=\begin{bmatrix} (\bar{y}_1 \vee y_2)\cdot x_1 \oplus y_2\cdot x_2 \\ (\bar{y}_1 \vee \bar{y}_2)\cdot x_1 \oplus \bar{y}_2\cdot x_2 \end{bmatrix}$ | $O_{2,4,3,1}=\begin{bmatrix} (y_1 \vee \bar{y}_2)\cdot x_1 \oplus \bar{y}_1\cdot x_2 \\ (y_1 \oplus y_2)\cdot x_1 \oplus (y_1 \vee \bar{y}_2)\cdot x_2 \end{bmatrix}$ | $O_{3,4,2,1}=\begin{bmatrix} (y_1 \vee \bar{y}_2)\cdot x_1 \oplus (y_1 \oplus y_2)\cdot x_2 \\ \bar{y}_1\cdot x_1 \oplus (y_1 \vee \bar{y}_2)\cdot x_2 \end{bmatrix}$ | $O_{4,3,2,1}=\begin{bmatrix} (y_1 \vee y_2)\cdot x_1 \oplus \bar{y}_2\cdot x_2 \\ \bar{y}_1\cdot x_1 \oplus (y_1 \vee y_2)\cdot x_2 \end{bmatrix}$ |

Отримані результати побудови груп моделей симетричних двохрозрядних двохоперандних операцій криптографічного кодування дозволяють перейти до побудови методу синтезу моделей симетричних двохрозрядних двохоперандних операцій криптографічного кодування на основі кортежів симетричних двохрозрядних одноопераднних операцій перетворення інформації

## 2.3 Метод синтезу моделей симетричних двохоперандних операцій криптографічного кодування на основі кортежів симетричних одноопераднних операцій перетворення інформації

Оцінимо кількість симетричних двохрозрядних двохоперандних операцій криптографічного кодування, які можна синтезувати та необхідно дослідити для застосування в захищених інформаційних системах критичної інфраструктури.

Відповідно до [99] симетричних двохрозрядних одноопераднних операцій криптографічного кодування існує 10. Ми синтезуємо і надалі будемо досліджувати операції, що будуються на основі кортежів з 4 одноопераднних операцій. Виходячи з цього кількість кортежів буде визначатися як кількість сполучень з 10 по 4:

$$C_n^m = \frac{n!}{m!\cdot(n-m)!} = \frac{10!}{4!\cdot(10-4)!} = 210. \qquad (2.16)$$

Оскільки з кожного кортежу будуються 24 симетричні двохрозрядні двохоперандні операції криптографічного кодування, то необхідно синтезувати і дослідити 5040 операцій.

На основі кількісних оцінок симетричних двохрозрядних двохоперандних операцій криптографічного кодування можна констатувати, що без застосування засобів обчислювальної техніки неможливо синтезувати і дослідити всю множину цих операцій. Виходячи з цього зауваження,

необхідно при розробці алгоритму реалізації методу приділити увагу можливості застосування його в системах автоматизації проектувальних робіт. Адже для розробників систем захисту інформації важливо не лише генерувати двохоперандні операції криптографічного кодування, а й генерувати операції, які будуть відповідати заданим вимогам.

Отримані в процесі дослідження результати синтезу потребують узагальнення. Для формулювання методу синтезу моделей симетричних двохоперандних операцій криптографічного кодування необхідно формалізувати гіпотезу, на основі якої буде побудовано метод. У процесі дослідження із трьох перевірених гіпотез гіпотеза про можливість побудови симетричних двохоперандних операцій на основі кортежів одноопераднних симетричних операцій стала найефективнішою. Формалізуємо основні поняття цієї гіпотези.

Двохрозрядна двохоперандна операція $O\begin{pmatrix} x_1, y_1 \\ x_2, y_2 \end{pmatrix}$ може використовуватися в криптографії, якщо існує операція $O'\begin{pmatrix} x_1, y_1 \\ x_2, k_2 \end{pmatrix}$, така що $O'(O\begin{pmatrix} x_1, y_1 \\ x_2, y_2 \end{pmatrix}) = \begin{bmatrix} x_1 \\ x_2 \end{bmatrix}$, за умови: $x_1 = conts$ , $x_2 = conts$ .

Якщо $O\begin{pmatrix} x_1, y_1 \\ x_2, y_2 \end{pmatrix} = O'\begin{pmatrix} x_1, y_1 \\ x_2, y_2 \end{pmatrix}$, то операція $O\begin{pmatrix} x_1, y_1 \\ x_2, y_2 \end{pmatrix}$ буде симетричною.

Двохоперандна операція буде симетричною

$$O\begin{pmatrix} x_1, y_1 \\ x_2, y_2 \end{pmatrix} = O'\begin{pmatrix} x_1, y_1 \\ x_2, y_2 \end{pmatrix} = \begin{cases} F_1\begin{pmatrix} x_1 \\ x_2 \end{pmatrix}, \ якщо\ y_1 = 0;\ y_2 = 0 \\ F_2\begin{pmatrix} x_1 \\ x_2 \end{pmatrix}, \ якщо\ y_1 = 0;\ y_2 = 1 \\ F_3\begin{pmatrix} x_1 \\ x_2 \end{pmatrix}, \ якщо\ y_1 = 1;\ y_2 = 0 \\ F_4\begin{pmatrix} x_1 \\ x_2 \end{pmatrix}, \ якщо\ y_1 = 1;\ y_2 = 1 \end{cases}, \qquad (2.17)$$

якщо $F_1(F_1\begin{pmatrix}x_1\\x_2\end{pmatrix})=\begin{bmatrix}x_1\\x_2\end{bmatrix}$, $F_2(F_2\begin{pmatrix}x_1\\x_2\end{pmatrix})=\begin{bmatrix}x_1\\x_2\end{bmatrix}$, $F_3(F_3\begin{pmatrix}x_1\\x_2\end{pmatrix})=\begin{bmatrix}x_1\\x_2\end{bmatrix}$,

$F_4(F_4\begin{pmatrix}x_1\\x_2\end{pmatrix})=\begin{bmatrix}x_1\\x_2\end{bmatrix}$.

Представимо симетричну операцію в кортежному запису:

$$O\begin{pmatrix}x_1, y_1\\x_2, y_2\end{pmatrix}=O'\begin{pmatrix}x_1, y_1\\x_2, y_2\end{pmatrix}=O_{1,2,3,4}\left(F_1\begin{pmatrix}x_1\\x_2\end{pmatrix},F_2\begin{pmatrix}x_1\\x_2\end{pmatrix},F_3\begin{pmatrix}x_1\\x_2\end{pmatrix},F_4\begin{pmatrix}x_1\\x_2\end{pmatrix}\right), \qquad (2.18)$$

якщо $F_1(F_1\begin{pmatrix}x_1\\x_2\end{pmatrix})=\begin{bmatrix}x_1\\x_2\end{bmatrix}$, $F_2(F_2\begin{pmatrix}x_1\\x_2\end{pmatrix})=\begin{bmatrix}x_1\\x_2\end{bmatrix}$, $F_3(F_3\begin{pmatrix}x_1\\x_2\end{pmatrix})=\begin{bmatrix}x_1\\x_2\end{bmatrix}$,

$F_4(F_4\begin{pmatrix}x_1\\x_2\end{pmatrix})=\begin{bmatrix}x_1\\x_2\end{bmatrix}$.

Якщо $O\begin{pmatrix}x_1, y_1\\x_2, y_2\end{pmatrix}$ – симетричні двохрозрядні двохоперандні операції криптографічного кодування, то $O_{\text{mod}}\begin{pmatrix}x_1, z_1\\x_2, z_2\end{pmatrix}$ – модифікована симетрична двохрозрядна двохоперандна операція криптографічного кодування, де $\begin{bmatrix}z_1\\z_2\end{bmatrix}=F_s\begin{pmatrix}y_1\\y_2\end{pmatrix}, \quad i\in\{1,...,24\}$.

Концепція синтезу симетричних двохрозрядних двохоперандних операцій криптографічного кодування побудована на основі виразу (2.17) і складається з двох етапів:

- На першому етапі необхідно побудувати кортежні моделі симетричних двохрозрядних двохоперандних операцій (2.18), на їх основі побудувати розширені кортежні моделі (2.17) і перейти від них до узагальнених моделей. Для цього необхідно:
  - на основі рівності $F_i(F_i\begin{pmatrix}x_1\\x_2\end{pmatrix})=\begin{bmatrix}x_1\\x_2\end{bmatrix}$ встановити всі симетричні одноопераднді операції (10 операцій);

- з вибраних операцій побудувати кортежі по 4 операції, і на їх основі побудувати кортежні моделі операцій (2.18);
- на основі кортежної моделі, підставивши в модель (2.17) моделі одноопераднних операцій, побудувати розширену кортежну модель;
- на основі розширеної кортежної моделі операції побудувати узагальнену модель операції

$$O = \begin{bmatrix} a_{11} \cdot x_1 \oplus a_{12} \cdot x_2 \oplus b_1 \\ a_{21} \cdot x_1 \oplus a_{22} \cdot x_2 \oplus b_2 \end{bmatrix}, \quad (2.19)$$

де $x_1$, $x_2$ – значення першого і другого розрядів (байтів, слів, подвійних слів) першого операнда, $y_{11}$, $y_{12}$, $y_{21}$, $y_{22}$ – значення коефіцієнтів, які задаються значенням двох розрядів (байтів, слів, подвійних слів) другого операнда, $b_1$ і $b_2$ – значення інверсій, які також задаються значеннями розрядів другого операнда.

Для цього треба:

- побудувати таблиці істинності для коефіцієнтів узагальненої моделі;
- шляхом мінімізації визначити коефіцієнти узагальненої моделі і підставити їх у вираз (2.19).

➢ На другому етапі необхідно на основі побудованої узагальненої моделі операції побудувати групу симетричних двохрозрядних двохоперандних операцій криптографічного кодування (24 операції). Для цього потрібно:

Варіант 1:

- виконати перестановку одноопераднних операцій у розширеній кортежній моделі.
- побудувати на основі мінімізації таблиці істинності модифіковану узагальнену модель операції.

Варіант 2:

- виконати перетворення узагальненої моделі двохопераднної операції шляхом перетворення другого операнда одноопераднною операцією та отримати модифіковану узагальнену модель операції.

Застосовуючи один із варіантів, побудувати повну групу моделей модифікованих двохрозрядних двохоперандних операцій для кожної моделі кортежної операції.

Слід зауважити, що, крім двохрозрядних операцій, існують симетричні двохоперандні операції іншої розрядності. Виходячи з цього, необхідно розробити метод синтезу симетричних двохоперандних операцій довільної розрядності, придатний для автоматизованої їх генерації, та розробити інформаційну технологію дослідження цих операцій і оцінки ефективності їх застосування.

Взявши за основу концепцію синтезу симетричних двохрозрядних двохоперандних операцій криптографічного кодування, враховуючи модель симетричних багаторозрядних двохоперандних операцій криптографічного кодування, було розроблено метод синтезу моделей симетричних двохоперандних операцій криптографічного кодування на основі кортежів симетричних одноопераднних операцій криптографічного кодування. Алгоритм реалізації цього методу полягає в наступному [4]:

1) визначити розрядність операцій ($n$), які необхідно синтезувати;

2) визначити підгрупу матричних операцій вибраної розмірності, на основі якої будуть синтезуватися симетричні двохоперандні операції;

3) вибрати всі симетричні одноопераднні однорозрядні операції ($k$), які входять у вибрану підгрупу;

4) з симетричних одноопераднних операцій побудувати кортеж, який включає $2^n$ операцій. Кількість кортежів визначається як $C_k^{2^n}$;

5) на основі упорядкованого набору симетричних одноопераднних операцій побудувати симетричну двохоперандну операцію заданої розрядності в кортежному представленні;

6) побудувати таблиці істинності коефіцієнтів узагальненої моделі операції;

7) шляхом мінімізації булевих функцій встановити залежності для розрахунку коефіцієнтів узагальненої моделі операції та побудувати модель операції;

8) внести (включити) синтезовану узагальнену модель симетричної двохоперандної операції в базу знань;

9) якщо це не остання перестановка одноопераднних операцій у кортежі ($=2^n!$), виконати наступну перестановку одноопераднних операцій у кортежі і перейти на пункт 5;

10) якщо це не останній кортеж одноопераднних операцій ($=C_k^{2^n}$), побудувати наступний кортеж і перейти на пункт 5;

11) узагальнити результати синтезу симетричних двохоперандних операцій.

Запропонований алгоритм реалізації методу синтезу моделей симетричних двохоперандних операцій криптографічного кодування на основі кортежів симетричних одноопераднних операцій дозволяє автоматизувати синтез операцій для подальшого аналізу та встановлення наборів груп операцій, придатних для застосування в захищених інформаційних системах критичної інфраструктури. Практична реалізація запропонованого методу синтезу буде розглядатися в четвертому розділі.

**Висновки до розділу 2**

Вперше побудовано метод синтезу моделей симетричних двохоперандних операцій криптографічного кодування на основі кортежів симетричних одноопераднних операцій шляхом встановлення взаємозв’язків

та моделювання коефіцієнтів наявності розрядів першого операнда в елементарних функціях операції, що забезпечує практичну побудову раніше не відомих симетричних двохоперандних операцій, і забезпечено можливість автоматизації створення бази знань для автоматизації досліджень операцій криптографічного захисту інформації:

1. Досліджено можливість синтезу моделей симетричних двохоперандних операцій криптографічного кодування на основі об’єднання за модулем моделей симетричних одноопераднних операцій перетворення операндів. Встановлено недоліки цього підходу.

2. Досліджено можливість синтезу симетричних двохоперандних операцій криптографічного кодування на основі дублювання та об’єднання за модулем моделей симетричних одноопераднних операцій. Встановлено недоліки цього підходу.

3. Досліджено можливість синтезу моделей симетричних двохрозрядних двохоперандних операцій криптографічного кодування на основі кортежів симетричних одноопераднних операцій перетворення інформації. Встановлено недоліки та переваги цього підходу.

4. Запропоновано алгоритм реалізації розробленого методу синтезу моделей симетричних двохоперандних операцій криптографічного кодування на основі кортежів симетричних одноопераднних операцій перетворення інформації.

5. Результати розділу опубліковано в [4, 8, 9, 12].

# РОЗДІЛ 3 СИНТЕЗ ГРУП СИМЕТРИЧНИХ ДВОХОПЕРАНДНИХ МОДИФІКОВАНИХ ОПЕРАЦІЙ БЛОКОВОГО ШИФРУВАННЯ

## 3.1 Узагальнення результатів синтезу груп симетричних модифікованих операцій порозрядного додавання за модулем два та лівостороннього додавання за модулем чотири

Традиційно в комп'ютерній криптографії використовується операція додавання за модулем два. Серед операцій криптографічного кодування до операції додавання за модулем два частково подібні симетричні операції, при цьому вони повністю відповідають вимогам до впровадження у відомі системи потокового шифрування. Проте досліджені й синтезовані в розділі 2 симетричні двохоперандні операції криптографічного кодування не можуть знайти широке застосування в блокових шифрах, тому що не дозволяють переставляти операнди місцями. Це обмеження не критичне, але значно ускладнює практичну реалізацію моделей операцій.

У підрозділі 1.3 наведено результати теоретичного дослідження обчислювального експерименту та синтезовано моделі двохрозрядних двохоперандних операцій криптографічного кодування, синтезованих на основі порозрядного додавання за модулем два (табл. 1.3). Моделі двохрозрядних двохоперандних операцій криптографічного кодування, синтезовані на основі лівостороннього додавання за модулем чотири, наведені в табл. 1.5.

В роботі [105] наведено метод синтезу групи двохрозрядних двохоперандних операцій криптографічного кодування, синтезованих на основі порозрядного додавання за модулем два, який полягає в наступному:

- операцію порозрядного додавання за модулем два ділять на підопераційї обробки першого ($x$) та другого ($k$) операндів $O_1^{\mathrm{mod}2} = \begin{bmatrix} x_1 \oplus k_1 \\ x_2 \oplus k_2 \end{bmatrix} = \begin{bmatrix} x_1 \\ x_2 \end{bmatrix} \oplus \begin{bmatrix} k_1 \\ k_2 \end{bmatrix}$;
- для синтезу двохрозрядних двохоперандних операцій базової групи необхідно над визначеними операціями обробки першого та другого операндів виконати двохрозрядні одноопераднідні операції базової групи (табл. 1.1);
- синтезувати додатково групу двохрозрядних двохоперандних операцій перестановки можна шляхом перестановки елементарних функцій в операціях базової групи;
- синтезувати додатково групу двохрозрядних двохоперандних операцій інверсії можна шляхом перебору варіантів інверсії елементарних функцій операцій базової групи та операцій перестановки.

У розробленому методі слинтезу групи двохрозрядних двохоперандних операцій криптографічного кодування, синтезованих на основі лівостороннього додавання за модулем чотири [109], використано аналогічний підхід, взявши за основу операцію лівостороннього додавання за модулем чотири. При виконанні поділу двохоперандної операції на операції обробки першого та другого операнда неможливо було виділити окремі операції обробки лише інформації першого операнда та обробки інформації другого операнда: $O_1^{\mathrm{mod}4\leftarrow} = \begin{bmatrix} x_1 \oplus x_2 \cdot k_2 \oplus k_1 \\ x_2 \oplus k_2 \end{bmatrix} = \begin{bmatrix} x_1 \\ x_2 \end{bmatrix} \oplus \begin{bmatrix} x_2 \cdot k_2 \oplus k_1 \\ k_2 \end{bmatrix}$. Поділ на окремі операції обробки операндів виконувався умовно. Крім того, не виключена ситуація, коли двохоперандну операцію неможливо буде розбити на операції обробки кожного окремого операнда взагалі. Виходячи з цього припущення, необхідно поміняти концепцію синтезу двохоперандних операцій на основі дублювання перетворення операцій обробки першого та другого операндів.

Новий підхід, який полягає в перетворенні двохоперандних операцій на одноопераднідні без їх поділу на підопераційї, запропоновано в [1].

Перевіримо коректність цього підходу на прикладі синтезу групи операцій порозрядного додавання за модулем два.

Введемо підстановку в операцію порозрядного долавання за модулем два:

$$O_1^{\text{mod}2} = \begin{bmatrix} x_1 \oplus k_1 \\ x_2 \oplus k_2 \end{bmatrix} = \begin{bmatrix} y_1 \\ y_2 \end{bmatrix}.$$

Синтезуємо першу двохоперандну операцію базової групи на основі першої одноопераднної операції базової групи:

$$F_1(O_1^{\text{mod}2}) = \begin{bmatrix} y_1 \\ y_2 \end{bmatrix} = \begin{bmatrix} x_1 \oplus k_1 \\ x_2 \oplus k_2 \end{bmatrix} = O_1^{\text{mod}2}.$$

Синтезуємо другу двохоперандну операцію базової групи на основі другої одноопераднної операції базової групи:

$$F_2(O_1^{\text{mod}2}) = \begin{bmatrix} y_1 \oplus y_2 \\ y_2 \end{bmatrix} = \begin{bmatrix} (x_1 \oplus k_1) \oplus (x_2 \oplus k_2) \\ x_2 \oplus k_2 \end{bmatrix} = O_2^{\text{mod}2}.$$

Синтезуємо третю двохоперандну операцію базової групи на основі третьої одноопераднної операції базової групи:

$$F_3(O_1^{\text{mod}2}) = \begin{bmatrix} y_1 \\ y_1 \oplus y_2 \end{bmatrix} = \begin{bmatrix} x_1 \oplus k_1 \\ (x_1 \oplus k_1) \oplus (x_2 \oplus k_2) \end{bmatrix} = O_3^{\text{mod}2}.$$

Синтезовані двохоперандні операції базової групи відповідають операціям, наведеним у табл. 1.3.

Синтезувати операції перестановки можна або переставивши елементарні функції в операціях $O_1^{\text{mod}2}$ – $O_3^{\text{mod}2}$, або виконавши над $O_1^{\text{mod}2}$ одноопераднні операції $F_4$ – $F_6$:

$$F_4(O_1^{\text{mod}2}) = \begin{bmatrix} y_2 \\ y_1 \end{bmatrix} = \begin{bmatrix} x_2 \oplus k_2 \\ x_1 \oplus k_1 \end{bmatrix} = O_4^{\text{mod}2};$$

$$F_5(O_1^{\text{mod}2}) = \begin{bmatrix} y_2 \\ y_1 \oplus y_2 \end{bmatrix} = \begin{bmatrix} x_2 \oplus k_2 \\ (x_1 \oplus k_1) \oplus (x_2 \oplus k_2) \end{bmatrix} = O_5^{\text{mod}2};$$

$$F_6(O_1^{\text{mod}2}) = \begin{bmatrix} y_1 \oplus y_2 \\ y_1 \end{bmatrix} = \begin{bmatrix} (x_1 \oplus k_1) \oplus (x_2 \oplus k_2) \\ x_1 \oplus k_1 \end{bmatrix} = O_6^{\text{mod}2}.$$

Синтезовані операції відповідають операціям $O_4^{\text{mod}2}$ – $O_6^{\text{mod}2}$, наведеним у табл. 1.3.

Виконавши над операціями $O_1^{\text{mod}2}$ – $O_6^{\text{mod}2}$ операції інверсії, отримаємо всю групу операцій, наведену в табл. 1.3.

Перевіримо коректність цього підходу на прикладі синтезу групи оперцій лівостороннього додавання за модулем чотири.

Введемо підстановку в операцію лівостороннього додавання за модулем чотири:

$$O_1^{\text{mod}4\leftarrow} = \begin{bmatrix} x_1 \oplus x_2 \cdot k_2 \oplus k_1 \\ x_2 \oplus k_2 \end{bmatrix} = \begin{bmatrix} y_1 \\ y_2 \end{bmatrix}.$$

Синтезуємо за аналогією двохрозрядні двохоперандні операції базової групи:

$$F_1(O_1^{\text{mod}4\leftarrow}) = \begin{bmatrix} y_1 \\ y_2 \end{bmatrix} = \begin{bmatrix} x_1 \oplus x_2 \cdot k_2 \oplus k_1 \\ x_2 \oplus k_2 \end{bmatrix} = O_1^{\text{mod}4\leftarrow};$$

$$F_2(O_1^{\text{mod}4\leftarrow}) = \begin{bmatrix} y_1 \oplus y_2 \\ y_2 \end{bmatrix} = \begin{bmatrix} (x_1 \oplus x_2 \cdot k_2 \oplus k_1) \oplus (x_2 \oplus k_2) \\ x_2 \oplus k_2 \end{bmatrix} = O_2^{\text{mod}4\leftarrow};$$

$$F_3(O_1^{\text{mod}4\leftarrow}) = \begin{bmatrix} y_1 \\ y_1 \oplus y_2 \end{bmatrix} = \begin{bmatrix} x_1 \oplus x_2 \cdot k_2 \oplus k_1 \\ (x_1 \oplus x_2 \cdot k_2 \oplus k_1) \oplus (x_2 \oplus k_2) \end{bmatrix} = O_3^{\text{mod}4\leftarrow}.$$

Синтезуємо за аналогією двохрозрядні двохоперандні операції групи перестановок:

$$F_4(O_1^{\text{mod}4\leftarrow}) = \begin{bmatrix} y_2 \\ y_1 \end{bmatrix} = \begin{bmatrix} x_2 \oplus k_2 \\ x_1 \oplus x_2 \cdot k_2 \oplus k_1 \end{bmatrix} = O_4^{\text{mod}4\leftarrow};$$

$$F_5(O_1^{\text{mod}4\leftarrow}) = \begin{bmatrix} y_2 \\ y_1 \oplus y_2 \end{bmatrix} = \begin{bmatrix} x_2 \oplus k_2 \\ x_2 \oplus k_2 (x_1 \oplus x_2 \cdot k_2 \oplus k_1) \oplus (x_2 \oplus k_2) \end{bmatrix} = O_5^{\text{mod}4\leftarrow};$$

$$F_6(O_1^{\text{mod4}\leftarrow}) = \begin{bmatrix} y_1 \oplus y_2 \\ y_1 \end{bmatrix} = \begin{bmatrix} (x_1 \oplus x_2 \cdot k_2 \oplus k_1) \oplus (x_2 \oplus k_2) \\ x_1 \oplus x_2 \cdot k_2 \oplus k_1 \end{bmatrix} = O_6^{\text{mod4}\leftarrow}.$$

Виконавши над операціями $O_1^{\text{mod4}\leftarrow}$ – $O_6^{\text{mod4}\leftarrow}$ операції інверсії, отримаємо математичну групу двохрозрядних двохоперандних операцій лівостороннього додавання за модулем чотири, наведену в табл. 1.5.

Запропонований метод синтезу груп двохрозрядних двохоперандних операцій криптографічного кодування дозволяє моделювати операції при значному зменшенні математичних перетворень. Проте перевірити коректність цього методу для синтезу всіх симетричних двохрозрядних двохоперандних операцій, які дозволяють перестановки операндів, неможливо без математичних моделей 3-ї та 4-ї груп операцій.

## 3.2 Дослідження і синтез групи симетричних модифікованих операцій правостороннього додавання за модулем чотири

Проведемо дослідження отриманої за результатами обчислювального експерименту третьої группи симетричних двохрозрядних двохоперандних операцій криптографічного кодування. Експериментально синтезовані операції цієї групи наведено в стовпчиках 5-6 табл. 1.2. Для побудови моделей операцій використаємо технологію побудови двохоперандних операцій криптографічного перетворення інформації за результатами моделювання [106], враховуючи вдосконалення за результатами використання, наведеними в [2, 105]. Підставимо в моделі операцій, представлені кортежами одноопераднних операцій, одноопераднні операції відповідно до табл. 1.1 і, мінімізувавши таблиці істинності [105], отримаємо такі моделі [2]:

$$O_{1,7,15,21}=\begin{cases} F_1\begin{pmatrix}x_1\\x_2\end{pmatrix}, \text{ якщо } y_1=0;\ y_2=0 \\ F_7\begin{pmatrix}x_1\\x_2\end{pmatrix}, \text{ якщо } y_1=0;\ y_2=1 \\ F_{15}\begin{pmatrix}x_1\\x_2\end{pmatrix}, \text{ якщо } y_1=1;\ y_2=0 \\ F_{21}\begin{pmatrix}x_1\\x_2\end{pmatrix}, \text{ якщо } y_1=1;\ y_2=1 \end{cases} = \begin{cases} \begin{bmatrix}x_1\\x_2\end{bmatrix}, \text{ якщо } k_1=0;\ k_2=0 \\ \begin{bmatrix}x_1\\x_2\oplus 1\end{bmatrix}, \text{якщо } k_1=0;\ k_2=1 \\ \begin{bmatrix}x_1\oplus 1\\x_1\oplus x_2\end{bmatrix}, \text{ якщо } k_1=1;\ k_2=0 \\ \begin{bmatrix}x_1\oplus 1\\x_1\oplus x_2\oplus 1\end{bmatrix}, \text{якщо } k_1=1;\ k_2=1 \end{cases} = \begin{bmatrix}x_1\oplus k_1\\x_1\cdot k_1\oplus x_2\oplus k_2\end{bmatrix};$$

$$O_{7,1,21,15}=\begin{cases} F_7\begin{pmatrix}x_1\\x_2\end{pmatrix}, \text{ якщо } y_1=0;\ y_2=0 \\ F_1\begin{pmatrix}x_1\\x_2\end{pmatrix}, \text{ якщо } y_1=0;\ y_2=1 \\ F_{21}\begin{pmatrix}x_1\\x_2\end{pmatrix}, \text{ якщо } y_1=1;\ y_2=0 \\ F_{15}\begin{pmatrix}x_1\\x_2\end{pmatrix}, \text{ якщо } y_1=1;\ y_2=1 \end{cases} = \begin{cases} \begin{bmatrix}x_1\\x_2\oplus 1\end{bmatrix}, \text{ якщо } k_1=0;\ k_2=0 \\ \begin{bmatrix}x_1\\x_2\end{bmatrix}, \text{якщо } k_1=0;\ k_2=1 \\ \begin{bmatrix}x_1\oplus 1\\x_1\oplus x_2\oplus 1\end{bmatrix}, \text{ якщо } k_1=1;\ k_2=0 \\ \begin{bmatrix}x_1\oplus 1\\x_1\oplus x_2\end{bmatrix}, \text{якщо } k_1=1;\ k_2=1 \end{cases} = \begin{bmatrix}x_1\oplus k_1\\x_1\cdot k_1\oplus x_2\oplus k_2\oplus 1\end{bmatrix};$$

$$O_{15,21,7,1}=\begin{cases} F_{15}\begin{pmatrix}x_1\\x_2\end{pmatrix}, \text{ якщо } y_1=0;\ y_2=0 \\ F_{21}\begin{pmatrix}x_1\\x_2\end{pmatrix}, \text{ якщо } y_1=0;\ y_2=1 \\ F_7\begin{pmatrix}x_1\\x_2\end{pmatrix}, \text{ якщо } y_1=1;\ y_2=0 \\ F_1\begin{pmatrix}x_1\\x_2\end{pmatrix}, \text{ якщо } y_1=1;\ y_2=1 \end{cases} = \begin{cases} \begin{bmatrix}x_1\oplus 1\\x_1\oplus x_2\end{bmatrix}, \text{ якщо } k_1=0;\ k_2=0 \\ \begin{bmatrix}x_1\oplus 1\\x_1\oplus x_2\oplus 1\end{bmatrix}, \text{якщо } k_1=0;\ k_2=1 \\ \begin{bmatrix}x_1\\x_2\oplus 1\end{bmatrix}, \text{ якщо } k_1=1;\ k_2=0 \\ \begin{bmatrix}x_1\\x_2\end{bmatrix}, \text{якщо } k_1=1;\ k_2=1 \end{cases} = \begin{bmatrix}x_1\oplus k_1\oplus 1\\x_1\cdot\bar{k}_1\oplus x_2\oplus k_1\oplus k_2\end{bmatrix};$$

$$O_{21,15,1,7}=\begin{cases} F_{21}\begin{pmatrix}x_1\\x_2\end{pmatrix}, \text{ якщо } y_1=0;\ y_2=0 \\ F_{15}\begin{pmatrix}x_1\\x_2\end{pmatrix}, \text{ якщо } y_1=0;\ y_2=1 \\ F_1\begin{pmatrix}x_1\\x_2\end{pmatrix}, \text{ якщо } y_1=1;\ y_2=0 \\ F_7\begin{pmatrix}x_1\\x_2\end{pmatrix}, \text{ якщо } y_1=1;\ y_2=1 \end{cases} = \begin{cases} \begin{bmatrix}x_1\oplus 1\\x_1\oplus x_2\oplus 1\end{bmatrix}, \text{ якщо } k_1=0;\ k_2=0 \\ \begin{bmatrix}x_1\oplus 1\\x_1\oplus x_2\end{bmatrix}, \text{якщо } k_1=0;\ k_2=1 \\ \begin{bmatrix}x_1\\x_2\end{bmatrix}, \text{ якщо } k_1=1;\ k_2=0 \\ \begin{bmatrix}x_1\\x_2\oplus 1\end{bmatrix}, \text{якщо } k_1=1;\ k_2=1 \end{cases} = \begin{bmatrix}x_1\oplus k_1\oplus 1\\x_1\cdot\bar{k}_1\oplus x_2\oplus k_1\oplus k_2\oplus 1\end{bmatrix};$$

$$O_{2,20,17,11}=\begin{cases} F_2\begin{pmatrix}x_1\\x_2\end{pmatrix}, \text{ якщо } y_1=0;\ y_2=0 \\ F_{20}\begin{pmatrix}x_1\\x_2\end{pmatrix}, \text{ якщо } y_1=0;\ y_2=1 \\ F_{17}\begin{pmatrix}x_1\\x_2\end{pmatrix}, \text{ якщо } y_1=1;\ y_2=0 \\ F_{11}\begin{pmatrix}x_1\\x_2\end{pmatrix}, \text{ якщо } y_1=1;\ y_2=1 \end{cases} = \begin{cases} \begin{bmatrix}x_1\oplus x_2\\x_2\end{bmatrix}, \text{ якщо } k_1=0;\ k_2=0 \\ \begin{bmatrix}x_1\oplus x_2\oplus 1\\x_2\oplus 1\end{bmatrix}, \text{ якщо } k_1=0;\ k_2=1 \\ \begin{bmatrix}x_2\oplus 1\\x_1\oplus x_2\end{bmatrix}, \text{якщо } k_1=1;\ k_2=0 \\ \begin{bmatrix}x_2\\x_1\oplus x_2\oplus 1\end{bmatrix}, \text{якщо } k_1=1;\ k_2=1 \end{cases} = \begin{bmatrix}x_1\cdot\bar{k}_1\oplus x_2\oplus k_1\oplus k_2\\x_1\cdot k_1\oplus x_2\oplus k_2\end{bmatrix};$$

$$O_{11,17,2,20}=\begin{cases} F_{11}\begin{pmatrix}x_1\\x_2\end{pmatrix}, \text{ якщо } y_1=0;\ y_2=0 \\ F_{17}\begin{pmatrix}x_1\\x_2\end{pmatrix}, \text{ якщо } y_1=0;\ y_2=1 \\ F_{2}\begin{pmatrix}x_1\\x_2\end{pmatrix}, \text{ якщо } y_1=1;\ y_2=0 \\ F_{20}\begin{pmatrix}x_1\\x_2\end{pmatrix}, \text{ якщо } y_1=1;\ y_2=1 \end{cases}=\begin{cases} \begin{bmatrix}x_2\\x_1\oplus x_2\oplus 1\end{bmatrix}, \text{ якщо } k_1=0;\ k_2=0 \\ \begin{bmatrix}x_2\oplus 1\\x_1\oplus x_2\end{bmatrix}, \text{ якщо } k_1=0;\ k_2=1 \\ \begin{bmatrix}x_1\oplus x_2\\x_2\end{bmatrix}, \text{ якщо } k_1=1;\ k_2=0 \\ \begin{bmatrix}x_1\oplus x_2\oplus 1\\x_2\oplus 1\end{bmatrix}, \text{ якщо } k_1=1;\ k_2=1 \end{cases}=\begin{bmatrix}x_1\cdot k_1\oplus x_2\oplus k_2\\x_1\cdot\bar{k}_1\oplus x_2\oplus k_1\oplus k_2\oplus 1\end{bmatrix};$$

$$O_{17,11,20,2}=\begin{cases} F_{17}\begin{pmatrix}x_1\\x_2\end{pmatrix}, \text{ якщо } y_1=0;\ y_2=0 \\ F_{11}\begin{pmatrix}x_1\\x_2\end{pmatrix}, \text{ якщо } y_1=0;\ y_2=1 \\ F_{20}\begin{pmatrix}x_1\\x_2\end{pmatrix}, \text{ якщо } y_1=1;\ y_2=0 \\ F_{2}\begin{pmatrix}x_1\\x_2\end{pmatrix}, \text{ якщо } y_1=1;\ y_2=1 \end{cases}=\begin{cases} \begin{bmatrix}x_2\oplus 1\\x_1\oplus x_2\end{bmatrix}, \text{ якщо } k_1=0;\ k_2=0 \\ \begin{bmatrix}x_2\\x_1\oplus x_2\oplus 1\end{bmatrix}, \text{ якщо } k_1=0;\ k_2=1 \\ \begin{bmatrix}x_1\oplus x_2\oplus 1\\x_2\oplus 1\end{bmatrix}, \text{ якщо } k_1=1;\ k_2=0 \\ \begin{bmatrix}x_1\oplus x_2\\x_2\end{bmatrix}, \text{ якщо } k_1=1;\ k_2=1 \end{cases}=\begin{bmatrix}x_1\cdot k_1\oplus x_2\oplus k_2\oplus 1\\x_1\cdot\bar{k}_1\oplus x_2\oplus k_1\oplus k_2\end{bmatrix};$$

$$O_{20,2,11,17}=\begin{cases} F_{20}\begin{pmatrix}x_1\\x_2\end{pmatrix}, \text{ якщо } y_1=0;\ y_2=0 \\ F_{2}\begin{pmatrix}x_1\\x_2\end{pmatrix}, \text{ якщо } y_1=0;\ y_2=1 \\ F_{11}\begin{pmatrix}x_1\\x_2\end{pmatrix}, \text{ якщо } y_1=1;\ y_2=0 \\ F_{17}\begin{pmatrix}x_1\\x_2\end{pmatrix}, \text{ якщо } y_1=1;\ y_2=1 \end{cases}=\begin{cases} \begin{bmatrix}x_1\oplus x_2\oplus 1\\x_2\oplus 1\end{bmatrix}, \text{ якщо } k_1=0;\ k_2=0 \\ \begin{bmatrix}x_1\oplus x_2\\x_2\end{bmatrix}, \text{ якщо } k_1=0;\ k_2=1 \\ \begin{bmatrix}x_2\\x_1\oplus x_2\oplus 1\end{bmatrix}, \text{ якщо } k_1=1;\ k_2=0 \\ \begin{bmatrix}x_2\oplus 1\\x_1\oplus x_2\end{bmatrix}, \text{ якщо } k_1=1;\ k_2=1 \end{cases}=\begin{bmatrix}x_1\cdot\bar{k}_1\oplus x_2\oplus k_1\oplus k_2\oplus 1\\x_1\cdot k_1\oplus x_2\oplus k_2\oplus 1\end{bmatrix};$$

$$O_{3,9,19,13}=\begin{cases} F_{3}\begin{pmatrix}x_1\\x_2\end{pmatrix}, \text{ якщо } y_1=0;\ y_2=0 \\ F_{9}\begin{pmatrix}x_1\\x_2\end{pmatrix}, \text{ якщо } y_1=0;\ y_2=1 \\ F_{19}\begin{pmatrix}x_1\\x_2\end{pmatrix}, \text{ якщо } y_1=1;\ y_2=0 \\ F_{13}\begin{pmatrix}x_1\\x_2\end{pmatrix}, \text{ якщо } y_1=1;\ y_2=1 \end{cases}=\begin{cases} \begin{bmatrix}x_1\\x_1\oplus x_2\end{bmatrix}, \text{ якщо } k_1=0;\ k_2=0 \\ \begin{bmatrix}x_1\\x_1\oplus x_2\oplus 1\end{bmatrix}, \text{ якщо } k_1=0;\ k_2=1 \\ \begin{bmatrix}x_1\oplus 1\\x_2\oplus 1\end{bmatrix}, \text{ якщо } k_1=1;\ k_2=0 \\ \begin{bmatrix}x_1\oplus 1\\x_2\end{bmatrix}, \text{ якщо } k_1=1;\ k_2=1 \end{cases}=\begin{bmatrix}x_1\oplus k_1\\x_1\cdot\bar{k}_1\oplus x_2\oplus k_1\oplus k_2\end{bmatrix};$$

$$O_{9,3,13,19}=\begin{cases} F_{9}\begin{pmatrix}x_1\\x_2\end{pmatrix}, \text{ якщо } y_1=0;\ y_2=0 \\ F_{3}\begin{pmatrix}x_1\\x_2\end{pmatrix}, \text{ якщо } y_1=0;\ y_2=1 \\ F_{13}\begin{pmatrix}x_1\\x_2\end{pmatrix}, \text{ якщо } y_1=1;\ y_2=0 \\ F_{19}\begin{pmatrix}x_1\\x_2\end{pmatrix}, \text{ якщо } y_1=1;\ y_2=1 \end{cases}=\begin{cases} \begin{bmatrix}x_1\\x_1\oplus x_2\oplus 1\end{bmatrix}, \text{ якщо } k_1=0;\ k_2=0 \\ \begin{bmatrix}x_1\\x_1\oplus x_2\end{bmatrix}, \text{ якщо } k_1=0;\ k_2=1 \\ \begin{bmatrix}x_1\oplus 1\\x_2\end{bmatrix}, \text{ якщо } k_1=1;\ k_2=0 \\ \begin{bmatrix}x_1\oplus 1\\x_2\oplus 1\end{bmatrix}, \text{ якщо } k_1=1;\ k_2=1 \end{cases}=\begin{bmatrix}x_1\oplus k_1\\x_1\cdot\bar{k}_1\oplus x_2\oplus k_1\oplus k_2\oplus 1\end{bmatrix};$$

$$O_{13,19,3,9}=\begin{cases}F_{13}\begin{pmatrix}x_1\\x_2\end{pmatrix}, \text{ якщо } y_1=0;\ y_2=0\\ F_{19}\begin{pmatrix}x_1\\x_2\end{pmatrix}, \text{ якщо } y_1=0;\ y_2=1\\ F_{3}\begin{pmatrix}x_1\\x_2\end{pmatrix}, \text{ якщо } y_1=1;\ y_2=0\\ F_{9}\begin{pmatrix}x_1\\x_2\end{pmatrix}, \text{ якщо } y_1=1;\ y_2=1\end{cases}=\begin{cases}\begin{bmatrix}x_1\oplus 1\\x_2\end{bmatrix}, \text{ якщо } k_1=0;\ k_2=0\\ \begin{bmatrix}x_1\oplus 1\\x_2\oplus 1\end{bmatrix}, \text{ якщо } k_1=0;\ k_2=1\\ \begin{bmatrix}x_1\\x_1\oplus x_2\end{bmatrix}, \text{ якщо } k_1=1;\ k_2=0\\ \begin{bmatrix}x_1\\x_1\oplus x_2\oplus 1\end{bmatrix}, \text{ якщо } k_1=1;\ k_2=1\end{cases}=\begin{bmatrix}x_1\oplus k_1\oplus 1\\x_1\cdot k_1\oplus x_2\oplus k_2\end{bmatrix};$$

$$O_{19,13,9,3}=\begin{cases}F_{19}\begin{pmatrix}x_1\\x_2\end{pmatrix}, \text{ якщо } y_1=0;\ y_2=0\\ F_{13}\begin{pmatrix}x_1\\x_2\end{pmatrix}, \text{ якщо } y_1=0;\ y_2=1\\ F_{9}\begin{pmatrix}x_1\\x_2\end{pmatrix}, \text{ якщо } y_1=1;\ y_2=0\\ F_{3}\begin{pmatrix}x_1\\x_2\end{pmatrix}, \text{ якщо } y_1=1;\ y_2=1\end{cases}=\begin{cases}\begin{bmatrix}x_1\oplus 1\\x_2\oplus 1\end{bmatrix}, \text{ якщо } k_1=0;\ k_2=0\\ \begin{bmatrix}x_1\oplus 1\\x_2\end{bmatrix}, \text{ якщо } k_1=0;\ k_2=1\\ \begin{bmatrix}x_1\\x_1\oplus x_2\oplus 1\end{bmatrix}, \text{ якщо } k_1=1;\ k_2=0\\ \begin{bmatrix}x_1\\x_1\oplus x_2\end{bmatrix}, \text{ якщо } k_1=1;\ k_2=1\end{cases}=\begin{bmatrix}x_1\oplus k_1\oplus 1\\x_1\cdot k_1\oplus x_2\oplus k_2\oplus 1\end{bmatrix};$$

$$O_{4,16,12,24}=\begin{cases}F_{4}\begin{pmatrix}x_1\\x_2\end{pmatrix}, \text{ якщо } y_1=0;\ y_2=0\\ F_{16}\begin{pmatrix}x_1\\x_2\end{pmatrix}, \text{ якщо } y_1=0;\ y_2=1\\ F_{12}\begin{pmatrix}x_1\\x_2\end{pmatrix}, \text{ якщо } y_1=1;\ y_2=0\\ F_{24}\begin{pmatrix}x_1\\x_2\end{pmatrix}, \text{ якщо } y_1=1;\ y_2=1\end{cases}=\begin{cases}\begin{bmatrix}x_2\\x_1\end{bmatrix}, \text{ якщо } k_1=0;\ k_2=0\\ \begin{bmatrix}x_2\oplus 1\\x_1\end{bmatrix}, \text{ якщо } k_1=0;\ k_2=1\\ \begin{bmatrix}x_1\oplus x_2\\x_1\oplus 1\end{bmatrix}, \text{ якщо } k_1=1;\ k_2=0\\ \begin{bmatrix}x_1\oplus x_2\oplus 1\\x_1\oplus 1\end{bmatrix}, \text{ якщо } k_1=1;\ k_2=1\end{cases}=\begin{bmatrix}x_1\cdot k_1\oplus x_2\oplus k_2\\x_1\oplus k_1\end{bmatrix};$$

$$O_{12,24,16,4}=\begin{cases}F_{12}\begin{pmatrix}x_1\\x_2\end{pmatrix}, \text{ якщо } y_1=0;\ y_2=0\\ F_{24}\begin{pmatrix}x_1\\x_2\end{pmatrix}, \text{ якщо } y_1=0;\ y_2=1\\ F_{16}\begin{pmatrix}x_1\\x_2\end{pmatrix}, \text{ якщо } y_1=1;\ y_2=0\\ F_{4}\begin{pmatrix}x_1\\x_2\end{pmatrix}, \text{ якщо } y_1=1;\ y_2=1\end{cases}=\begin{cases}\begin{bmatrix}x_1\oplus x_2\\x_1\oplus 1\end{bmatrix}, \text{ якщо } k_1=0;\ k_2=0\\ \begin{bmatrix}x_1\oplus x_2\oplus 1\\x_1\oplus 1\end{bmatrix}, \text{ якщо } k_1=0;\ k_2=1\\ \begin{bmatrix}x_2\oplus 1\\x_1\end{bmatrix}, \text{ якщо } k_1=1;\ k_2=0\\ \begin{bmatrix}x_2\\x_1\end{bmatrix}, \text{ якщо } k_1=1;\ k_2=1\end{cases}=\begin{bmatrix}x_1\cdot \bar{k}_1\oplus x_2\oplus k_1\oplus k_2\\x_1\oplus k_1\oplus 1\end{bmatrix};$$

$$O_{16,4,24,12}=\begin{cases}F_{16}\begin{pmatrix}x_1\\x_2\end{pmatrix}, \text{ якщо } y_1=0;\ y_2=0\\ F_{4}\begin{pmatrix}x_1\\x_2\end{pmatrix}, \text{ якщо } y_1=0;\ y_2=1\\ F_{24}\begin{pmatrix}x_1\\x_2\end{pmatrix}, \text{ якщо } y_1=1;\ y_2=0\\ F_{12}\begin{pmatrix}x_1\\x_2\end{pmatrix}, \text{ якщо } y_1=1;\ y_2=1\end{cases}=\begin{cases}\begin{bmatrix}x_2\oplus 1\\x_1\end{bmatrix}, \text{ якщо } k_1=0;\ k_2=0\\ \begin{bmatrix}x_2\\x_1\end{bmatrix}, \text{ якщо } k_1=0;\ k_2=1\\ \begin{bmatrix}x_1\oplus x_2\oplus 1\\x_1\oplus 1\end{bmatrix}, \text{ якщо } k_1=1;\ k_2=0\\ \begin{bmatrix}x_1\oplus x_2\\x_1\oplus 1\end{bmatrix}, \text{ якщо } k_1=1;\ k_2=1\end{cases}=\begin{bmatrix}x_1\cdot k_1\oplus x_2\oplus k_2\oplus 1\\x_1\oplus k_1\end{bmatrix};$$

$$O_{24,12,4,16}=\begin{cases}F_{24}\begin{pmatrix}x_1\\x_2\end{pmatrix}, \text{ якщо } y_1=0;\ y_2=0\\ F_{12}\begin{pmatrix}x_1\\x_2\end{pmatrix}, \text{ якщо } y_1=0;\ y_2=1\\ F_{4}\begin{pmatrix}x_1\\x_2\end{pmatrix}, \text{ якщо } y_1=1;\ y_2=0\\ F_{16}\begin{pmatrix}x_1\\x_2\end{pmatrix}, \text{ якщо } y_1=1;\ y_2=1\end{cases}=\begin{cases}\begin{bmatrix}x_1\oplus x_2\oplus 1\\ x_1\oplus 1\end{bmatrix}, \text{ якщо } k_1=0;\ k_2=0\\ \begin{bmatrix}x_1\oplus x_2\\ x_1\oplus 1\end{bmatrix}, \text{ якщо } k_1=0;\ k_2=1\\ \begin{bmatrix}x_2\\ x_1\end{bmatrix}, \text{ якщо } k_1=1;\ k_2=0\\ \begin{bmatrix}x_2\oplus 1\\ x_1\end{bmatrix}, \text{ якщо } k_1=1;\ k_2=1\end{cases}=\begin{bmatrix}x_1\cdot\bar{k}_1\oplus x_2\oplus k_1\oplus k_2\oplus 1\\ x_1\oplus k_1\oplus 1\end{bmatrix};$$

$$O_{5,23,8,14}=\begin{cases}F_{5}\begin{pmatrix}x_1\\x_2\end{pmatrix}, \text{ якщо } y_1=0;\ y_2=0\\ F_{23}\begin{pmatrix}x_1\\x_2\end{pmatrix}, \text{ якщо } y_1=0;\ y_2=1\\ F_{8}\begin{pmatrix}x_1\\x_2\end{pmatrix}, \text{ якщо } y_1=1;\ y_2=0\\ F_{14}\begin{pmatrix}x_1\\x_2\end{pmatrix}, \text{ якщо } y_1=1;\ y_2=1\end{cases}=\begin{cases}\begin{bmatrix}x_2\\ x_1\oplus x_2\end{bmatrix}, \text{ якщо } k_1=0;\ k_2=0\\ \begin{bmatrix}x_2\oplus 1\\ x_1\oplus x_2\oplus 1\end{bmatrix}, \text{ якщо } k_1=0;\ k_2=1\\ \begin{bmatrix}x_1\oplus x_2\\ x_2\oplus 1\end{bmatrix}, \text{ якщо } k_1=1;\ k_2=0\\ \begin{bmatrix}x_1\oplus x_2\oplus 1\\ x_2\end{bmatrix}, \text{ якщо } k_1=1;\ k_2=1\end{cases}=\begin{bmatrix}x_1\cdot k_1\oplus x_2\oplus k_2\\ x_1\cdot\bar{k}_1\oplus x_2\oplus k_1\oplus k_2\end{bmatrix};$$

$$O_{8,14,23,5}=\begin{cases}F_{8}\begin{pmatrix}x_1\\x_2\end{pmatrix}, \text{ якщо } y_1=0;\ y_2=0\\ F_{14}\begin{pmatrix}x_1\\x_2\end{pmatrix}, \text{ якщо } y_1=0;\ y_2=1\\ F_{23}\begin{pmatrix}x_1\\x_2\end{pmatrix}, \text{ якщо } y_1=1;\ y_2=0\\ F_{5}\begin{pmatrix}x_1\\x_2\end{pmatrix}, \text{ якщо } y_1=1;\ y_2=1\end{cases}=\begin{cases}\begin{bmatrix}x_1\oplus x_2\\ x_2\oplus 1\end{bmatrix}, \text{ якщо } k_1=0;\ k_2=0\\ \begin{bmatrix}x_1\oplus x_2\oplus 1\\ x_2\end{bmatrix}, \text{ якщо } k_1=0;\ k_2=1\\ \begin{bmatrix}x_2\oplus 1\\ x_1\oplus x_2\oplus 1\end{bmatrix}, \text{ якщо } k_1=1;\ k_2=0\\ \begin{bmatrix}x_2\\ x_1\oplus x_2\end{bmatrix}, \text{ якщо } k_1=1;\ k_2=1\end{cases}=\begin{bmatrix}x_1\cdot\bar{k}_1\oplus x_2\oplus k_1\oplus k_2\\ x_1\cdot k_1\oplus x_2\oplus k_2\oplus 1\end{bmatrix};$$

$$O_{14,8,5,23}=\begin{cases}F_{14}\begin{pmatrix}x_1\\x_2\end{pmatrix}, \text{ якщо } y_1=0;\ y_2=0\\ F_{8}\begin{pmatrix}x_1\\x_2\end{pmatrix}, \text{ якщо } y_1=0;\ y_2=1\\ F_{5}\begin{pmatrix}x_1\\x_2\end{pmatrix}, \text{ якщо } y_1=1;\ y_2=0\\ F_{23}\begin{pmatrix}x_1\\x_2\end{pmatrix}, \text{ якщо } y_1=1;\ y_2=1\end{cases}=\begin{cases}\begin{bmatrix}x_1\oplus x_2\oplus 1\\ x_2\end{bmatrix}, \text{ якщо } k_1=0;\ k_2=0\\ \begin{bmatrix}x_1\oplus x_2\\ x_2\oplus 1\end{bmatrix}, \text{ якщо } k_1=0;\ k_2=1\\ \begin{bmatrix}x_2\\ x_1\oplus x_2\end{bmatrix}, \text{ якщо } k_1=1;\ k_2=0\\ \begin{bmatrix}x_2\oplus 1\\ x_1\oplus x_2\oplus 1\end{bmatrix}, \text{ якщо } k_1=1;\ k_2=1\end{cases}=\begin{bmatrix}x_1\cdot\bar{k}_1\oplus x_2\oplus k_1\oplus k_2\oplus 1\\ x_1\cdot k_1\oplus x_2\oplus k_2\end{bmatrix};$$

$$O_{23,5,14,8}=\begin{cases}F_{23}\begin{pmatrix}x_1\\x_2\end{pmatrix}, \text{ якщо } y_1=0;\ y_2=0\\ F_{5}\begin{pmatrix}x_1\\x_2\end{pmatrix}, \text{ якщо } y_1=0;\ y_2=1\\ F_{14}\begin{pmatrix}x_1\\x_2\end{pmatrix}, \text{ якщо } y_1=1;\ y_2=0\\ F_{8}\begin{pmatrix}x_1\\x_2\end{pmatrix}, \text{ якщо } y_1=1;\ y_2=1\end{cases}=\begin{cases}\begin{bmatrix}x_2\oplus 1\\ x_1\oplus x_2\oplus 1\end{bmatrix}, \text{ якщо } k_1=0;\ k_2=0\\ \begin{bmatrix}x_2\\ x_1\oplus x_2\end{bmatrix}, \text{ якщо } k_1=0;\ k_2=1\\ \begin{bmatrix}x_1\oplus x_2\oplus 1\\ x_2\end{bmatrix}, \text{ якщо } k_1=1;\ k_2=0\\ \begin{bmatrix}x_1\oplus x_2\\ x_2\oplus 1\end{bmatrix}, \text{ якщо } k_1=1;\ k_2=1\end{cases}=\begin{bmatrix}x_1\cdot k_1\oplus x_2\oplus k_2\oplus 1\\ x_1\cdot\bar{k}_1\oplus x_2\oplus k_1\oplus k_2\oplus 1\end{bmatrix};$$

$$O_{6,18,22,10}=\begin{cases} F_6\begin{pmatrix}x_1\\x_2\end{pmatrix}, \text{ якщо } y_1=0;\ y_2=0 \\ F_{18}\begin{pmatrix}x_1\\x_2\end{pmatrix}, \text{ якщо } y_1=0;\ y_2=1 \\ F_{22}\begin{pmatrix}x_1\\x_2\end{pmatrix}, \text{ якщо } y_1=1;\ y_2=0 \\ F_{10}\begin{pmatrix}x_1\\x_2\end{pmatrix}, \text{ якщо } y_1=1;\ y_2=1 \end{cases} = \begin{cases} \begin{bmatrix}x_1\oplus x_2\\ x_1\end{bmatrix}, \text{ якщо } k_1=0;\ k_2=0 \\ \begin{bmatrix}x_1\oplus x_2\oplus 1\\ x_1\end{bmatrix}, \text{ якщо } k_1=0;\ k_2=1 \\ \begin{bmatrix}x_2\oplus 1\\ x_1\oplus 1\end{bmatrix}, \text{ якщо } k_1=1;\ k_2=0 \\ \begin{bmatrix}x_2\\ x_1\oplus 1\end{bmatrix}, \text{ якщо } k_1=1;\ k_2=1 \end{cases} = \begin{bmatrix}x_1\cdot\bar{k}_1\oplus x_2\oplus k_1\oplus k_2\\ x_1\oplus k_1\end{bmatrix};$$

$$O_{10,22,6,18}=\begin{cases} F_{10}\begin{pmatrix}x_1\\x_2\end{pmatrix}, \text{ якщо } y_1=0;\ y_2=0 \\ F_{22}\begin{pmatrix}x_1\\x_2\end{pmatrix}, \text{ якщо } y_1=0;\ y_2=1 \\ F_6\begin{pmatrix}x_1\\x_2\end{pmatrix}, \text{ якщо } y_1=1;\ y_2=0 \\ F_{18}\begin{pmatrix}x_1\\x_2\end{pmatrix}, \text{ якщо } y_1=1;\ y_2=1 \end{cases} = \begin{cases} \begin{bmatrix}x_2\\ x_1\oplus 1\end{bmatrix}, \text{ якщо } k_1=0;\ k_2=0 \\ \begin{bmatrix}x_2\oplus 1\\ x_1\oplus 1\end{bmatrix}, \text{ якщо } k_1=0;\ k_2=1 \\ \begin{bmatrix}x_1\oplus x_2\\ x_1\end{bmatrix}, \text{ якщо } k_1=1;\ k_2=0 \\ \begin{bmatrix}x_1\oplus x_2\oplus 1\\ x_1\end{bmatrix}, \text{ якщо } k_1=1;\ k_2=1 \end{cases} = \begin{bmatrix}x_1\cdot k_1\oplus x_2\oplus k_2\\ x_1\oplus k_1\oplus 1\end{bmatrix};$$

$$O_{18,6,10,22}=\begin{cases} F_{18}\begin{pmatrix}x_1\\x_2\end{pmatrix}, \text{ якщо } y_1=0;\ y_2=0 \\ F_6\begin{pmatrix}x_1\\x_2\end{pmatrix}, \text{ якщо } y_1=0;\ y_2=1 \\ F_{10}\begin{pmatrix}x_1\\x_2\end{pmatrix}, \text{ якщо } y_1=1;\ y_2=0 \\ F_{22}\begin{pmatrix}x_1\\x_2\end{pmatrix}, \text{ якщо } y_1=1;\ y_2=1 \end{cases} = \begin{cases} \begin{bmatrix}x_1\oplus x_2\oplus 1\\ x_1\end{bmatrix}, \text{ якщо } k_1=0;\ k_2=0 \\ \begin{bmatrix}x_1\oplus x_2\\ x_1\end{bmatrix}, \text{ якщо } k_1=0;\ k_2=1 \\ \begin{bmatrix}x_2\\ x_1\oplus 1\end{bmatrix}, \text{ якщо } k_1=1;\ k_2=0 \\ \begin{bmatrix}x_2\oplus 1\\ x_1\oplus 1\end{bmatrix}, \text{ якщо } k_1=1;\ k_2=1 \end{cases} = \begin{bmatrix}x_1\cdot\bar{k}_1\oplus x_2\oplus k_1\oplus k_2\oplus 1\\ x_1\oplus k_1\end{bmatrix};$$

$$O_{22,10,18,6}=\begin{cases} F_{22}\begin{pmatrix}x_1\\x_2\end{pmatrix}, \text{ якщо } y_1=0;\ y_2=0 \\ F_{10}\begin{pmatrix}x_1\\x_2\end{pmatrix}, \text{ якщо } y_1=0;\ y_2=1 \\ F_{18}\begin{pmatrix}x_1\\x_2\end{pmatrix}, \text{ якщо } y_1=1;\ y_2=0 \\ F_6\begin{pmatrix}x_1\\x_2\end{pmatrix}, \text{ якщо } y_1=1;\ y_2=1 \end{cases} = \begin{cases} \begin{bmatrix}x_2\oplus 1\\ x_1\oplus 1\end{bmatrix}, \text{ якщо } k_1=0;\ k_2=0 \\ \begin{bmatrix}x_2\\ x_1\oplus 1\end{bmatrix}, \text{ якщо } k_1=0;\ k_2=1 \\ \begin{bmatrix}x_1\oplus x_2\oplus 1\\ x_1\end{bmatrix}, \text{ якщо } k_1=1;\ k_2=0 \\ \begin{bmatrix}x_1\oplus x_2\\ x_1\end{bmatrix}, \text{ якщо } k_1=1;\ k_2=1 \end{cases} = \begin{bmatrix}x_1\cdot k_1\oplus x_2\oplus k_2\oplus 1\\ x_1\oplus k_1\oplus 1\end{bmatrix}.$$

В таблицях істинності третьої групи операцій наявна таблиця істинності, яка була визначена як операція правостороннього додавання за модулем чотири ($O_1^{\text{mod}4\rightarrow}$). Таблицю істинності цієї операції та узагальненої операції з точністю до перестановки ($O_i^{\text{mod}4\rightarrow}$) наведено в табл. 3.1.

Враховуючи те, що всі моделі операцій третьої групи, включаючи двохрозрядну двохоперандну операцію правостороннього додавання за модулем чотири, можна приступити до перевірки гіпотези про синтез групи моделей операцій на основі заданої.

Таблиця 3.1

**Таблиця істинності операцій $O_1^{\text{mod}4\rightarrow}$ и $O_i^{\text{mod}4\rightarrow}$**

| **Операція** | $O_1^{\text{mod}4\rightarrow}$ | | | | $O_i^{\text{mod}4\rightarrow}$ | | | |
|---|---|---|---|---|---|---|---|---|
| **Значення операндів** | **00** | **01** | **10** | **11** | **00** | **01** | **10** | **11** |
| **00** | **00** | **01** | **10** | **11** | **a** | **b** | **c** | **d** |
| **01** | **01** | **00** | **11** | **10** | **b** | **a** | **d** | **c** |
| **10** | **10** | **11** | **01** | **00** | **c** | **d** | **b** | **a** |
| **11** | **11** | **10** | **00** | **01** | **d** | **c** | **a** | **b** |
| $a \neq b \neq c \neq d \in \{00; 01; 10; 11\}$, $i \in \{1; 2; ...; 24\}$ | | | | | | | | |

Синтез групи операцій будемо проводити на основі двохрозрядної двохоперандної операції правостороннього додавання за модулем чотири, яка дозволяє переставляти інформацію між операндами. Введемо підстановку в операцію правостороннього додавання за модулем чотири:

$$O_1^{\text{mod}4\rightarrow} = \begin{bmatrix} x_1 \oplus k_1 \\ x_1 \cdot k_1 \oplus x_2 \oplus k_2 \end{bmatrix} = \begin{bmatrix} y_1 \\ y_2 \end{bmatrix};$$

$$y_1 = x_1 \oplus k_1; \qquad y_2 = x_1 \cdot k_1 \oplus x_2 \oplus k_2.$$

Синтезуємо першу двохоперандну операцію базової групи на основі першої одноопераднної операції базової групи:

$$F_1(O_1^{\text{mod}4\rightarrow}) = \begin{bmatrix} y_1 \\ y_2 \end{bmatrix} = \begin{bmatrix} x_1 \oplus k_1 \\ x_1 \cdot k_1 \oplus x_2 \oplus k_2 \end{bmatrix} = O_1^{\text{mod}4\rightarrow} = O_{1,7,15,21}.$$

Синтезуємо другу двохоперандну операцію базової групи на основі другої одноопераднної операції базової групи:

$$F_2(O_1^{\text{mod}4\rightarrow}) = \begin{bmatrix} y_1 \oplus y_2 \\ y_2 \end{bmatrix} = \begin{bmatrix} (x_1 \oplus k_1) \oplus (x_1 \cdot k_1 \oplus x_2 \oplus k_2) \\ x_1 \cdot k_1 \oplus x_2 \oplus k_2 \end{bmatrix} = O_2^{\text{mod}4\rightarrow} = O_{2,20,17,11}.$$

Синтезуємо третю двохоперандну операцію базової групи на основі третьої одноопераднної операції базової групи:

$$F_3(O_1^{\text{mod}4\rightarrow}) = \begin{bmatrix} y_1 \\ y_1 \oplus y_2 \end{bmatrix} = \begin{bmatrix} x_1 \oplus k_1 \\ (x_1 \oplus k_1) \oplus (x_2 \oplus k_2) \end{bmatrix} = O_3^{\text{mod}4\rightarrow} = O_{3,9,19,13}.$$

Синтезувємо операції перестановки, виконавши над $O_1^{\text{mod}4\rightarrow}$ одноопернадні операції $F_4 - F_6$:

$$F_4(O_1^{\text{mod}4\rightarrow}) = \begin{bmatrix} y_2 \\ y_1 \end{bmatrix} = \begin{bmatrix} x_1 \cdot k_1 \oplus x_2 \oplus k_2 \\ x_1 \oplus k_1 \end{bmatrix} = O_4^{\text{mod}4\rightarrow} = O_{4,16,12,24};$$

$$F_5(O_1^{\text{mod}4\rightarrow}) = \begin{bmatrix} y_2 \\ y_1 \oplus y_2 \end{bmatrix} = \begin{bmatrix} x_1 \cdot k_1 \oplus x_2 \oplus k_2 \\ (x_1 \oplus k_1) \oplus (x_1 \cdot k_1 \oplus x_2 \oplus k_2) \end{bmatrix} = O_5^{\text{mod}4\rightarrow} = O_{5,23,8,14};$$

$$F_6(O_1^{\text{mod}4\rightarrow}) = \begin{bmatrix} y_1 \oplus y_2 \\ y_1 \end{bmatrix} = \begin{bmatrix} (x_1 \oplus k_1) \oplus (x_1 \cdot k_1 \oplus x_2 \oplus k_2) \\ x_1 \oplus k_1 \end{bmatrix} = O_6^{\text{mod}4\rightarrow} = O_{6,18,22,10}.$$

Синтезуємо операції инверсії, виконавши над $O_1^{\text{mod}4\rightarrow}$ одноопернадні операції $F_7 - F_{24}$:

$$F_7(O_1^{\text{mod}4\rightarrow}) = \begin{bmatrix} y_1 \\ y_2 \oplus 1 \end{bmatrix} = \begin{bmatrix} x_1 \oplus k_1 \\ x_1 \cdot k_1 \oplus x_2 \oplus k_2 \oplus 1 \end{bmatrix} = O_7^{\text{mod}4\rightarrow} = O_{7,1,21,15};$$

$$F_8(O_1^{\text{mod}4\rightarrow}) = \begin{bmatrix} y_1 \oplus y_2 \\ y_2 \oplus 1 \end{bmatrix} = \begin{bmatrix} (x_1 \oplus k_1) \oplus (x_1 \cdot k_1 \oplus x_2 \oplus k_2) \\ x_1 \cdot k_1 \oplus x_2 \oplus k_2 \oplus 1 \end{bmatrix} = O_8^{\text{mod}4\rightarrow} = O_{8,14,23,5};$$

$$F_9(O_1^{\text{mod}4\rightarrow}) = \begin{bmatrix} y_1 \\ y_1 \oplus y_2 \oplus 1 \end{bmatrix} = \begin{bmatrix} x_1 \oplus k_1 \\ (x_1 \oplus k_1) \oplus (x_2 \oplus k_2) \oplus 1 \end{bmatrix} = O_9^{\text{mod}4\rightarrow} = O_{9,3,13,19};$$

$$F_{10}(O_1^{\text{mod}4\rightarrow}) = \begin{bmatrix} y_2 \\ y_1 \oplus 1 \end{bmatrix} = \begin{bmatrix} x_1 \cdot k_1 \oplus x_2 \oplus k_2 \\ x_1 \oplus k_1 \oplus 1 \end{bmatrix} = O_{10}^{\text{mod}4\rightarrow} = O_{10,22,6,18};$$

$$F_{11}(O_1^{\text{mod}4\rightarrow}) = \begin{bmatrix} y_2 \\ y_1 \oplus y_2 \oplus 1 \end{bmatrix} = \begin{bmatrix} x_1 \cdot k_1 \oplus x_2 \oplus k_2 \\ (x_1 \oplus k_1) \oplus (x_1 \cdot k_1 \oplus x_2 \oplus k_2) \oplus 1 \end{bmatrix} = O_{11}^{\text{mod}4\rightarrow} = O_{11,17,2,20};$$

$$F_{12}(O_1^{\text{mod}4\rightarrow}) = \begin{bmatrix} y_1 \oplus y_2 \\ y_1 \oplus 1 \end{bmatrix} = \begin{bmatrix} (x_1 \oplus k_1) \oplus (x_1 \cdot k_1 \oplus x_2 \oplus k_2) \\ x_1 \oplus k_1 \oplus 1 \end{bmatrix} = O_{12}^{\text{mod}4\rightarrow} = O_{12,24,16,4};$$

$$F_{13}(O_1^{\text{mod}4\rightarrow}) = \begin{bmatrix} y_1 \oplus 1 \\ y_2 \end{bmatrix} = \begin{bmatrix} x_1 \oplus k_1 \oplus 1 \\ x_1 \cdot k_1 \oplus x_2 \oplus k_2 \end{bmatrix} = O_{13}^{\text{mod}4\rightarrow} = O_{13,19,3,9};$$

$$F_{14}(O_1^{\text{mod}4\rightarrow}) = \begin{bmatrix} y_1 \oplus y_2 \oplus 1 \\ y_2 \end{bmatrix} = \begin{bmatrix} (x_1 \oplus k_1) \oplus (x_1 \cdot k_1 \oplus x_2 \oplus k_2) \oplus 1 \\ x_1 \cdot k_1 \oplus x_2 \oplus k_2 \end{bmatrix} = O_{14}^{\text{mod}4\rightarrow} = O_{14,8,5,23};$$

$$F_{15}(O_1^{\text{mod4}\rightarrow}) = \begin{bmatrix} y_1 \oplus 1 \\ y_1 \oplus y_2 \end{bmatrix} = \begin{bmatrix} x_1 \oplus k_1 \oplus 1 \\ (x_1 \oplus k_1) \oplus (x_2 \oplus k_2) \end{bmatrix} = O_{15}^{\text{mod4}\rightarrow} = O_{15,21,7,1};$$

$$F_{16}(O_1^{\text{mod4}\rightarrow}) = \begin{bmatrix} y_2 \oplus 1 \\ y_1 \end{bmatrix} = \begin{bmatrix} x_1 \cdot k_1 \oplus x_2 \oplus k_2 \oplus 1 \\ x_1 \oplus k_1 \end{bmatrix} = O_{16}^{\text{mod4}\rightarrow} = O_{16,4,24,12};$$

$$F_{17}(O_1^{\text{mod4}\rightarrow}) = \begin{bmatrix} y_2 \oplus 1 \\ y_1 \oplus y_2 \end{bmatrix} = \begin{bmatrix} x_1 \cdot k_1 \oplus x_2 \oplus k_2 \oplus 1 \\ (x_1 \oplus k_1) \oplus (x_1 \cdot k_1 \oplus x_2 \oplus k_2) \end{bmatrix} = O_{17}^{\text{mod4}\rightarrow} = O_{17,11,20,2};$$

$$F_{18}(O_1^{\text{mod4}\rightarrow}) = \begin{bmatrix} y_1 \oplus y_2 \oplus 1 \\ y_1 \end{bmatrix} = \begin{bmatrix} (x_1 \oplus k_1) \oplus (x_1 \cdot k_1 \oplus x_2 \oplus k_2) \oplus 1 \\ x_1 \oplus k_1 \end{bmatrix} = O_{18}^{\text{mod4}\rightarrow} = O_{18,6,10,22};$$

$$F_{19}(O_1^{\text{mod4}\rightarrow}) = \begin{bmatrix} y_1 \oplus 1 \\ y_2 \oplus 1 \end{bmatrix} = \begin{bmatrix} x_1 \oplus k_1 \oplus 1 \\ x_1 \cdot k_1 \oplus x_2 \oplus k_2 \oplus 1 \end{bmatrix} = O_{19}^{\text{mod4}\rightarrow} = O_{13,19,3,9};$$

$$F_{20}(O_1^{\text{mod4}\rightarrow}) = \begin{bmatrix} y_1 \oplus y_2 \oplus 1 \\ y_2 \oplus 1 \end{bmatrix} = \begin{bmatrix} (x_1 \oplus k_1) \oplus (x_1 \cdot k_1 \oplus x_2 \oplus k_2) \oplus 1 \\ x_1 \cdot k_1 \oplus x_2 \oplus k_2 \oplus 1 \end{bmatrix} = O_{20}^{\text{mod4}\rightarrow} = O_{20,2,11,17};$$

$$F_{21}(O_1^{\text{mod4}\rightarrow}) = \begin{bmatrix} y_1 \oplus 1 \\ y_1 \oplus y_2 \oplus 1 \end{bmatrix} = \begin{bmatrix} x_1 \oplus k_1 \oplus 1 \\ (x_1 \oplus k_1) \oplus (x_2 \oplus k_2) \oplus 1 \end{bmatrix} = O_{21}^{\text{mod4}\rightarrow} = O_{21,15,1,7};$$

$$F_{22}(O_1^{\text{mod4}\rightarrow}) = \begin{bmatrix} y_2 \oplus 1 \\ y_1 \oplus 1 \end{bmatrix} = \begin{bmatrix} x_1 \cdot k_1 \oplus x_2 \oplus k_2 \oplus 1 \\ x_1 \oplus k_1 \oplus 1 \end{bmatrix} = O_{22}^{\text{mod4}\rightarrow} = O_{22,10,18,6};$$

$$F_{23}(O_1^{\text{mod4}\rightarrow}) = \begin{bmatrix} y_2 \oplus 1 \\ y_1 \oplus y_2 \oplus 1 \end{bmatrix} = \begin{bmatrix} x_1 \cdot k_1 \oplus x_2 \oplus k_2 \oplus 1 \\ (x_1 \oplus k_1) \oplus (x_1 \cdot k_1 \oplus x_2 \oplus k_2) \oplus 1 \end{bmatrix} = O_{23}^{\text{mod4}\rightarrow} = O_{23,5,14,8};$$

$$F_{24}(O_1^{\text{mod4}\rightarrow}) = \begin{bmatrix} y_1 \oplus y_2 \oplus 1 \\ y_1 \oplus 1 \end{bmatrix} = \begin{bmatrix} (x_1 \oplus k_1) \oplus (x_1 \cdot k_1 \oplus x_2 \oplus k_2) \oplus 1 \\ x_1 \oplus k_1 \oplus 1 \end{bmatrix} = O_{24}^{\text{mod4}\rightarrow} = O_{24,12,4,16}.$$

Як видно з наведених результатів синтезу, отримані моделі операцій повністю співпадають з моделями, які побудовано за результатами обчислювального експерименту. Отримані моделі було класифіковано за групами і наведено в зведеній табл. 3.2 [2].

Таблиця 3.2

**Двохрозрядні двохоперандні операції криптографічного кодування, синтезовані на основі правостороннього додавання за модулем чотири**

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

Запропонований підхід дозволив коректно синтезувати групу симетричних двохрозрядних двохоперандних операцій правостороннього

додавання за модулем чотири (третю), отриману за результатами обчислювального експерименту.

## 3.3 Дослідження і синтез четвертої групи симетричних модифікованих операцій, отриманих за результатами обчислювального експерименту

Експериментально синтезовані операції четвертої групи симетричних модифікованих операцій наведено в стовпчиках 7-8 табл. 1.2.

Побудуємо математичні моделі цих операцій і проведемо їх аналіз та дослідження аналогічно з синтезом, аналізом та дослідженнями групи симетричних модифікованих операцій правостороннього додавання за модулем чотири, наведеними в підрозділі 3.2.

$$O_{1,10,16,19}=\begin{cases} F_1\begin{pmatrix}x_1\\x_2\end{pmatrix},\ якщо\ y_1=0;\ y_2=0 \\ F_{10}\begin{pmatrix}x_1\\x_2\end{pmatrix},\ якщо\ y_1=0;\ y_2=1 \\ F_{16}\begin{pmatrix}x_1\\x_2\end{pmatrix},\ якщо\ y_1=1;\ y_2=0 \\ F_{19}\begin{pmatrix}x_1\\x_2\end{pmatrix},\ якщо\ y_1=1;\ y_2=1 \end{cases}=\begin{cases} \begin{bmatrix}x_1\\x_2\end{bmatrix},\ якщо k_1=0;\ k_2=0 \\ \begin{bmatrix}x_2\\x_1\oplus 1\end{bmatrix},\ якщо k_1=0;\ k_2=1 \\ \begin{bmatrix}x_2\oplus 1\\x_1\end{bmatrix},\ якщо k_1=1;\ k_2=0 \\ \begin{bmatrix}x_1\oplus 1\\x_2\oplus 1\end{bmatrix},\ якщо k_1=1;\ k_2=1 \end{cases}=\begin{bmatrix} x_1\cdot(\overline{k_1\oplus k_2})\oplus x_2\cdot(k_1\oplus k_2)\oplus k_1 \\ x_1\cdot(k_1\oplus k_2)\oplus x_2\cdot(\overline{k_1\oplus k_2})\oplus k_2 \end{bmatrix};$$

$$O_{10,19,1,16}=\begin{cases} F_1\begin{pmatrix}x_1\\x_2\end{pmatrix},\ якщо\ y_1=0;\ y_2=0 \\ F_9\begin{pmatrix}x_1\\x_2\end{pmatrix},\ якщо\ y_1=0;\ y_2=1 \\ F_1\begin{pmatrix}x_1\\x_2\end{pmatrix},\ якщо\ y_1=1;\ y_2=0 \\ F_{16}\begin{pmatrix}x_1\\x_2\end{pmatrix},\ якщо\ y_1=1;\ y_2=1 \end{cases}=\begin{cases} \begin{bmatrix}x_2\\x_1\oplus 1\end{bmatrix},\ якщо k_1=0;\ k_2=0 \\ \begin{bmatrix}x_1\oplus 1\\x_2\oplus 1\end{bmatrix},\ якщо k_1=0;\ k_2=1 \\ \begin{bmatrix}x_1\\x_2\end{bmatrix},\ якщо k_1=1;\ k_2=0 \\ \begin{bmatrix}x_2\oplus 1\\x_1\end{bmatrix},\ якщо k_1=1;\ k_2=1 \end{cases}=\begin{bmatrix} x_1\cdot(k_1\oplus k_2)\oplus x_2\cdot(\overline{k_1\oplus k_2})\oplus k_2 \\ x_1\cdot(\overline{k_1\oplus k_2})\oplus x_2\cdot(k_1\oplus k_2)\oplus k_1\oplus 1 \end{bmatrix};$$

$$O_{16,1,19,10}=\begin{cases} F_{16}\begin{pmatrix}x_1\\x_2\end{pmatrix}, & якщо\, y_1=0;\ y_2=0 \\ F_{1}\begin{pmatrix}x_1\\x_2\end{pmatrix}, & якщо\, y_1=0;\ y_2=1 \\ F_{19}\begin{pmatrix}x_1\\x_2\end{pmatrix}, & якщо\, y_1=1;\ y_2=0 \\ F_{10}\begin{pmatrix}x_1\\x_2\end{pmatrix}, & якщо\, y_1=1;\ y_2=1 \end{cases} = \begin{cases} \begin{bmatrix}x_2\oplus 1\\ x_1\end{bmatrix}, & якщо k_1=0;\ k_2=0 \\ \begin{bmatrix}x_1\\ x_2\end{bmatrix}, & якщо k_1=0;\ k_2=1 \\ \begin{bmatrix}x_1\oplus 1\\ x_2\oplus 1\end{bmatrix}, & якщо k_1=1;\ k_2=0 \\ \begin{bmatrix}x_2\\ x_1\oplus 1\end{bmatrix}, & якщо k_1=1;\ k_2=1 \end{cases} = \begin{bmatrix} x_1\cdot(k_1\oplus k_2)\oplus x_2\cdot(\overline{k_1\oplus k_2})\oplus k_2\oplus 1 \\ x_1\cdot(\overline{k_1\oplus k_2})\oplus x_2\cdot(k_1\oplus k_2)\oplus k_1 \end{bmatrix};$$

$$O_{19,16,10,1}=\begin{cases} F_{19}\begin{pmatrix}x_1\\x_2\end{pmatrix}, & якщо\, y_1=0;\ y_2=0 \\ F_{16}\begin{pmatrix}x_1\\x_2\end{pmatrix}, & якщо\, y_1=0;\ y_2=1 \\ F_{10}\begin{pmatrix}x_1\\x_2\end{pmatrix}, & якщо\, y_1=1;\ y_2=0 \\ F_{1}\begin{pmatrix}x_1\\x_2\end{pmatrix}, & якщо\, y_1=1;\ y_2=1 \end{cases} = \begin{cases} \begin{bmatrix}x_1\oplus 1\\ x_2\oplus 1\end{bmatrix}, & якщо k_1=0;\ k_2=0 \\ \begin{bmatrix}x_2\oplus 1\\ x_1\end{bmatrix}, & якщо k_1=0;\ k_2=1 \\ \begin{bmatrix}x_2\\ x_1\oplus 1\end{bmatrix}, & якщо k_1=1;\ k_2=0 \\ \begin{bmatrix}x_1\\ x_2\end{bmatrix}, & якщо k_1=1;\ k_2=1 \end{cases} = \begin{bmatrix} x_1\cdot(\overline{k_1\oplus k_2})\oplus x_2\cdot(k_1\oplus k_2)\oplus k_1\oplus 1 \\ x_1\cdot(k_1\oplus k_2)\oplus x_2\cdot(\overline{k_1\oplus k_2})\oplus k_2\oplus 1 \end{bmatrix};$$

$$O_{2,24,18,8}=\begin{cases} F_{2}\begin{pmatrix}x_1\\x_2\end{pmatrix}, & якщо\, y_1=0;\ y_2=0 \\ F_{24}\begin{pmatrix}x_1\\x_2\end{pmatrix}, & якщо\, y_1=0;\ y_2=1 \\ F_{18}\begin{pmatrix}x_1\\x_2\end{pmatrix}, & якщо\, y_1=1;\ y_2=0 \\ F_{8}\begin{pmatrix}x_1\\x_2\end{pmatrix}, & якщо\, y_1=1;\ y_2=1 \end{cases} = \begin{cases} \begin{bmatrix}x_1\oplus x_2\\ x_2\end{bmatrix}, & якщо k_1=0;\ k_2=0 \\ \begin{bmatrix}x_1\oplus x_2\oplus 1\\ x_1\oplus 1\end{bmatrix}, & якщо k_1=0;\ k_2=1 \\ \begin{bmatrix}x_1\oplus x_2\oplus 1\\ x_1\end{bmatrix}, & якщо k_1=1;\ k_2=0 \\ \begin{bmatrix}x_1\oplus x_2\\ x_2\oplus 1\end{bmatrix}, & якщо k_1=1;\ k_2=1 \end{cases} = \begin{bmatrix} x_1\oplus x_2\oplus k_1\oplus k_2 \\ x_1\cdot(k_1\oplus k_2)\oplus x_2\cdot(\overline{k_1\oplus k_2})\oplus k_2 \end{bmatrix};$$

$$O_{8,18,24,2}=\begin{cases} F_{8}\begin{pmatrix}x_1\\x_2\end{pmatrix}, & якщо\, y_1=0;\ y_2=0 \\ F_{18}\begin{pmatrix}x_1\\x_2\end{pmatrix}, & якщо\, y_1=0;\ y_2=1 \\ F_{24}\begin{pmatrix}x_1\\x_2\end{pmatrix}, & якщо\, y_1=1;\ y_2=0 \\ F_{2}\begin{pmatrix}x_1\\x_2\end{pmatrix}, & якщо\, y_1=1;\ y_2=1 \end{cases} = \begin{cases} \begin{bmatrix}x_1\oplus x_2\\ x_2\oplus 1\end{bmatrix}, & якщо k_1=0;\ k_2=0 \\ \begin{bmatrix}x_1\oplus x_2\oplus 1\\ x_1\end{bmatrix}, & якщо k_1=0;\ k_2=1 \\ \begin{bmatrix}x_1\oplus x_2\oplus 1\\ x_1\oplus 1\end{bmatrix}, & якщо k_1=1;\ k_2=0 \\ \begin{bmatrix}x_1\oplus x_2\\ x_2\end{bmatrix}, & якщо k_1=1;\ k_2=1 \end{cases} = \begin{bmatrix} x_1\oplus x_2\oplus k_1\oplus k_2 \\ x_1\cdot(k_1\oplus k_2)\oplus x_2\cdot(\overline{k_1\oplus k_2})\oplus k_2\oplus 1 \end{bmatrix};$$

$$O_{18,2,8,24}=\begin{cases} F_{18}\begin{pmatrix}x_1\\x_2\end{pmatrix}, & якщо\, y_1=0;\ y_2=0 \\ F_{2}\begin{pmatrix}x_1\\x_2\end{pmatrix}, & якщо\, y_1=0;\ y_2=1 \\ F_{8}\begin{pmatrix}x_1\\x_2\end{pmatrix}, & якщо\, y_1=1;\ y_2=0 \\ F_{24}\begin{pmatrix}x_1\\x_2\end{pmatrix}, & якщо\, y_1=1;\ y_2=1 \end{cases} = \begin{cases} \begin{bmatrix}x_1\oplus x_2\oplus 1\\ x_1\end{bmatrix}, & якщо k_1=0;\ k_2=0 \\ \begin{bmatrix}x_1\oplus x_2\\ x_2\end{bmatrix}, & якщо k_1=0;\ k_2=1 \\ \begin{bmatrix}x_1\oplus x_2\\ x_2\oplus 1\end{bmatrix}, & якщо k_1=1;\ k_2=0 \\ \begin{bmatrix}x_1\oplus x_2\oplus 1\\ x_1\oplus 1\end{bmatrix}, & якщо k_1=1;\ k_2=1 \end{cases} = \begin{bmatrix} x_1\oplus x_2\oplus k_1\oplus k_2\oplus 1 \\ x_1\cdot(\overline{k_1\oplus k_2})\oplus x_2\cdot(k_1\oplus k_2)\oplus k_1 \end{bmatrix};$$

$$O_{24,8,2,18}=\begin{cases} F_{24}\begin{pmatrix}x_1\\x_2\end{pmatrix}, \text{ якщо } y_1=0;\ y_2=0 \\ F_{8}\begin{pmatrix}x_1\\x_2\end{pmatrix}, \text{ якщо } y_1=0;\ y_2=1 \\ F_{2}\begin{pmatrix}x_1\\x_2\end{pmatrix}, \text{ якщо } y_1=1;\ y_2=0 \\ F_{18}\begin{pmatrix}x_1\\x_2\end{pmatrix}, \text{ якщо } y_1=1;\ y_2=1 \end{cases} = \begin{cases} \begin{bmatrix}x_1\oplus x_2\oplus 1\\ x_1\oplus 1\end{bmatrix}, \text{ якщо } k_1=0;\ k_2=0 \\ \begin{bmatrix}x_1\oplus x_2\\ x_2\oplus 1\end{bmatrix}, \text{ якщо } k_1=0;\ k_2=1 \\ \begin{bmatrix}x_1\oplus x_2\\ x_2\end{bmatrix}, \text{ якщо } k_1=1;\ k_2=0 \\ \begin{bmatrix}x_1\oplus x_2\oplus 1\\ x_1\end{bmatrix}, \text{ якщо } k_1=1;\ k_2=1 \end{cases} = \begin{bmatrix}x_1\oplus x_2\oplus k_1\oplus k_2\oplus 1\\ x_1\cdot\overline{(k_1\oplus k_2)}\oplus x_2\cdot(k_1\oplus k_2)\oplus k_1\oplus 1\end{bmatrix};$$

$$O_{3,11,23,15}=\begin{cases} F_{3}\begin{pmatrix}x_1\\x_2\end{pmatrix}, \text{ якщо } y_1=0;\ y_2=0 \\ F_{11}\begin{pmatrix}x_1\\x_2\end{pmatrix}, \text{ якщо } y_1=0;\ y_2=1 \\ F_{23}\begin{pmatrix}x_1\\x_2\end{pmatrix}, \text{ якщо } y_1=1;\ y_2=0 \\ F_{15}\begin{pmatrix}x_1\\x_2\end{pmatrix}, \text{ якщо } y_1=1;\ y_2=1 \end{cases} = \begin{cases} \begin{bmatrix}x_1\\ x_1\oplus x_2\end{bmatrix}, \text{ якщо } k_1=0;\ k_2=0 \\ \begin{bmatrix}x_2\\ x_1\oplus x_2\oplus 1\end{bmatrix}, \text{ якщо } k_1=0;\ k_2=1 \\ \begin{bmatrix}x_2\oplus 1\\ x_1\oplus x_2\oplus 1\end{bmatrix}, \text{ якщо } k_1=1;\ k_2=0 \\ \begin{bmatrix}x_1\oplus 1\\ x_1\oplus x_2\end{bmatrix}, \text{ якщо } k_1=1;\ k_2=1 \end{cases} = \begin{bmatrix}x_1\cdot(k_1\oplus k_2)\oplus x_2\cdot\overline{(k_1\oplus k_2)}\oplus k_1\\ x_1\oplus x_2\oplus k_1\oplus k_2\end{bmatrix};$$

$$O_{11,15,3,23}=\begin{cases} F_{11}\begin{pmatrix}x_1\\x_2\end{pmatrix}, \text{ якщо } y_1=0;\ y_2=0 \\ F_{15}\begin{pmatrix}x_1\\x_2\end{pmatrix}, \text{ якщо } y_1=0;\ y_2=1 \\ F_{3}\begin{pmatrix}x_1\\x_2\end{pmatrix}, \text{ якщо } y_1=1;\ y_2=0 \\ F_{23}\begin{pmatrix}x_1\\x_2\end{pmatrix}, \text{ якщо } y_1=1;\ y_2=1 \end{cases} = \begin{cases} \begin{bmatrix}x_2\\ x_1\oplus x_2\oplus 1\end{bmatrix}, \text{ якщо } k_1=0;\ k_2=0 \\ \begin{bmatrix}x_1\oplus 1\\ x_1\oplus x_2\end{bmatrix}, \text{ якщо } k_1=0;\ k_2=1 \\ \begin{bmatrix}x_1\\ x_1\oplus x_2\end{bmatrix}, \text{ якщо } k_1=1;\ k_2=0 \\ \begin{bmatrix}x_2\oplus 1\\ x_1\oplus x_2\oplus 1\end{bmatrix}, \text{ якщо } k_1=1;\ k_2=1 \end{cases} = \begin{bmatrix}x_1\cdot(k_1\oplus k_2)\oplus x_2\cdot\overline{(k_1\oplus k_2)}\oplus k_2\\ x_1\oplus x_2\oplus k_1\oplus k_2\oplus 1\end{bmatrix};$$

$$O_{15,23,11,3}=\begin{cases} F_{15}\begin{pmatrix}x_1\\x_2\end{pmatrix}, \text{ якщо } y_1=0;\ y_2=0 \\ F_{23}\begin{pmatrix}x_1\\x_2\end{pmatrix}, \text{ якщо } y_1=0;\ y_2=1 \\ F_{11}\begin{pmatrix}x_1\\x_2\end{pmatrix}, \text{ якщо } y_1=1;\ y_2=0 \\ F_{3}\begin{pmatrix}x_1\\x_2\end{pmatrix}, \text{ якщо } y_1=1;\ y_2=1 \end{cases} = \begin{cases} \begin{bmatrix}x_1\oplus 1\\ x_1\oplus x_2\end{bmatrix}, \text{ якщо } k_1=0;\ k_2=0 \\ \begin{bmatrix}x_2\oplus 1\\ x_1\oplus x_2\oplus 1\end{bmatrix}, \text{ якщо } k_1=0;\ k_2=1 \\ \begin{bmatrix}x_2\\ x_1\oplus x_2\oplus 1\end{bmatrix}, \text{ якщо } k_1=1;\ k_2=0 \\ \begin{bmatrix}x_1\\ x_1\oplus x_2\end{bmatrix}, \text{ якщо } k_1=1;\ k_2=1 \end{cases} = \begin{bmatrix}x_1\cdot\overline{(k_1\oplus k_2)}\oplus x_2\cdot(k_1\oplus k_2)\oplus k_1\oplus 1\\ x_1\oplus x_2\oplus k_1\oplus k_2\end{bmatrix};$$

$$O_{23,3,15,11}=\begin{cases} F_{23}\begin{pmatrix}x_1\\x_2\end{pmatrix}, \text{ якщо } y_1=0;\ y_2=0 \\ F_{3}\begin{pmatrix}x_1\\x_2\end{pmatrix}, \text{ якщо } y_1=0;\ y_2=1 \\ F_{15}\begin{pmatrix}x_1\\x_2\end{pmatrix}, \text{ якщо } y_1=1;\ y_2=0 \\ F_{11}\begin{pmatrix}x_1\\x_2\end{pmatrix}, \text{ якщо } y_1=1;\ y_2=1 \end{cases} = \begin{cases} \begin{bmatrix}x_2\oplus 1\\ x_1\oplus x_2\oplus 1\end{bmatrix}, \text{ якщо } k_1=0;\ k_2=0 \\ \begin{bmatrix}x_1\\ x_1\oplus x_2\end{bmatrix}, \text{ якщо } k_1=0;\ k_2=1 \\ \begin{bmatrix}x_1\oplus 1\\ x_1\oplus x_2\end{bmatrix}, \text{ якщо } k_1=1;\ k_2=0 \\ \begin{bmatrix}x_2\\ x_1\oplus x_2\oplus 1\end{bmatrix}, \text{ якщо } k_1=1;\ k_2=1 \end{cases} = \begin{bmatrix}x_1\cdot(k_1\oplus k_2)\oplus x_2\cdot\overline{(k_1\oplus k_2)}\oplus k_2\oplus 1\\ x_1\oplus x_2\oplus k_1\oplus k_2\oplus 1\end{bmatrix};$$

$$O_{4,13,7,22}=\begin{cases} F_4\begin{pmatrix}x_1\\x_2\end{pmatrix}, \text{ якщо } y_1=0;\ y_2=0 \\ F_{13}\begin{pmatrix}x_1\\x_2\end{pmatrix}, \text{ якщо } y_1=0;\ y_2=1 \\ F_7\begin{pmatrix}x_1\\x_2\end{pmatrix}, \text{ якщо } y_1=1;\ y_2=0 \\ F_{22}\begin{pmatrix}x_1\\x_2\end{pmatrix}, \text{ якщо } y_1=1;\ y_2=1 \end{cases} = \begin{cases} \begin{bmatrix}x_2\\x_1\end{bmatrix}, \text{ якщо } k_1=0;\ k_2=0 \\ \begin{bmatrix}x_1\oplus 1\\x_2\end{bmatrix}, \text{ якщо } k_1=0;\ k_2=1 \\ \begin{bmatrix}x_1\\x_2\oplus 1\end{bmatrix}, \text{ якщо } k_1=1;\ k_2=0 \\ \begin{bmatrix}x_2\oplus 1\\x_1\oplus 1\end{bmatrix}, \text{ якщо } k_1=1;\ k_2=1 \end{cases} = \begin{bmatrix} x_1\cdot(k_1\oplus k_2)\oplus x_2\cdot(\overline{k_1\oplus k_2})\oplus k_2 \\ x_1\cdot(\overline{k_1\oplus k_2})\oplus x_2\cdot(k_1\oplus k_2)\oplus k_1 \end{bmatrix};$$

$$O_{7,4,22,13}=\begin{cases} F_7\begin{pmatrix}x_1\\x_2\end{pmatrix}, \text{ якщо } y_1=0;\ y_2=0 \\ F_4\begin{pmatrix}x_1\\x_2\end{pmatrix}, \text{ якщо } y_1=0;\ y_2=1 \\ F_{22}\begin{pmatrix}x_1\\x_2\end{pmatrix}, \text{ якщо } y_1=1;\ y_2=0 \\ F_{13}\begin{pmatrix}x_1\\x_2\end{pmatrix}, \text{ якщо } y_1=1;\ y_2=1 \end{cases} = \begin{cases} \begin{bmatrix}x_1\\x_2\oplus 1\end{bmatrix}, \text{ якщо } k_1=0;\ k_2=0 \\ \begin{bmatrix}x_2\\x_1\end{bmatrix}, \text{ якщо } k_1=0;\ k_2=1 \\ \begin{bmatrix}x_2\oplus 1\\x_1\oplus 1\end{bmatrix}, \text{ якщо } k_1=1;\ k_2=0 \\ \begin{bmatrix}x_1\oplus 1\\x_2\end{bmatrix}, \text{ якщо } k_1=1;\ k_2=1 \end{cases} = \begin{bmatrix} x_1\cdot(\overline{k_1\oplus k_2})\oplus x_2\cdot(k_1\oplus k_2)\oplus k_1 \\ x_1\cdot(k_1\oplus k_2)\oplus x_2\cdot(\overline{k_1\oplus k_2})\oplus k_2\oplus 1 \end{bmatrix};$$

$$O_{13,22,4,7}=\begin{cases} F_{13}\begin{pmatrix}x_1\\x_2\end{pmatrix}, \text{ якщо } y_1=0;\ y_2=0 \\ F_{22}\begin{pmatrix}x_1\\x_2\end{pmatrix}, \text{ якщо } y_1=0;\ y_2=1 \\ F_4\begin{pmatrix}x_1\\x_2\end{pmatrix}, \text{ якщо } y_1=1;\ y_2=0 \\ F_7\begin{pmatrix}x_1\\x_2\end{pmatrix}, \text{ якщо } y_1=1;\ y_2=1 \end{cases} = \begin{cases} \begin{bmatrix}x_1\oplus 1\\x_2\end{bmatrix}, \text{ якщо } k_1=0;\ k_2=0 \\ \begin{bmatrix}x_2\oplus 1\\x_1\oplus 1\end{bmatrix}, \text{ якщо } k_1=0;\ k_2=1 \\ \begin{bmatrix}x_2\\x_1\end{bmatrix}, \text{ якщо } k_1=1;\ k_2=0 \\ \begin{bmatrix}x_1\\x_2\oplus 1\end{bmatrix}, \text{ якщо } k_1=1;\ k_2=1 \end{cases} = \begin{bmatrix} x_1\cdot(\overline{k_1\oplus k_2})\oplus x_2\cdot(k_1\oplus k_2)\oplus k_1\oplus 1 \\ x_1\cdot(k_1\oplus k_2)\oplus x_2\cdot(\overline{k_1\oplus k_2})\oplus k_2 \end{bmatrix};$$

$$O_{22,7,13,4}=\begin{cases} F_{22}\begin{pmatrix}x_1\\x_2\end{pmatrix}, \text{ якщо } y_1=0;\ y_2=0 \\ F_7\begin{pmatrix}x_1\\x_2\end{pmatrix}, \text{ якщо } y_1=0;\ y_2=1 \\ F_{13}\begin{pmatrix}x_1\\x_2\end{pmatrix}, \text{ якщо } y_1=1;\ y_2=0 \\ F_4\begin{pmatrix}x_1\\x_2\end{pmatrix}, \text{ якщо } y_1=1;\ y_2=1 \end{cases} = \begin{cases} \begin{bmatrix}x_2\oplus 1\\x_1\oplus 1\end{bmatrix}, \text{ якщо } k_1=0;\ k_2=0 \\ \begin{bmatrix}x_1\\x_2\oplus 1\end{bmatrix}, \text{ якщо } k_1=0;\ k_2=1 \\ \begin{bmatrix}x_1\oplus 1\\x_2\end{bmatrix}, \text{ якщо } k_1=1;\ k_2=0 \\ \begin{bmatrix}x_2\\x_1\end{bmatrix}, \text{ якщо } k_1=1;\ k_2=1 \end{cases} = \begin{bmatrix} x_1\cdot(k_1\oplus k_2)\oplus x_2\cdot(\overline{k_1\oplus k_2})\oplus k_2\oplus 1 \\ x_1\cdot(\overline{k_1\oplus k_2})\oplus x_2\cdot(k_1\oplus k_2)\oplus k_1\oplus 1 \end{bmatrix};$$

$$O_{5,21,9,17}=\begin{cases} F_5\begin{pmatrix}x_1\\x_2\end{pmatrix}, \text{ якщо } y_1=0;\ y_2=0 \\ F_{21}\begin{pmatrix}x_1\\x_2\end{pmatrix}, \text{ якщо } y_1=0;\ y_2=1 \\ F_9\begin{pmatrix}x_1\\x_2\end{pmatrix}, \text{ якщо } y_1=1;\ y_2=0 \\ F_{17}\begin{pmatrix}x_1\\x_2\end{pmatrix}, \text{ якщо } y_1=1;\ y_2=1 \end{cases} = \begin{cases} \begin{bmatrix}x_2\\x_1\oplus x_2\end{bmatrix}, \text{ якщо } k_1=0;\ k_2=0 \\ \begin{bmatrix}x_1\oplus 1\\x_1\oplus x_2\oplus 1\end{bmatrix}, \text{ якщо } k_1=0;\ k_2=1 \\ \begin{bmatrix}x_1\\x_1\oplus x_2\oplus 1\end{bmatrix}, \text{ якщо } k_1=1;\ k_2=0 \\ \begin{bmatrix}x_2\oplus 1\\x_1\oplus x_2\end{bmatrix}, \text{ якщо } k_1=1;\ k_2=1 \end{cases} = \begin{bmatrix} x_1\cdot(k_1\oplus k_2)\oplus x_2\cdot(\overline{k_1\oplus k_2})\oplus k_2 \\ x_1\oplus x_2\oplus k_1\oplus k_2 \end{bmatrix};$$

$$O_{9,5,17,21}=\begin{cases} F_9\begin{pmatrix}x_1\\x_2\end{pmatrix}, \text{ якщо } y_1=0;\ y_2=0 \\ F_5\begin{pmatrix}x_1\\x_2\end{pmatrix}, \text{ якщо } y_1=0;\ y_2=1 \\ F_{17}\begin{pmatrix}x_1\\x_2\end{pmatrix}, \text{ якщо } y_1=1;\ y_2=0 \\ F_{21}\begin{pmatrix}x_1\\x_2\end{pmatrix}, \text{ якщо } y_1=1;\ y_2=1 \end{cases} = \begin{cases} \begin{bmatrix}x_1\\x_1\oplus x_2\oplus 1\end{bmatrix}, \text{ якщо } k_1=0;\ k_2=0 \\ \begin{bmatrix}x_2\\x_1\oplus x_2\end{bmatrix}, \text{ якщо } k_1=0;\ k_2=1 \\ \begin{bmatrix}x_2\oplus 1\\x_1\oplus x_2\end{bmatrix}, \text{ якщо } k_1=1;\ k_2=0 \\ \begin{bmatrix}x_1\oplus 1\\x_1\oplus x_2\oplus 1\end{bmatrix}, \text{ якщо } k_1=1;\ k_2=1 \end{cases} = \begin{bmatrix} x_1\cdot(\overline{k_1\oplus k_2})\oplus x_2\cdot(k_1\oplus k_2)\oplus k_1 \\ x_1\oplus x_2\oplus k_1\oplus k_2\oplus 1 \end{bmatrix};$$

$$O_{17,9,21,5}=\begin{cases} F_{17}\begin{pmatrix}x_1\\x_2\end{pmatrix}, \text{ якщо } y_1=0;\ y_2=0 \\ F_9\begin{pmatrix}x_1\\x_2\end{pmatrix}, \text{ якщо } y_1=0;\ y_2=1 \\ F_{21}\begin{pmatrix}x_1\\x_2\end{pmatrix}, \text{ якщо } y_1=1;\ y_2=0 \\ F_5\begin{pmatrix}x_1\\x_2\end{pmatrix}, \text{ якщо } y_1=1;\ y_2=1 \end{cases} = \begin{cases} \begin{bmatrix}x_2\oplus 1\\x_1\oplus x_2\end{bmatrix}, \text{ якщо } k_1=0;\ k_2=0 \\ \begin{bmatrix}x_1\\x_1\oplus x_2\oplus 1\end{bmatrix}, \text{ якщо } k_1=0;\ k_2=1 \\ \begin{bmatrix}x_1\oplus 1\\x_1\oplus x_2\oplus 1\end{bmatrix}, \text{ якщо } k_1=1;\ k_2=0 \\ \begin{bmatrix}x_2\\x_1\oplus x_2\end{bmatrix}, \text{ якщо } k_1=1;\ k_2=1 \end{cases} = \begin{bmatrix} x_1\cdot(k_1\oplus k_2)\oplus x_2\cdot(\overline{k_1\oplus k_2})\oplus k_2\oplus 1 \\ x_1\oplus x_2\oplus k_1\oplus k_2 \end{bmatrix};$$

$$O_{21,17,5,9}=\begin{cases} F_{21}\begin{pmatrix}x_1\\x_2\end{pmatrix}, \text{ якщо } y_1=0;\ y_2=0 \\ F_{17}\begin{pmatrix}x_1\\x_2\end{pmatrix}, \text{ якщо } y_1=0;\ y_2=1 \\ F_5\begin{pmatrix}x_1\\x_2\end{pmatrix}, \text{ якщо } y_1=1;\ y_2=0 \\ F_9\begin{pmatrix}x_1\\x_2\end{pmatrix}, \text{ якщо } y_1=1;\ y_2=1 \end{cases} = \begin{cases} \begin{bmatrix}x_1\oplus 1\\x_1\oplus x_2\oplus 1\end{bmatrix}, \text{ якщо } k_1=0;\ k_2=0 \\ \begin{bmatrix}x_2\oplus 1\\x_1\oplus x_2\end{bmatrix}, \text{ якщо } k_1=0;\ k_2=1 \\ \begin{bmatrix}x_2\\x_1\oplus x_2\end{bmatrix}, \text{ якщо } k_1=1;\ k_2=0 \\ \begin{bmatrix}x_1\\x_1\oplus x_2\oplus 1\end{bmatrix}, \text{ якщо } k_1=1;\ k_2=1 \end{cases} = \begin{bmatrix} x_1\cdot(\overline{k_1\oplus k_2})\oplus x_2\cdot(k_1\oplus k_2)\oplus k_1\oplus 1 \\ x_1\oplus x_2\oplus k_1\oplus k_2\oplus 1 \end{bmatrix};$$

$$O_{6,14,20,12}=\begin{cases} F_6\begin{pmatrix}x_1\\x_2\end{pmatrix}, \text{ якщо } y_1=0;\ y_2=0 \\ F_{14}\begin{pmatrix}x_1\\x_2\end{pmatrix}, \text{ якщо } y_1=0;\ y_2=1 \\ F_{20}\begin{pmatrix}x_1\\x_2\end{pmatrix}, \text{ якщо } y_1=1;\ y_2=0 \\ F_{12}\begin{pmatrix}x_1\\x_2\end{pmatrix}, \text{ якщо } y_1=1;\ y_2=1 \end{cases} = \begin{cases} \begin{bmatrix}x_1\oplus x_2\\x_1\end{bmatrix}, \text{ якщо } k_1=0;\ k_2=0 \\ \begin{bmatrix}x_1\oplus x_2\oplus 1\\x_2\end{bmatrix}, \text{ якщо } k_1=0;\ k_2=1 \\ \begin{bmatrix}x_1\oplus x_2\oplus 1\\x_2\oplus 1\end{bmatrix}, \text{ якщо } k_1=1;\ k_2=0 \\ \begin{bmatrix}x_1\oplus x_2\\x_1\oplus 1\end{bmatrix}, \text{ якщо } k_1=1;\ k_2=1 \end{cases} = \begin{bmatrix} x_1\oplus x_2\oplus k_1\oplus k_2 \\ x_1\cdot(\overline{k_1\oplus k_2})\oplus x_2\cdot(k_1\oplus k_2)\oplus k_1 \end{bmatrix};$$

$$O_{12,20,14,6}=\begin{cases} F_{12}\begin{pmatrix}x_1\\x_2\end{pmatrix}, \text{ якщо } y_1=0;\ y_2=0 \\ F_{20}\begin{pmatrix}x_1\\x_2\end{pmatrix}, \text{ якщо } y_1=0;\ y_2=1 \\ F_{14}\begin{pmatrix}x_1\\x_2\end{pmatrix}, \text{ якщо } y_1=1;\ y_2=0 \\ F_6\begin{pmatrix}x_1\\x_2\end{pmatrix}, \text{ якщо } y_1=1;\ y_2=1 \end{cases} = \begin{cases} \begin{bmatrix}x_1\oplus x_2\\x_1\oplus 1\end{bmatrix}, \text{ якщо } k_1=0;\ k_2=0 \\ \begin{bmatrix}x_1\oplus x_2\oplus 1\\x_2\oplus 1\end{bmatrix}, \text{ якщо } k_1=0;\ k_2=1 \\ \begin{bmatrix}x_1\oplus x_2\oplus 1\\x_2\end{bmatrix}, \text{ якщо } k_1=1;\ k_2=0 \\ \begin{bmatrix}x_1\oplus x_2\\x_1\end{bmatrix}, \text{ якщо } k_1=1;\ k_2=1 \end{cases} = \begin{bmatrix} x_1\oplus x_2\oplus k_1\oplus k_2 \\ x_1\cdot(\overline{k_1\oplus k_2})\oplus x_2\cdot(k_1\oplus k_2)\oplus k_1\oplus 1 \end{bmatrix};$$

$$O_{14,12,6,20}=\begin{cases} F_{14}\begin{pmatrix}x_1\\x_2\end{pmatrix}, \text{ якщо } y_1=0;\ y_2=0 \\ F_{12}\begin{pmatrix}x_1\\x_2\end{pmatrix}, \text{ якщо } y_1=0;\ y_2=1 \\ F_{6}\begin{pmatrix}x_1\\x_2\end{pmatrix}, \text{ якщо } y_1=1;\ y_2=0 \\ F_{20}\begin{pmatrix}x_1\\x_2\end{pmatrix}, \text{ якщо } y_1=1;\ y_2=1 \end{cases} = \begin{cases} \begin{bmatrix}x_1\oplus x_2\oplus 1\\ x_2\end{bmatrix}, \text{ якщо } k_1=0;\ k_2=0 \\ \begin{bmatrix}x_1\oplus x_2\\ x_1\oplus 1\end{bmatrix}, \text{ якщо } k_1=0;\ k_2=1 \\ \begin{bmatrix}x_1\oplus x_2\\ x_1\end{bmatrix}, \text{ якщо } k_1=1;\ k_2=0 \\ \begin{bmatrix}x_1\oplus x_2\oplus 1\\ x_2\oplus 1\end{bmatrix}, \text{ якщо } k_1=1;\ k_2=1 \end{cases} = \begin{bmatrix}x_1\oplus x_2\oplus k_1\oplus k_2\oplus 1\\ x_1\cdot(k_1\oplus k_2)\oplus x_2\cdot\overline{(k_1\oplus k_2)}\oplus k_2\end{bmatrix};$$

$$O_{20,6,12,14}=\begin{cases} F_{20}\begin{pmatrix}x_1\\x_2\end{pmatrix}, \text{ якщо } y_1=0;\ y_2=0 \\ F_{6}\begin{pmatrix}x_1\\x_2\end{pmatrix}, \text{ якщо } y_1=0;\ y_2=1 \\ F_{12}\begin{pmatrix}x_1\\x_2\end{pmatrix}, \text{ якщо } y_1=1;\ y_2=0 \\ F_{14}\begin{pmatrix}x_1\\x_2\end{pmatrix}, \text{ якщо } y_1=1;\ y_2=1 \end{cases} = \begin{cases} \begin{bmatrix}x_1\oplus x_2\oplus 1\\ x_2\oplus 1\end{bmatrix}, \text{ якщо } k_1=0;\ k_2=0 \\ \begin{bmatrix}x_1\oplus x_2\\ x_1\end{bmatrix}, \text{ якщо } k_1=0;\ k_2=1 \\ \begin{bmatrix}x_1\oplus x_2\\ x_1\oplus 1\end{bmatrix}, \text{ якщо } k_1=1;\ k_2=0 \\ \begin{bmatrix}x_1\oplus x_2\oplus 1\\ x_2\end{bmatrix}, \text{ якщо } k_1=1;\ k_2=1 \end{cases} = \begin{bmatrix}x_1\oplus x_2\oplus k_1\oplus k_2\oplus 1\\ x_1\cdot(k_1\oplus k_2)\oplus x_2\cdot\overline{(k_1\oplus k_2)}\oplus k_2\oplus 1\end{bmatrix}.$$

У табл. 3.3 наведено таблицю істинності першої побудованої операції $O_{1,10,16,19}$ ($O_1^{4\oplus}$) та узагальненої операції четвертої групи з точністю до перестановки ($O_i^{4\oplus}$).

Одним із шляхів підтвердження правильності запропонованої гіпотези стосовно можливості синтезу груп симетричних операцій служить перевірка її коректності на повній множині груп операцій. Для цього перевіримо останню групу моделей операцій, яка ще не перевірялася. Синтез операцій будемо проводити на основі операції $O_1^{4\oplus}$, яка входить до цієї групи.

Таблиця 3.3

**Таблиця істинності операцій $O_1^{4\oplus}$ и $O_i^{4\oplus}$**

| **Операція** | $O_1^{4\oplus}$ | | | | $O_i^{4\oplus}$ | | | |
|---|---|---|---|---|---|---|---|---|
| **Значення операндів** | **00** | **01** | **10** | **11** | **00** | **01** | **10** | **11** |
| **00** | **00** | **01** | **10** | **11** | **a** | **b** | **c** | **d** |
| **01** | **01** | **11** | **00** | **10** | **b** | **d** | **a** | **c** |
| **10** | **10** | **00** | **11** | **01** | **c** | **a** | **d** | **b** |
| **11** | **11** | **10** | **01** | **00** | **d** | **c** | **b** | **a** |
| $a \neq b \neq c \neq d \in \{00; 01; 10; 11\}$, $i \in \{1; 2; ...; 24\}$ | | | | | | | | |

Введемо підстановку в операцію $O_1^{4\oplus}$:

$$O_1^{4\oplus} = \begin{bmatrix} x_1 \cdot (\overline{k_1 \oplus k_2}) \oplus x_2 \cdot (k_1 \oplus k_2) \oplus k_1 \\ x_1 \cdot (k_1 \oplus k_2) \oplus x_2 \cdot (\overline{k_1 \oplus k_2}) \oplus k_2 \end{bmatrix} = \begin{bmatrix} y_1 \\ y_2 \end{bmatrix};$$

$$y_1 = x_1 \cdot (\overline{k_1 \oplus k_2}) \oplus x_2 \cdot (k_1 \oplus k_2) \oplus k_1; \qquad y_2 = x_1 \cdot (k_1 \oplus k_2) \oplus x_2 \cdot (\overline{k_1 \oplus k_2}) \oplus k_2.$$

Синтезуємо першу двохоперандну операцію базової групи на основі першої одноопераднної операції базової групи:

$$F_1(O_1^{4\oplus}) = \begin{bmatrix} y_1 \\ y_2 \end{bmatrix} = \begin{bmatrix} x_1 \cdot (\overline{k_1 \oplus k_2}) \oplus x_2 \cdot (k_1 \oplus k_2) \oplus k_1 \\ x_1 \cdot (k_1 \oplus k_2) \oplus x_2 \cdot (\overline{k_1 \oplus k_2}) \oplus k_2 \end{bmatrix} = O_1^{4\oplus} = O_{1,10,16,19}.$$

Синтезуємо другу двохоперандну операцію базової групи на основі другої одноопераднної операції базової групи:

$$F_2(O_1^{4\oplus}) = \begin{bmatrix} y_1 \oplus y_2 \\ y_2 \end{bmatrix} = \begin{bmatrix} x_1 \oplus x_2 \oplus k_1 \oplus k_2) \\ x_1 \cdot (k_1 \oplus k_2) \oplus x_2 \cdot (\overline{k_1 \oplus k_2}) \oplus k_2 \end{bmatrix} = O_2^{4\oplus} = O_{2,24,18,8}.$$

Синтезуємо третю двохоперандну операцію базової групи на основі третьої одноопераднної операції базової групи:

$$F_3(O_1^{4\oplus}) = \begin{bmatrix} y_1 \\ y_1 \oplus y_2 \end{bmatrix} = \begin{bmatrix} x_1 \cdot (\overline{k_1 \oplus k_2}) \oplus x_2 \cdot (k_1 \oplus k_2) \oplus k_1 \\ x_1 \oplus x_2 \oplus k_1 \oplus k_2 \end{bmatrix} = O_3^{4\oplus} = O_{3,11,23,15}.$$

Синтезуємо операції перестановки, виконавши над $O_1^{4\oplus}$ одноопераднні операції $F_4$ – $F_6$:

$$F_4(O_1^{4\oplus}) = \begin{bmatrix} y_2 \\ y_1 \end{bmatrix} = \begin{bmatrix} x_1 \cdot (k_1 \oplus k_2) \oplus x_2 \cdot (\overline{k_1 \oplus k_2}) \oplus k_2 \\ x_1 \cdot (\overline{k_1 \oplus k_2}) \oplus x_2 \cdot (k_1 \oplus k_2) \oplus k_1 \end{bmatrix} = O_4^{4\oplus} = O_{4,13,7,22};$$

$$F_5(O_1^{4\oplus}) = \begin{bmatrix} y_2 \\ y_1 \oplus y_2 \end{bmatrix} = \begin{bmatrix} x_1 \cdot (k_1 \oplus k_2) \oplus x_2 \cdot (\overline{k_1 \oplus k_2}) \oplus k_2 \\ x_1 \oplus x_2 \oplus k_1 \oplus k_2 \end{bmatrix} = O_5^{4\oplus} = O_{5,21,9,17};$$

$$F_6(O_1^{4\oplus}) = \begin{bmatrix} y_1 \oplus y_2 \\ y_1 \end{bmatrix} = \begin{bmatrix} x_1 \oplus x_2 \oplus k_1 \oplus k_2 \\ x_1 \cdot (\overline{k_1 \oplus k_2}) \oplus x_2 \cdot (k_1 \oplus k_2) \oplus k_1 \end{bmatrix} = O_6^{4\oplus} = O_{6,14,20,12}\,.$$

Синтезуємо операції инверсії, виконавши над $O_1^{4\oplus}$ однооперандні операції $F_7$ – $F_{24}$:

$$F_7(O_1^{4\oplus}) = \begin{bmatrix} y_1 \\ y_2 \oplus 1 \end{bmatrix} = \begin{bmatrix} x_1 \cdot (\overline{k_1 \oplus k_2}) \oplus x_2 \cdot (k_1 \oplus k_2) \oplus k_1 \\ x_1 \cdot (k_1 \oplus k_2) \oplus x_2 \cdot (\overline{k_1 \oplus k_2}) \oplus k_2 \oplus 1 \end{bmatrix} = O_7^{4\oplus} = O_{7,4,22,13};$$

$$F_8(O_1^{4\oplus}) = \begin{bmatrix} y_1 \oplus y_2 \\ y_2 \oplus 1 \end{bmatrix} = \begin{bmatrix} x_1 \oplus x_2 \oplus k_1 \oplus k_2 \\ x_1 \cdot (k_1 \oplus k_2) \oplus x_2 \cdot (\overline{k_1 \oplus k_2}) \oplus k_2 \oplus 1 \end{bmatrix} = O_8^{4\oplus} = O_{8,18,24,2};$$

$$F_9(O_1^{4\oplus}) = \begin{bmatrix} y_1 \\ y_1 \oplus y_2 \oplus 1 \end{bmatrix} = \begin{bmatrix} x_1 \cdot (\overline{k_1 \oplus k_2}) \oplus x_2 \cdot (k_1 \oplus k_2) \oplus k_1 \\ x_1 \oplus x_2 \oplus k_1 \oplus k_2 \oplus 1 \end{bmatrix} = O_9^{4\oplus} = O_{9,5,17,21};$$

$$F_{10}(O_1^{4\oplus}) = \begin{bmatrix} y_2 \\ y_1 \oplus 1 \end{bmatrix} = \begin{bmatrix} x_1 \cdot (k_1 \oplus k_2) \oplus x_2 \cdot (\overline{k_1 \oplus k_2}) \oplus k_2 \\ x_1 \cdot (\overline{k_1 \oplus k_2}) \oplus x_2 \cdot (k_1 \oplus k_2) \oplus k_1 \oplus 1 \end{bmatrix} = O_{10}^{4\oplus} = O_{10,19,1,16};$$

$$F_{11}(O_1^{4\oplus}) = \begin{bmatrix} y_2 \\ y_1 \oplus y_2 \oplus 1 \end{bmatrix} = \begin{bmatrix} x_1 \cdot (k_1 \oplus k_2) \oplus x_2 \cdot (\overline{k_1 \oplus k_2}) \oplus k_2 \\ x_1 \oplus x_2 \oplus k_1 \oplus k_2 \oplus 1 \end{bmatrix} = O_{11}^{4\oplus} = O_{11,15,3,23};$$

$$F_{12}(O_1^{4\oplus}) = \begin{bmatrix} y_1 \oplus y_2 \\ y_1 \oplus 1 \end{bmatrix} = \begin{bmatrix} x_1 \oplus x_2 \oplus k_1 \oplus k_2 \\ x_1 \cdot (\overline{k_1 \oplus k_2}) \oplus x_2 \cdot (k_1 \oplus k_2) \oplus k_1 \oplus 1 \end{bmatrix} = O_{12}^{4\oplus} = O_{12,20,14,6};$$

$$F_{13}(O_1^{4\oplus}) = \begin{bmatrix} y_1 \oplus 1 \\ y_2 \end{bmatrix} = \begin{bmatrix} x_1 \cdot (\overline{k_1 \oplus k_2}) \oplus x_2 \cdot (k_1 \oplus k_2) \oplus k_1 \oplus 1 \\ x_1 \cdot (k_1 \oplus k_2) \oplus x_2 \cdot (\overline{k_1 \oplus k_2}) \oplus k_2 \end{bmatrix} = O_{13}^{4\oplus} = O_{13,22,4,7};$$

$$F_{14}(O_1^{4\oplus}) = \begin{bmatrix} y_1 \oplus y_2 \oplus 1 \\ y_2 \end{bmatrix} = \begin{bmatrix} x_1 \oplus x_2 \oplus k_1 \oplus k_2 \oplus 1 \\ x_1 \cdot (k_1 \oplus k_2) \oplus x_2 \cdot (\overline{k_1 \oplus k_2}) \oplus k_2 \end{bmatrix} = O_{14}^{4\oplus} = O_{14,12,6,20};$$

$$F_{15}(O_1^{4\oplus})=\begin{bmatrix} y_1\oplus 1 \\ y_1\oplus y_2 \end{bmatrix}=\begin{bmatrix} x_1\cdot(\overline{k_1\oplus k_2})\oplus x_2\cdot(k_1\oplus k_2)\oplus k_1\oplus 1 \\ x_1\oplus x_2\oplus k_1\oplus k_2 \end{bmatrix}=O_{15}^{4\oplus}=O_{15,23,11,3};$$

$$F_{16}(O_1^{4\oplus})=\begin{bmatrix} y_2\oplus 1 \\ y_1 \end{bmatrix}=\begin{bmatrix} x_1\cdot(k_1\oplus k_2)\oplus x_2\cdot(\overline{k_1\oplus k_2})\oplus k_2\oplus 1 \\ x_1\cdot(\overline{k_1\oplus k_2})\oplus x_2\cdot(k_1\oplus k_2)\oplus k_1 \end{bmatrix}=O_{16}^{4\oplus}=O_{16,1,19,10};$$

$$F_{17}(O_1^{4\oplus})=\begin{bmatrix} y_2\oplus 1 \\ y_1\oplus y_2 \end{bmatrix}=\begin{bmatrix} x_1\cdot(k_1\oplus k_2)\oplus x_2\cdot(\overline{k_1\oplus k_2})\oplus k_2\oplus 1 \\ x_1\oplus x_2\oplus k_1\oplus k_2 \end{bmatrix}=O_{17}^{4\oplus}=O_{17,9,21,5};$$

$$F_{18}(O_1^{4\oplus})=\begin{bmatrix} y_1\oplus y_2\oplus 1 \\ y_1 \end{bmatrix}=\begin{bmatrix} x_1\oplus x_2\oplus k_1\oplus k_2\oplus 1 \\ x_1\cdot(\overline{k_1\oplus k_2})\oplus x_2\cdot(k_1\oplus k_2)\oplus k_1 \end{bmatrix}=O_{18}^{4\oplus}=O_{18,2,8,24};$$

$$F_{19}(O_1^{4\oplus})=\begin{bmatrix} y_1\oplus 1 \\ y_2\oplus 1 \end{bmatrix}=\begin{bmatrix} x_1\cdot(\overline{k_1\oplus k_2})\oplus x_2\cdot(k_1\oplus k_2)\oplus k_1\oplus 1 \\ x_1\cdot(k_1\oplus k_2)\oplus x_2\cdot(\overline{k_1\oplus k_2})\oplus k_2\oplus 1 \end{bmatrix}=O_{19}^{4\oplus}=O_{19,16,10,1};$$

$$F_{20}(O_1^{4\oplus})=\begin{bmatrix} y_1\oplus y_2\oplus 1 \\ y_2\oplus 1 \end{bmatrix}=\begin{bmatrix} x_1\oplus x_2\oplus k_1\oplus k_2\oplus 1 \\ x_1\cdot(k_1\oplus k_2)\oplus x_2\cdot(\overline{k_1\oplus k_2})\oplus k_2\oplus 1 \end{bmatrix}=O_{20}^{4\oplus}=O_{20,6,12,14};$$

$$F_{21}(O_1^{4\oplus})=\begin{bmatrix} y_1\oplus 1 \\ y_1\oplus y_2\oplus 1 \end{bmatrix}=\begin{bmatrix} x_1\cdot(\overline{k_1\oplus k_2})\oplus x_2\cdot(k_1\oplus k_2)\oplus k_1\oplus 1 \\ x_1\oplus x_2\oplus k_1\oplus k_2\oplus 1 \end{bmatrix}=O_{21}^{4\oplus}=O_{21,17,5,9};$$

$$F_{22}(O_1^{4\oplus})=\begin{bmatrix} y_2\oplus 1 \\ y_1\oplus 1 \end{bmatrix}=\begin{bmatrix} x_1\cdot(k_1\oplus k_2)\oplus x_2\cdot(\overline{k_1\oplus k_2})\oplus k_2\oplus 1 \\ x_1\cdot(\overline{k_1\oplus k_2})\oplus x_2\cdot(k_1\oplus k_2)\oplus k_1\oplus 1 \end{bmatrix}=O_{22}^{4\oplus}=O_{22,7,13,4};$$

$$F_{23}(O_1^{4\oplus})=\begin{bmatrix} y_2\oplus 1 \\ y_1\oplus y_2\oplus 1 \end{bmatrix}=\begin{bmatrix} x_1\cdot(k_1\oplus k_2)\oplus x_2\cdot(\overline{k_1\oplus k_2})\oplus k_2\oplus 1 \\ x_1\oplus x_2\oplus k_1\oplus k_2\oplus 1 \end{bmatrix}=O_{23}^{4\oplus}=O_{23,3,15,11};$$

$$F_{24}(O_1^{4\oplus})=\begin{bmatrix} y_1\oplus y_2\oplus 1 \\ y_1\oplus 1 \end{bmatrix}=\begin{bmatrix} x_1\oplus x_2\oplus k_1\oplus k_2\oplus 1 \\ x_1\cdot(\overline{k_1\oplus k_2})\oplus x_2\cdot(k_1\oplus k_2)\oplus k_1\oplus 1 \end{bmatrix}=O_{24}^{4\oplus}=O_{24,8,2,18}.$$

Отримані в процесі синтезу результати повністю співпали з формалізованими результатами обчислювального експерименту. Класифікацію отриманих моделей операцій четвертої групи наведено в табл. 3.4 [6].

Таблиця 3.4

**Двохрозрядні двохоперандні операції криптографічного кодування, синтезовані на основі операції $O_1^{4\oplus}$**

| **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** | $F_4=\begin{bmatrix}x_2\\x_1\end{bmatrix}$ | $O_4^{4\oplus}=\begin{bmatrix}x_1\cdot(k_1\oplus k_2)\oplus x_2\cdot(\overline{k_1\oplus k_2})\oplus k_2\\x_1\cdot(\overline{k_1\oplus k_2})\oplus x_2\cdot(k_1\oplus k_2)\oplus k_1\end{bmatrix}$ | $O_{10}^{4\oplus}=\begin{bmatrix}x_1\cdot(k_1\oplus k_2)\oplus x_2\cdot(\overline{k_1\oplus k_2})\oplus k_2\\x_1\cdot(\overline{k_1\oplus k_2})\oplus x_2\cdot(k_1\oplus k_2)\oplus k_1\oplus 1\end{bmatrix}$ |
| | | $O_{16}^{4\oplus}=\begin{bmatrix}x_1\cdot(k_1\oplus k_2)\oplus x_2\cdot(\overline{k_1\oplus k_2})\oplus k_2\oplus 1\\x_1\cdot(\overline{k_1\oplus k_2})\oplus x_2\cdot(k_1\oplus k_2)\oplus k_1\end{bmatrix}$ | $O_{22}^{4\oplus}=\begin{bmatrix}x_1\cdot(k_1\oplus k_2)\oplus x_2\cdot(\overline{k_1\oplus k_2})\oplus k_2\oplus 1\\x_1\cdot(\overline{k_1\oplus k_2})\oplus x_2\cdot(k_1\oplus k_2)\oplus k_1\oplus 1\end{bmatrix}$ |
| | $F_5=\begin{bmatrix}x_2\\x_1\oplus x_2\end{bmatrix}$ | $O_5^{4\oplus}=\begin{bmatrix}x_1\cdot(k_1\oplus k_2)\oplus x_2\cdot(\overline{k_1\oplus k_2})\oplus k_2\\x_1\oplus x_2\oplus k_1\oplus k_2\end{bmatrix}$ | $O_{11}^{4\oplus}=\begin{bmatrix}x_1\cdot(k_1\oplus k_2)\oplus x_2\cdot(\overline{k_1\oplus k_2})\oplus k_2\\x_1\oplus x_2\oplus k_1\oplus k_2\oplus 1\end{bmatrix}$ |
| | | $O_{17}^{4\oplus}=\begin{bmatrix}x_1\cdot(k_1\oplus k_2)\oplus x_2\cdot(\overline{k_1\oplus k_2})\oplus k_2\oplus 1\\x_1\oplus x_2\oplus k_1\oplus k_2\end{bmatrix}$ | $O_{23}^{4\oplus}=\begin{bmatrix}x_1\cdot(k_1\oplus k_2)\oplus x_2\cdot(\overline{k_1\oplus k_2})\oplus k_2\oplus 1\\x_1\oplus x_2\oplus k_1\oplus k_2\oplus 1\end{bmatrix}$ |
| | $F_6=\begin{bmatrix}x_1\oplus x_2\\x_1\end{bmatrix}$ | $O_6^{4\oplus}=\begin{bmatrix}x_1\oplus x_2\oplus k_1\oplus k_2\\x_1\cdot(\overline{k_1\oplus k_2})\oplus x_2\cdot(k_1\oplus k_2)\oplus k_1\end{bmatrix}$ | $O_{12}^{4\oplus}=\begin{bmatrix}x_1\oplus x_2\oplus k_1\oplus k_2\\x_1\cdot(\overline{k_1\oplus k_2})\oplus x_2\cdot(k_1\oplus k_2)\oplus k_1\oplus 1\end{bmatrix}$ |
| | | $O_{18}^{4\oplus}=\begin{bmatrix}x_1\oplus x_2\oplus k_1\oplus k_2\oplus 1\\x_1\cdot(\overline{k_1\oplus k_2})\oplus x_2\cdot(k_1\oplus k_2)\oplus k_1\end{bmatrix}$ | $O_{24}^{4\oplus}=\begin{bmatrix}x_1\oplus x_2\oplus k_1\oplus k_2\oplus 1\\x_1\cdot(\overline{k_1\oplus k_2})\oplus x_2\cdot(k_1\oplus k_2)\oplus k_1\oplus 1\end{bmatrix}$ |

Результати синтезу відомих груп симетричних двохрозрядних двохоперандних модифікованих операцій та вперше отриманих груп симетричних двохрозрядних двохоперандних модифікованих операцій підтвердили коректність запропонованої концепції синтезу симетричних двохоперандних операцій. При цьому слід відзначити, що запропонована концепція виключає необхідність прийняття компромісного рішення при поділі двохоперандної операції, на основі якої проводиться синтез на підопераціі.

Отримані результати дозволяють перейти до формалізації процесу синтезу та розробки методу синтезу симетричних двохоперандних операцій криптографічного кодування інформації для блокового шифрування

## 3.4 Метод синтезу симетричних двохоперандних операцій криптографічного кодування інформації для блокового шифрування

Отримані в розділі результати дослідження процесів синтезу вже відомих двох груп симетричних двохрозрядних двохоперандних операцій криптографічного кодування та вперше синтезованих двох груп симетричних двохрозрядних двохоперандних операцій криптографічного кодування дозволяють вдосконалити метод синтезу раніше відомих двох груп операцій [105]. Відомий метод синтезу базувався на поділі операції криптоперетворення на дві підопераціі обробки першого і другого операндів та перетворенні однаковими одноопераднимиопераціями двохоперандних операцій. У формалізованому представленні цей процес синтезу полягає в наступному.

Якщо

$$O\begin{pmatrix} x_1, k_1 \\ x_2, k_2 \end{pmatrix} = \begin{bmatrix} f_1(x_1, x_2, k_1, k_2) \\ f_2(x_1, x_2, k_1, k_2) \end{bmatrix} = \begin{bmatrix} f_1^*(x_1, x_2) \\ f_2^*(x_1, x_2) \end{bmatrix} \oplus \begin{bmatrix} f_1^*(k_1, k_2) \\ f_2^*(k_1, k_2) \end{bmatrix} = O\begin{pmatrix} x_1 \\ x_2 \end{pmatrix} \oplus O\begin{pmatrix} k_1 \\ k_2 \end{pmatrix},$$

то $O_i\begin{pmatrix} x_1, k_1 \\ x_2, k_2 \end{pmatrix} = F_i(O\begin{pmatrix} x_1 \\ x_2 \end{pmatrix}) \oplus F_i(O\begin{pmatrix} k_1 \\ k_2 \end{pmatrix})$.

Запропонована концепція, на основі якої в цьому розділі синтезовано всі чотири групи симетричних операцій, полягає в наступному.

Якщо $O\begin{pmatrix} x_1, k_1 \\ x_2, k_2 \end{pmatrix} = \begin{bmatrix} f_1(x_1, x_2, k_1, k_2) \\ f_2(x_1, x_2, k_1, k_2) \end{bmatrix} = \begin{bmatrix} y_1 \\ y_2 \end{bmatrix}$, де $y_1 = f_1(x_1, x_2, k_1, k_2)$,

$y_2 = f_2(x_1, x_2, k_1, k_2)$, то $O_i\begin{pmatrix} x_1, k_1 \\ x_2, k_2 \end{pmatrix} = F_i(O\begin{pmatrix} y_1 \\ y_2 \end{pmatrix})$.

Виходячи з цього, алгоритм удосконаленого методу синтезу симетричних двохрозрядних двохоперандних операцій криптографічного кодування інформації для блокового шифрування полягає в наступному:

- визначається (вибирається) симетрична двохрозрядна двохоперандна операція криптографічного кодування інформації, на основі якої буде синтезуватися група операцій;
- на основі вибраної операції визначаються підстановки змінних, якщо $O\begin{pmatrix} x_1, k_1 \\ x_2, k_2 \end{pmatrix} = \begin{bmatrix} f_1(x_1, x_2, k_1, k_2) \\ f_2(x_1, x_2, k_1, k_2) \end{bmatrix} = \begin{bmatrix} y_1 \\ y_2 \end{bmatrix}$, то $y_1 = f_1(x_1, x_2, k_1, k_2)$, $y_2 = f_2(x_1, x_2, k_1, k_2)$;
- на основі симетричних двохрозрядних одноопераднних операцій базової групи ($F_1$ – $F_3$), виконавши перетворення $O_i\begin{pmatrix} x_1, k_1 \\ x_2, k_2 \end{pmatrix} = F_i(O\begin{pmatrix} y_1 \\ y_2 \end{pmatrix})$, де $i \in \{1; 2; 3\}$, синтезуємо двохрозрядні двохоперандні операції базової групи;
- синтезувати додатково групу симетричних двохрозрядних двохоперандних операцій перестановки можна шляхом перестановки елементарних функцій в двохрозрядних двохоперандних операціях базової групи;

- синтезувати додатково групу симетричних двохрозрядних двохоперандних операцій інверсії можна шляхом перебору варіантів інверсії елементарних функцій операцій базової групи та операцій перестановки.

Синтезувати групу симетричних двохрозрядних двохоперандних операцій криптографічного кодування можна шляхом виконання над вибраною операцією всієї групи одноопераднних операцій (24 операції), проте при необхідності синтезувати всю групу операцій другий варіант методу буде складніше реалізувати за необхідності виконання значно більшої кількості перетворень моделей операцій.

Запропонована концепція дозволяє синтезувати групи симетричних двохоперандних операцій з довільною розрядністю. Для цього в запропоновану концепцію необхідно внести узагальнюючі зміни, які полягають в наступному.

$$\text{Якщо } O\begin{pmatrix} x_1, k_1 \\ x_2, k_2 \\ \cdot\ \cdot\ \cdot \\ x_n, k_n \end{pmatrix} = \begin{bmatrix} f_1\ (x_1, x_2, .., x_n, k_1, k_2, .., k_n) \\ f_2\ (x_1, x_2, .., x_n, k_1, k_2, .., k_n) \\ \cdot\ \cdot\ \cdot\ \cdot \\ f_n\ (x_1, x_2, .., x_n, k_1, k_2, .., k_n) \end{bmatrix} = \begin{bmatrix} y_1 \\ y_2 \\ \cdots \\ y_n \end{bmatrix},$$

де $y_1 = f_1(x_1, x_2, .., x_n, k_1, k_2, .., k_n)$, $y_2 = f_2(x_1, x_2, .., x_n, k_1, k_2, .., k_n)$, …. , $y_n = f_n(x_1, x_2, .., x_n, k_1, k_2, .., k_n)$,

$$\text{то } O_i\begin{pmatrix} x_1, k_1 \\ x_2, k_2 \\ \cdot\ \cdot\ \cdot \\ x_n, k_n \end{pmatrix} = F_i(O\begin{pmatrix} y_1 \\ y_2 \\ \cdots \\ y_n \end{pmatrix}).$$

Виходячи з вдосконаленої концепції, алгоритм реалізації методу синтезу симетричних двохоперандних операцій криптографічного кодування інформації для блокового шифрування, який не був відомий раніше, можна представити наступним чином:

1) виходячи з задач проектування, визначається розрядність двохоперандних операцій ($n$), які необхідно синтезувати;

2) визначається (вибирається) симетрична двохоперандна операція криптографічного кодування заданої розрядності, на основі якої буде синтезуватися група операцій;
3) на основі вибраної операції визначаються підстановки змінних;
4) якщо $O\begin{pmatrix} x_1, k_1 \\ x_2, k_2 \\ \dots \\ x_n, k_n \end{pmatrix} = \begin{bmatrix} f_1(x_1, x_2, .., x_n, k_1, k_2, .., k_n) \\ f_2(x_1, x_2, .., x_n, k_1, k_2, .., k_n) \\ \dots \\ f_n(x_1, x_2, .., x_n, k_1, k_2, .., k_n) \end{bmatrix} = \begin{bmatrix} y_1 \\ y_2 \\ \dots \\ y_n \end{bmatrix}$, то

$y_1 = f_1(x_1, x_2, .., x_n, k_1, k_2, .., k_n)$, $y_2 = f_2(x_1, x_2, .., x_n, k_1, k_2, .., k_n)$, …. ,

$y_n = f_n(x_1, x_2, .., x_n, k_1, k_2, .., k_n)$;

5) на основі симетричних двохрозрядних одноопераднних операцій базової групи ( $F_1 - F_k$, $k$ – кількість одноопераднних операцій в базовій групі), виконавши перетворення $O_i\begin{pmatrix} x_1, k_1 \\ x_2, k_2 \\ \dots \\ x_n, k_n \end{pmatrix} = F_i(O\begin{pmatrix} y_1 \\ y_2 \\ \dots \\ y_n \end{pmatrix})$,

де $i \in \{1; 2; k\}$, синтезуємо двохрозрядні двохоперандні операції базової групи;
6) синтезувати додатково групу симетричних двохрозрядних двохоперандних операцій перестановки можна шляхом перестановки елементарних функцій в двохоперандних операціях базової групи. Кількість перестановок елементарних функцій в операції визначається як $n!$ [99];
7) синтезувати додатково групу симетричних двохрозрядних двохоперандних операцій інверсії можна шляхом перебору варіантів інверсії елементарних функцій операцій базової групи та операцій перестановки. Кількість варіантів інверсії елементарних функцій в операції визначається як $2^n$ [99].

Синтезувати групи симетричних двохоперандних операцій криптографічного кодування заданої розрядності можна шляхом виконання над вибраною операцією одноопераднних операцій такої самої заданої розрядності. Максимальна кількість синтезованих операцій буде визначатися як $k \cdot n! \cdot 2^n$ операцій.

На прикладі синтезу групи симетричних двохрозрядних двохоперандних операцій криптографічного кодування запропонований метод забезпечує можливість синтезу групи двохоперандних операцій (24 операції) на основі будь-якої операції з цієї групи.

Особливості реалізації запропонованого методу при розрядності операндів більше двох буде розглянуто в наступному розділі.

**Висновки до розділу 3**

Вперше розроблено метод синтезу груп моделей симетричних двохоперандних операцій криптографічного кодування для блокового шифрування на основі заданої симетричної двохоперандної операції шляхом виконання над нею одноопераднних операцій криптографічного перетворення за умови однакової розрядності, що забезпечує побудову моделей раніше не відомих симетричних двохоперандних операцій, які забезпечують можливість перестановки інформації між операндами, необхідної для розширення можливостей застосування в захищених інформаційних системах критичної інфраструктури при реалізації блокового шифрування:

1. На основі узагальнення методів та результатів синтезу груп симетричних модифікованих операцій порозрядного додавання за модулем два та лівостороннього додавання за модулем чотири запропоновано концепцію синтезу, яка дозволяє об’єднати методи синтезу груп симетричних двохрозрядних двохоперандних операцій, які досліджувалися.

2. Вперше синтезовано та класифіковано групу симетричних модифікованих операцій правостороннього додавання за модулем чотири, що

забезпечує збільшення варіативності криптоалгоритмів за рахунок застосування цієї групи операцій.

3. На основі запропонованої концепції синтезовано четверту групу симетричних модифікованих двохоперандних операцій, отриманих за результатами обчислювального експерименту, та підтверджено коректність отриманого результату.

4. Дослідивши результати синтезу відомих та вперше отриманих груп симетричних модифікованих двохоперандних операцій і можливості застосування запропонованої концепції синтезу, розроблено метод синтезу моделей симетричних двохоперандних операцій криптографічного кодування для блокового шифрування на основі заданої симетричної двохоперандної операції.

5. Результати розділу опубліковано в [1, 2, 6].

# РОЗДІЛ 4 ІНФОРМАЦІЙНА ТЕХНОЛОГІЯ МОДЕЛЮВАННЯ ТА ДОСЛІДЖЕННЯ СИМЕТРИЧНИХ ОПЕРАЦІЙ КРИПТОГРАФІЧНОГО КОДУВАННЯ ДЛЯ ЗАХИЩЕНИХ ІНФОРМАЦІЙНИХ СИСТЕМ КРИТИЧНОЇ ІНФРАСТРУКТУРИ

## 4.1 Реалізація методу синтезу моделей симетричних двохоперандних операцій криптографічного кодування на основі кортежів симетричних одноопераднних операцій для систем блокового шифрування

Розглянемо можливість синтезу симетричних трьохрозрядних двохоперандних операцій криптографічного кодування. Синтезувати симетричні трьохрозрядні двохоперандні операції криптографічного кодування будемо відповідно до методу синтезу моделей симетричних двохоперандних операцій криптографічного кодування на основі кортежів симетричних одноопераднних операцій [4, 5]. Алгоритм реалізації цього методу наведено в підрозділі 2.3.

Серед трьохрозрядних одноопераднних операцій найбільш дослідженими є матричні операції криптографічного кодування. При проведенні дослідження обмежимо вхідні дані лише базовою групою трьохрозрядних одноопераднних операцій криптографічного кодування [94], які наведено в табл. 4.1.

Відповідно до табл. 4.1 базова група включає 28 операцій, серед яких 12 операцій, а саме $F_1$, $F_2$, $F_3$, $F_4$, $F_5$, $F_6$, $F_7$, $F_8$, $F_9$, $F_{10}$, $F_{19}$ і $F_{24}$, є симетричними. Оскільки трьохрозрядна двохоперандна операція криптографічного кодування включає два операнди по три розряди, то вона буде будуватися з кортежів по 8 одноопераднних операцій. Це пов’язано з тим, що значення трьох розрядів псевдовипадкової послідовності, за відсутності надлишковості, забезпечують вибір однієї з 8 одноопераднних операцій перетворення інформації.

Таблиця 4.1

**Базова група трьохрозрядних одноопераднихматричних операцій криптографічного кодування**

| | | | |
|---|---|---|---|
| $F_1^k = F_1^d = \begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix}$ | $F_8^k = F_8^d = \begin{pmatrix} x_1 \oplus x_2 \oplus x_3 \\ x_2 \\ x_3 \end{pmatrix}$ | $F_{15}^k = \begin{pmatrix} x_1 \oplus x_2 \oplus x_3 \\ x_2 \oplus x_3 \\ x_3 \end{pmatrix}$<br>$F_{15}^d = \begin{pmatrix} x_1 \oplus x_2 \\ x_2 \oplus x_3 \\ x_3 \end{pmatrix}$ | $F_{22}^k = \begin{pmatrix} x_1 \oplus x_2 \\ x_2 \\ x_1 \oplus x_3 \end{pmatrix}$<br>$F_{22}^d = \begin{pmatrix} x_1 \oplus x_2 \\ x_2 \\ x_1 \oplus x_2 \oplus x_3 \end{pmatrix}$ |
| $F_2^k = F_2^d = \begin{pmatrix} x_1 \oplus x_2 \\ x_2 \\ x_3 \end{pmatrix}$ | $F_9^k = F_9^d = \begin{pmatrix} x_1 \\ x_1 \oplus x_2 \oplus x_3 \\ x_3 \end{pmatrix}$ | $F_{16}^k = \begin{pmatrix} x_1 \oplus x_2 \oplus x_3 \\ x_1 \oplus x_3 \\ x_3 \end{pmatrix}$<br>$F_{16}^d = \begin{pmatrix} x_2 \oplus x_3 \\ x_1 \oplus x_2 \\ x_3 \end{pmatrix}$ | $F_{23}^k = \begin{pmatrix} x_1 \oplus x_2 \\ x_2 \oplus x_3 \\ x_3 \end{pmatrix}$<br>$F_{23}^k = \begin{pmatrix} x_1 \oplus x_2 \oplus x_3 \\ x_2 \oplus x_3 \\ x_3 \end{pmatrix}$ |
| $F_3^k = F_3^d = \begin{pmatrix} x_1 \\ x_1 \oplus x_2 \\ x_3 \end{pmatrix}$ | $F_{10}^k = F_{10}^d = \begin{pmatrix} x_1 \\ x_2 \\ x_1 \oplus x_2 \oplus x_3 \end{pmatrix}$ | $F_{17}^k = \begin{pmatrix} x_1 \\ x_1 \oplus x_2 \\ x_2 \oplus x_3 \end{pmatrix}$<br>$F_{17}^d = \begin{pmatrix} x_1; \\ x_1 \oplus x_2 \\ x_1 \oplus x_2 \oplus x_3 \end{pmatrix}$ | $F_{24}^k = F_{24}^k = \begin{pmatrix} x_1 \oplus x_3 \\ x_2 \oplus x_3 \\ x_3 \end{pmatrix}$ |
| $F_4^k = F_4^d = \begin{pmatrix} x_1 \oplus x_3 \\ x_2 \\ x_3 \end{pmatrix}$ | $F_{11}^k = \begin{pmatrix} x_1 \\ x_1 \oplus x_2 \\ x_1 \oplus x_2 \oplus x_3 \end{pmatrix}$<br>$F_{11}^d = \begin{pmatrix} x_1 \\ x_1 \oplus x_2 \\ x_2 \oplus x_3 \end{pmatrix}$ | $F_{18}^k = \begin{pmatrix} x_1 \\ x_2 \oplus x_3 \\ x_1 \oplus x_3 \end{pmatrix}$<br>$F_{18}^d = \begin{pmatrix} x_1 \\ x_1 \oplus x_2 \oplus x_3 \\ x_1 \oplus x_3 \end{pmatrix}$ | $F_{25}^k = \begin{pmatrix} x_1 \oplus x_3 \\ x_1 \oplus x_2 \\ x_3 \end{pmatrix}$<br>$F_{25}^d = \begin{pmatrix} x_1 \oplus x_3 \\ x_1 \oplus x_2 \oplus x_3 \\ x_3 \end{pmatrix}$ |
| $F_5^k = F_5^d = \begin{pmatrix} x_1 \\ x_2 \\ x_1 \oplus x_3 \end{pmatrix}$ | $F_{12}^k = \begin{pmatrix} x_1 \\ x_1 \oplus x_3 \\ x_1 \oplus x_2 \oplus x_3 \end{pmatrix}$<br>$F_{12}^d = \begin{pmatrix} x_1 \\ x_2 \oplus x_3 \\ x_1 \oplus x_2 \end{pmatrix}$ | $F_{19}^k = F_{19}^d = \begin{pmatrix} x_1 \\ x_1 \oplus x_2 \\ x_1 \oplus x_3 \end{pmatrix}$ | $F_{26}^k = \begin{pmatrix} x_1 \oplus x_3 \\ x_1 \oplus x_2 \\ x_1 \oplus x_2 \oplus x_3 \end{pmatrix}$<br>$F_{26}^d = \begin{pmatrix} x_1 \oplus x_2 \oplus x_3 \\ x_1 \oplus x_3 \\ x_2 \oplus x_3 \end{pmatrix}$ |
| $F_6^k = F_6^d = \begin{pmatrix} x_1 \\ x_2 \oplus x_3 \\ x_3 \end{pmatrix}$ | $F_{13}^k = \begin{pmatrix} x_1 \oplus x_2 \oplus x_3 \\ x_2 \\ x_1 \oplus x_2 \end{pmatrix}$<br>$F_{13}^d = \begin{pmatrix} x_2 \oplus x_3 \\ x_2 \\ x_1 \oplus x_3 \end{pmatrix}$ | $F_{20}^k = \begin{pmatrix} x_1 \oplus x_2 \\ x_2 \\ x_2 \oplus x_3 \end{pmatrix}$<br>$F_{20}^d = \begin{pmatrix} x_1 \oplus x_2 \\ x_2 \\ x_1 \oplus x_2 \oplus x_3 \end{pmatrix}$ | $F_{27}^k = \begin{pmatrix} x_1 \oplus x_3 \\ x_2 \oplus x_3 \\ x_1 \oplus x_2 \oplus x_3 \end{pmatrix}$<br>$F_{27}^d = \begin{pmatrix} x_2 \oplus x_3 \\ x_1 \oplus x_3 \\ x_1 \oplus x_2 \oplus x_3 \end{pmatrix}$ |

| | | | |
|---|---|---|---|
| $F_7^k = F_7^d = \begin{pmatrix} x_1 \\ x_2 \\ x_2 \oplus x_3 \end{pmatrix}$ | $F_{14}^k = \begin{pmatrix} x_1 \oplus x_2 \oplus x_3 \\ x_2 \\ x_2 \oplus x_3 \end{pmatrix}$ | $F_{21}^k = \begin{pmatrix} x_1 \oplus x_3 \\ x_2 \\ x_2 \oplus x_3 \end{pmatrix}$ | $F_{28}^k = \begin{pmatrix} x_1 \oplus x_2 \\ x_2 \oplus x_3 \\ x_1 \oplus x_2 \oplus x_3 \end{pmatrix}$ |
| | $F_{14}^d = \begin{pmatrix} x_1 \oplus x_3 \\ x_2 \\ x_2 \oplus x_3 \end{pmatrix}$ | $F_{21}^d = \begin{pmatrix} x_1 \oplus x_2 \oplus x_3 \\ x_2 \\ x_2 \oplus x_3 \end{pmatrix}$ | $F_{28}^d = \begin{pmatrix} x_2 \oplus x_3 \\ x_1 \oplus x_2 \oplus x_3 \\ x_1 \oplus x_3 \end{pmatrix}$ |

Виходячи з цього, встановимо кількість кортежів, на основі яких будемо будувати групи двохоперандних операцій:

$$C_n^m = C_{12}^8 = \frac{12!}{8! \cdot (12-8)!} = 495. \qquad (4.1)$$

Розглянемо перший кортеж з перших 8 симетричних трьохрозрядних одноопераднних операцій і побудуємо на його основі симетричну двохоперандну операцію.

$$O_{1,2,3,4,5,6,7,8} = \begin{cases} F_1\begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix}, \text{ якщо } y_1 = 0;\ y_2 = 0;\ y_3 = 0 \\ F_2\begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix}, \text{ якщо } y_1 = 0;\ y_2 = 0;\ y_3 = 1 \\ F_3\begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix}, \text{ якщо } y_1 = 0;\ y_2 = 1;\ y_3 = 0 \\ F_4\begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix}, \text{ якщо } y_1 = 0;\ y_2 = 1;\ y_3 = 1 \\ F_5\begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix}, \text{ якщо } y_1 = 1;\ y_2 = 0;\ y_3 = 0 \\ F_6\begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix}, \text{ якщо } y_1 = 1;\ y_2 = 0;\ y_3 = 1 \\ F_7\begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix}, \text{ якщо } y_1 = 1;\ y_2 = 1;\ y_3 = 0 \\ F_8\begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix}, \text{ якщо } y_1 = 1;\ y_2 = 1;\ y_3 = 1 \end{cases} = \begin{cases} \begin{bmatrix} x_1 \\ x_2 \\ x_3 \end{bmatrix}, \text{якщо } y_1 = 0;\ y_2 = 0;\ y_3 = 0 \\ \begin{bmatrix} x_1 \oplus x_2 \\ x_2 \\ x_3 \end{bmatrix}, \text{ якщо } y_1 = 0;\ y_2 = 0;\ y_3 = 1 \\ \begin{bmatrix} x_1 \\ x_1 \oplus x_2 \\ x_3 \end{bmatrix}, \text{якщо } y_1 = 0;\ y_2 = 1;\ y_3 = 0 \\ \begin{bmatrix} x_1 \oplus x_3 \\ x_2 \\ x_3 \end{bmatrix}, \text{якщо } y_1 = 0;\ y_2 = 1;\ y_3 = 1 \\ \begin{bmatrix} x_1 \\ x_2 \\ x_1 \oplus x_3 \end{bmatrix}, \text{якщо } y_1 = 1;\ y_2 = 0;\ y_3 = 0 \\ \begin{bmatrix} x_1 \\ x_2 \oplus x_3 \\ x_3 \end{bmatrix}, \text{якщо } y_1 = 1;\ y_2 = 0;\ y_3 = 1 \\ \begin{bmatrix} x_1 \\ x_2 \\ x_2 \oplus x_3 \end{bmatrix}, \text{якщо } y_1 = 1;\ y_2 = 1;\ y_3 = 0 \\ \begin{bmatrix} x_1 \oplus x_2 \oplus x_3 \\ x_2 \\ x_3 \end{bmatrix}, \text{якщо } y_1 = 1;\ y_2 = 1;\ y_3 = 1 \end{cases}. \qquad (4.2)$$

Матричну симетричну трьохрозрядну двохоперандну операцію криптографічного кодування, побудовану на основі операцій базової групи, в загальному вигляді можна представити як:

$$O = \begin{bmatrix} y_{11} \cdot x_1 \oplus y_{12} \cdot x_2 \oplus y_{13} \cdot x_3 \\ y_{21} \cdot x_1 \oplus y_{22} \cdot x_2 \oplus y_{23} \cdot x_3 \\ y_{31} \cdot x_1 \oplus y_{32} \cdot x_2 \oplus y_{33} \cdot x_3 \end{bmatrix}, \quad (4.3)$$

де $x_1$, $x_2$, $x_3$ – значення першого, другого і третього розрядів (байтів, слів, подвійних слів) першого операнда, $y_{11}$, $y_{12}$, $y_{13}$, $y_{21}$, $y_{22}$, $y_{23}$, $y_{31}$, $y_{32}$ і $y_{33}$ – значення коефіцієнтів, які задаються значенням трьох розрядів (байтів, слів, подвійних слів) другого операнда.

Загальний вигляд операції (4.3) буде коректним, тому що в базових операціях відсутні перестановки елементарних функцій та їх інверсії [99].

Для формалізації кортежної моделі операції (4.2) і представленні її за допомогою узагальненої моделі (4.3) необхідно отримати значення коефіцієнтів $y_{11}$, $y_{12}$, $y_{13}$, $y_{21}$, $y_{22}$, $y_{23}$, $y_{31}$, $y_{32}$ і $y_{33}$. Для встановлення виразів, якими описуються ці коефіцієнти, побудуємо таблицю істинності та підставимо в неї ознаки наявності чи відсутності відповідних розрядів першого операнда залежно від значень другого операнда. Таблицю істинності коефіцієнтів узагальненої моделі операції (4.2) наведено в табл. 4.2.

Таблиця 4.2

**Таблиця істинності коефіцієнтів узагальненої моделі операції (4.2)**

| **Значення другого операнда** | | | **Елементарна функція 1** | | | **Елементарна функція 2** | | | **Елементарна функція 3** | | |
|---|---|---|---|---|---|---|---|---|---|---|---|
| $y_1$ | $y_2$ | $y_3$ | $y_{11}$ | $y_{12}$ | $y_{13}$ | $y_{21}$ | $y_{22}$ | $y_{23}$ | $y_{31}$ | $y_{32}$ | $y_{33}$ |
| 0 | 0 | 0 | 1 | 0 | 0 | | 1 | | | | 1 |
| 0 | 0 | 1 | 1 | 1 | 0 | | 1 | | | | 1 |
| 0 | 1 | 0 | 1 | 0 | 0 | 1 | 1 | | | | 1 |
| 0 | 1 | 1 | 1 | 0 | 1 | | 1 | | | | 1 |
| 1 | 0 | 0 | 1 | 0 | 0 | | 1 | | 1 | | 1 |
| 1 | 0 | 1 | 1 | 0 | 0 | | 1 | 1 | | | 1 |
| 1 | 1 | 0 | 1 | 0 | 0 | | 1 | | | 1 | 1 |
| 1 | 1 | 1 | 1 | 1 | 1 | | 1 | | | | 1 |

Виконавши мінімізацію таблиць істинності, отримаємо:

$y_{11} = 1$;

$y_{12} = y_1 \cdot y_2 \cdot y_3 \vee \overline{y}_1 \cdot \overline{y}_2 \cdot y_3 = (y_1 \cdot y_2 \vee \overline{y}_1 \cdot \overline{y}_2) \cdot y_3 = (\overline{y_1 \oplus y_2}) \cdot y_3$;

$y_{13} = y_2 \cdot y_3$;

$$y_{21} = \overline{y}_1 \cdot y_2 \cdot \overline{y}_3;$$

$$y_{22} = 1;$$

$$y_{23} = y_1 \cdot \overline{y}_2 \cdot y_3;$$

$$y_{31} = y_1 \cdot \overline{y}_2 \cdot \overline{y}_3;$$

$$y_{32} = y_1 \cdot y_2 \cdot \overline{y}_3;$$

$$y_{33} = 1.$$

Підставивши визначені коефіцієнти в модель (4.3), отримаємо:

$$O_{1,2,3,4,5,6,7,8} = \begin{bmatrix} x_1 \oplus (\overline{y_1 \oplus y_2}) \cdot y_3 \cdot x_2 \oplus y_2 \cdot y_3 \cdot x_3 \\ \overline{y}_1 \cdot y_2 \cdot \overline{y}_3 \cdot x_1 \oplus x_2 \oplus y_1 \cdot \overline{y}_2 \cdot y_3 \cdot x_3 \\ y_1 \cdot \overline{y}_2 \cdot \overline{y}_3 \cdot x_1 \oplus y_1 \cdot y_2 \cdot \overline{y}_3 \cdot x_2 \oplus x_3 \end{bmatrix}. \qquad (4.4)$$

Виконаємо перестановку симетричних одноопераднних операцій в двохоперандній операції (4.2), наприклад:

$$O_{8,2,3,5,4,1,7,6} = \begin{cases} F_8\begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix}, \text{ якщо } y_1 = 0;\ y_2 = 0;\ y_3 = 0 \\ F_2\begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix}, \text{ якщо } y_1 = 0;\ y_2 = 0;\ y_3 = 1 \\ F_3\begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix}, \text{ якщо } y_1 = 0;\ y_2 = 1;\ y_3 = 0 \\ F_5\begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix}, \text{ якщо } y_1 = 0;\ y_2 = 1;\ y_3 = 1 \\ F_4\begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix}, \text{ якщо } y_1 = 1;\ y_2 = 0;\ y_3 = 0 \\ F_1\begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix}, \text{ якщо } y_1 = 1;\ y_2 = 0;\ y_3 = 1 \\ F_7\begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix}, \text{ якщо } y_1 = 1;\ y_2 = 1;\ y_3 = 0 \\ F_6\begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix}, \text{ якщо } y_1 = 1;\ y_2 = 1;\ y_3 = 1 \end{cases} = \begin{cases} \begin{bmatrix} x_1 \oplus x_2 \oplus x_3 \\ x_2 \\ x_3 \end{bmatrix}, \text{ якщо } y_1 = 0;\ y_2 = 0;\ y_3 = 0 \\ \begin{bmatrix} x_1 \oplus x_2 \\ x_2 \\ x_3 \end{bmatrix}, \text{ якщо } y_1 = 0;\ y_2 = 0;\ y_3 = 1 \\ \begin{bmatrix} x_1 \\ x_1 \oplus x_2 \\ x_3 \end{bmatrix}, \text{ якщо } y_1 = 0;\ y_2 = 1;\ y_3 = 0 \\ \begin{bmatrix} x_1 \\ x_2 \\ x_1 \oplus x_3 \end{bmatrix}, \text{ якщо } y_1 = 0;\ y_2 = 1;\ y_3 = 1 \\ \begin{bmatrix} x_1 \oplus x_3 \\ x_2 \\ x_3 \end{bmatrix}, \text{ якщо } y_1 = 1;\ y_2 = 0;\ y_3 = 0 \\ \begin{bmatrix} x_1 \\ x_2 \\ x_3 \end{bmatrix}, \text{ якщо } y_1 = 1;\ y_2 = 0;\ y_3 = 1 \\ \begin{bmatrix} x_1 \\ x_2 \\ x_2 \oplus x_3 \end{bmatrix}, \text{ якщо } y_1 = 1;\ y_2 = 1;\ y_3 = 0 \\ \begin{bmatrix} x_1 \\ x_2 \oplus x_3 \\ x_3 \end{bmatrix}, \text{ якщо } y_1 = 1;\ y_2 = 1;\ y_3 = 1 \end{cases}. \qquad (4.5)$$

Таблицю істинності коефіцієнтів узагальненої моделі операції (4.5) наведено в табл. 4.3.

Таблиця 4.3

**Таблиця істинності коефіцієнтів узагальненої моделі операції (4.5)**

| **Значення другого операнда** | | | **Елементарна функція 1** | | | **Елементарна функція 2** | | | **Елементарна функція 3** | | |
|---|---|---|---|---|---|---|---|---|---|---|---|
| $y_1$ | $y_2$ | $y_3$ | $y_{11}$ | $y_{12}$ | $y_{13}$ | $y_{21}$ | $y_{22}$ | $y_{23}$ | $y_{31}$ | $y_{32}$ | $y_{33}$ |
| 0 | 0 | 0 | 1 | 1 | 1 | 0 | 1 | 0 | 0 | 0 | 1 |
| 0 | 0 | 1 | 1 | 1 | 0 | 0 | 1 | 0 | 0 | 0 | 1 |
| 0 | 1 | 0 | 1 | 0 | 0 | 1 | 1 | 0 | 0 | 0 | 1 |
| 0 | 1 | 1 | 1 | 0 | 0 | 0 | 1 | 0 | 1 | 0 | 1 |
| 1 | 0 | 0 | 1 | 0 | 1 | 0 | 1 | 0 | 0 | 0 | 1 |
| 1 | 0 | 1 | 1 | 0 | 0 | 0 | 1 | 0 | 0 | 0 | 1 |
| 1 | 1 | 0 | 1 | 0 | 0 | 0 | 1 | 0 | 0 | 1 | 1 |
| 1 | 1 | 1 | 1 | 0 | 0 | 0 | 1 | 1 | 0 | 0 | 1 |

Виконавши мінімізацію таблиць істинності і підставивши її результати в загальну модель (4.5), отримаємо:

$$O_{1,2,3,4,5,6,7,8} = \begin{bmatrix} x_1 \oplus \bar{y}_1 \cdot \bar{y}_2 \cdot x_2 \oplus \bar{y}_2 \cdot \bar{y}_3 \cdot x_3 \\ \bar{y}_1 \cdot y_2 \cdot \bar{y}_3 \cdot x_1 \oplus x_2 \oplus y_1 \cdot y_2 \cdot y_3 \cdot x_3 \\ \bar{y}_1 \cdot y_2 \cdot y_3 \cdot x_1 \oplus y_1 \cdot y_2 \cdot \bar{y}_3 \cdot x_2 \oplus x_3 \end{bmatrix}. \qquad (4.6)$$

Виконаємо ще одну перестановку симетричних одноопераднних операцій у двохопераднній операції (4.2), наприклад:

$$O_{1,6,3,2,5,8,7,4} = \begin{cases} F_1\begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix}, \text{ якщо } y_1 = 0;\ y_2 = 0;\ y_3 = 0 \\ F_6\begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix}, \text{ якщо } y_1 = 0;\ y_2 = 0;\ y_3 = 1 \\ F_3\begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix}, \text{ якщо } y_1 = 0;\ y_2 = 1;\ y_3 = 0 \\ F_2\begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix}, \text{ якщо } y_1 = 0;\ y_2 = 1;\ y_3 = 1 \\ F_5\begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix}, \text{ якщо } y_1 = 1;\ y_2 = 0;\ y_3 = 0 \\ F_8\begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix}, \text{ якщо } y_1 = 1;\ y_2 = 0;\ y_3 = 1 \\ F_7\begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix}, \text{ якщо } y_1 = 1;\ y_2 = 1;\ y_3 = 0 \\ F_4\begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix}, \text{ якщо } y_1 = 1;\ y_2 = 1;\ y_3 = 1 \end{cases} = \begin{cases} \begin{bmatrix} x_1 \\ x_2 \\ x_3 \end{bmatrix}, \text{якщо } y_1 = 0;\ y_2 = 0;\ y_3 = 0 \\ \begin{bmatrix} x_1 \\ x_2 \oplus x_3 \\ x_3 \end{bmatrix}, \text{ якщо } y_1 = 0;\ y_2 = 0;\ y_3 = 1 \\ \begin{bmatrix} x_1 \\ x_1 \oplus x_2 \\ x_3 \end{bmatrix}, \text{якщо } y_1 = 0;\ y_2 = 1;\ y_3 = 0 \\ \begin{bmatrix} x_1 \oplus x_2 \\ x_2 \\ x_3 \end{bmatrix}, \text{якщо } y_1 = 0;\ y_2 = 1;\ y_3 = 1 \\ \begin{bmatrix} x_1 \\ x_2 \\ x_1 \oplus x_3 \end{bmatrix}, \text{якщо } y_1 = 1;\ y_2 = 0;\ y_3 = 0 \\ \begin{bmatrix} x_1 \oplus x_2 \oplus x_3 \\ x_2 \\ x_3 \end{bmatrix}, \text{якщо } y_1 = 1;\ y_2 = 0;\ y_3 = 1 \\ \begin{bmatrix} x_1 \\ x_2 \\ x_2 \oplus x_3 \end{bmatrix}, \text{якщо } y_1 = 1;\ y_2 = 1;\ y_3 = 0 \\ \begin{bmatrix} x_1 \oplus x_3 \\ x_2 \\ x_3 \end{bmatrix}, \text{якщо } y_1 = 1;\ y_2 = 1;\ y_3 = 1 \end{cases}. \qquad (4.7)$$

Таблицю істинності коефіцієнтів узагальненої моделі операції (4.7) наведено в табл. 4.4.

Таблиця 4.4

**Таблиця істинності коефіцієнтів узагальненої моделі операції (4.7)**

| **Значення другого операнда** | | | **Елементарна функція 1** | | | **Елементарна функція 2** | | | **Елементарна функція 3** | | |
|---|---|---|---|---|---|---|---|---|---|---|---|
| $y_1$ | $y_2$ | $y_3$ | $y_{11}$ | $y_{12}$ | $y_{13}$ | $y_{21}$ | $y_{22}$ | $y_{23}$ | $y_{31}$ | $y_{32}$ | $y_{33}$ |
| 0 | 0 | 0 | 1 | 0 | 0 | 0 | 1 | 0 | 0 | 0 | 1 |
| 0 | 0 | 1 | 1 | 0 | 0 | 0 | 1 | 1 | 0 | 0 | 1 |
| 0 | 1 | 0 | 1 | 0 | 0 | 1 | 1 | 0 | 0 | 0 | 1 |
| 0 | 1 | 1 | 1 | 1 | 0 | 0 | 1 | 0 | 0 | 0 | 1 |
| 1 | 0 | 0 | 1 | 0 | 0 | 0 | 1 | 0 | 1 | 0 | 1 |
| 1 | 0 | 1 | 1 | 1 | 1 | 0 | 1 | 0 | 0 | 0 | 1 |
| 1 | 1 | 0 | 1 | 0 | 0 | 0 | 1 | 0 | 0 | 1 | 1 |
| 1 | 1 | 1 | 1 | 0 | 1 | 0 | 1 | 0 | 0 | 0 | 1 |

На основі мінімізації таблиць істинності (табл. 4.4) отримаємо:

$$O_{1,6,3,2,5,8,7,4} = \begin{bmatrix} x_1 \oplus (\overline{y_1 \oplus y_2}) \cdot y_3 \cdot x_2 \oplus y_1 \cdot y_3 \cdot x_3 \\ \bar{y}_1 \cdot y_2 \cdot \bar{y}_3 \cdot x_1 \oplus x_2 \oplus y_1 \cdot \bar{y}_2 \cdot \bar{y}_3 \cdot x_3 \\ y_1 \cdot \bar{y}_2 \cdot \bar{y}_3 \cdot x_1 \oplus y_1 \cdot y_2 \cdot \bar{y}_3 \cdot x_2 \oplus x_3 \end{bmatrix}. \quad (4.8)$$

Як видно з моделей (4.4), (4.6), (4.8), різні варіанти перестановки одноопераднних операцій в кортежі приводять до різної складності двохоперандних операцій.

Визначимо кількість симетричних трьохрозрядних двохоперандних операцій криптографічного кодування, які можуть бути побудовані на основі базової групи трьохрозрядних одноопераднних матричних операцій криптографічного кодування.

Кількість кортежів з симетричних трьохрозрядних одноопераднних матричних операцій базової групи відповідно до (4.1) буде 495 операцій. З кожного кортежу на основі перестановки одноопераднних операцій буде отримано $P_8 = 8! = 40320$ операцій. Виходячи з цього, кількість симетричних трьохрозрядних двохоперандних операцій криптографічного кодування, які будуть побудовані на основі лише базової групи трьохрозрядних

одноопераднних матричних операцій криптографічного кодування, буде дорівнювати $C_{12}^{8} \cdot P_8 = 495 \cdot 40320 = 19958400.$

Отримана кількість операцій свідчить про те, що без автоматизованої системи, яка реалізує технологію синтезу і дослідження симетричних двохоперандних операцій криптографічного кодування, визначити операції, які ефективно будуть реалізувати захищену інформаційну систему критичної інфраструктури, неможливо.

## 4.2 Реалізація методу синтезу груп симетричних двохоперандних операцій криптографічного кодування інформації для систем потокового шифрування

Розглянемо синтез симетричних трьохрозрядних двоопераднних операцій криптографічного кодування.

Кількість одноопераднних операцій криптографічного кодування визначається [110]:

$$K_o^1(n) = 2^n! \tag{4.10}$$

$$K_o^1(n) = K_{об}(n) \cdot K_{оп}(n) \cdot K_{ои}(n) = K_{об}(n) \cdot n! \cdot 2^n, \tag{4.11}$$

де $n$ – розрядність операції, $K_{об}(n)$, $K_{оп}(n) = n!$, $K_{ои}(n) = 2^n$ – кількість базових операцій, операцій перестановки і операцій інверсії відповідно.

На підставі виразів (4.10) та (4.11) кількість двохрозрядних одноопераднних операцій криптографічного кодування визначається:

$K_o^1(2) = 4! = 24 \quad K_o^1(2) = K_{об}(2) \cdot 2! \cdot 2^2 = 3 \cdot 6 \cdot 4 = 24.$

Оскільки за результатами експерименту існує 96 симетричних двохрозрядних двохоперандних операцій, і вони становлять 4 групи по 24 операції, можна припустити, що $K_o^2(2) = 96 = 4 \cdot 2^2!$ Отже,

$$K_o^2(n) = k \cdot 2^n!, \tag{4.12}$$

де $k$ – кількість груп симетричних $n$-розрядних двохоперандних операцій криптографічного кодування.

Кількість операцій у кожній групі симетричних трьохрозрядних двохоперандних операцій відповідно до (4.12) визначається $K_o^2(3) = k \cdot 2^3! = k \cdot 8!$ і становить 40320 операцій [5].

На практиці нині синтезувати групу з такої кількості операцій неможливо. Це пов'язано з відсутністю єдиного математичного апарату, що дозволяє моделювати всю сукупність трьохрозрядних одноопераднних операцій [110]. Тому в процесі синтезу симетричних трьохрозрядних двохоперандних операцій обмежимося лише синтезом базових двохоперандних операцій на основі матричних одноопераднних операцій.

Відповідно до [94] кількість базових трьохрозрядних одноопераднних матричних операцій становить 28 операцій. Ці операції наведено в табл. 4.1. Тому в процесі синтезу симетричних трьохрозрядних двохоперандних матричних операцій криптографічного кодування будемо використовувати нумерацію одноопераднних операцій відповідно до табл. 4.1.

Для застосування методу синтезу груп симетричних двохоперандних операцій криптографічного кодування інформації для систем блокового шифрування необхідно встановити симетричну двохоперандну операцію, на основі якої будемо проводити синтез.

Розглянемо більш детально операцію $O_1^{4\oplus}$, на основі якої проводився синтез четвертої групи симетричних двохоперандних операцій криптографічного кодування:

$$O_1^{4\oplus} = \begin{bmatrix} x_1 \cdot (\overline{k_1 \oplus k_2}) \oplus x_2 \cdot (k_1 \oplus k_2) \oplus k_1 \\ x_1 \cdot (k_1 \oplus k_2) \oplus x_2 \cdot (\overline{k_1 \oplus k_2}) \oplus k_2 \end{bmatrix} = \begin{bmatrix} x_1 \oplus k_1 \oplus (x_1 \oplus x_2) \cdot (k_1 \oplus k_2) \\ x_2 \oplus k_2 \oplus (x_1 \oplus x_2) \cdot (k_1 \oplus k_2) \end{bmatrix}. \quad (4.13)$$

Виходячи з виразу (4.13), операцію $O_1^{4\oplus}$ можна назвати операцією порозрядного додавання за модулем два з корекцією.

При розробці методу синтезу груп симетричних двохоперандних операцій криптографічного кодування синтез проводився на основі операцій:

- додавання за модулем два:
  - порозрядне додавання за модулем два;
  - порозрядне додавання за модулем два з корекцією;
- додавання за модулем чотири:
  - лівостороннє додавання за модулем чотири;
  - правостороннє додавання за модулем чотири.

Враховуючи те, що перестановки елементарних функцій в операціях не впливають на кількість груп модифікованих операцій з точністю до перестановки, а єдиною операцією, яка реалізує перекодування біта інформації, незалежно від біт, є порозрядне додавання за модулем два, можна визначити такий перелік операцій:

- додавання за модулем два:
  - порозрядне додавання за модулем два:

$$O_1 = \begin{bmatrix} x_1 \oplus k_1 \\ x_2 \oplus k_2 \\ x_3 \oplus k_3 \end{bmatrix}; \tag{4.14}$$

  - порозрядне додавання за модулем два з корекцією;

$$O_1 = \begin{bmatrix} x_1 \oplus k_1 \oplus (x_1 \oplus x_2) \cdot (k_1 \oplus k_2) \\ x_2 \oplus k_2 \oplus (x_1 \oplus x_2) \cdot (k_1 \oplus k_2) \\ x_3 \oplus k_3 \end{bmatrix}; \tag{4.15}$$

$$O_1 = \begin{bmatrix} x_1 \oplus k_1 \oplus (x_1 \oplus x_2) \cdot (k_1 \oplus k_2) \\ x_2 \oplus k_2 \\ x_3 \oplus k_3 \oplus (x_1 \oplus x_3) \cdot (k_1 \oplus k_3) \end{bmatrix}; \tag{4.16}$$

$$O_1 = \begin{bmatrix} x_1 \oplus k_1 \\ x_2 \oplus k_2 \oplus (x_1 \oplus x_2) \cdot (k_1 \oplus k_2) \\ x_3 \oplus k_3 \oplus (x_2 \oplus x_3) \cdot (k_2 \oplus k_3) \end{bmatrix}; \tag{4.17}$$

- додавання за модулем чотири:
  - лівостороннє додавання за модулем чотири:

$$O_1 = \begin{bmatrix} x_1 \oplus k_1 \oplus x_2 \cdot k_2 \\ x_2 \oplus k_2 \\ x_3 \oplus k_3 \end{bmatrix}; \quad (4.18)$$

$$O_1 = \begin{bmatrix} x_1 \oplus k_1 \oplus x_3 \cdot k_3 \\ x_2 \oplus k_2 \\ x_3 \oplus k_3 \end{bmatrix}; \quad (4.19)$$

$$O_1 = \begin{bmatrix} x_1 \oplus k_1 \\ x_2 \oplus k_2 \oplus x_3 \cdot k_3 \\ x_3 \oplus k_3 \end{bmatrix}; \quad (4.20)$$

- правостороннє додавання за модулем чотири:

$$O_1 = \begin{bmatrix} x_1 \oplus k_1 \\ x_2 \oplus k_2 \oplus x_1 \cdot k_1 \\ x_3 \oplus k_3 \end{bmatrix}; \quad (4.21)$$

$$O_1 = \begin{bmatrix} x_1 \oplus k_1 \\ x_2 \oplus k_2 \\ x_3 \oplus k_3 \oplus x_1 \cdot k_1 \end{bmatrix}; \quad (4.22)$$

$$O_1 = \begin{bmatrix} x_1 \oplus k_1 \\ x_2 \oplus k_2 \\ x_3 \oplus k_3 \oplus x_2 \cdot k_2 \end{bmatrix}; \quad (4.23)$$

➢ додавання за модулем вісім:

- лівостороннє додавання за модулем вісім:

$$O_1 = \begin{bmatrix} x_1 \oplus k_1 \oplus (x_2 \cdot k_2 \vee x_2 \cdot x_3 \cdot k_3 \vee k_2 \cdot x_3 \cdot k_3) \\ x_2 \oplus k_2 \oplus x_3 \cdot k_3 \\ x_3 \oplus k_3 \end{bmatrix}; \quad (4.24)$$

$$O_1 = \begin{bmatrix} x_1 \oplus k_1 \oplus (x_3 \cdot k_3 \vee x_3 \cdot x_2 \cdot k_2 \vee k_3 \cdot x_2 \cdot k_2) \\ x_2 \oplus k_2 \\ x_3 \oplus k_3 \oplus x_2 \cdot k_2 \end{bmatrix}; \quad (4.25)$$

- правостороннє додавання за модулем вісім:

$$O_1 = \begin{bmatrix} x_1 \oplus k_1 \\ x_2 \oplus k_2 \oplus x_1 \cdot k_1 \\ x_3 \oplus k_3 \oplus (x_2 \cdot k_2 \vee x_2 \cdot x_1 \cdot k_1 \vee k_2 \cdot x_1 \cdot k_1) \end{bmatrix}; \quad (4.26)$$

$$O_1 = \begin{bmatrix} x_1 \oplus k_1 \oplus x_1 \cdot k_1 \\ x_2 \oplus k_2 \\ x_3 \oplus k_3 \oplus (x_1 \cdot k_1 \vee x_1 \cdot x_2 \cdot k_2 \vee k_1 \cdot x_2 \cdot k_2) \end{bmatrix}. \qquad (4.27)$$

Операції (4.14) – (4.27) відрізняються математичним представленням і таблицями істинності операцій. Крім того, відрізняються узагальнені таблиці операцій з точністю до перестановки. Виходячи з цього, на основі запропонованого методу синтезу буде побудовано не менше 14 груп симетричних двохоперандних операцій криптографічного кодування інформації для систем блокового шифрування.

Синтезуємо базову групу симетричних трьохрозрядних двохоперандних матричних операцій криптографічного кодування на основі операції (4.15). Для цього введемо підстановку в операцію

$$O_1 = \begin{bmatrix} x_1 \oplus k_1 \oplus (x_1 \oplus x_2) \cdot (k_1 \oplus k_2) \\ x_2 \oplus k_2 \oplus (x_1 \oplus x_2) \cdot (k_1 \oplus k_2) \\ x_3 \oplus k_3 \end{bmatrix} = \begin{bmatrix} y_1 \\ y_2 \\ y_3 \end{bmatrix},$$

$y_1 = x_1 \oplus k_1 \oplus (x_1 \oplus x_2) \cdot (k_1 \oplus k_2)$; $y_2 = x_2 \oplus k_2 \oplus (x_1 \oplus x_2) \cdot (k_1 \oplus k_2)$; $y_3 = x_3 \oplus k_3$.

Використавши базові трьохрозрядні одноопераднді матричні операції, наведені в табл. 4.1, отримаємо 28 базових трьохрозрядних одноопераднді матричних операцій:

$$O_1 = F_1(O_1) = \begin{bmatrix} y_1 \\ y_2 \\ y_3 \end{bmatrix} = \begin{bmatrix} x_1 \oplus k_1 \oplus (x_1 \oplus x_2) \cdot (k_1 \oplus k_2) \\ x_2 \oplus k_2 \oplus (x_1 \oplus x_2) \cdot (k_1 \oplus k_2) \\ x_3 \oplus k_3 \end{bmatrix};$$

$$O_2 = F_2(O_1) = \begin{bmatrix} y_1 \oplus y_2 \\ y_2 \\ y_3 \end{bmatrix} = \begin{bmatrix} x_1 \oplus k_1 \oplus x_2 \oplus k_2 \\ x_2 \oplus k_2 \oplus (x_1 \oplus x_2) \cdot (k_1 \oplus k_2) \\ x_3 \oplus k_3 \end{bmatrix};$$

$$O_3 = F_3(O_1) = \begin{bmatrix} y_1 \\ y_1 \oplus y_2 \\ y_3 \end{bmatrix} = \begin{bmatrix} x_1 \oplus k_1 \oplus (x_1 \oplus x_2) \cdot (k_1 \oplus k_2) \\ x_1 \oplus k_1 \oplus x_2 \oplus k_2 \\ x_3 \oplus k_3 \end{bmatrix};$$

$$O_4 = F_4(O_1) = \begin{bmatrix} y_1 \oplus y_3 \\ y_2 \\ y_3 \end{bmatrix} = \begin{bmatrix} x_1 \oplus k_1 \oplus x_3 \oplus k_3 \oplus (x_1 \oplus x_2) \cdot (k_1 \oplus k_2) \\ x_2 \oplus k_2 \oplus (x_1 \oplus x_2) \cdot (k_1 \oplus k_2) \\ x_3 \oplus k_3 \end{bmatrix};$$

$$O_5 = F_5(O_1) = \begin{bmatrix} y_1 \\ y_2 \\ y_1 \oplus y_3 \end{bmatrix} = \begin{bmatrix} x_1 \oplus k_1 \oplus (x_1 \oplus x_2) \cdot (k_1 \oplus k_2) \\ x_2 \oplus k_2 \oplus (x_1 \oplus x_2) \cdot (k_1 \oplus k_2) \\ x_1 \oplus k_1 \oplus x_3 \oplus k_3 \oplus (x_1 \oplus x_2) \cdot (k_1 \oplus k_2) \end{bmatrix};$$

$$O_6 = F_6(O_1) = \begin{bmatrix} y_1 \\ y_2 \oplus y_3 \\ y_3 \end{bmatrix} = \begin{bmatrix} x_1 \oplus k_1 \oplus (x_1 \oplus x_2) \cdot (k_1 \oplus k_2) \\ x_2 \oplus k_2 \oplus x_3 \oplus k_3 \oplus (x_1 \oplus x_2) \cdot (k_1 \oplus k_2) \\ x_3 \oplus k_3 \end{bmatrix};$$

$$O_7 = F_7(O_1) = \begin{bmatrix} y_1 \\ y_2 \\ y_2 \oplus y_3 \end{bmatrix} = \begin{bmatrix} x_1 \oplus k_1 \oplus (x_1 \oplus x_2) \cdot (k_1 \oplus k_2) \\ x_2 \oplus k_2 \oplus (x_1 \oplus x_2) \cdot (k_1 \oplus k_2) \\ x_2 \oplus k_2 \oplus x_3 \oplus k_3 \oplus (x_1 \oplus x_2) \cdot (k_1 \oplus k_2) \end{bmatrix};$$

$$O_8 = F_8(O_1) = \begin{bmatrix} y_1 \oplus y_2 \oplus y_3 \\ y_2 \\ y_3 \end{bmatrix} = \begin{bmatrix} x_1 \oplus k_1 \oplus x_2 \oplus k_2 \oplus x_3 \oplus k_3 \\ x_2 \oplus k_2 \oplus (x_1 \oplus x_2) \cdot (k_1 \oplus k_2) \\ x_3 \oplus k_3 \end{bmatrix};$$

$$O_9 = F_9(O_1) = \begin{bmatrix} y_1 \\ y_1 \oplus y_2 \oplus y_3 \\ y_3 \end{bmatrix} = \begin{bmatrix} x_1 \oplus k_1 \oplus (x_1 \oplus x_2) \cdot (k_1 \oplus k_2) \\ x_1 \oplus k_1 \oplus x_2 \oplus k_2 \oplus x_3 \oplus k_3 \\ x_3 \oplus k_3 \end{bmatrix};$$

$$O_{10} = F_{10}(O_1) = \begin{bmatrix} y_1 \\ y_2 \\ y_1 \oplus y_2 \oplus y_3 \end{bmatrix} = \begin{bmatrix} x_1 \oplus k_1 \oplus (x_1 \oplus x_2) \cdot (k_1 \oplus k_2) \\ x_2 \oplus k_2 \oplus (x_1 \oplus x_2) \cdot (k_1 \oplus k_2) \\ x_1 \oplus k_1 \oplus x_2 \oplus k_2 \oplus x_3 \oplus k_3 \end{bmatrix};$$

$$O_{11} = F_{11}(O_1) = \begin{bmatrix} y_1 \\ y_1 \oplus y_2 \\ y_1 \oplus y_2 \oplus y_3 \end{bmatrix} = \begin{bmatrix} x_1 \oplus k_1 \oplus (x_1 \oplus x_2) \cdot (k_1 \oplus k_2) \\ x_1 \oplus k_1 \oplus x_2 \\ x_1 \oplus k_1 \oplus x_2 \oplus x_3 \oplus k_3 \end{bmatrix};$$

$$O_{12} = F_{12}(O_1) = \begin{bmatrix} y_1 \\ y_1 \oplus y_3 \\ y_1 \oplus y_2 \oplus y_3 \end{bmatrix} = \begin{bmatrix} x_1 \oplus k_1 \oplus (x_1 \oplus x_2) \cdot (k_1 \oplus k_2) \\ x_2 \oplus k_2 \oplus x_3 \oplus k_3 \oplus (x_1 \oplus x_2) \cdot (k_1 \oplus k_2) \\ x_1 \oplus k_1 \oplus x_2 \oplus k_2 \oplus x_3 \oplus k_3 \end{bmatrix};$$

$$O_{13} = F_{13}(O_1) = \begin{bmatrix} y_1 \oplus y_2 \oplus y_3 \\ y_2 \\ y_1 \oplus y_2 \end{bmatrix} = \begin{bmatrix} x_1 \oplus k_1 \oplus x_2 \oplus k_2 \oplus x_3 \oplus k_3 \\ x_2 \oplus k_2 \oplus (x_1 \oplus x_2) \cdot (k_1 \oplus k_2) \\ x_1 \oplus k_1 \oplus x_2 \oplus k_2 \end{bmatrix};$$

$$O_{14} = F_{14}(O_1) = \begin{bmatrix} y_1 \oplus y_2 \oplus y_3 \\ y_2 \\ y_2 \oplus y_3 \end{bmatrix} = \begin{bmatrix} x_1 \oplus k_1 \oplus x_2 \oplus k_2 \oplus x_3 \oplus k_3 \\ x_2 \oplus k_2 \oplus (x_1 \oplus x_2) \cdot (k_1 \oplus k_2) \\ x_2 \oplus k_2 \oplus x_3 \oplus k_3 \oplus (x_1 \oplus x_2) \cdot (k_1 \oplus k_2) \end{bmatrix};$$

$$O_{15} = F_{15}(O_1) = \begin{bmatrix} y_1 \oplus y_2 \oplus y_3 \\ y_2 \oplus y_3 \\ y_3 \end{bmatrix} = \begin{bmatrix} x_1 \oplus k_1 \oplus x_2 \oplus k_2 \oplus x_3 \oplus k_3 \\ x_2 \oplus k_2 \oplus x_3 \oplus k_3 \oplus (x_1 \oplus x_2) \cdot (k_1 \oplus k_2) \\ x_3 \oplus k_3 \end{bmatrix};$$

$$O_{16} = F_{16}(O_1) = \begin{bmatrix} y_1 \oplus y_2 \oplus y_3 \\ y_1 \oplus y_3 \\ y_3 \end{bmatrix} = \begin{bmatrix} x_1 \oplus k_1 \oplus x_2 \oplus k_2 \oplus x_3 \oplus k_3 \\ x_1 \oplus k_1 \oplus x_3 \oplus k_3 \oplus (x_1 \oplus x_2) \cdot (k_1 \oplus k_2) \\ x_3 \oplus k_3 \end{bmatrix};$$

$$O_{17} = F_{17}(O_1) = \begin{bmatrix} y_1 \\ y_1 \oplus y_2 \\ y_2 \oplus y_3 \end{bmatrix} = \begin{bmatrix} x_1 \oplus k_1 \oplus (x_1 \oplus x_2) \cdot (k_1 \oplus k_2) \\ x_1 \oplus k_1 \oplus x_2 \oplus k_2 \\ x_2 \oplus k_2 \oplus x_3 \oplus k_3 \oplus (x_1 \oplus x_2) \cdot (k_1 \oplus k_2) \end{bmatrix};$$

$$O_{18} = F_{18}(O_1) = \begin{bmatrix} y_1 \\ y_2 \oplus y_3 \\ y_1 \oplus y_3 \end{bmatrix} = \begin{bmatrix} x_1 \oplus k_1 \oplus (x_1 \oplus x_2) \cdot (k_1 \oplus k_2) \\ x_2 \oplus k_2 \oplus x_3 \oplus k_3 \oplus (x_1 \oplus x_2) \cdot (k_1 \oplus k_2) \\ x_1 \oplus k_1 \oplus x_3 \oplus k_3 \oplus (x_1 \oplus x_2) \cdot (k_1 \oplus k_2) \end{bmatrix};$$

$$O_{19} = F_{19}(O_1) = \begin{bmatrix} y_1 \\ y_1 \oplus y_2 \\ y_1 \oplus y_3 \end{bmatrix} = \begin{bmatrix} x_1 \oplus k_1 \oplus (x_1 \oplus x_2) \cdot (k_1 \oplus k_2) \\ x_1 \oplus k_1 \oplus x_2 \oplus k_2 \\ x_1 \oplus k_1 \oplus x_3 \oplus k_3 \oplus (x_1 \oplus x_2) \cdot (k_1 \oplus k_2) \end{bmatrix};$$

$$O_{20} = F_{20}(O_1) = \begin{bmatrix} y_1 \oplus y_2 \\ y_2 \\ y_2 \oplus y_3 \end{bmatrix} = \begin{bmatrix} x_1 \oplus k_1 \oplus x_2 \oplus k_2 \\ x_2 \oplus k_2 \oplus (x_1 \oplus x_2) \cdot (k_1 \oplus k_2) \\ x_2 \oplus k_2 \oplus x_3 \oplus k_3 \oplus (x_1 \oplus x_2) \cdot (k_1 \oplus k_2) \end{bmatrix};$$

$$O_{21} = F_{21}(O_1) = \begin{bmatrix} y_1 \oplus y_3 \\ y_2 \\ y_2 \oplus y_3 \end{bmatrix} = \begin{bmatrix} x_1 \oplus k_1 \oplus x_3 \oplus k_3 \\ x_2 \oplus k_2 \oplus (x_1 \oplus x_2) \cdot (k_1 \oplus k_2) \\ x_2 \oplus k_2 \oplus x_3 \oplus k_3 \oplus (x_1 \oplus x_2) \cdot (k_1 \oplus k_2) \end{bmatrix};$$

$$O_{22} = F_{22}(O_1) = \begin{bmatrix} y_1 \oplus y_2 \\ y_2 \\ y_1 \oplus y_3 \end{bmatrix} = \begin{bmatrix} x_1 \oplus k_1 \oplus x_2 \oplus k_2 \\ x_2 \oplus k_2 \oplus (x_1 \oplus x_2) \cdot (k_1 \oplus k_2) \\ x_1 \oplus k_1 \oplus x_3 \oplus k_3 \oplus (x_1 \oplus x_2) \cdot (k_1 \oplus k_2) \end{bmatrix};$$

$$O_{23} = F_{23}(O_1) = \begin{bmatrix} y_1 \oplus y_2 \\ y_2 \oplus y_3 \\ y_3 \end{bmatrix} = \begin{bmatrix} x_1 \oplus k_1 \oplus x_2 \oplus k_2 \\ x_2 \oplus k_2 \oplus x_3 \oplus k_3 \oplus (x_1 \oplus x_2) \cdot (k_1 \oplus k_2) \\ x_3 \oplus k_3 \end{bmatrix};$$

$$O_{24} = F_{24}(O_1) = \begin{bmatrix} y_1 \oplus y_3 \\ y_2 \oplus y_3 \\ y_3 \end{bmatrix} = \begin{bmatrix} x_1 \oplus k_1 \oplus x_3 \oplus k_3 \oplus (x_1 \oplus x_2) \cdot (k_1 \oplus k_2) \\ x_2 \oplus k_2 \oplus x_3 \oplus k_3 \oplus (x_1 \oplus x_2) \cdot (k_1 \oplus k_2) \\ x_3 \oplus k_3 \end{bmatrix};$$

$$O_{25} = F_{25}(O_1) = \begin{bmatrix} y_1 \oplus y_3 \\ y_1 \oplus y_2 \\ y_3 \end{bmatrix} = \begin{bmatrix} x_1 \oplus k_1 \oplus x_3 \oplus k_3 \oplus (x_1 \oplus x_2) \cdot (k_1 \oplus k_2) \\ x_1 \oplus k_1 \oplus x_2 \oplus k_2 \\ x_3 \oplus k_3 \end{bmatrix};$$

$$O_{26} = F_{26}(O_1) = \begin{bmatrix} y_1 \oplus y_3 \\ y_1 \oplus y_2 \\ y_1 \oplus y_2 \oplus y_3 \end{bmatrix} = \begin{bmatrix} x_1 \oplus k_1 \oplus x_3 \oplus k_3 \oplus (x_1 \oplus x_2) \cdot (k_1 \oplus k_2) \\ x_1 \oplus k_1 \oplus x_2 \oplus k_2 \\ x_1 \oplus k_1 \oplus x_2 \oplus k_2 \oplus x_3 \oplus k_3 \end{bmatrix};$$

$$O_{27} = F_{27}(O_1) = \begin{bmatrix} y_1 \oplus y_3 \\ y_2 \oplus y_3 \\ y_1 \oplus y_2 \oplus y_3 \end{bmatrix} = \begin{bmatrix} x_1 \oplus k_1 \oplus x_3 \oplus k_3 \oplus (x_1 \oplus x_2) \cdot (k_1 \oplus k_2) \\ x_2 \oplus k_2 \oplus x_3 \oplus k_3 \oplus (x_1 \oplus x_2) \cdot (k_1 \oplus k_2) \\ x_1 \oplus k_1 \oplus x_2 \oplus k_2 \oplus x_3 \oplus k_3 \end{bmatrix};$$

$$O_{28} = F_{28}(O_1) = \begin{bmatrix} y_1 \oplus y_2 \\ y_2 \oplus y_3 \\ y_1 \oplus y_2 \oplus y_3 \end{bmatrix} = \begin{bmatrix} x_1 \oplus k_1 \oplus x_2 \oplus k_2 \\ x_2 \oplus k_2 \oplus x_3 \oplus k_3 \oplus (x_1 \oplus x_2) \cdot (k_1 \oplus k_2) \\ x_1 \oplus k_1 \oplus x_2 \oplus k_2 \oplus x_3 \oplus k_3 \end{bmatrix}.$$

Для перевірки коректності результатів синтезу отриманих симетричних матричних операцій було застосовано вимоги до симетричності операцій, заданих таблицями істинності [111]. Додатково кожна операція перевірялася, враховуючи повний перебір усіх вхідних даних.

На основі кожної синтезованої базової симетричної трьохрозрядної двохоперандної операції буде побудовано 6 операцій перестановки.

Застосувавши інверсію елементарних функцій, з кожної отриманої операції буде побудовано 8 операцій інверсії.

Виходячи з цього, застосування запропонованого методу синтезу груп симетричних двохоперандних операцій криптографічного кодування інформації для систем блокового шифрування на основі однієї симетричної операції забезпечить побудову групи з 1344 матричних операцій.

Оскільки отримані в підрозділі операції (4.14) – (4.27) належать до різних груп операцій з точністю до перестановки, то буде синтезовано 18816 операцій.

Розроблений метод синтезу груп симетричних двохоперандних операцій криптографічного кодування інформації дозволяє забезпечити можливість збільшення варіативності полегшених криптоалгоритмів. Крім цього, синтез симетричних операцій криптографічного кодування, що належать різним математичним групам, підвищує криптостійкість алгоритму. Застосування двохоперандних операцій криптографічного кодування, до яких належать синтезовані операції, призводить до незначного збільшення складності, пов’язаної з реалізацією синтезу операцій як на апаратному, так і на програмному рівнях [92].

Максимальна кількість синтезованих операцій на основі базової групи трьохрозрядних одноопераднних матричних операцій становить 564480 операцій. Проте їх реалізація ускладнена відсутністю єдиного математичного апарату, який описує ці операції та методи їх синтезу й аналізу [112–114]. Тому при реалізації методу синтезу груп симетричних двохоперандних операцій криптографічного кодування інформації для дослідження та вибору операцій, необхідних для побудови систем блокового шифрування операцій в базах знань та даних, треба представляти інформацію як математичними моделями, так і таблицями істинності.

## 4.3 Інформаційна технологія моделювання та дослідження симетричних операцій криптографічного кодування та оцінка її ефективності

Розглянуті в цьому розділі приклади реалізації методу синтезу моделей симетричних двохоперандних операцій криптографічного кодування на основі кортежів симетричних одноопераднних операцій та методу синтезу груп симетричних двохоперандних операцій криптографічного кодування показали спроможність їх практичної реалізації. Слід зауважити, що наведені практичні результати синтезу дають можливість автоматизувати синтез операцій та груп симетричних двохоперандних операцій криптографічного кодування.

Отримані результати дослідження можуть бути використані для удосконалення методів побудови інформаційних систем та інформаційних технологій, які забезпечують моделювання процесів криптографічного перетворення інформації для проведення досліджень, спрямованих на розвиток теоретичних і практичних аспектів розвитку кібербезпеки і комп’ютерної інженерії [7].

Перші спроби побудови інформаційної системи та інформаційної технології для побудови і дослідження логічних функцій та одноопераднних операцій наведено в [96, 115]. Розроблена структура програмного забезпечення включала:

- блок графічного інтерфейсу користувача;
- блок логічного аналізатора команд;
- блок кодування-декодування;
- модуль запису в файл.

Враховуючи отриманий досвід використання цієї інформаційної технології, виникла необхідність її удосконалення. В основу удосконалення

будо покладено низку запатентованих технічних рішень [116–120], а також отримано нові наукові результати [101, 121–123].

За результатами удосконалення структура програмного забезпечення дослідження логічних функцій для криптографії стала включати [11, 124]:

- блок управління;
- блок синтезу логічних функцій;
- блок синтезу груп логічних функцій;
- блок аналізу логічних функцій;
- блок дослідження логічних функцій на лавиновий ефект;
- блок статистичної обробки логічних функцій;
- блок підготовки та формування результатів дослідження;
- інтерфейс користувача.

Реалізоване на основі цієї структури програмне забезпечення забезпечує побудову моделей одноопераднних операцій криптографічного перетворення на рівні таблиць істинності операцій. На основі таблиць істинності проводиться статистичний аналіз результатів перетворення інформації лише на лавиновий і строгий лавиновий ефект [125–127].

Основні підходи, покладені в основу побудови розглянутої інформаційної системи, дозволяють будувати і досліджувати лише одноопераднді операції. Реалізація пошуку моделей одноопераднних операцій на основі повного перебору не дозволяє досліджувати операції розрядністю більше трьох.

Застосування методу поєднання логічних функцій (елементарних функцій) для синтезу операцій, що також реалізується на основі повного перебору варіантів поєднання, дозволило синтезувати чотирьохрозрядні одноопераднді операції криптографічного перетворення.

Існуюча інформаційна технологія побудови та дослідження одноопераднних операцій криптографічного кодування не забезпечує

можливості синтезу двохоперандних операцій криптографічного кодування. Синтез двохоперандних операцій має низку особливостей, крім того, симетричні двохоперандні операції є підгрупою двохоперандних операцій і для їх побудови необхідні свої специфічні методи, які побудовано в дисертаційній роботі. Особливості цих методів дозволяють генерувати операції групи операцій без перебору множини симетричних і несиметричних операцій.

Метод синтезу моделей симетричних двохоперандних операцій криптографічного кодування на основі кортежів симетричних одноопераднних операцій і метод синтезу груп симетричних двохоперандних операцій криптографічного кодування базуються на використанні одноопераднних операцій криптографічного кодування, на основі яких виконується перетворення моделей двохоперандних операцій.

Реалізувати методи синтезу симетричних двохоперандних операцій без застосування одноопераднних операцій неможливо. Виходячи з цього, методи моделювання та дослідження одноопераднних операцій можна розглядати як основу інформаційної технології моделювання та синтезу симетричних двохоперандних операцій. Побудовані метод синтезу моделей симетричних двохоперандних операцій і метод синтезу груп симетричних двохоперандних операцій можна розглядати як надбудову над методами синтезу одноопераднних операцій. В свою чергу, медод синтезу груп симетричних двохоперандних операцій криптографічного кодування базується на використанні моделей симетричних двохоперандних операцій криптографічного кодування.

Ієрархічну структуру технології моделювання симетричних двохоперандних операцій криптографічного кодування зображено на рис. 4.1.

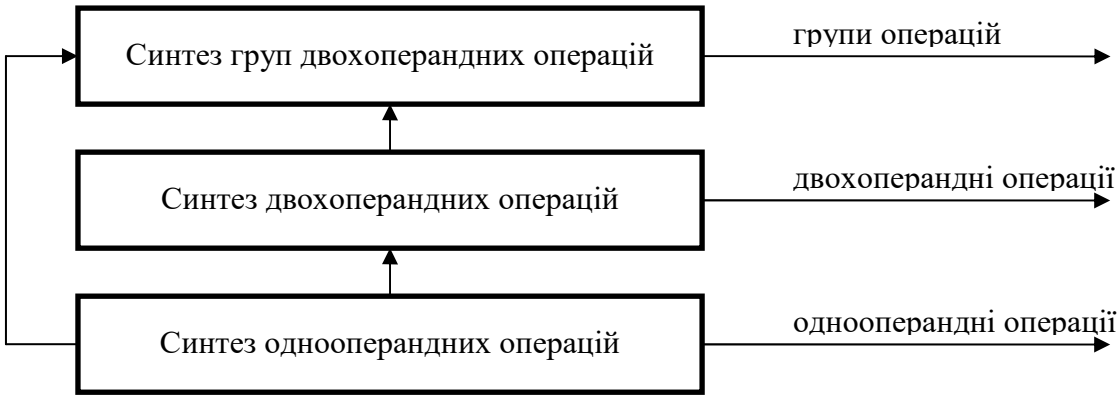


Рис. 4.1. Ієрархічна структура технології моделювання симетричних двохоперандних операцій криптографічного кодування

Наведена на рис. 4.1 структура технології моделювання симетричних двохоперандних операцій криптографічного кодування моделює три вихідні множини:

- множину одноопераднних операцій;
- множину симетричних двохоперандних операцій;
- множину груп симетричних двохоперандних операцій.

При розробці криптографічних алгоритмів використовувалися не всі синтезовані операції та згенеровані групи операцій множин. Можливість використання визначається властивостями операцій і властивостями множин операцій. Структуру системи контролю результатів синтезу зображено на рис. 4.2.

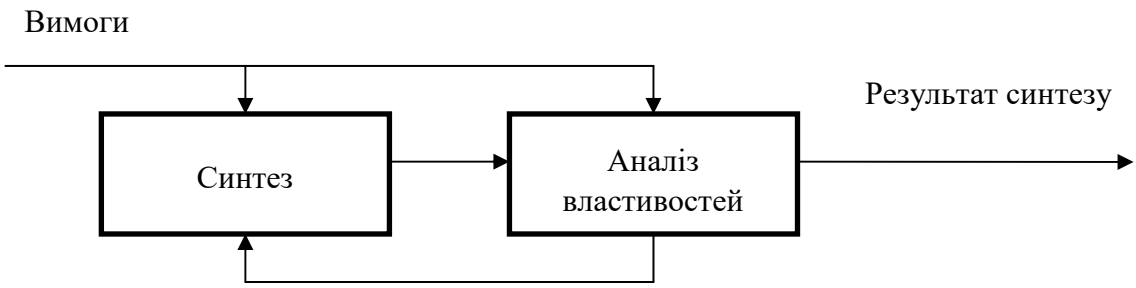


Рис. 4.2. Структура системи контролю результатів синтезу

На структурній схемі блок синтезу забезпечує синтез одноопераднних або двохоперандних операцій криптографічного кодування, або груп (послідовностей) двохоперандних операцій. Блок аналізу властивостей забезпечує контроль і фільтрацію синтезованих операцій чи їх послідовностей. Під вимогами до синтезу й аналізу будемо розуміти набори вхідних сигналів, необхідних для проведення синтезу операцій або послідовностей операцій з заданими властивостями. Результатом синтезу є операції чи послідовності операцій, які відповілають заданим властивостям.

Системи контролю результатів синтезу використовуються як для відбору результатів синтезу, так і для дослідження процесів синтезу. Основною задачею дослідження є встановлення взаємозв'язків між вимогами до синтезу і його результатами, які необхідні для практичного застосування операцій криптографічного кодування в захищених інформаційних системах критичної інфраструктури.

Потрібно відзначити, що на різних рінях ієрархічної структури технології моделювання симетричних двохоперандних операцій криптографічного кодування повинні використовуватися різні вимоги до результатів синтезу.

- На рівні синтезу одноопераднних операцій необхідно проводити аналіз синтезованих операцій на відповідність вимогам:
  - для їх самостійного використання в криптоалгоритмах;
  - для їх використання при синтезі симетричних двохоперандних операцій;
  - для їх використання при генерації груп (послідовностей) симетричних двохоперандних операцій.
- На рівні синтезу симетричних двохоперандних операцій необхідно проводити аналіз синтезованих операцій на відповідність вимогам:
  - для їх самостійного використання в криптоалгоритмах;
  - для їх використання при генерації груп (послідовностей) симетричних двохоперандних операцій.

- На рівні синтезу груп (послідовностей) симетричних двохоперандних операцій необхідно проводити аналіз синтезованих операцій на відповідність вимогам:
  - для їх самостійного використання в потокових шифрах на основі статистичного аналізу згенерованих послідовностей результатів виконання операцій. Для проведення оцінки результати перетворення інтерпретуються як псевдовипадкові послідовності і перевіряються на стійкість до лінійного криптоаналізу [128]. Перевірка проводиться на основі відомих методик за допомогою стандартизованих пакетів прикладних програм, наприклад на основі вимог статистичних тестів NIST STS (NIST Statistical test Suite). Цей набір тестів використовувався при попередньому відборі блокових шифрів у конкурсі на новий національний стандарт США.

Реалізація ієрархічної структури технології моделювання симетричних двохоперандних операцій криптографічного кодування вимагає для кожного рівня ієрархії синтезу моделей одноопераднних операцій, які відповідають різним вимогам. Крім того, частота синтезу одноопераднних операцій криптографічного кодування для реалізації функцій кожного рівня різна. Враховуючи ці особливості, які створюють додаткові горизонтальні і вертикальні зв’язки, структуру технології моделювання симетричних двохоперандних операцій криптографічного кодування можна деталізувати. Деталізовану структуру технології моделювання симетричних двохоперандних операцій криптографічного кодування зображено на рис. 4.3.

Як видно з рис. 4.3, ієрархічна структура технології моделювання симетричних двохоперандних операцій криптографічного кодування розділяється на три практично незалежні потоки, тому що на кожному рівні наявні свої, не залежні від інших рівнів, вимоги.

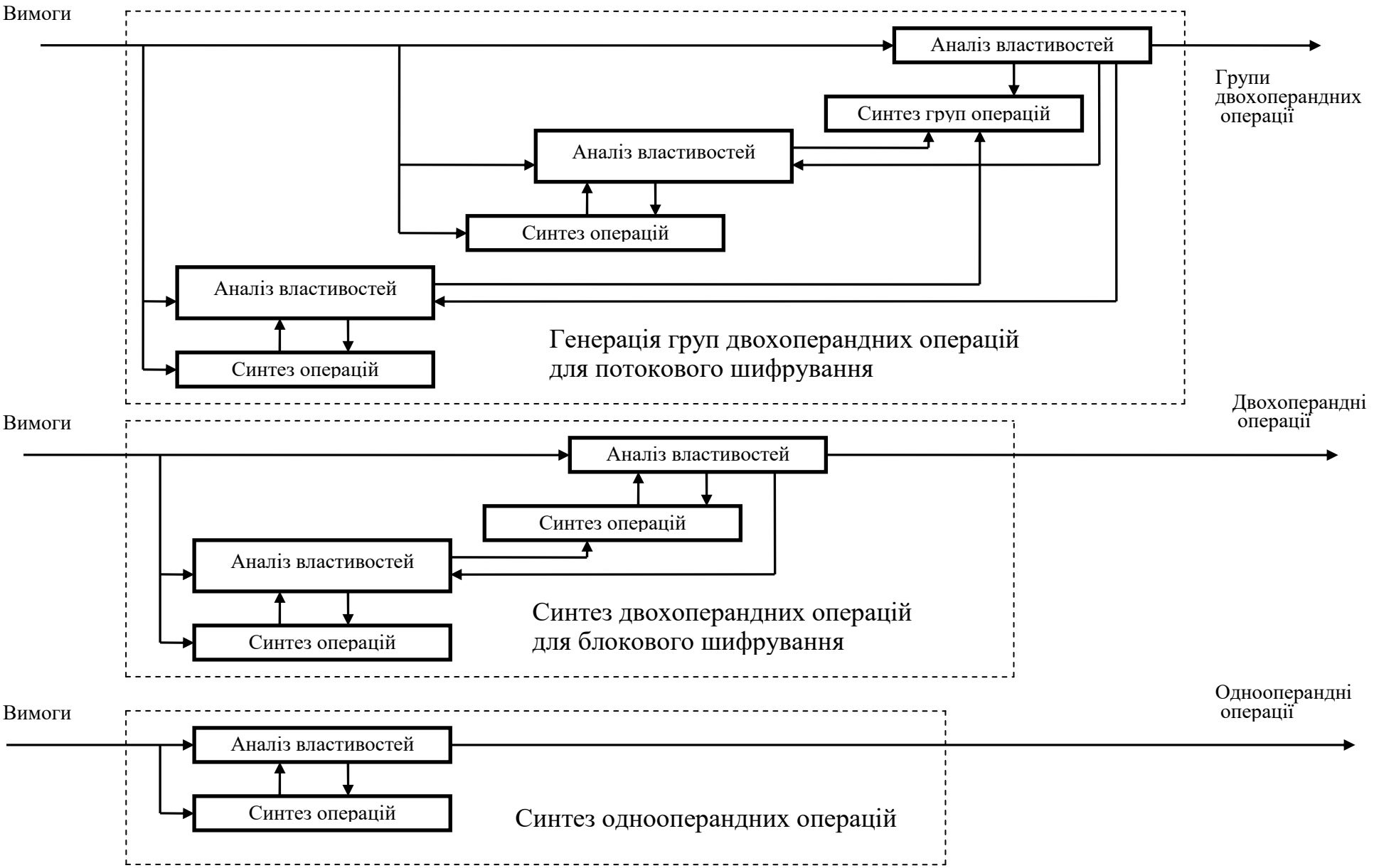


Рис. 4.3. Структура технології моделювання симетричних двохоперандних операцій криптографічного кодування

На кожному рівні наявні однакові блоки, які дублюються і реалізація яких призводить до колосального зростання обчислювальної складності.

Вирішення задачі зменшення необхідних обчислювальних ресурсів полягає в застосуванні бази даних і бази знань. База даних повинна зберігати синтезовані моделі операцій, параметри синтезу і властивості синтезованих операцій моделей. База знань повинна включати моделі реалізації методів синтезу і корінні моделі операцій. Корінними моделями симетричних операцій у цьому дослідженні названо моделі симетричних двохоперандних операцій, на основі яких проводиться синтез груп операцій. Оскільки синтез групи операцій можна реалізувати на основі будь-якої операції з цієї групи, то достатньо зберігати одну операцію.

Оскільки при дослідженні та застосуванні псевдовипадкових груп операцій важливу роль відіграють послідовності ключових операцій, то їх разом з отриманими характеристиками необхідно зберігати в базі даних.

Виходячи з цих вимог, структура інформаційної системи для реалізації технології моделювання симетричних двохоперандних операцій криптографічного кодування повинна включати:

- підсистему введення-виведення даних (моделей, параметрів, оцінок, запитів симтеми тощо), яка включає:
  - модуль введення вхідних даних і параметрів;
  - модуль виведення результатів моделювання та проміжних результатів;
  - модуль інтерфейсу неформалізованих ситуацій;
- підсистему управління режимами роботи;
- підсистему пошуку (введення) корінних симетричних двохоперандних операцій;
- базу даних;
- базу знань;
- підсистему синтезу операцій, яка включає:
  - модуль синтезу одноопераднних операцій;
  - модуль синтезу симетричних двохоперандних операцій;
  - модуль управління синтезом симетричних двохоперандних операцій;

- підсистему статистичного дослідження та класифікації операцій, яка включає:
  - модуль статистичного дослідження одноопераднних операцій;
  - модуль класифікації одноопераднних операцій;
  - модуль статистичного дослідження симетричних двохоперандних операцій;
  - модуль класифікації симетричних двохоперандних операцій;
  - модуль неформалізованих ситуацій;
- підсистему генерації послідовностей симетричних двохоперандних операцій, яка включає:
  - модуль управління стратегіями генерації послідовностей симетричних двохоперандних операцій;
  - модуль формування і зберігання траєкторії генерації;
  - модуль генерації послідовностей симетричних двохоперандних операцій;
  - модуль статистичного дослідження послідовностей симетричних двохоперандних операцій (реалізується стандартизованими пакетами прикладних програм);
- модуль формування узагальнених оцінок дослідження.

Для встановлення взаємозв’язків між модулями і підсистемами інформаційної технології необхідно проаналізувати алгоритми синтезу та аналізу на всіх трьох ієрархічних рівнях функціонування інформаційної технології.

Коректне встановлення взаємозв’язків між алгоритмами і програмами реалізації ієрархічних рівнів для ефективного функціонування інформаційної технології можливе лише при виборі єдиного підходу для представлення:

- елементарних функцій;
- одноопераднних операцій;
- двохоперандних симетричних операцій;
- послідовностей двохоперандних симетричних операцій.

Ця задача ускладнюється тим, що навіть для трьохрозрядних одноопераднних операцій криптографічного кодування не визначено єдиного математичного апарату для синтезу і дослідження операцій [113, 114, 129]. Проте всі моделі операцій криптографічного кодування можуть бути описані таблицями істинності або мінімальними диз'юнктивно-нормальними функціями, отриманими після мінімізації таблиць істинності. Як свідчать результати [114], дискретне представлення моделей операцій мінімальними диз'юнктивно-нормальними формами не завжди ефективне при їх дослідженні. На користь використання як опису моделей таблицями істинності служить відсутність класифікацій моделей навіть одноопераднних операцій розрядністю більше трьох. Розробимо алгоритми функціонування інформаційної технології моделювання симетричних двохоперандних операцій криптографічного кодування на основі переробки та опрацювання таблиць істинності операцій.

Алгоритм синтезу одноопераднних операцій криптографічного кодування зображено на рис. 4.4.

Алгоритм синтезу симетричних двохоперандних операцій криптографічного кодування для блокового шифрування зображено на рис. 4.5.

Алгоритм синтезу груп симетричних двохоперандних операцій криптографічного кодування для блокового і потокового шифрування зображено на рис. 4.6.

Наведені алгоритми функціонування інформаційної технології на різних рівнях ієрархії пов'язані між собою через базу даних та базу знань. Слід відзначити, що не всі елементи структури інформаційної системи в явному вигляді прописані (задіяні) в алгоритмах функціонування. Це рішення було прийняте на основі наступного:

- зменшення складності програмного забезпечення;
- зменшення часу виконання завдань моделювання та оцінки результатів, адже він суттєво впливає на ефективність проведення наукових та прикладних досліджень;

- необхідність експлуатації цієї системи лише висококваліфікованими науковими фахівцями в галузях інформаційних систем, інформаційних технологій, телекомунікацій та кібербезпеки;
- високе інтелектуальне навантаження при формалізації завдань та обробки їх результатів.

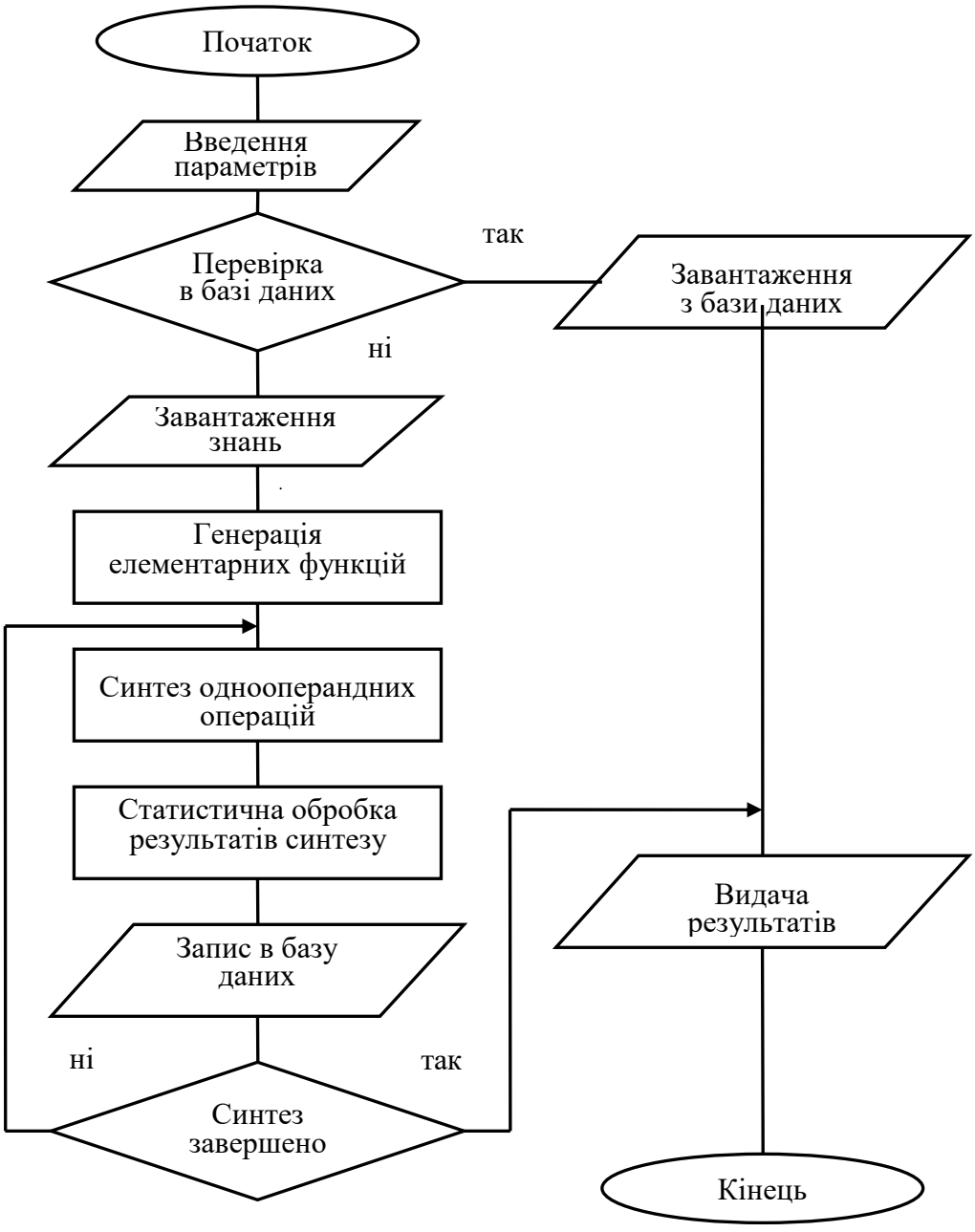


Рис. 4.4. Алгоритм синтезу одноопераднних операцій криптографічного кодування

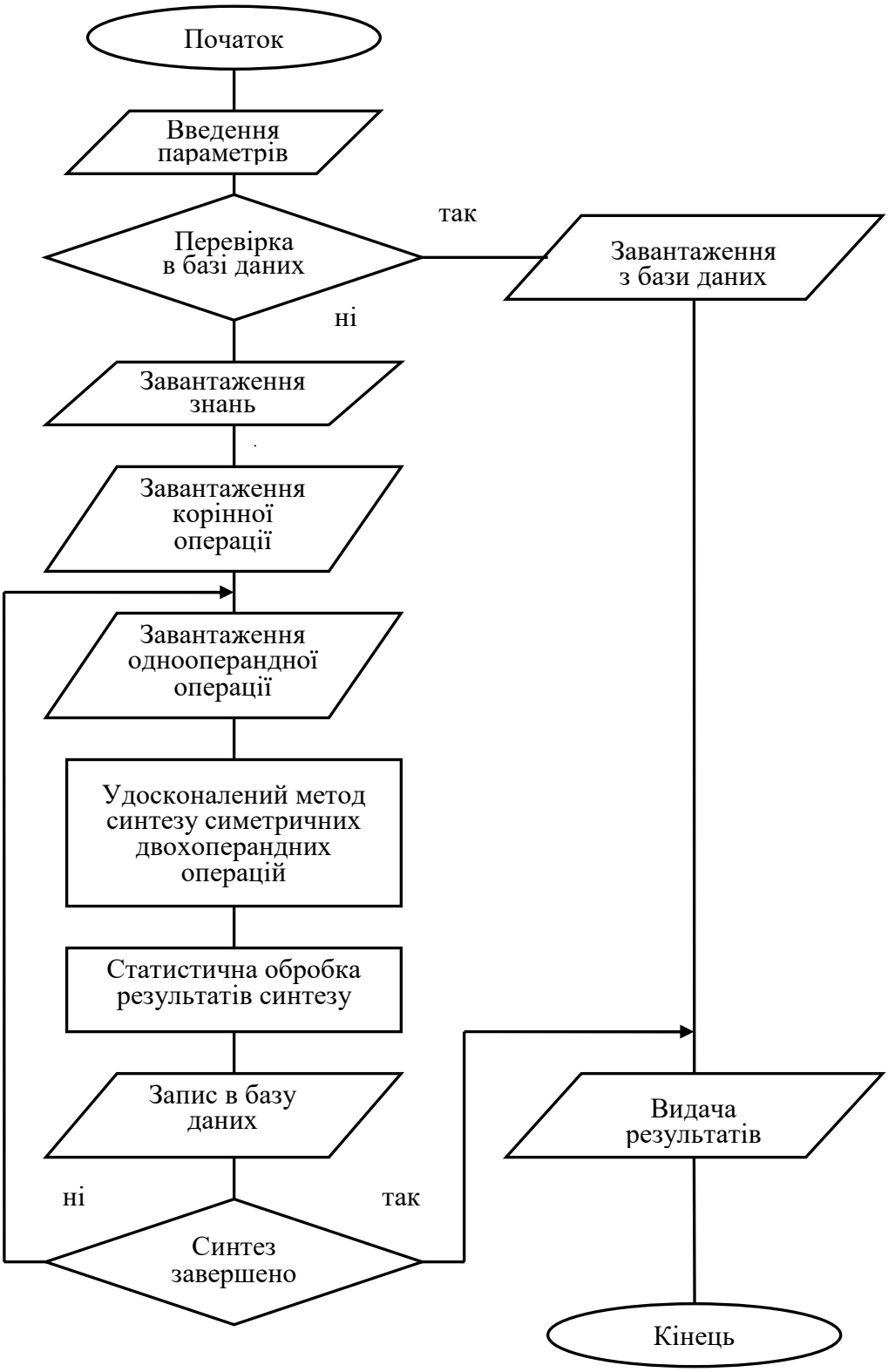


Рис. 4.5. Алгоритм синтезу симетричних двохоперандних операцій криптографічного кодування для блокового шифрування

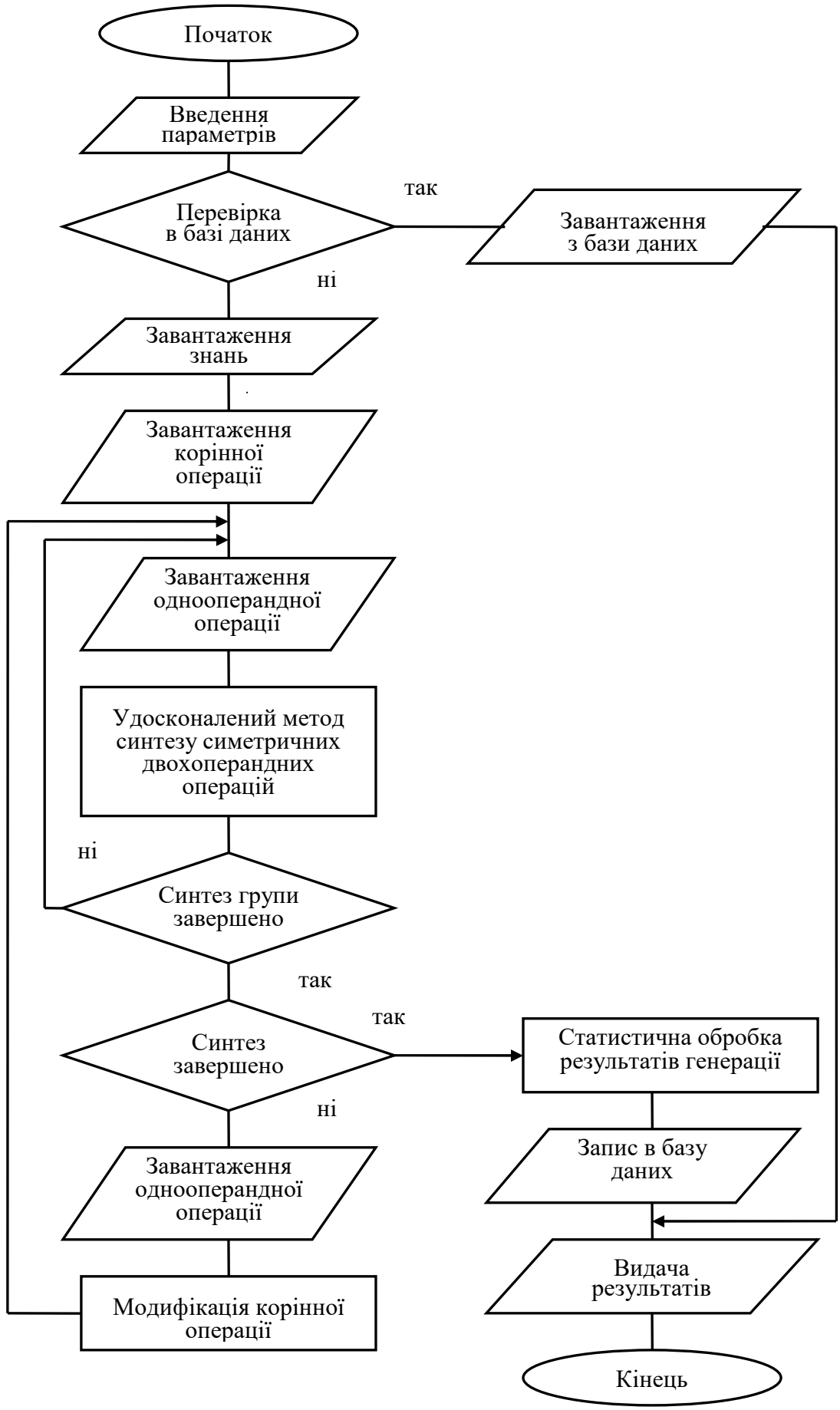


Рис. 4.6. Алгоритм синтезу груп симетричних двохоперандних операцій криптографічного кодування для блокового і потокового шифрування

Ця інформаційна система забезпечує вирішення значної частини завдань моделювання та оцінки результатів, які виникають у процесі дослідження симетричних двохоперандних операцій криптографічного кодування. Впроваджені при розробці інформаційної технології нові методи синтезу операцій та їх груп дозволяють значно зменшити негативний вплив комбінаторного зростання кількості моделей операцій криптографічного кодування при збільшенні розрядності.

**Висновки до розділу 4**

Удосконалено методи побудови інформаційних систем та інформаційних технологій моделювання і дослідження операцій криптографічного кодування на основі розроблених методів синтезу моделей та математичних груп моделей симетричних двохоперандних операцій криптографічного кодування шляхом їх використання як надбудови над методами побудови одноопераднних операцій, що забезпечило можливість автоматизації генерації та дослідження симетричних двохоперандних операцій і послідовностей симетричних двохоперандних операцій для застосування в захищених інформаційних системах критичної інфраструктури:

1. Досліджено особливості реалізації методу синтезу моделей симетричних двохоперандних операцій криптографічного кодування на основі кортежів симетричних одноопераднних операцій для систем блокового шифрування. Наведено приклади побудови моделей з трьохрозрядних одноопераднних матричних операцій криптографічного кодування. Ці операції можуть бути використані для побудови груп симетричних двохоперандних операцій.

2. Серед симетричних двохоперандних операцій криптографічного кодування особливе місце займають операції, які допускають перестановку операндів місцями (комутативні операції). На основі отриманих практичних результатів запропоновано алгоритм пошуку симетричних комутативних двохоперандних операцій. Розглянуто реалізацію методу синтезу груп симетричних двохоперандних операцій криптографічного кодування

інформації для систем потокового шифрування на прикладі однієї вибраної симетричної комутативної операції. Встановлено особливості реалізації цього методу при використанні в інформаційній технології моделювання операцій.

3. Розроблені методи синтезу симетричних двохоперандних операцій та груп операцій послужили основою для удосконалення методів побудови інформаційних систем та інформаційних технологій моделювання і дослідження операцій криптографічного кодування. Розроблена ієрархічна структура інформаційної системи забезпечує функціонування інформаційної технології моделювання симетричних двохоперандних операцій криптографічного кодування. Наведені алгоритми функціонування інформаційної технології на різних рівнях ієрархії пов’язані між собою через базу даних та базу знань. Це забезпечило зменшення негативного впливу комбінаторного зростання кількості моделей операцій криптографічного кодування при збільшенні їх розрядності. Побудована інформаційна технологія вперше дозволила автоматизувати цілеспрямований процес синтезу та дослідження моделей симетричних двохоперандних операцій криптографічного кодування.

4. Результати розділу опубліковано в [3, 4, 5, 7, 10, 11].

# ВИСНОВКИ

У дисертаційному дослідженні вирішено важливу науково-технічну задачу підвищення продуктивності наукових досліджень процесів покращення захищеності інформаційних систем критичної інфраструктури шляхом створення нових методів моделювання та аналізу симетричних операцій криптографічного кодування:

1. Розроблено метод синтезу моделей симетричних двохоперандних операцій криптографічного кодування. В основу розробленого методу покладено об’єднання кортежів таблиць істинності симетричних одноопераднних операцій, описаних елементарними функціями. Для побудови дискретної моделі симетричної двохоперандної операції криптографічного кодування проводиться мінімізація коефіцієнтів наявності розрядів першого операнда в наборах елементарних функцій симетричних одноопераднних операціях з подальшим об’єднанням відповідних елементарних функцій на основі результатів мінімізації в симетричну двохоперандну операцію. Побудовані математичні моделі симетричних двохоперандних операцій забезпечують простір для їх практичної реалізації як на програмному, так і на апаратному рівнях. Отримані моделі симетричних двохоперандних операцій служать фундаментом для подальшого моделювання операцій з точністю до перестановки та формування бази даних моделей для автоматизації досліджень операцій криптографічного захисту інформації. В базах даних симетричні двохоперандні операції можуть бути представленими як дискретними моделями, так і таблицями істинності.

2. Розроблено метод синтезу груп моделей симетричних двохоперандних операцій криптографічного кодування для блокового шифрування на основі заданої симетричної двохоперандної операції. Для побудови симетричної двохоперандної операції криптографічного кодування з точністю до перестановки виконується перетворення моделі заданої операції одноопераднною операцією. Це перетворення приводить до побудови нової симетричної двохоперандної операції, яка має іншу таблицю істинності й описується іншою математичною моделлю. При послідовному застосуванні над

заданою симетричною двохоперандною операцією групи одноопераднихоперацій буде побудована група симетричних двохоперандних операцій криптографічного кодування. Синтезовані операції цієї групи, крім їх симетричності, забезпечують можливість перестановки інформації між операндами (комутативність операцій). Симетричність і комутативність двохоперандних операцій значно розширюють можливості їх практичного застосування в захищених інформаційних системах критичної інфраструктури при реалізації блокового шифрування.

3. Удосконалено методи побудови інформаційних систем та інформаційних технологій моделювання і дослідження операцій криптографічного кодування. В основу удосконалення покладено розроблені методи синтезу операцій і груп симетричних двохоперандних операцій криптографічного кодування. Запропоновано ієрархічну структуру інформаційної технології моделювання і дослідження операцій криптографічного кодування, де розроблені методи синтезу симетричних двохоперандних операцій використовуються як надбудова над відомими методами побудови одноопераднихоперацій. Забезпечення вертикальних і горизонтальних зв’язків в удосконаленій інформаційній технології моделювання і дослідження операцій криптографічного кодування реалізується на основі використання бази даних і бази знань. У базі даних зберігаються моделі одно- і двохоперандних операцій та результати їх досліджень. База знань зберігає формалізовані методи побудови та перебудови операцій і траєкторії генерації псевдовипадкових послідовностей операції криптоперетворення. Удосконалення методів побудови інформаційних систем та інформаційних технологій забезпечило можливість автоматизації генерації та дослідження симетричних двохоперандних операцій і послідовностей симетричних двохоперандних операцій для застосування в захищених інформаційних системах критичної інфраструктури.

4. Практична цінність дисертаційного дослідження полягає в застосуванні отриманих результатів для побудови інформаційної технології моделювання і дослідження симетричних операцій криптографічного кодування та оцінки

ефективності їх застосування. Основною метою застосування розробленої технології є визначення наборів багаторозрядних симетричних двохоперандних операцій, які, ставши багатоваріантною альтернативою додавання за модулем, забезпечать підвищення якості блокових шифрів для захищених інформаційних систем критичної інфраструктури. Побудовані автором алгоритми реалізації розроблених методів використано при створенні елементів програмного забезпечення запропонованої інформаційної технології. Отримані результати дослідження дозволили синтезувати 96 симетричних двохрозрядних двохоперандних операцій, які становлять 4 групи по 24 операції в кожній. Лише на основі трьохрозрядних одноопераднних матричних операцій було синтезовано і досліджено 18816 симетричних трьохрозрядних двохоперандних операцій, які становлять 14 груп по 1344 операції у кожній.

Результати дисертаційного дослідження впроваджено в навчальний процес Черкаського державного технологічного університету на кафедрі інформаційних технологій проектування і кафедрі інформаційної безпеки та комп’ютерної інженерії, та у виробничу діяльність ПАТ «Черкасиавтотранс».

# СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. 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

2. 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

3. Прокопенко Т. О., Можаєв М. О., Рудницький С. В., Рудницька Ю. В. Програмування режиму ненавантаженого резервування у комп'ютерних системах критичного застосування. *Вісник Черкаського державного технологічного університету*. Черкаси: ЧДТУ, 2020. № 4. С. 77–83. DOI: https://doi.org/10.24025/2306-4412.4.2020.221845

4. 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.

5. Lada N., Rudnytska Yu. Implementation of a method for synthesizing groups of symmetric double-operand operations of cryptographic information coding for block encryption systems. *Innovative Technologies and Scientific Solutions for Industries / Information Technology*. 2022. No. 2 (20). DOI: https://doi.org/10.30837/ITSSI.2022.20.035

6. Rudnytskyi V., Babenko V., Lada N., Tarasenko Ya., Rudnytska Yu. 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. P. 182–194. ISSN 1613-0073 **(Scopus)**

7. Prokopenko T., Tarasenko Ya., Lavdanska O., Rudnytskyi S., Rudnytska Yu. Developing the comprehensive technology for alternative management of complex organizational and technological objects in the conditions of cyber threats. *Workshop on Cybersecurity Providing in Information and Telecommunication Systems (CPITS II 2021)*, Oct. 26, 2021. Kyiv, Ukraine: CEUR Workshop Proceedings, 2022. P. 170–181. ISSN 1613-0073 **(Scopus)**

8. Лада Н. В., Рудницька Ю. В. Класифікація груп несиметричних двохоперандних операцій криптоперетворення інформації на основі перестановочних схем їх синтезу. *Проблеми інформатизації: матеріали Шостої міжнар. наук.-техн. конф.*: тези доп., Черкаси – Баку – Бельсько-Бяла – Харків, 14–16 листоп. 2018 р. Черкаси: ЧДТУ; Баку: ВА ЗС АР, Бельсько-Бяла: УТіГН, Харків: НТУ «ХПІ», 2018. С. 11.

9. 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.

10. 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.

11. 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.

12. 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.

13. Загрози національній безпеці України. Термінологічний словник з питань запобігання та протидії легалізації (відмиванню) доходів, одержаних злочинним шляхом, фінансуванню тероризму, фінансуванню розповсюдження зброї масового знищення та корупції / А. Г. Чубенко, М. В. Лошицький, Д. М. Павлов та ін. Київ: Ваіте, 2018. С. 265. ISBN 978-617-7627-10-3

14. Про рішення Ради національної безпеки і оборони України від 5 травня 2014 року «Про заходи щодо зміцнення національної безпеки України у воєнній сфері»: Указ Президента України № 453/2014.

15. Загрози критичній інфраструктурі та їх вплив на стан національної безпеки (моніторинг реалізації Стратегії національної безпеки): аналіт. записка Нац. ін-ту стратег. дослідж. Берез. 2017 р.

16. Єрменчук О. П. Основні підходи до організації захисту критичної інфраструктури в країнах Європи: досвід для України: монографія. Дніпро: Дніпроп. держ. ун-т внутр. справ, 2018. 180 с.

17. Зелена книга з питань захисту критичної інфраструктури в Україні: зб. матеріалів міжнар. експерт. нарад / упоряд. Д. С. Бірюков, С. І. Кондратов; за заг. ред. О. М. Суходолі. Київ: НІСД, 2016. 176 с.

18. Про невідкладні заходи з нейтралізації загроз енергетичній безпеці України та посилення захисту критичної інфраструктури: рішення Ради нац. безпеки і оборони України від 16 лют. 2017 р.: введ. в дію Указом Президента України від 16 лют. 2017 р. № 37/2017.

19. Про удосконалення заходів забезпечення захисту об’єктів критичної інфраструктури: рішення Ради нац. безпеки і оборони України від 29 груд. 2016 р.: введ. в дію Указом Президента України від 16 січ. 2017 р. № 8.

20. Богуш В. М., Юдін О. К. Інформаційна безпека держави. Київ: МК-Прес, 2005. 432 с.

21. Політика інформаційної безпеки: підручник / О. Л. Голубенко, В. О. Хорошко, О. С. Петров та ін. Луганськ: Вид-во СНУ ім. В. Даля, 2009. 300 с.

22. Єжова Л. Ф., Мачалін І. О., Невойт Я. В., Хорошко В. О. Управління інформаційною безпекою: в 2 т. Київ: Вид-во ДУІКТ, 2011. 236 с.

23. Жиляєв І. Б., Семенченко А. І. Організаційно-правові механізми розвитку національної системи кібербезпеки України: стан та перспективи. *Стратегічні пріоритети*. 2017. № 4. С. 55–61.

24. Концептуальні засади впровадження організаційно-технічної моделі кіберзахисту України / О. Потій, А. Семенченко, Д. Дубов та ін. *Захист інформації.* Січ.-берез. 2021. Т. 23. № 1. С. 42–55.

25. Про інформацію: Закон України за станом на 02 жовт. 1992 р. № 2657-XII / Верховна Рада України (редакція станом на 15 черв. 2022 р.).

26. Про захист інформації в інформаційно-телекомунікаційних системах: Закон України за станом на 05 лип. 1994 р. № 80/94-ВР / Верховна Рада України (редакція станом на 01 лип. 2022 р.).

27. ДСТУ 3396.1-96 Захист інформації. Технічний захист інформації. Порядок проведення робіт.

28. ДСТУ 3396.2-97 Захист інформації. Технічний захист інформації. Терміни та визначення.

29. ДСТУ 2226-93 Автоматизовані системи. Терміни та визначення.

30. Положення про дозвільний порядок проведення робіт з технічного захисту інформації для власних потреб: затв. наказом ДСТСЗІ СБ України від 23 лют. 2002 № 9 і зареєстр. в М-ві юстиції України 13 берез. 2002 р. за № 245/6533.

31. Про затвердження переліку обов’язкових етапів робіт під час проектування, впровадження та експлуатації систем і засобів автоматизованої обробки та передачі даних: постанова Кабінету Міністрів України від 04 лют. 1998 р. № 121.

32. Положення про державну експертизу в сфері технічного захисту інформації: затв. наказом ДСТСЗІ СБ України від 29 груд. 1999 р. № 62 і зареєстр. в М-ві юстиції України 24 січ. 2000 р. за № 40/4261.

33. Дрейс Ю. О. Аналіз базової термінології і негативних наслідків кібератак на інформаційно-телекомунікаційні системи об’єктів критичної

інфраструктури держави. *Захист інформації*. НАУ, 2017. Т. 19. ISSN 2410-7840. DOI: https://doi.org/10.18372/2410-7840.19.11900

34. Мохор В., Цуркан В., Бакалинський О., Дорогий Я. Метод концептуалізування системних досліджень систем управління інформаційною безпекою. *Information Technology and Security*. 2020.

35. Згуровський М. З., Панкратова Н. Д. Основи системного аналізу. Київ: Вид. дім ВНУ, 2007. 544 с.

36. Гончар С. Ф. Оцінювання ризиків кібербезпеки інформаційних систем об'єктів критичної інфраструктури: монографія. Київ: Альфа реклама, 2019. 176 с.

37. Салієва О. В., Яремчук Ю. Є. Дослідження достовірності впливу загроз на рівень захищеності комп'ютерної мережі, визначеного за сценарним моделювання на основі когнітивного підходу. *Вісник Вінницького політехнічного інституту.* 2020. № 4. С. 98–104.

38. Яремчук Ю. Є., Салієва О. В. Оцінювання рівня захищеності об'єкта критичної інфраструктури. *Інформаційно-телекомунікаційні системи і технології та кібербезпека: нові виклики, нові завдання*: матеріали наук.-практ. конф. Київ, 2020. С. 280–281.

39. Ушатов В., Сєвєрінов О. В. Проблеми оперативного виявлення і реагування на інциденти інформаційної безпеки. *Global Cyber Security Forum*: матеріали Першого міжнар. наук.-практ. форуму, 14–16 листоп. 2019 р. Харків: ХНУРЕ, 2019. С. 104–105.

40. Козлова К. В., Хорошко В. О. Кількісна оцінка захисту радіоелектронних об'єктів. *Захист інформації*: зб. наук. пр. 2007. № 1. С. 30–32.

41. Сучасні інформаційні технології в кібербезпеці: монографія / А. С. Довбиш, В. К. Ободяк, І. В. Шелехов та ін.; за ред. В. К. Ободяка, І. В. Шелехова. Суми: Сумський держ. ун-т, 2021. 348 с.

42. Гончар С. Ф., Комаров М. Ю. Безпека інформації в комп'ютерних системах та мережах об'єктів критичної інфраструктури: монографія / Нац. акад. наук України, Ін-т проблем моделювання в енергетиці ім. Г. Є. Пухова. Київ, 2021. 120 с.

43. Дудикевич В. Б., Опірський І. Р. Аналіз моделей захисту інформації в інформаційних мережах держави. *Системи обробки інформації*. 2016. Вип. 4. С. 86–89.

44. Опірський І. Р. Класифікація моделей захисту інформації в інформаційних мережах держави. *Науковий вісник НЛТУ України*. 2015. Вип. 25.10. С. 329–335.

45. ДСТУ 7624:2014 "Інформаційні технології. Криптографічний захист інформації. Алгоритм симетричного блокового перетворення"; http://uas.org.ua/ua/services/standartizatsiya

46. ДСТУ ISO/IEC 18033:2015 (ISO/IEC 18033-3:2010, ILD) "Інформаційні технології. Методи захист. Алгоритми шифрування. Частина 3. Блокові шифри"; http://uas.org.ua/ua/services/standartizatsiya

47. ДСТУ ГОСТ 28147:2009 "Системы обработки информации. Защита криптографическая. Алгоритмы криптографического преобразования; http://uas.org.ua/ua/services/standartizatsiya

48. ДСТУ 8845:2019 "Інформаційні технології. Криптографічний захист інформації. Алгоритм симетричного потокового перетворення"; http://uas.org.ua/ua/services/standartizatsiya

49. ДСТУ ISO/IEC 18033:2015 (ISO/IEC 18033-3:2010, ILD) "Інформаційні технології. Методи захист. Алгоритми шифрування. Частина 4. Потокові шифри"; http://uas.org.ua/ua/services/standartizatsiya

50. ДСТУ 4145-2002 "Інформаційні технології. Криптографічний захист інформації. Цифровий підпис, що ґрунтується на еліптичних кривих. Формування та перевіряння"; http://uas.org.ua/ua/services/standartizatsiya

51. ДСТУ 7564:2014 "Інформаційні технології. Криптографічний захист інформації. Функція ґешування"; http://uas.org.ua/ua/services/standartizatsiya

52. Горбенко І. Д. Симетричний блоковий шифр "Калина" – новий національний стандарт України / І. Д. Горбенко, Р. В. Олійников, О. В. Казимиров, В. І. та ін. *Радиотехника*. 2015. - Вып. 181. С. 5-22.

53. Horváth M., Buttyán L. Cryptographic obfuscation. A survey. SpringerBriefs in computer science. *Springer International Publishing*. Cham: Springer, 2020. P. 107.

DOI: https://doi.org/10.1007/978-3-319-98041-6

54. Mohamed K. S. New frontiers in cryptography. Quantum, blockchain, lightweight, chaotic and DNA. *Springer International Publishing*. Cham: Springer, 2020. P. 104. DOI: https://doi.org/10.1007/978-3-030-58996-7

55. Selected Areas in Cryptography: 27th International Conference, Oct. 21–23 / O. Dunkelman, M. J. Jacobson, Jr., C. O'Flynn (Eds). Halifax, NS, Canada (Virtual Event). Revised Selected Papers, *Springer International Publishing*. Cham: Springer, 2020. P. 722. DOI: https://doi.org/10.1007/978-3-030-81652-0

56. Reverse engineering iot devices: Effective techniques and methods / O. Shwartz, Y. Mathov, M. Bohadana et al. *IEEE Internet of Things Journal*. 2018. P. 1–1.

57. Biryukov A., Perrin L. State of the art in lightweight symmetric cryptography. *Cryptology ePrint Archive*. 2017. Report 2017/511. URL: http://eprint.iacr.org/2017/511

58. McKay K. A., Bassham L., Turan M. S., Mouha N. Nistir 8114 - report on lightweight cryptography. 2016.

59. Shannon C. Communication theory of secrecy systems. *Bell System Technical Journal*. 1949. Vol. 28 (4). P. 656–715.

60. ISO/IEC 29192-1:2012. Information Technology – Security Techniques – Lightweight Cryptography – Part 1: General. 2012. URL: http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=56425

61. ISO/IEC 29192-2:2012. Information Technology – Security Techniques – Lightweight Cryptography – Part 2: Block Ciphers. 2012. URL: http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=56552 NISTIR 8114 REPORT ON LIGHTWEIGHT CRYPTOGRAPHY 19. This publication is available free of charge from: https://doi.org/10.6028/NIST.IR.8114

62. ISO/IEC 29192-3:2012. Information Technology – Security Techniques – Lightweight Cryptography – Part 3: Stream Ciphers. 2012. URL: http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=56426

63. Hatzivasilis G., Fysarakis K., Papaefstathiou I., Manifavas Ch. A review of lightweight block ciphers. *J. Cryptographic Engineering*. 2018. Vol. 8 (2). P. 141–184.

DOI: https://doi.org/10.1007/s13389-017-0160-y

64. Pushing the limits: A very compact and a threshold implementation of AES / A. Moradi, A. Poschmann, S. Ling et al. *Advances in Cryptology – EUROCRYPT*, May 15–19, 2011 / Kenneth G. Paterson (Ed.). Vol. 6632 of Lecture Notes in Computer Science. Tallinn, Estonia: Springer, 2011. P. 69–88.

65. Berger T. P., Francq Ju., Minier M., Gaël T. Extended generalized feistel networks using matrix representation to propose a new lightweight block cipher: Lilliput. *IEEE Trans. Computers*. 2016. Vol. 65 (7). P. 2074–2089.

66. Journault A., Standaert F.-X., Varici K. Improving the security and efficiency of block ciphers based on ls-designs. *Des. Codes Cryptography*. 2017. Vol. 82 (1–2). P. 495–509. URL: https://link.springer.com/article/10.1007/s10623-016-0193-8

67. Rogaway Ph., Bellare M., Black J. Ocb: A block-cipher mode of operation for efficient authenticated encryption. *ACM Transactions on Information and System Security*. 2003. Vol. 6 (3). P. 365–403.

68. Manifavas Ch., Hatzivasilis G., Fysarakis K., Papaefstathiou Ya. A survey of lightweight stream ciphers for embedded systems. *Security and Communication Networks*. 2016. Vol. 9 (10). P. 1226–1246. DOI: https://doi.org/10.1002/sec.1399

69. Hummingbird: ultra-lightweight cryptography for resource-constrained devices / D. Engels, X. Fan, G. Gong et al. *Financial Cryptography and Data Security (FC 2010)*. Springer, 2010. Vol. 6054. P. 3–18. DOI: https://doi.org/10.1007/978-3-642-14992-4_2

70. Meng Th. X., Buchanan W. Lightweight Cryptographic Algorithms on Resource-Constrained Devices. Preprints. 2020. DOI: https://doi.org/10.20944/PREPRINTS202009.0302.V1

71. Juels A., Weis S. A. Authenticating pervasive devices with human protocols. *Advances in Cryptology (CRYPTO 2005)*. Springer, 2005. P. 293–308.

72. Avoine G., Hernandez-Castro J. Security of Ubiquitous Computing Systems. Selected Topics. Springer, 2021. 265 p. DOI: https://doi.org/10.1007/978-3-030-10591-4

73. Aumasson J.-P., Henzen L., Meier W., Naya-Plasencia M. Quark: A

lightweight hash. *Journal of Cryptology*. 2013. Vol. 26 (2). P. 313–339. DOI: https://doi.org/10.1007/s00145- 012-9125-6

74. Feldhofer M., Rechberger C. A case against currently used hash functions in rfid protocols. *On the Move to Meaningful Internet Systems (OTM 2006)*, Oct. 29–Nov. 3, 2006. Montpellier, France, 2006. P. 372–381.

75. Li T., Wu H., Wang X., Bao F. Sensec design. i2r sensor network flagship project (snfp: security part): Technical report-tr v1.0, 2005.

76. Tulp: A family of lightweight message authentication codes for body sensor networks / Zh. Gong, P. H. Hartel, S. Nikova et al. *J. Comput. Sci. Technol*. 2014. Vol. 29 (1). P. 53–68.

77. The secrets of profiling for side-channel analysis: Feature selection matters / S. Picek, A. Heuser, A. Jovic et al. *IACR Cryptology ePrint Archive 2017*. P. 1110.

78. Post-Quantum Cryptography / D. J. Bernstein, J. Buchmann, E. Dahmen (Eds). Berlin – Heidelberg: Springer-Verlag, 2009. P. 246. DOI: https://doi.org/10.1007/978-3-540-88702-7

79. Shang T., Liu J. Secure Quantum Network Coding Theory. Singapore: Springer, 2020. P. 283, DOI: https://doi.org/10.1007/978-981-15-3386-0

80. Grosso V., Leurent G., Standaert F.-X., Varici K. LS-designs: Bitslice encryption for efficient masked software implementations. *Fast Software Encryption (FSE)*, March 3–5, 2014 / C. Cid, C. Rechberger (Eds). Vol. 8540 of Lecture Notes in Computer Science. London, UK: Springer, 2015. P. 18–37.

81. Pessl P., Hutter M. Pushing the limits of sha-3 hardware implementations to fit on rfid. *Cryptographic Hardware and Embedded Systems (CHES 2013)*, Aug. 20–23, 2013. Santa Barbara, CA, USA, 2013. P. 126–141.

82. Rabbit: A new high-performance stream cipher / M. Boesgaard, M. Vesterager, T. Pedersen et al. *Fast Software Encryption (FSE 2003)*, Febr. 24–26, 2003 / T. Johansson (Ed.). Vol. 2887 of Lecture Notes in Computer Science. Lund, Sweden: Springer, 2003. P. 307–329.

83. Liu L., Wang B., Wei Sh. Reconfigurable Cryptographic Processor. Singapore: Springer, 2018. P. 386. DOI: https://doi.org/10.1007/978-981-10-8899-5

84. Cagli E., Dumas C., Prouff E. Convolutional neural networkswith data

augmentation against jitter-based countermeasures - profiling attacks without preprocessing. *Cryptographic Hardware and Embedded Systems (CHES 2017)*: Proc. 19th Int. Conf., Sept. 25–28, 2017. Taipei, Taiwan, 2017. P. 45–68.

85. Khovratovich D., Rechberger C. The local attack: Cryptanalysis of the authenticated encryption scheme ale. *Selected Areas in Cryptography (SAC 2013).* Burnaby, Canada. Aug. 14–16, 2013. P. 174–184.

86. FELICS – fair evaluation of lightweight cryptographic systems / D.-D. Dinu, A. Biryukov, J. Großschädl et al. *NIST Workshop on Lightweight Cryptography 2015*. National Institute of Standards and Technology (NIST), 2015.

87. Lu Y., Meier W., Vaudenay S. The conditional correlation attack: A practical attack on bluetooth encryption. *Advances in Cryptology (CRYPTO 2005)*, Aug. 14–18, 2005. Santa Barbara, California, USA, 2005. P. 97–117.

88. Enhancing power analysis attacks against cryptographic devices / M. Bucci, L. Giancane, R. Luzzi et al. *IET Circuits, Devices & Systems*. 2008. Vol. 2 (3). P. 298–305.

89. Рудницький В. М., Пантелєєва Н. М., Бабенко В. Г. Визначення множини логічних функцій для синтезу цифрових пристроїв систем захисту інформації. *Системи управління, навігації та зв'язку*: зб. наук. пр. Київ, 2008. Вип. 4 (8). С. 155–157.

90. 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. Харків: ХУПС ім. І. Кожедуба, 2011. № 2 (6). С. 112–114.

91. Рудницький В. М., Мельник О. Г, Сисоєнко С. Г, Пустовіт М. О. Дослідження методу підвищення стійкості комп'ютерних криптографічних алгоритмів. *Вісник Черкаського державного технологічного університету*. Черкаси: ЧДТУ, 2017. № 3. С. 5–9.

92. Rudnytskyi V., Opirskyy I., Melnyk O., Pustovit M. The implementation of strict stable cryptographic coding operations. *Сучасні інформаційні системи*: щокварт. наук.-техн. журн. Харків: НТУ «ХПІ», 2019. Т. 3. № 4. С. 109–114.

93. Рудницький В. М., Опірський І. Р., Мельник О. Г, Пустовіт М. О.

Синтез групи операцій строгого стійкого криптографічного кодування для побудови потокових шифрів. *Безпека інформації*: наук. журн. 2018. Т. 24. № 3. С. 195–200.

94. Рудницький В. М., Шувалова Л. А., Нестеренко О. Б. Побудова примітивів строгого стійкого кодування мінімальної складності. *Вісник Черкаського державного технологічного університету.* Черкаси: ЧДТУ, 2018. № 1. С. 21–26.

95. Рудницький В. М., Миронець І. В., Бабенко В. Г. Методологія підвищення оперативності доступу до конфіденційних інформаційних ресурсів. *Системи обробки інформації*: зб. наук. пр. Харків: Харк. ун-т Повітряних Сил ім. Івана Кожедуба, 2010. Вип. 5 (86). С. 15–19.

96. Бабенко В. Г., Рудницький В. М., Дахно Т. В. Технологія визначення спеціальних логічних функцій для систем захисту інформації. *Вісник інженерної академії України.* 2007. Вип. 3–4. С. 64–67.

97. Рудницький В. М., Шувалова Л. А., Нестеренко О. Б. Синтез операцій криптографічного перетворення за критерієм строгого стійкого кодування. *Вісник інженерної академії України:* часопис. Київ, 2016. Вип. 3. С. 105–108.

98. Рудницький В. М., Бабенко В. Г. Модель уніфікованого пристрою криптографічного перетворення інформації. *Системи обробки інформації*: зб. наук. пр. Харків, 2009. Вип. 1 (9). С. 173–177.

99. 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.

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

101. Рудницький В. М., Пантелєєва Н. М., Бабенко В. Г. Моделювання логічного пристрою для систем захисту інформації. *Проблеми і перспективи розвитку банківської системи України*: зб. наук. пр. Суми, 2006. Т. 18. С. 185–190.

102. 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.

103. 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.

104. 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.

105. 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.

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

107. Побудова двохрозрядних двохоперандних операцій строгого стійкого криптографічного кодування / В. М. Рудницький, Н. В. Лада, І. М. Федотова-Півень та ін. *Системи управління, навігації та зв'язку*. Полтава: ПНТУ, 2018. Вип. 6 (52). С. 113–115.

108. 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. URL: http://suchasnaspetstehnika.com/journal/ukr/2019_4/6.pdf

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

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

111. Криптографическое кодирование: кол. монография / под ред. В. Н. Рудницкого, В. Я. Мильчевича. Харьков: Щедрая усадьба плюс, 2014.

240 с.

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

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

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

115. Бабенко В. Г., Рудницький В. М., Дахно Т. В. Результати моделювання логічних функцій для криптографії. *Сучасні інформаційні системи. Проблеми та тенденції розвитку*: зб. матеріалів Другої міжнар. наук. конф. Харків: ХНУРЕ, 2007. С. 421–422.

116. Пристрій для виконання логічних операцій одної змінної в двійково-четвірковій системі числення: пат. 27818 Україна. МПК H03M 13/00. № u 2007 08646 / В. М. Рудницький, Н. М. Пантелєєва, В. Г. Бабенко; заявл. 27.07.2007; опубл. 12.11.07, Бюл. № 18. 4 с.

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

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

119. Пристрій для виконання логічних операцій криптографічного перетворення: деклараційний патент на корисну модель 46617 Україна, МПК H03M 13/00. № u200908000 / В. М. Рудницький, Є. В. Паціра, І. В. Миронець, В. Г. Бабенко; заявл. 29.07.2009; опубл. 25.12.2009, Бюл. № 24. 3 с.

120. Пристрій для виконання логічних операцій криптографічного

перетворення: деклараційний патент на корисну модель 46618 Україна, МПК H03M 13/00. № u200908001 / В. М. Рудницький, Є. В. Паціра, І. В. Миронець, В. Г. Бабенко; заявл. 29.07.2009; опубл. 25.12.2009, Бюл. № 24. 3 с.

121. Рудницький В. М., Пантелєєва Н. М., Бабенко В. Г. Моделювання логічного пристрою для систем захисту інформації. *Банківська система України в умовах глобалізації фінансових ринків*: матеріали міжнар. наук.-практ. конф., 18–20 жовт. 2006 р. Черкаси: Черк. банк. ін-т УАБС НБУ, 2006. С. 137–138.

122. Квасников В. П., Рудницкий В. Н., Бабенко В. Г. Синтез таблиц минимальных кодовых расстояний по Хеммингу *Електроніка та системи управління.* 2006. № 3 (9). С. 47–52.

123. Рудницький В. М., Бабенко В. Г. Властивості таблиць мінімальних кодових відстаней за Хеммінгом. *Сімнадцята наукова сесія Осередку Наукового товариства ім. Шевченка у Черкасах*: матеріали доп. на засіданнях секцій і комісій, 14–24 берез. 2007 р. / за ред. В. В. Масненка. Черкаси: Осер. НТШ у Черк., 2007. С. 206–208.

124. Миронюк Т. А. Методи та засоби синтезу операцій перестановок, керованих інформацією, для комп'ютерних криптографічних систем: дис. канд. техн. наук: 05.13.05. Черкаси, 2017. 184 с.

125. Feistel H. Cryptography and computer privacy. *Scientific American.* 1973. Vol. 228 (5). P. 15–23.

126. Mollin R. A. Codes: The Guide to Secrecy from Ancient to Modern Times. Chapman & Hall/CRC, 2005. P. 142.

127. Cusick Th. W., Stanica P., Stănică P. Cryptographic Boolean Functions and Applications. Academic Press, 2009. P. 25.

128. Фергюсон Н., Шнайер Б. Практическая криптография: пер. с англ. Москва: Изд. дом «Вильямс», 2005. 424 с.:ил.

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

# ДОДАТОК А

## Список публікацій, в яких опубліковані основні наукові результати дисертації

1. 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

2. 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

3. Прокопенко Т. О., Можаєв М. О., Рудницький С. В., Рудницька Ю. В. Програмування режиму ненавантаженого резервування у комп'ютерних системах критичного застосування. *Вісник Черкаського державного технологічного університету*. Черкаси: ЧДТУ, 2020. № 4. С. 77–83. DOI: https://doi.org/10.24025/2306-4412.4.2020.221845

4. 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.

5. Lada N., Rudnytska Yu. Implementation of a method for synthesizing groups of symmetric double-operand operations of cryptographic information coding for block encryption systems. *Innovative Technologies and Scientific Solutions for Industries / Information Technology*. 2022. No. 2 (20). DOI: https://doi.org/10.30837/ITSSI.2022.20.035

6. Rudnytskyi V., Babenko V., Lada N., Tarasenko Ya., Rudnytska Yu. 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. P. 182–194. ISSN 1613-0073 **(Scopus)**

7. Prokopenko T., Tarasenko Ya., Lavdanska O., Rudnytskyi S., Rudnytska Yu. Developing the comprehensive technology for alternative management of complex organizational and technological objects in the conditions of cyber threats. *Workshop on Cybersecurity Providing in Information and Telecommunication Systems (CPITS II 2021)*, Oct. 26, 2021. Kyiv, Ukraine: CEUR Workshop Proceedings, 2022. P. 170–181. ISSN 1613-0073 **(Scopus)**

*Список публікацій, які засвідчують апробацію матеріалів дисертації:*

8. Лада Н. В., Рудницька Ю. В. Класифікація груп несиметричних двохоперандних операцій криптоперетворення інформації на основі перестановочних схем їх синтезу. *Проблеми інформатизації: матеріали Шостої міжнар. наук.-техн. конф.*: тези доп., Черкаси – Баку – Бельсько-Бяла – Харків, 14–16 листоп. 2018 р. Черкаси: ЧДТУ; Баку: ВА ЗС АР, Бельсько-Бяла: УТіГН, Харків: НТУ «ХПІ», 2018. С. 11.

9. 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.

10. 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.

11. 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.

12. 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.

# ДОДАТОК Б

## Документи про впровадження результатів дисертаційної роботи

**«ЗАТВЕРДЖУЮ»**
Ректор Черкаського
державного технологічного
університету
_____ Олег ГРИГОР
«06» ·березня 2022р.

**АКТ**
**впровадження результатів дисертаційної роботи**
**Рудницької Юлії Володимирівни 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., старшого викладача кафедри інформаційних технологій проектування к.т.н., Тарасенко Я.В., розглянувши матеріали дисертаційного дослідження Рудницької Юлії Володимирівни, 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:

– інформаційна технологія моделювання і дослідження операцій криптографічного кодування;

– побудовані групи моделей симетричних двохоперандних операцій криптографічного кодування;

– генератор псевдовипадкової послідовності симетричних двохоперандних операцій криптографічного кодування для систем потокового шифрування.

2. При виконанні курсових і кваліфікаційних робіт використовуються запропоновані методики синтезу моделей симетричних двохоперандних операцій криптографічного кодування на основі кортежів симетричних одноопераднних операцій для блокового шифрування на основі заданої симетричної двохоперандних операцій.

Завідувач кафедри ІТП, д.т.н., професор Т.О. Прокопенко
Доцент кафедри ІТП, к.т.н., доц. О.В.Лавданська
Старший викладач кафедри ІТП, к.т.н. Я.В. Тарасенко

**«ЗАТВЕРДЖУЮ»**

Ректор Черкаського
державного технологічного
університету

_____ Олег ГРИГОР
«29» вересня 2022р.

**АКТ**
**впровадження результатів дисертаційної роботи**
**Рудницької Юлії Володимирівни 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., доцента Бабенко В.Г., доцента кафедри інформаційної безпеки та комп'ютерної інженерії к.т.н., доцента Хрульова М.В., доцента кафедри інформаційної безпеки та комп'ютерної інженерії к.т.н., доцента Шувалової Л.А., розглянувши матеріали дисертаційного дослідження Рудницької Юлії Володимирівни, встановила наступне:

При підготовці бакалаврів за спеціальністю 12 «Кібербезпека» в курсі лекцій з дисциплін «Комплексні системи захисту інформації», «Програмний захист інформації в інформаційно-комунікаційних системах» використовуються результати дисертаційного дослідження, а саме:

– метод синтезу моделей симетричних двохоперандних операцій криптографічного кодування на основі кортежів симетричних одноопераднних операцій;

– метод синтезу груп моделей симетричних двохоперандних операцій криптографічного кодування на основі заданих симетричних двохоперандних операцій, для реалізації генератора псевдовипадкових криптографічних перетворень інформації.

Наведені наукові результати використовуються при виконанні кваліфікаційних робіт магістрів за спеціальністю 123 «Комп'ютерна інженерія» на освітній програмі «Системне програмування».

Професор кафедри ІБ та КІ, д.т.н., доц. В.Г.Бабенко
Доцент кафедри ІБ та КІ, к.т.н., доц. М.В. Хрульов
Доцент кафедри ІБ та КІ, к.т.н., доц. Л.А. Шувалова

# ДОВІДКА

про впровадження результатів дисертаційної роботи
Рудницької Юлії Володимирівни у професійну діяльность
Приватного акціонерного товариства (ПрАТ)
«Черкасиавтотранс»

У професійній діяльності Приватного акціонерного товариства (ПрАТ) «Черкасиавтотранс» використовуються наступні наукові результати, отримані Рудницькою Юлією Володимирівною при роботі над дисертаційним дослідженням, а саме:

- технологія криптографічного перетворення інформації на основі кортежів симетричних одноопераднних операцій;
- математичні моделі та алгоритми криптографічного кодування для блокового шифрування на основі заданої симетричної двохоперандних операцій.

Дані наукові результати реалізовані на основі спеціалізованого модуля операційної системи.

Впровадження розробленого програмного продукту дозволило забезпечити підвищення рівня конфіденційності поточної інформації, яка зберігається на електронних носіях Приватного акціонерного товариства (ПрАТ) «Черкасиавтотранс».

Генеральний директор

Приватного акціонерного товариства (ПрАТ)
«Черкасиавтотранс»
24.10.2022 В.П. Соломенний