МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ЧЕРКАСЬКИЙ ДЕРЖАВНИЙ ТЕХНОЛОГІЧНИЙ УНІВЕРСИТЕТ

Кваліфікаційна наукова праця
на правах рукопису

Підласий Дмитро Андрійович

УДК 004.421.5:004.056.55

ДИСЕРТАЦІЯ

МЕТОД СИНТЕЗУ СЕТ-ОПЕРАЦІЙ НА ОСНОВІ ЕЛЕМЕНТАРНИХ ФУНКЦІЙ ОПЕРАЦІЙ, КЕРОВАНИХ ІНФОРМАЦІЄЮ

123 – комп'ютерна інженерія

12 – інформаційні 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.

_____ Д. А. ПІДЛАСИЙ

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

Черкаси – 2026

АНОТАЦІЯ

Підласий Д.А. Метод синтезу СЕТ-операцій на основі елементарних функцій операцій, керованих інформацією. – Кваліфікаційна наукова праця на правах рукопису.

Дисертація на здобуття наукового ступеня доктора філософії за спеціальністю 123 «Комп`ютерна інженерія». – Черкаський державний технологічний університет, Черкаси, 2026.

Дисертаційна робота присвячена підвищенню варіативності малоресурсних потокових шифрів випадкової підстановки за рахунок розробки і впровадження методу синтезу СЕТ-операцій на основі елементарних функцій операцій, керованих інформацією, які забезпечують можливість подвійного управління процесом криптографічного перетворення як від ключової послідовності, так і від вхідної інформації, при збільшенні кількості таблиць підстановки, що реалізуються в криптоалгоритмі.

У першому розділі за результатами аналізу областей застосування малоресурсного комп’ютеризованого захисту цифрової інформації була встановлена необхідність розширення і впровадження засобів малоресурсної криптографії. Проведений аналіз методів та засобів малоресурсного захисту інформації показав, що більшість малоресурсних криптоалгоритмів фактично є спрощеними версіями відомих повноцінних криптографічних алгоритмів. Проведено огляд публікацій по одному із перспективних напрямків малоресурсної криптографії – СЕТ-шифруванню, яке базується на використанні таблиць підстановок, представлених дискретними моделями. На основі проведеного аналізу сучасного стану і перспектив розвитку СЕТ-шифрування було сформульовано мету і завдання дисертаційного дослідження.

В другому розділі на основі дискретних моделей елементарних функцій операцій, керованих інформацією, отриманих за результатами обчислювального експерименту, побудовані дискретно-алгебраїчні моделі елементарних функцій операцій, керованих інформацією. Визначена основна властивість елементарних функцій операцій, керованих інформацією, яка полягає в тому,

що вибір операції логічного додавання або логічного множення двох вхідних Сі-квантів інформації визначається значенням третього управляючого Сі-кванта вхідної інформації. Встановлено, що для управління вибором логічної операції, яка визначає результат перетворення вхідної інформації елементарною функцією операції керованою інформацією, може бути використано будь який вхідний Сі-квант інформації. На основі зміни управляючих Сі-квантів інформації запропоновано технологію багатоваріантного синтезу дискретно-алгебраїчних моделей елементарних функцій операцій, керованих інформацією. На прикладі дискретно-алгебраїчного опису елементарних функцій розроблено багатоваріантний метод синтезу моделей елементарних функцій операцій, керованих інформацією. Для спрощення процесів подальшого дослідження синтезу і аналізу СЕТ-операцій, побудованих на основі елементарних функцій операцій, керованих інформацією, запропоновано використання дискретно-казуальних моделей елементарних функцій. Встановлено, що використання дискретно-казуального опису дозволяє будувати багатоваріантні дискретно-казуальні моделі елементарних функцій на основі розробленого методу синтезу моделей елементарних функцій операцій, керованих інформацією.

В третьому розділі в процесі дослідження встановлено, що кожну СЕТ-операцію, побудовану на основі елементарних функцій операцій, керованих інформацією, можна представити за допомогою 27 моделей операції при використанні 27 варіантів послідовності ключових елементів. Аналіз результатів обчислювального експерименту по моделюванню СЕТ-операцій на основі елементарних функцій операцій, керованих інформацією дозволив запропонувати підхід до побудови базової групи СЕТ-операцій, яка містить лише симетричні операції. Побудова базової групи з лише симетричних СЕТ-операцій суттєво зменшує обсяг дослідження через зняття потреби в пошуку обернених СЕТ-операцій, адже прямі і обернені операції співпадають. Для оцінки різних варіантів побудови базової групи і результатів їх реалізації запропоновано використовувати критерій простоти побудови і критерій відмінності відповідних елементарних функцій в СЕТ-операціях.

Запропоновано моделі синтезу базової групи СЕТ-операцій на основі елементарних функцій операцій, керованих інформацією за критерієм простоти їх побудови. Запропоновано моделі синтезу базової групи СЕТ-операцій на основі елементарних функцій операцій, керованих інформацією за критерієм відмінності відповідних елементарних функцій. Запропоновано моделі синтезу групи СЕТ-операцій на основі варіантів поєднання операцій базової групи з операціями перестановки елементарних функцій і операціями інверсії елементарних функцій. Отримані моделі покладено в основу удосконалення методу синтезу ЗСі-квантових одноопераднних СЕТ-операцій.

В четвертому розділі на основі узагальнення особливостей дискретно-казуального моделювання двохоперандних СЕТ-операції перестановок керованих інформацією запропоновано моделювання двохоперандних СЕТ-операції на основі елементарних функцій операцій, керованих інформацією реалізовувати шляхом поєднання в кортежі симетричних одноопераднних операцій. Поєднання симетричних СЕТ-операцій забезпечує зменшення ресурсів криптографічної системи. Для побудови систем потокового шифрування на основі однієї двохоперандної СЕТ-операції і групи модифікованих СЕТ-операцій доцільно синтезувати двохоперандні СЕТ-операції на основі елементарних функцій операцій, керованих інформацією на основі критерію відмінності відповідних елементарних функцій та простоти побудови базової групи одноопераднних СЕТ-операцій. Запропоновано послідовність перетворень кортежу одноопераднних операцій, реалізація якої забезпечила синтез дискретно-казуальної моделі двохоперандної СЕТ-операції на основі елементарних функцій операцій, керованих інформацією за критерієм простоти побудови базової групи одноопераднних СЕТ-операцій. Побудовано дискретно-казуальну модель двохоперандної СЕТ-операції на основі елементарних функцій операцій, керованих інформацією за критерієм відмінності відповідних елементарних функцій. Встановлено особливості синтезу цих моделей СЕТ-операцій. Досліджено особливості побудови криптографічних систем, які реалізують СЕТ-операції на основі елементарних

функцій операцій, керованих інформацією. Через неспівпадання розрядностей відображення алфавіту і розрядності блоку перетворення, такі СЕТ-операції забезпечують міжсимвольне перемішування та розсіювання біт вхідної інформації. Реалізація цих СЕТ-операцій забезпечила можливість подвійного управління процесом криптографічного перетворення від ключової послідовності і від вхідної інформації. Побудовані криптографічні системи, які реалізують симетричні двохоперандні СЕТ-операції на основі елементарних функцій операцій, керованих інформацією для перетворення 3Сі-квантів інформації (3 біт інформації), забезпечують можливість збільшення кількості використаних в процесі шифрування модифікованих таблиць підстановок до 192. За результатами тестування побудованих криптографічних систем, стійкість шифрограм до статистичного криптоаналізу відповідає вимогам методики NIST STS.

Наукова новизна отриманих результатів:

1. вперше запропоновано метод синтезу елементарних функцій операцій, керованих інформацією, на основі відомих дискретних моделей елементарних функцій, отриманих за результатами обчислювального експерименту, за допомогою встановлення і формалізації взаємозв’язків між дискретними змінними, що забезпечило можливість побудови повних множин дискретно-алгебраїчних і дискретно-казуальних моделей елементарних функцій операцій, керованих інформацією для спрощення подальшого дослідження синтезу СЕТ-операцій на основі елементарних функцій операцій, керованих інформацією;
2. вперше побудовано метод синтезу 3Сі-квантових СЕТ-операцій на основі елементарних функцій операцій, керованих інформацією шляхом синтезу базових груп симетричних одноопераднних СЕТ-операцій за критерієм простоти їх побудови та критерієм відмінності відповідних елементарних функцій, багатоваріантного представлення СЕТ-операцій дискретно-казуальними моделями, мінімізації взаємозв’язків в кортежі одноопераднних СЕТ-операцій при побудові двохоперандної СЕТ-

операції, що забезпечило можливість подвійного управління процесом криптографічного перетворення при зменшенні складності реалізації СЕТ-операцій.

3. удосконалено системи потокового шифрування на основі випадкових підстановок шляхом застосування двохоперандних СЕТ-операції на основі елементарних функцій операцій, керованих інформацією і генераторів модифікованих СЕТ-операцій, що забезпечило можливість подвійного управління процесом криптографічного перетворення від ключової послідовності і від вхідної інформації, збільшило кількість таблиць підстановки до 192 (кількість СЕТ-операцій в групі операцій на основі елементарних функцій операцій, керованих інформацією) для перетворення 3 Сі-квантів інформації (3 біт інформації). Стійкість результатів шифрування до статистичного криптоаналізу відповідає вимогам методики NIST STS.

Практичне значення отриманих результатів.

Практична цінність роботи полягає в отриманні придатних в практиці побудови комп`ютерних криптографічних систем з нових моделей і операцій криптоперетворення їх функціональних схем і криптоалгоритмів для реалізації СЕТ-операцій на основі елементарних функцій операцій, керованих інформацією. Загалом, отримані практичні результати забезпечують побудову криптографічних систем з подвійним управлінням процесом криптографічного перетворення, збільшують варіативність криптоалгоритмів шляхом використання 192 таблиць підстановки для перетворення 3 Сі-квантів інформації (трьох біт інформації) Для побудови симетричних двохоперандних СЕТ-операцій може бути виконистано 4096 варіантів базових групп, які містять лише симетричні одноопераднді СЕТ-операції. На основі реалізації побудованими двохопераднними СЕТ-операціями псевдовипадкових міжсимвольних перетворень і розсіювання символів досягається стійкість результатів шифрування до статистичного криптоаналізу відповідно до методики NIST STS.

Результати дисертаційного дослідження Підласого Дмитра Андрійовича, а саме удосконалена система комп'ютерного потокового шифрування на основі випадкових підстановок операцій, керованих інформацією, використані при розробці макету захищеної системи дистанційного управління наземним самохідним роботизованим комплексом. Впроваджена система потокового шифрування реалізована на рівні програмного модуля системи управління роботизованим комплексом "MOROZ-02L".

Ключові слова: СЕТ-операції, операції керовані інформацією, моделювання систем, комп’ютерна криптографічна система, потокове шифрування, мало ресурсна криптографія.

ABSTRACT

Pidlasyi D. A. Method of synthesis of CET operations based on elementary functions of data-controlled operations. – Qualifying scientific work on the rights of manuscripts.

Thesis for the level of higher education – Doctor of Philosophy on Specialty 123 – “Computer Engineering”. – Cherkasy State Technological University, Cherkasy, 2026.

The following thesis is dedicated to increasing the variability of lightweight stream ciphers of random substitutions by developing and implementing a method of synthesis of CET operations based on elementary functions of data-controlled operations, capable of enabling dual control of cryptographic transformation by both the key sequence and incoming data. The thesis also studies the systems’ possible modifications for increasing the number of substitution tables in the cryptographic algorithm.

The first section explains the necessity of expanding and implementing lightweight cryptography according to the analysis of the state of modern computerized lightweight data security. Studying the methods of lightweight cryptography allows us to conclude that the majority of lightweight cryptographic algorithms are, in fact, simplified versions of the existing contemporary cryptographic algorithms. We have also analyzed modern research papers dedicated to one of the most prominent branches of lightweight cryptography, specifically the CET encryption, which revolves around the application of substitution tables in the form of discrete models. Summarizing this analysis of both the contemporary state and development opportunities of CET encryption, we have defined the purposes and objectives of this thesis.

The second section describes the discrete and algebraic models of elementary functions of data-controlled operations. The models were created based on discrete models of elementary functions of data-controlled operations, acquired in the end of the conducted simulation experiment. We have defined the primary attribute of elementary functions of data-controlled operations: selecting an operation of logical

addition or logical multiplication of the two incoming data Ci-quanta is determined by the value of the third controlling Ci-quantum of incoming data. Further discovery shows that any incoming data Ci-quantum can be used for selecting a logical operation for determining the result of transforming the incoming data by an elementary function of data-controlled operation. A multiple-option synthesis technology of discrete and algebraic models of elementary functions of data-controlled operations is described. The technology is based on the alteration of the controlling data Ci-quanta. Furthermore, a multiple-option synthesis method for models of elementary functions of data-controlled operations is developed using a discrete and algebraic description of elementary functions as an example. We also suggested using discrete and casual models of elementary functions to simplify further research related to the synthesis and analysis of CET operations, created based on elementary functions of data-controlled operations. In conclusion, the utilization of discrete and casual description enables the creation of multiple-option discrete and casual models of elementary functions. The process is based on the developed method used for the synthesis of models of elementary functions of data-controlled operations.

We describe our findings regarding CET operations in the third section. During our research, we have established that any CET operation, created based on elementary functions of data-controlled operations, can be described by the 27 operation models with 27 options of key elements sequences. Having analyzed the results of the conducted simulation experiment related to the modeling of CET operations based on elementary functions of data-controlled operations, we have defined a new approach to creating a base group of CET operations. This new group consists of symmetric operations only. Building a base group out of symmetric CET operations only greatly reduces the complexity of our research by making the task of searching for inverse CET operations obsolete, since both direct and inverse operations correlate. We have proposed to use creation simplicity criterion and discrepancy criterion of the relevant elementary functions in CET operations for evaluating different options for creating the base group and the results of their

implementation; In addition, the following synthesis models are described and suggested for use: synthesis model for the base group of CET operations based on elementary functions of data-controlled operations with respect to creation simplicity criterion; synthesis model for the base group of CET operations based on elementary functions of data-controlled operations with respect to discrepancy criterion of the relevant elementary functions; synthesis model for a group of CET operations based on different combinations of operations from the base group with permutation operations of elementary functions and inversion operations of elementary functions. The acquired models have become the foundation for improving the method used for the synthesis of 3Ci-quanta one-operand CET operations.

In the final fourth section, we analyze and suggest the method of modeling the two-operand CET operations based on elementary functions of data-controlled operations by combining symmetric one-operand operations within a tuple. Generalization of attributes related to discrete and casual modeling of two-operand CET operations of data-controlled permutations serves as the base of our suggestion. Overall, combining symmetric CET operations makes cryptographic systems lighter. We suggest synthesizing two-operand CET operations based on elementary functions of data-controlled operations and creation simplicity criterion of the base group of one-operand CET operations and discrepancy criterion of the relevant elementary functions. This is useful for the development of stream encryption systems based on one two-operand CET operation and a group of modified CET operations. We have described the transformation sequence of a tuple of one-operand operations. Executing this sequence enables the synthesis of discrete and casual model of a two-operand CET operation based on elementary functions of data-controlled operations with respect to the creation simplicity criterion of the base group of one-operand CET operations. We have then developed the discrete and casual models of a two-operand CET operation based on elementary functions of data-controlled operations with respect to the discrepancy criterion of the relevant elementary functions. We have also defined the peculiarities of synthesizing these models of CET operations. The attributes related to the development of cryptographic systems used for implementing

CET operations based on elementary functions of data-controlled operations are present among the researched topics as well. Discrepancy in bitness of the alphabet and the transformation block enables the usage of these CET operations for conducting intersymbol mixing and dispersion of the incoming data bits. When executed properly, they are also applicable for dual control of cryptographic transformation by both the key sequence and incoming data. Overall, the created cryptographic systems, which execute symmetric two-operand CET operations based on elementary functions of data-controlled operations to transform 3 data Ci-quant (3 data bits), provide options to increase the number of modified substitution tables, utilized during encryption, to 192. The results of testing the created cryptographic systems show resistance of cryptograms to static cryptographic analysis according to NIST STS.

Scientific novelty of the acquired results:

1. In this work, we have introduced a novel method for synthesizing the elementary functions of data-controlled operations based on the known discrete models of elementary functions, which we acquired at the end of the conducted simulation experiment by defining and formalizing the connections between discrete variables. This enabled the creation of full sets of both discrete and algebraic, as well as discrete and casual models of elementary functions of data-controlled operations, thus simplifying further research related to the synthesis of CET operations based on elementary functions of data-controlled operations;
2. We have created a method for synthesizing the 3Ci-quanta CET operations based on elementary functions of data-controlled operations. This was achieved by synthesizing the base groups of symmetric one-operand CET-operations based on several criteria, specifically the criteria of simplicity and discrepancy of the relevant elementary functions; by multi-option presentation of CET-operations through discrete and casual models; by minimizing the relationships in a tuple of single-operand CET-operations during creation of a two-operand CET-operation. This enabled the option for executing the dual

control of a cryptographic transformation while simultaneously decreasing the execution complexity of a CET-operation;

3. Finally, we have improved the stream encryption systems based on random substitutions by implementing two-operand CET operations based on elementary functions of data-controlled operations and generators of the modified CET-operations. This enabled the option for executing the dual control of cryptographic transformation by both the key sequence and incoming data, as well as increased the number of substitution tables that are used to transform 3 data Ci-quanta (3 data bits) to 192 (number of CET operations in a group of operations based on elementary functions of data-controlled operations). Overall, the encryption results are resistant to static cryptographic analysis according to NIST STS.

Practical application of the acquired results:

The practical significance of this paper lies in the acquired functional schemes and cryptographic algorithms for the execution of CET operations based on elementary functions of data-controlled operations. Both of these are applicable for usage in the creation of computer cryptographic systems with new models and operations of cryptographic transformation. Overall, the acquired results enable the creation of cryptographic systems with dual control over the cryptographic transformation, and increase the variability of cryptographic algorithms by using 192 substitution tables for the transformation of 3 data Ci-quanta (3 data bits). Symmetric two-operand CET operations are possible to create by using 4096 options of base groups consisting of symmetric one-operand CET operations only. The aforementioned resistance of the encryption results to static cryptographic analysis according to NIST STS is achieved based on the execution of the pseudorandom intersymbol transformations and symbol dispersion by the created two-operand CET operations.

The results, described by Pidlasyi Dmytro Andriiovych in their thesis, specifically the improved computer stream encryption system based on random substitutions of data-controlled operations, were practically applied in the

development of a model of secured system for remote control of a robotic unmanned ground vehicle (UGV). The stream encryption system in question is implemented at the level of a software unit, used for control of the robotic system MOROZ-02L.

Keywords: CET operations, data-controlled operations, systems modeling, computer cryptographic system, stream encryption, lightweight cryptography.

СПИСОК ПУБЛІКАЦІЙ ЗДОБУВАЧА:

1. Рудницький В. М., Лада Н. В., Кучук Г. А., Підласий Д. А. Архітектура СЕТ-операцій і технології потокового шифрування = Architecture of CET-operations and stream encryption technologies : монографія / Черкаси : видавець Пономаренко Р. В., 2024. 374 с. ISBN 978-966-2554-81-6. URL : https://dndivsovt.com/index.php/monograph/issue/view/22/22 (дата звернення: 13.09.2024).
2. Ларін В. В., Рудницький В. М., Підласий Д. А. Оцінка статистичних властивостей результатів шифрування на основі операцій, керованих інформацією. *Наукові праці Державного науково-дослідного інституту випробування і сертифікації озброєння та військової техніки*. 2024. Т. 22. № 4. С. 121–127. DOI : https://doi.org/10.37701/dndivsovt.22.2024.15 (дата звернення: 09.04.2025).
3. Підласий Д. А. Дослідження і синтез елементарних функцій операцій, керованих інформацією / *Технології розвитку безпілотних систем* : кол. монографія. Т. 2. Безекіпажні системи, розд. / [В. Г. Бабенко та ін. ; під ред. В. М. Рудницького]. Черкаси : видавець Третяков О. М., 2025. 207 с. С. 55–90. ISBN 978-617-8725-03-7. DOI : https://doi.org/10.5281/zenodo.19191122 (дата звернення: 28.03.2026).
4. Рудницький В. М., Ларін В. В., Мельник О. Г., Підласий Д. А. Дискретно-казуальне представлення моделей елементарних функцій і СЕТ-операцій. *Системи управління, навігації та зв'язку.* 2023. № 4. С. 96–101. DOI : https://doi.org/10.26906/SUNZ.2023.4.096 (дата звернення: 15.02.2024).
5. Рудницький В. М., Лада Н. В., Ларін В. В., Підласий Д. А. Дискретно-казуальне моделювання елементарних функцій операцій, керованих інформацією. *Системи управління, навігації та зв'язку.* 2024. С. 139–142. DOI : https://doi.org/10.26906/SUNZ.2024.4.139 (дата звернення: 11.02.2025).
6. Рудницький В. М. , Лада Н. В., Підласий Д. А., Мельник О. Г. Синтез дискретно-алгебраїчних моделей елементарних функцій операцій,

керованих інформацією. Кібербезпека: освіта, наука, техніка. 2024. Т. 3, вип. 23. С. 6–16. DOI : https://doi.org/ 10.28925/2663-4023.2024.23.616 (дата звернення: 25.06.2025).

7. Рудницький, В. М., Тарасенко, Я. В., Лада, Н. В., Бабенко, В. Г., & Підласий, Д. А. (2025). АНАЛІЗ РЕЗУЛЬТАТІВ МОДЕЛЮВАННЯ СЕТ-ОПЕРАЦІЙ НА ОСНОВІ ЕЛЕМЕНТАРНИХ ФУНКЦІЙ ОПЕРАЦІЙ КЕРОВАНИХ ІНФОРМАЦІЄЮ. *Системи та технології*, *70*(2), 258-263. DOI: https://doi.org/10.32782/2521-6643-2025-2-70.29 (дата звернення: 11.01.2026).
8. V. Rudnytskyi, N. Lada, V. Larin, D. Holovniak, H. Haponenko, D. Pidlasyi and T. Stabetska. Discrete and casual modeling of CET-operations of data-controlled permutations. *Journal of Xidian University.* 2024. Vol. 18, iss. 6. P. 747–767. URL : https://drive.google.com/file/d/1iYOUKC7OuDlVXW81GDrhx09VkM9dQZz_/view (дата звернення: 08.02.2025).
9. V. Rudnytskyi, N. Lada, V. Larin, V. Tkachenko, T. Korotkyi, D. Pidlasyi and D. Tarasenko. Information system for modeling and research of pseudorandom sequences of CET-operations for post quantum stream encryption. *Journal of Xidian University.* 2024. Vol. 18, iss. 7. P. 1284–1298. DOI : https://doi.org/10.5281/Zenodo.13096683 (дата звернення: 09.02.2025).
10. V. Rudnytskyi1, V. Babenko, N. Lada, T. Stabetska, D. Pidlasyi, L. Parkhuts. Modeling of a cryptographic network based on application of CET-operations. *Workshop on Cyber Security and Data Protection II, CSDP-II.* Lviv, 2025. Vol. 4042. P. 64–79. URL : https://ceur-ws.org/Vol-4042/paper5.pdf (дата звернення: 15.02.2026).
11. V. Rudnytskyi, N. Lada, V. Babenko, H. Kuchuk, D. Pidlasyi, D. Kamak and Ye. Ivashchenko. Modeling of groups of dual-cycle non-commutative two-operand CET-operations. *Journal of Xidian University.* 2024. Vol. 18, iss. 10. P. 916–

958. DOI : https://doi.org/10.5281/Zenodo.13992956 (дата звернення: 11.02.2025).

12. V. Rudnytskyi, N. Lada, V. Larin, O. Melnyk, T. Stebetska, T. Korotkyi, D. Pidlasyi. Usage of non-commutative two-operand CET-operations in limited resources stream ciphers. *Journal of Xidian University*. 2024. Vol. 18, iss. 5. P. 1105–1120. DOI : https://doi.org/10.5281/Zenodo.11253625 (дата звернення: 03.06.2025).

Список публікацій, які засвідчують апробацію матеріалів дисертації:

1. Підласий Д. А. Мультиваріантне представлення CET-операцій на основі елементарних функцій операцій, керованих інформацією. *Сучасні напрями розвитку інформаційно-комунікаційних технологій та засобів управління* : *тези доповідей шістнадцятої міжнародної науково-технічної конференції (м. Баку – Харків – Жиліна, 29–30 квітня 2026 р.)* : зб. наукових праць. Т 3. 2026. С. 14. DOI : https://doi.org/10.32620/ICT.26.t3 (дата звернення: 05.05.2026).
2. Рудницький В. М., Ларін В. В. , Підласий Д. А. Дискретно-казуальне моделювання двохоперандних CET-операцій для потокового шифрування. *Новітні технології – для захисту повітряного простору : матеріали XXII міжнародної наукової конференції Харківського національного. університету Повітряних Сил імені Івана Кожедуба (м. Харків, 08–09 квітня 2026 р.)* : зб. наукових праць. 2026. С. 556. URL : https://hups.mil.gov.ua/wp-content/uploads/admission-university/naukovij_centr/XXI%D0%86_mizhnarodna_naukova_konferencia_KhNUPS_2026_V2.pdf (дата звернення: 15.05.2026).
3. Рудницький В. М., Безменов С. О., Підласий Д. А. Аналіз елементарних функцій операцій, керованих інформацією. *Безпілотна авіація у сучасній збройній боротьбі* : *матеріали науково-практичної конференції інженерно-авіаційного факультету Харківського національного. Університету Повітряних Сил імені Івана Кожедуба. (м. Харків, 7 грудня*

2023 року.) : зб. наукових праць. 2023. С. 25. URL : https://www.hups.mil.gov.ua/assets/doc/science/stud-conf/bpla-hnups-konf.pdf (дата звернення: 16.04.2024).

ЗМІСТ

ВСТУП

Актуальність теми.

Сьогодні розвиток комп’ютерних систем і мереж нерозривно пов’язаний з вдосконаленням їх інформаційної і кібернетичної безпеки, адже захист конфіденційної інформації і персональних даних від зловмисників є однією із нагальних проблем. Підвищення ефективності вирішення цієї проблеми важливе для державних і приватних установ, підприємств та організацій, а також для пересічних громадян, наприклад для тих, хто спілкується в соціальних мережах. Наразі комп’ютерна криптографія залишається основним і найефективнішим засобом захисту інформації в цифровому просторі. Проте використання стандартизованих криптографічних систем не завжди доцільно, тому що вартість систем захисту не повинна перевершувати вартості інформації, яка захищається. Тому виникає необхідність і доцільність розвитку малоресурсної комп’ютерної криптографії.

Значний внесок у розвиток комп`ютерних криптографічних систем та інформаційної безпеки комп`ютерних мереж зробили вітчизняні і зарубіжні науковці: Горбенко І. Д., Задірака В. К., Кузнецов Ю. В., Дорошкевич П. В., Дудикевич В. Б., Опірський І. Р., Ободяк В. К., Потій А. В., Шеннон К. Є., Месси Дж. Л., Брюс Шнайер, S. Banik, A. Shamir, R. L. Rivest, A. Bogdanov, C. P. Ekwueme, I. H. Adam, M. E. Hellman, J. Gubbi, R. Buyya тощо.

Дослідженнями нових операцій на основі булевих функцій для побудови мало ресурсних систем криптографічного перетворення інформації займалися Лужецький В. А., Романкевич О. М., Дмитришин О. В. тощо. Проте отримані операції складають лише незначну частину СЕТ-операцій, на основі яких будуються системи СЕТ-шифрування.

Одним із перспективних напрямків розвитку СЕТ-шифрування є побудова криптографічних систем на основі операцій, керованих інформацією. На сьогоднішній день в роботах Рудницького В. М., Миронюк Т. В., Лади Н. В. тощо досліджено лише СЕТ-операції перестановок, керованих інформацією. Дослідження СЕТ-операцій на основі елементарних функцій операцій,

керованих інформацією, не проводились через складність математичного опису. Проте застосування СЕТ-операцій, керованих інформацією, дозволяє будувати потокові шифри з подвійним управлінням процесом криптографічного перетворення.

Отже можна стверджувати, що тема дисертаційного дослідження «Метод синтезу СЕТ-операцій на основі елементарних функцій операцій, керованих інформацією» є актуальною.

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

Дисертаційна робота виконана відповідно до плану науково-дослідних робіт Черкаського державного технологічного університету, а її тематика відповідає Закону України «Про перспективні напрямки наукових досліджень» від 2006 року зі змінами від 2022 року. Отримані в дисертаційній роботі наукові результати включені в НДР Черкаського державного технологічного університету «Методи та засоби синтеза груп симетричних двухоперандних операцій криптографічного кодування для малоресурсних криптоалгоритмів» (ДР № 0121U114390) і «Дослідження шляхів розвитку потокового шифрування на основі криптографічного кодування» (ДР № 0121U114389), у яких автор брав участь як виконавець.

Мета і завдання дослідження. Основною метою дослідження є підвищення варіативності малоресурсних потокових шифрів випадкової підстановки за рахунок розробки і впровадження методу синтезу СЕТ-операцій на основі елементарних функцій операцій, керованих інформацією, які забезпечують можливість подвійного управління процесом криптографічного перетворення, як від ключової послідовності, так і від вхідної інформації, при збільшенні кількості таблиць підстановки, що реалізуються в криптоалгоритмі

Для досягнення поставленої мети сформульовано і вирішено такі завдання:

1. Розробити метод синтезу елементарних функцій операцій, керованих інформацією, на основі відомих дискретних моделей елементарних функцій, отриманих за результатами обчислювального експерименту;

2. Розробити метод синтезу ЗСі-квантових СЕТ-операцій, побудованих на основі елементарних функцій операцій, керованих інформацією, які забезпечать можливість подвійного управління процесом криптографічного перетворення інформації;
3. Удосконалити системи потокового шифрування на основі випадкових підстановок.

Об’єкт дослідження – процеси малоресурсного криптографічного перетворення інформації.

Предмет дослідження – моделі СЕТ-операцій на основі елементарних функцій операцій, керованих інформацією, для малоресурсних систем потокового шифрування з подвійним управлінням криптоперетворенням.

Методи дослідження. У процесі розробки методу синтезу елементарних функцій операцій, керованих інформацією, було використано математичний апарат теорії інформації, теорії алгоритмів, криптографії, дискретної математики, методи комп’ютерного і функціонального моделювання.

Для розробки методу синтезу ЗСі-квантових СЕТ-операцій, побудованих на основі елементарних функцій операцій, керованих інформацією, були використані: основи теорії СЕТ-шифрування, дискретна математика, теорія алгоритмів, методи комп’ютерного моделювання та обчислювального експерименту, дискретно-казуальна логіка.

Для удосконалення систем потокового шифрування на основі випадкових підстановок були використані: теорія криптографії із застосуванням методів дискретної математики, теорія алгоритмів, методи комп’ютерного моделювання та математична статистика.

Наукова новизна одержаних результатів. Під час вирішення поставлених задач автором одержано такі результати:

1. вперше запропоновано метод синтезу елементарних функцій операцій, керованих інформацією, на основі відомих дискретних моделей елементарних функцій, отриманих за результатами обчислювального експерименту, за допомогою встановлення і формалізації взаємозв’язків

між дискретними змінними, що забезпечило можливість побудови повних множин дискретно-алгебраїчних і дискретно-казуальних моделей елементарних функцій операцій, керованих інформацією, для спрощення подальшого дослідження синтезу СЕТ-операцій на основі елементарних функцій операцій, керованих інформацією;

2. вперше побудовано метод синтезу 3Сі-квантових СЕТ-операцій на основі елементарних функцій операцій, керованих інформацією, шляхом синтезу базових груп симетричних одноопераднних СЕТ-операцій за критерієм простоти їх побудови та критерієм відмінності відповідних елементарних функцій, багатоваріантного представлення СЕТ-операцій дискретно-казуальними моделями, мінімізації взаємозв'язків в кортежі одноопераднних СЕТ-операцій при побудові двохоперандної СЕТ-операції, що забезпечило можливість подвійного управління процесом криптографічного перетворення при зменшенні складності реалізації СЕТ-операцій.
3. удосконалено системи потокового шифрування на основі випадкових підстановок шляхом застосування двохоперандних СЕТ-операції на основі елементарних функцій операцій, керованих інформацією, і генераторів модифікованих СЕТ-операцій, що забезпечило можливість подвійного управління процесом криптографічного перетворення від ключової послідовності і від вхідної інформації, збільшило кількість таблиць підстановки до 192 (кількість СЕТ-операцій в групі операцій на основі елементарних функцій операцій, керованих інформацією) для перетворення 3 Сі-квантів інформації (3 біт інформації). Стійкість результатів шифрування до статистичного криптоаналізу відповідає вимогам методики NIST STS.

Практичне значення отриманих результатів. Практична цінність роботи полягає в отриманні придатних в практиці побудови комп'ютерних криптографічних систем з нових моделей і операцій криптографічного перетворення їх функціональних схем і криптографічних алгоритмів для реалізації СЕТ-операцій на основі елементарних функцій операцій, керованих

інформацією. Сукупно отримані практичні результати забезпечують побудову криптографічних систем з подвійним управлінням процесом криптографічного перетворення, збільшують варіативність криптографічних алгоритмів шляхом використання 192 таблиць підстановки для перетворення 3 Сі-квантів інформації (трьох біт інформації). Для побудови симетричних двохоперандних СЕТ-операцій може бути використано 4096 варіантів базових групп, які містять лише симетричні одноопераднді СЕТ-операції. На основі реалізації побудованими двохоперандними СЕТ-операціями псевдовипадкових міжсимвольних перетворень і розсіювання символів досягається стійкість результатів шифрування до статистичного криптоаналізу відповідно до методики NIST STS.

Результати дисертаційного дослідження Підласого Дмитра Андрійовича, а саме удосконалена система комп'ютерного потокового шифрування на основі випадкових підстановок операцій, керованих інформацією, використані при розробці макету захищеної системи дистанційного управління наземним самохідним роботизованим комплексом. Впроваджена система потокового шифрування реалізована на рівні програмного модуля системи управління роботизованим комплексом "MOROZ-02L".

Особистий внесок здобувача. Всі нові результати дисертаційної роботи отримано автором самостійно. Роботи [31, 32] опубліковані одноосібно. У наукових працях, опублікованих у співавторстві, з питань, що стосуються цього дослідження, автору належать: визначення кортежів одноопераднді СЕТ-операцій для моделювання криптографічної мережі на основі двохоперандних СЕТ-операцій [67], застосування дискретно-казуальної логіки для побудови СЕТ-операцій на основі елементарних функцій операцій, керованих інформацією [41, 47], побудова моделей елементарних функцій операцій, керованих інформацією, на основі дискретно-алгебраїчної логіки [39, 48], визначення підгруп СЕТ-операцій на основі елементарних функцій операцій, керованих інформацією, для побудови симетричних базових груп операцій криптографічного перетворення [52], аналіз моделей криптографічних систем

на основі одноопераднних СЕТ-операцій [48], взаємні перетворення моделей СЕТ-операцій [68, 79], мінімізація дискретно-казуальних моделей двохоперандних СЕТ-операцій, керованих інформацією, [36, 79], модифікація двохоперандних СЕТ-операцій [61], узагальнення результатів статистичного тестування СЕТ-операцій, керованих інформацією, [28].

Апробація результатів дисертації проходила на таких наукових заходах: науково-практична конференція «Безпілотна авіація у сучасній збройній боротьбі» (Харків, 2023), Workshop on Cyber security and data protection II (CSDP-II, Львів, 2025), XXII міжнародна наукова конференція Харківського національного університету Повітряних Сил ім. Івана Кожедуба «Новітні технології для захисту повітряного простору» (Харків, 2026), XVII міжнародна наукова конференція Академії збройних сил Азербайджану (Алмата-Харків, 2026).

Публікації. Основні положення дисертації опубліковано у 15 друкованих працях, зокрема: у 4 статтях у фахових виданнях України, статті опублікованій за результатами конференції, яка проіндексована в науково-метричній базі SCOPUS, 2 колективних монографіях, в одній з яких опубліковано одноосібний розділ, в матеріалах двох міжнародних наукових конференцій, і науково-практичної конференції Харківського національного університету Повітряних Сил ім. Івана Кожедуба.

Структура і обсяг дисертації. Робота складається зі вступу, чотирьох розділів, висновків, списку використаних джерел, додатків. Загальний обсяг дисертації – 203 сторінки. Основний зміст викладений на 145 сторінках включно з 17 таблицями та 7 рисунками. Список використаних джерел містить 126 найменувань. Робота містить 4 додатки.

РОЗДІЛ 1. КОМП'ЮТЕРНА КРИПТОГРАФІЯ І МАЛОРЕСУРСНИЙ ЗАХИСТ ІНФОРМАЦІЇ

1.1. Області застосування малоресурсного захисту цифрової інформації

Загальновизнаним в сучасному світі є факт використання інформаційних технологій як невід'ємного елементу життя людства, оскільки вони використовуються не лише в економіці та галузях промисловості, але і в побуті. Цій сфері людської діяльності, зокрема її впливу на розвиток економіки та суспільства, присвячено чимало наукових праць як вітчизняних [9, 21, 49], так і зарубіжних [101, 122, 126] дослідників.

Значним чинником, що обумовлює важливість інформаційних технологій є нова технологічна парадигма, яку дослідники називають «Інтернетом речей» (англ. Internet of Things, IoT). Відповідно до визначення дослідників CRYPTEC, IoT — це потужна та комплексна мережа, що дозволяє користувачам «з'єднуватися з будь-ким або будь-чим будь-де і в будь-який час» [93]. Концепція Інтернету речей передбачає можливість утворення єдиної мережі із залученням не лише традиційних інформаційно-комунікаційних технологій (Information and Communication Technologies, ICT) на кшталт персональних комп'ютерів, смартфонів, таблоїдів, але й таких елементів як автомобілі, роботи, та навіть цілі будівлі. Але фахівці робочої групи CRYPTEC зазначають, що визначити повний спектр приладів з можливістю під'єднання до Інтернету наразі неможливо, як неможливо точно спрогнозувати спосіб їх використання за умов такого під'єднання. За їх словами, «в час Інтернету речей слід бути готовими до будь-яких неочікуваних сценаріїв» [28]. Більш детально особливості IoT розглянуто в [88, 91, 102, 107, 110, 119, 120]

Очевидним негативним аспектом інформатизації та комп'ютеризації життя сучасної людини є значне загострення питання безпеки даних. Поширення приладів (терміналів) з доступом до Інтернету речей посилює

глобальну онлайн-мережу з одночасним збільшенням потреби в захисті інформації користувачів від несанкціонованого доступу [93]. Однак єдиний та надійний метод криптографічного захисту інформації, який передбачає ефективну програмну та/або апаратну реалізацію на всіх типах цільових пристроїв, наразі відсутній [86]. Наприклад, наявний та найрозповсюдженіший алгоритм захисту даних AES (англ. Advanced Encryption Standard) доволі потужний та відомий завдяки хорошій ефективності. Він використовується в пристроях «високого» класу, вбудованих системах, також можлива його імплементація в деяких пристроях «низького» рівня, хоча й з певними обмеженнями [115]. Типовими та загальновідомими прикладами технологій «високого рівня» є різноманітні термінали, датчики, пристрої зчитування інформації, пристрої з вбудованою операційною системою (крім звичайних персональних комп'ютерів), які можуть бути під’єднані до мережі Інтернет і навіть об'єднані в бездротову мережу тощо [88]. Однак використання звичайних криптографічних алгоритмів на кшталт вищевказаного AES в пристроях з обмеженими ресурсами (малоресурсних пристроях та/або системах) зазвичай доволі складне або взагалі неможливе [115]. Сьогодні існує велика кількість малоресурсних пристроїв, з-поміж яких виокремлюють:

- RFID-зчитувачі (англ. Radio Frequency Identification);
- Смарт-картки;
- Бездротові сенсори;
- Індикатори, датчики, контролери тощо [18, 93, 104, 120].

Слід зазначити, що ключовими проблемами реалізації традиційної криптографії в пристроях з можливістю під’єднання до Інтернету речей є зазвичай низька обчислювальна потужність, обмежені ресурси пам'яті, невелика фізична площа (розмір) для належної збірки, низька енергоємність батареї або акумулятора (або їх повна відсутність) [88, 89, 93].

Обмеженість використання наявних криптографічних алгоритмів в малоресурсних системах обумовлює потребу в розробці окремої теоретичної та практичної бази для криптографічного захисту даних в малоресурсних

пристроях. В сучасній інформатиці ця специфічна область досліджується завдяки підгалузі криптографії, що відома як малоресурсна криптографія (англ. lightweight cryptography). Цим терміном позначається розділ криптографії, метою якого є розробка алгоритмів для використання в пристроях, в яких ускладнена або неможлива реалізація стандартних методів криптографічного захисту через обмежені ресурси (пам'ять, потужність, розмір тощо) [85]. Детальний аналіз визначення малоресурсної криптографії представлено в [86, 87, 89, 99].

На думку дослідників, малоресурсну криптографію можливо розглядати як своєрідний компроміс між такими категоріями, як вартість реалізації, швидкість, безпека, продуктивність та енергоспоживання на пристроях з обмеженими ресурсами. При цьому основна мотивація для використання малоресурсної криптографії — підвищення безпеки даних шляхом оптимального розподілу наявних ресурсів системи, зокрема меншого обсягу пам'яті, менших обчислювальних потужностей та меншого енергоспоживання. Цю позицію проаргументовано в [16, 17, 95, 100].

Врахування вищевказаної інформації дає підстави вважати, що використання малоресурсної криптографії найбільш доцільне та ефективне в приладах та/або системах, що передбачають потребу розподілу наявного об’єму пам’яті та потужності ЦП між багатьма програмами або додатками, та/або мають обмежений енергоресурс. Наукові праці [90, 93-95, 100, 118] пропонують детальний аналіз аспектів використання малоресурсної криптографії включно з основними сферами. З-поміж основних областей використання малоресурсного захисту інформації можливо виокремити такі:

- Мобільний зв’язок, зокрема в смартфонах і таблоїдах;
- Домашні електроприлади, зокрема телевізори з технологією Smart TV;
- Додатки та прилади, що використовують RFID;
- Датчики та сенсори в різних галузях промисловості;
- Промислові системи;
- Автомобільна галузь.

Слід зазначити, що наявні стандарти малоресурсної криптографії, зокрема вітчизняний стандарт ДСТУ [1, 2] та зарубіжний ISO/IEC 29192-2:2019 [80-82], не описують чітких критеріїв, за допомогою яких можливо класифікувати криптографічний алгоритм як «малоресурсний» [106]. Але загальною рисою таких алгоритмів є надзвичайно низькі вимоги до основних ресурсів приладів та/або систем. Основними з-поміж таких ресурсів є:

- Розмір, потрібний для належної реалізації в апаратному аспекті;
- Обчислювальна потужність невеликих (мікро-) процесорів чи контролерів;
- Оперативна пам'ять (RAM);
- Постійна пам'ять (ROM) [84, 112, 118].

Основною перевагою використання малоресурсного захисту інформації є насамперед можливість імплементації відповідних шифрів та алгоритмів в системи та/або пристрої з обмеженими ресурсами. У порівнянні з малоресурсною криптографією, такі стандарти шифрування, як попередньо описаний американський AES [115], обробляють інформацію досить швидко, проте подібні шифри потребують значний об’єм ROM і RAM системи для належної реалізації. Високі вимоги до апаратних ресурсів значно ускладнюють та/або унеможливлюють використання відповідних алгоритмів в пристроях з обмеженими можливостями, зокрема з обмеженим кінцевим запасом енергії та обсягом пам'яті. За таких умов малоресурсні шифри показують значно кращі результати. Слід також зазначити, що малоресурний захист інформації можливо забезпечити значно простіше з меншими грошовими та енергетичними витратами порівняно з традиційними криптографічними алгоритмами. Наукові праці [93, 105, 107, 116, 121] підтверджують ці тези та дозволяють констатувати, що основними перевагами малоресурсного шифрування в порівнянні з традиційною криптографією є:

- Нижча вартість;
- Нижчі вимоги до енергоспоживання;
- Нижчі вимоги до апаратних та програмних ресурсів систем.

Було зазначено, що малоресурсні алгоритми використовуються переважно в пристроях з обмеженими ресурсами. Однак вищевказані переваги надають малоресурсній криптографії потенціал для використанням в мережах наступного покоління, зокрема в кібернетичних системах, або таких, що прямо пов’язані з Інтернетом речей [88, 93]. Відповідний висновок можливо зробити з факту, що більшість приладів з можливістю під’єднання до Інтернету речей навряд-чи використовуватимуть потужний центральний процесор з високою продуктивністю. Слід завжди враховувати ймовірність використання в мережі приладів з низькою обчислювальною здатністю, об’ємом пам’яті, а також обмеженими запасами енергії порівняно з потужними інформаційно-комунікаційними технологіями сучасного зразку. Це робить малоресурсну криптографію перспективним рішенням для захисту даних в приладах та/або системах з обмеженими ресурсами через менше навантаження на центральний процесор, менший необхідний об’єм пам’яті для реалізації, а також нижчу затримку [93, 89, 102].

З метою висвітлення особливостей малоресурсного захисту інформації в порівнянні з традиційною криптографією, ми здійснили детальний аналіз методів і засобів малоресурсного шифрування в підрозділі 1.2.

1.2. Методи та засоби малоресурсного захисту інформації

Ефективне використання малоресурсної криптографії передбачає потребу в застосуванні низки специфічних методів та засобів, що відрізняються від звичних алгоритмів захисту інформації. Методи і засоби малоресурсної криптографії детально розглядаються в [85-87, 93, 91, 99, 106, 108, 118]. Аналіз відповідних наукових праць дає підстави стверджувати, що загалом малоресурсне шифрування має переваги порівняно з традиційними криптографічними алгоритмами. Ці переваги простежуються принаймні в одному з таких критеріїв:

- Комплексність каналу зв’язку (англ. circuit size);
- Енергоспоживання;
- Затримка;
- Необхідний об’єм пам’яті.

Малоресурсний алгоритм є основним методом захисту інформації в малоресурсному шифруванні. Приклади малоресурсних алгоритмів та їх особливості наведено в [70, 85, 86, 93, 104, 106]. Їх основне призначення — забезпечити приватність даних та/або їх автентифікація. Вибір алгоритму залежить від мети, яку ставить користувач, та специфіки приладів або систем, дані яких потребують захисту. Їх налаштування передбачає можливість визначення та зміни одного або декількох параметрів (атрибутів), до яких належать:

- Довжина ключа. Цей параметр є фундаментальним для забезпечення належного захисту, а отже потребує врахування всіх умов реалізації малоресурсного алгоритму;
- Довжина блоку. Цей параметр прямо впливає на криптографічну ефективність блокових шифрів. Наприклад, використання блоків з малою довжиною значно обмежує кількість даних, які можливо зашифрувати за допомогою блокового шифру;
- Кількість даних, що обробляється та частотність оновлення ключа. Додатковим заходом підвищення криптографічної безпеки є періодичне оновлення ключа за наявності такої можливості, оскільки стійкість криптографічного алгоритму знижується після кожної успішної обробки даних. Якщо ключ неможливо змінити, зокрема у випадку його жорсткого кодування, слід завчасно визначити ліміт на кількість даних, що обробляється, та припинити роботу приладу перш ніж буде досягнуто визначеного ліміту;
- Сценарії для можливого використання. Малоресурсні шифри зазвичай використовуються для попередження лінійних (linear) та диференційованих (differential) атак. Проте їх спрощена архітектура

робить їх вразливими до інших, більш комплексних видів атак, зокрема атак на зв’язаних ключах (англ. related-key attack), атак на відомих ключах (англ. known-key attack), та атак на основі обраного ключа (англ. chosen-key attack). Це зумовлює потребу завчасного визначення сценаріїв використання малоресурсних шифрів з метою забезпечення максимального захисту в необхідних пристроях та/або системах;

- Простір реалізації. Малоресурсний захист інформації можливо використовувати в різних приладах та/або системах. Відповідні алгоритми слід обирати залежно від простору їх використання, зокрема апаратного або програмного.

Використання малоресурсних алгоритмів шифрування інформації також залежить від галузі, системи або пристрої якої потребують криптографічного захисту. Спираючись на наукові праці [70, 87, 90, 91, 93, 94, 98, 113], розглянемо приклади використання малоресурсного захисту в різних сферах:

- Домашнє використання. Для захисту домашніх електроприладів використовуються малоресурсні криптографічні алгоритми на кшталт SPECK. Системи Smart TV, що наразі широко використовуються в побуті, передбачають можливість використання ширшого спектру алгоритмів, зокрема SPECK, SIMON, Piccolo, і TWINE;
- RFID-зчитувачі. Ці прилади часто використовуються в логістиці, що обумовлює потребу в захисті даних. Малоресурсні шифри на кшталт SIMON, SPECK, Piccolo та PRINCE вважаються надійними для використання в RFID-зчитувачах;
- Датчики. Ефективність малоресурсних шифрів варіюється залежно від типу датчиків, для захисту яких вони використовуються. Наприклад, в датчиках сільськогосподарського призначення ефективно працюють малоресурсні схеми автентифікації, зокрема JAMBU-SIMON, SILC-PRESENT, ACORN, Ascon та Minalpher, або шифри на кшталт SPECK, SIMON, PRESENT, TWINE та Midori. Шифри SIMON, SPECK, Picollo та

PRESENT також показують високу ефективність при використанні для захисту даних в медичних датчиках;

- Промислові системи. Ефективний захист інформації в промислових системах можливо досягти за допомогою шифрів Midori та PRINCE;
- Автомобільна галузь. Малоресурсні алгоритми Midori, PRINCE, PRESENT та SIMON часто використовуються для захисту інформації в автомобільних приладах, наприклад в системах автоматизованого керування автотранспортом.

Результати вищевказаних досліджень разом з [29, 104, 105, 114] показують, що за останнє десятиліття було запропоновано низку малоресурсних криптопримітивів, які часто переважають стандартні криптографічні алгоритми в контексті продуктивності. Такі малоресурсні примітиви зазвичай не проєктуються для використання в потужних приладах, проте їх належна реалізація може накладати значні обмеження на спроби зловмисників отримати несанкціонований доступ до інформації. Основними факторами для аналізу та оцінки їх якості є: розмір блоку, розмір ключа, структура та кількість раундів. Найвідомішими є чотири типи малоресурсних криптографічних примітивів, до яких належать:

- Малоресурсні блокові шифри (англ. Lightweight Block Ciphers);
- Малоресурсні потокові шифри (англ. Lightweight Stream Ciphers);
- Малоресурсні хеш-функції (англ. Lightweight Hash Functions);
- Криптографія еліптичних кривих (англ. Elliptic Curves Cryptography).

Як було зазначено в підрозділі 1.1, основні властивості малоресурсної криптографії описано в стандарті ISO/IEC 29192-2:2019 [80-82], де їх характеристика здійснюється на основі цільових платформ. В стандарті також детально описані аспекти малоресурсності, що впливають на функціонування відповідних платформ. Основними в апаратному аспекті є розмір мікросхеми та її енергоспоживання, а в програмному — обсяг потрібної пам'яті для роботи програмного забезпечення.

В контексті проєктування, малоресурсні алгоритми мають менший розміри блоків в порівнянні зі звичайними шифрами. Якщо розмір блоку в звичайному шифрі становить зазвичай 64 або 128 біт, то в аналогічних малоресурсних шифрах цей розмір коливається від 32 до 64 біт [24, 27]. Крім того, малоресурсні алгоритми також мають менший розмір ключів, що впливає на простоту їх використання. Водночас безпека, разом з продуктивністю та вартістю, є важливим показником для будь-якого алгоритму малоресурсної криптографії. Стійкість будь-якого малоресурсного алгоритму до атак можливо виміряти за допомогою криптоаналізу. Його сенс полягає в ідентифікації слабких місць алгоритму та розробці потенційних методів дешифрування [21, 49].

Особливу увагу в контексті нашого дослідження варто звернути на праці вітчизняного дослідника Деменка Є. [16, 17]. Він приділяє значну увагу аналізу криптографії з симетричним ключем через можливість її використання в пристроях, котрі мають значні ресурсні обмеження. Це пов’язано насамперед з тим, що імплементація асиметричних шифрів потребує значно більше обчислювальних ресурсів. Порівняльний аналіз криптографії з симетричними та асиметричними ключами наведено в таблиці 1.1.

Варто зазначити, що криптографія з симетричним ключем оперує основними функціями, зокрема блоковими або потоковими шифрами [17]. В криптографічній стандартизації малоресурсних примітивів розглядають як програмний, так і апаратний аспекти безпеки, котрі, зазвичай, послуговуються різними метриками. Основна різниця полягає в тому, що програмні метрики включають цикли, пам'ять і цикл на байт, а апаратні метрики враховують пропускну здатність, площу, співвідношення по всій площі. Тому здійснити пряме порівняння цих двох показників доволі складно, про що свідчать джерела [85, 86].

Завдяки аналізу джерел [16, 17] можливо детально проаналізувати попередньо згадані види криптографії з симетричними та асиметричними ключами. Аналіз здійснено завдяки таблиці 1. 1.

Таблиця 1.1

Порівняння криптографії з симетричним та асиметричними ключами

Параметр	**Особливості**	
	Криптографія з симетричним ключем	**Криптографія з асиметричним ключем**
Ключ	Один загальний приватний ключ	Унікальна пара з приватного та публічного ключів. Генерація відкритих ключів залежить від криптографічних алгоритмів, що ґрунтуються на односторонніх математичних функціях.
Кількість ключів	Експоненційно пропорційна кількості користувачів	Лінійно пропорційна кількості користувачів
Швидкість шифрування та комплексність алгоритмів	Шифрування відбувається швидко через простоту алгоритмів, що використовуються	Процес шифрування відбувається повільніше через те, що для використання та обробки різних ключів використовуються комплексні алгоритми, які потребують більше часу для належної реалізації.
Апаратна складність	Не потребує потужного та коштовного апаратного забезпечення.	Потребує потужне апаратне забезпечення через комплексність алгоритмів.
Сфери використання	Здебільшого використовується для передачі великих обсягів даних.	Невеликі транзакції, автентифікація та встановлення безпечного каналу зв'язку, що передує фактичній передачі даних.
Приклади алгоритмів	RSA, DSA, ECC	Потокові шифри: Trivium, Chacha, WG-8, Espresso, Grain 128. Блокові шифри: AES, DES, 3DES, Blowfish, Twofish, Curupira, PRESENT, KATAN. TEA, Humming Bird, RECTANGLE, SIMON

В контексті захисту даних, симетричне шифрування використовує однаковий ключ при шифруванні та розшифруванні даних. Загалом цей метод є безпечним і відносно швидким. Його основним недоліком є спільне

використання ключа двома комунікантами. Зловмисник може розшифрувати дані, якщо має доступ до ключа. Алгоритми з симетричним ключем навпаки забезпечують конфіденційність і цілісність даних, але не гарантують автентифікацію. Цей тип шифрування використовує три типи алгоритмів, в основі яких покладено хешування, потокові та блокові шифри [18, 29, 70].

Найбільш актуальними в межах цього дослідження є блокові шифри — різновид симетричних шифрів, в яких обробляється відразу весь блок. Блокові шифри використовуються для побудови хеш-функцій та кодів автентифікації повідомлень (англ. Message Authentification Code). Полегшені блокові шифри створюються на основі двох типів структур: мережи підстановки-перестановки (англ. Substitution-Permutation Network) та мережи Фейстеля. Детальний огляд блокових шифрів наведено в працях [80, 83, 90, 92, 94, 105, 113, 114].

Іншою важливою категорією, що розглядається в [91, 98, 114] є мережа Фейстеля — шифр, що передбачає декілька раундів шифрування та ділить вхідний блок на дві частини. В кожному раунді шифрування або дешифрування він обробляє лише одну половину. Самі ж половини блоку міняються місцями між раундами ліворуч і праворуч. Головною перевагою такого шифрування є використання однакового програмного коду для шифрування та дешифрування, що знижує кількість необхідної пам'яті. Мережу Фейстеля можливо реалізувати на апаратних засобах з середньою та низькою потужністю, проте ця структура погано працює на приладах з малою затримкою [98]. Мережа підстановки-перестановки навпаки працює швидше, але не передбачає розкладу ключів. Відсутність ключового розкладу робить систему вразливою до атак, проте при однаковій стійкості та однакових витратах енергії, мережа підстановки-перестановки є більш придатною, оскільки вона потребує меншого раунду виконання. Отже ця структура передбачає менші енерговитрати за аналогічних умов [116].

Класичним прикладом алгоритму на основі мережі підстановки-перестановки є попередньо згаданий алгоритм AES [115], який було коротко охарактеризовано в підрозділі 1.1. Цей алгоритм працює на 128-бітному блоці з

128, 192 та 256-бітними варіантами ключів. Крім того, мінімальна вимога величини, відомої під назвою «еквівалент воріт» (англ. Gate Equivalent, GE), зафіксована для AES, становить близько 2400. Хоча такий показник нижчий за середній на 23%, реалізація алгоритму AES в реальному часі в невеликих та малоресурсних приладах і системах ускладнена [93]. Досягнення належної реалізації та високої продуктивності можливо виключно при забезпеченні системи додатковими ресурсами.

Відповідно до [81-83, 90, 93, 99], малоресурсні шифри повинні відповідати таким чотирьом вимогам для забезпечення максимальної ефективності при експлуатації:

- Шифр потребує мінімальний обсяг пам'яті для реалізації;
- Шифр потребує низьку кількість енергії;
- Шифр має низьке значення еквівалентів воріт (GE), що забезпечує ефективну апаратну реалізацію;
- Шифр забезпечує достатній рівень безпеки.

Роботи [84, 93, 115, 118] розглядають еталони блокових шифрів в сучасній криптографії. Ними є алгоритми AES, PRESENT та CLEFIA. Найпоширенішим є AES, оскільки в 2002 році саме він був визначений як стандарт для шифрування. Незважаючи на те, що AES не є малоресурсним шифром, цей алгоритм використовується в багатьох системах і пристроях Інтернету речей. PRESENT та CLEFIA також є стандартизованими шифрами, але їх розглядають як малоресурсні. В цілому, атрибути цих шифрів можливо використовувати як еталон для оцінювання якості інших малоресурсних шифрів.

Окрім блокових і потокових шифрів, хеш-функцій та криптографії еліптичних кривих, малоресурсне шифрування можливо здійснювати на основі CET-операцій. Тому вважаємо необхідним розглянути особливості реалізації малоресурсної криптографії з використанням CET-операцій в підрозділі 1.3.

1.3. Малоресурсний захист інформації на основі CET-шифрування

Незважаючи на наявні стандарти малоресурсної криптографії, аспект захисту інформації в малоресурсних системах потокового шифрування наразі недостатньо досліджений в сучасній інформатиці. Перспективним рішенням для покращення якості малоресурсного потокового шифрування є використання CET-операцій на основі додавання за модулем два. В цьому контексті особливе значення належить операціям перестановки операндів, оскільки з їх допомогою можливо здійснювати шифрування вхідної інформації та послідовності для блокування. Багато вітчизняних дослідників, зокрема Рудницький В. М. [35-48, 72-77], Бабенко В. Г. [4-7, 42], Лада Н. В. [3, 25, 62-66], Тарасенко Я. В. [42, 60], Короткий Т. К. [34, 38, 70] та інші присвятили свої наукові праці дослідженню ефективності таких операцій в малоресурсній криптографії. Отже, в цьому підрозділі ми аналізуємо перспективи використання CET-шифрування для захисту інформації в малоресурсних пристроях і системах.

Фундаментальним в контексті цього дослідження є поняття «CET-операція». За визначенням вітчизняного вченого Рудницького В. М., який зробив значний внесок в дослідження цієї теми [24, 72-77], CET-операцією є операція в теорії криптографічного кодування (англ. CET — Cryptographic Encoding Theory). Фактично, вона є пронумерованим набором елементарних функцій. Ці функції використовуються для утворення вихідного Сі-кванту (англ. ci-quantum — cryptographic information quantum) інформації після оброблення вхідних Сі-квантів інформації. За своєю сутністю Сі-квант є мінімальним обсягом інформації, що використовується в CET-операції. Форма Сі-квантів варіюється залежно від варіанту використання CET-операції. Вони можуть існувати у вигляді бітів, байтів, слів, подвійних слів тощо. Класифікація CET-операцій здійснюється відповідно до кількості операндів та кількості Сі-квантів інформації, що кодується. Наприклад, існують 2 або 3 Сі-квантові CET-операції, тобто такі, що кодують два або три Сі-кванти інформації [3, 22].

Слід звернути увагу, що СЕТ-операції неможливо розглядати як просту перестановку або підстановку. Як відомо, перестановка — будь-яке відображення елементів множини самої на себе, а підстановка — пронумерована послідовність елементів множини, що забезпечує їх взаємооднозначне відображення. Ці визначення дозволяють розглядати СЕТ-операцію як підстановку значень, яких набувають вхідні та/або вихідні біти (Сі-кванти) інформації. Проте такі операції реалізують насамперед перетворення дискретної інформації, при якому вихідний біт (Сі-квант) інформації є функцією від вхідних бітів (Сі-квантів). Врахування цього аспекту дає підстави використовувати термін «таблиця підстановки» для аналізу сутності СЕТ-операцій. Але варто зауважити, що порівняння СЕТ-операцій з таблицями підстановки має сенс виключно для операцій з одним (одноопераднних) операцій. СЕТ-операції з декількома (багатьма, тобто багатоопернадні) операндами використовують декілька таблиць підстановок. Їх кількість визначається загальною кількістю біт (Сі-квантів) в операндах. Отже у підсумку можна стверджувати, що СЕТ-операція є набором таблиць підстановки, які представлені дискретною моделлю [3, 22].

Для кращого розуміння сутності СЕТ-операцій, вважаємо доцільним розглянути приклад, з якого почалося їх дослідження. Перш за все, в основу традиційного потокового шифрування покладено послідовне побітове додаванню інформації і псевдовипадкової послідовності за модулем два. Результат такого додавання для біта інформації залежить від псевдовипадкової послідовності, зокрема значення її біта: він залишиться незмінним, або буде інвертованим. Отже можливе здійснення двох операцій над одним бітом інформації. операція повтору (біт псевдовипадкової послідовності дорівнює нулю), та операція інверсії (біт псевдовипадкової послідовності дорівнює один) [3, 22].

Проаналізуємо трансформацію двох біт інформації x^1 та x^2. Множина їх значень складається з чотирьох елементів: «00», «01», «10» та «11». Два біти інформації можливо опрацювати завдяки чотирьом наборам. Кожний набір

містить дві операції для перетворення одного біта інформації. Комбінації можуть складатися з:

- Двох операцій повтору;
- Операції повтору та операції інверсії;
- Операції інверсії і операції повтору;
- Двох операцій інверсії.

Результатом виконання операції перетворення першого біта інформації є перший біт результату перетворення, а сама ця операція буде першою елементарною функцією. Відповідно результатом виконання операції перетворення другого біта інформації є другий біт результату перетворення, а сама ця операція буде другого елементарною функцією. Обидві ці функції використовуються для криптографічного перетворення двох біт інформації. У випадку, якщо біт інформації вважається Сі-квантом інформації, то набори цих елементарних функцій можливо розглядати як чотири 2 Сі-квантові СЕТ-операції. Таке поєднання елементарних функцій в межах операцій дозволяє здійснювати перетворення будь-яких елементів, наприклад двох біт, двох байт, двох слів тощо. В цьому прикладі ототожнення Сі-кванта інформації з бітом інформації спрощує сприйняття сутності СЕТ-операцій [3, 22].

Всі розглянуті СЕТ-операції трансформують вхідні Сі-кванти інформації в вихідні, а другий вхідний — в другий вихідний. Це перетворення Сі-квантів здійснюється незалежно один від одного. Проте іноді можлива залежність одного вихідного Сі-кванту інформації від декількох вхідних. Така залежність призводить до збільшення складності СЕТ-операцій [3, 22]. Проте не залежно від складності вихідні Сі-кванти формуються незалежно один від іншого і тому виконання операції може бути паралельним.

Всі варіанти перетворення двох біт інформації (зокрема 24) наведено у таблиці [3, 22]. Її можливо розглядати як таблицю істинності двадцяти чотирьох 2 Сі-квантових СЕТ-операцій. Ці СЕТ-операції будуються на основі об’єднання дискретних представлень стовпців вихідних даних таблиць істинності операцій. Представлені таблиці істинності для 24 СЕТ-операцій забезпечують реалізацію

всіх можливих варіантів перетворення 2 вхідних Сі-квантів інформації. Таблиці істинності розглянутих чотирьох 2 Сі-квантових СЕТ-операцій представлені за номерами 1, 7, 13 і 19 [3, 22].

Вищевказана інформація дає нам підстави стверджувати, що СЕТ-операції є доволі перспективним рішенням в контексті малоресурсної криптографії. Їх використання відкриває нові можливості в проєктуванні ефективних засобів захисту для малоресурсних систем. Дослідження таких можливостей безпосередньо пов’язане з метою нашого дисертаційного дослідження.

1.4. Мета та завдання дисертаційного дослідження

Моделі СЕТ-операцій є об’єднанням дискретних моделей перетворення наборів вхідних Сі-квантів інформації у вихідний Сі-квант шифрограми. Представленням криптографічних перетворень на основі булевих функцій займалися Лужецький В. А. [10-13], Деменко Є. Є. [18-19], Дмитришин О. В. [11] та інші вітчизняні дослідники. Проте отримані ними результати досліджень принципово не відрізняються від результатів дослідження СЕТ-операцій. Зокрема згадані автори розробляли дискретні моделі наперед визначених операцій перетворення інформації для їх використання в криптографічних алгоритмах. На відміну від описаних ними операцій, СЕТ-операції відображають дискретні моделі таблиць підстановок [4, 20, 56]. Наприклад, якщо в першому випадку для всіх варіантів перетворення двох біт достатньо чотирьох варіантів побудови результату булевою функцією, то при СЕТ-шифрування може бути реалізовано до 24 дискретних моделей таблиць підстановок (СЕТ-операцій) [37, 44]. Для перетворення трьох біт інформації в першому випадку достатньо восьми варіантів побудови результату булевою функцією, а в другому може бути реалізовано до 40320 дискретних моделей таблиць підстановок [5, 14, 26, 45]. З наведеного прикладу можливо

констатувати, що СЕТ-шифрування і СЕТ-операції забезпечують суттєве розширення варіативності крипто алгоритмів за рахунок значного збільшення кількості таблиць підстановки, які можна одночасно використати в криптографічному алгоритмі [70]. Для перетворення одного байта інформації може бути використано до 258 таблиць підстановки, а це значно більше 10 в 250 степені [88].

Оскільки дискретні моделі таблиць підстановок повинні вибиратися псевдовипадковою, то і побудовані потокові СЕТ-шифри можна віднести до шифрів псевдовипадкових підстановок [53].

Особливе місце серед ЗСі-квантових елементарних функцій займають елементарні функції керовані інформацією. Вони відрізняються від інших тим, що Сі-квант результату перетворення прямо залежить від одного з вхідних Сі-квантів, якому належить управління [30, 46]. СЕТ-операції, що побудовані на основі елементарних функцій керованих інформацією, також є СЕТ-операціями керованими інформацією.

Відповідно до класифікації ЗСі-квантових елементарних функцій, до елементарних функцій керованих інформацією, належать елементарні функції перестановок керованих інформацією, і елементарні функції операцій, керованих інформацією, [6, 15]. На основі даних елементарних функцій будуються СЕТ-операції перестановок керованих інформацією, [35, 43, 50, 51]. Також можлива побудова СЕТ-операції на основі елементарні функції операцій, керованих інформацією.

Загалом СЕТ-операції на основі елементарних функцій операцій, керованих інформацією, належать до СЕТ-операцій, які забезпечують нелінійні криптографічні перетворення. Тому їх дослідження пов’язані із складністю вибору і використання математичного апарату.

На відміну від інших елементарних функцій і СЕТ-операцій, елементарні функції і СЕТ-операції перестановок керованих інформацією, мають однаково прості дискретні моделі представлення. Складність дискретної моделі елементарної функції аналогічна складності функції двохрозрядного додавання

по модулю 2. Незначна складність дискретних моделей елементарних функцій і СЕТ-операцій в процесі досліджень дозволила обмежитися використанням математичного апарату дискретної математики для опису моделей нелінійного криптографічного перетворення.

Через значну складність елементарних функцій в операціях на основі елементарних функцій операцій, керованих інформацією, порівняно з елементарними функціями перестановок керованих інформацією, їх дослідження на основі дискретної математики є достатньо складним. В цьому полягає причина з якої цій групі СЕТ-операцій не приділялося достатньої уваги.

Алгоритми реалізації СЕТ-операцій перестановок керованих інформацією, і СЕТ-операцій на основі елементарних функцій операцій, керованих інформацією, прямо керуються вхідною інформацією. Тому потокові шифри, що побудовані на основі даних СЕТ-операцій, будуть керуватися як псевдовипадковою послідовністю, яка забезпечує вибір СЕТ-операцій для криптоперетворення, так і вхідною інформацією, яка забезпечує управління виконанням вибраних СЕТ-операцій [27, 38]. Використання подвійного управління приводе до суттєвого ускладнення процесів криптографічного аналізу.

Публікація результатів наукових досліджень, в яких використано дискретно-казуальне моделювання, створило підґрунтя для можливості синтезу і дослідження елементарних функцій на основі операцій, керованих інформацією, і СЕТ-операцій на основі елементарних функцій операцій, керованих інформацією.

Проаналізувавши сучасний стан та можливі перспективи розвитку СЕТ-шифрування, основною метою нашого дослідження є підвищення варіативності малоресурсних потокових шифрів випадкової підстановки за рахунок розробки і впровадження методу синтезу СЕТ-операцій на основі елементарних функцій операцій, керованих інформацією, які забезпечують можливість подвійного управління процесом криптографічного перетворення, як від ключової

послідовності, так і від вхідної інформації, при збільшенні кількості таблиць підстановки, що реалізуються в криптоалгоритмі

Для досягнення поставленої мети, в дисертаційній роботі необхідно вирішити наступні завдання:

1. Розробити метод синтезу елементарних функцій операцій, керованих інформацією, на основі відомих дискретних моделей елементарних функцій, отриманих за результатами обчислювального експерименту;
2. Розробити метод синтезу ЗСі-квантових СЕТ-операцій, побудованих на основі елементарних функцій операцій, керованих інформацією, які забезпечать можливість подвійного управління процесом криптографічного перетворення інформації;
3. Удосконалити системи потокового шифрування на основі випадкових підстановок.

Висновки до розділу 1.

1. На основі аналізу областей застосування мало ресурсного комп’ютеризованого захисту цифрової інформації було констатовано необхідність розширення і впровадження і різні сфери людської діяльності засоби малоресурсної криптографії.

2. Проведений аналіз методів та засобів мало ресурсного захисту інформації показав недостатню самостійність розвитку цього напрямку комп’ютерної криптографії. Цей висновок базується на тому, що більшість малоресурсних криптоалгоритмів є, по суті, спрощеними версіями відомих повноцінних криптографічних алгоритмів.

3. Одним із перспективних напрямків мало ресурсної криптографії є СЕТ-шифрування, яке базується на використанні таблиць підстановок, що представлені дискретними моделями.

4. Проведений аналіз сучасного стану і перспектив розвитку СЕТ-шифрування дозволив сформулювати мету і завдання дисертаційного дослідження.

РОЗДІЛ 2. ДОСЛІДЖЕННЯ І СИНТЕЗ ЕЛЕМЕНТАРНИХ ФУНКЦІЙ ОПЕРАЦІЙ, КЕРОВАНИХ ІНФОРМАЦІЄЮ

2.1. Дослідження елементарних функцій операцій, керованих інформацією, на основі дискретно-алгебраїчних моделей

2.1.1 Синтез дискретно-алгебраїчних моделей елементарних функцій операцій, керованих інформацією

2.1.1.1 Синтез дискретно-алгебраїчних моделей прямих елементарних функцій операцій, керованих інформацією

Серед трьохрозрядних елементарних функцій, які можуть використовуватися в криптографічних перетвореннях, на сьогоднішній день не досліджувались елементарні функції операцій, керованих інформацією. Проте ці елементарні функції мають важливе значення в теорії шифрування, адже дозволяють будувати ЗСі-квантові одноопераднідні СЕТ-операції, які керуються інформацією [48].

Відповідно до класифікації трьох розрядних елементарних функцій для криптографічних перетворень, [32] група елементарних функцій операцій, керованих інформацією, містить 8 елементарних функцій [48]. Ці елементарні функції наведені в табл. 2.1. Індекси елементарних функцій в цій таблиці відповідають значенню десяткової цифри результату перетворення, за умови впорядкування повної множини вхідних даних по зростанню їх значень [48].

Таблиця 2.1

Группа елементарних функцій операцій, керованих інформацією,

Элементарна функція	Результат реалізації	Элементарна функція	Результат реалізації
$f_{23} = x_1 \cdot x_2 \vee x_1 \cdot x_3 \vee x_2 \cdot x_3$	00010111	$f_{232} = \bar{x}_1 \cdot \bar{x}_2 \vee \bar{x}_1 \cdot \bar{x}_3 \vee \bar{x}_2 \cdot \bar{x}_3$	11101000
$f_{43} = x_1 \cdot x_2 \vee x_1 \cdot \bar{x}_3 \vee x_2 \cdot \bar{x}_3$	00101011	$f_{212} = \bar{x}_1 \cdot \bar{x}_2 \vee \bar{x}_1 \cdot x_3 \vee \bar{x}_2 \cdot x_3$	11010100
$f_{77} = x_1 \cdot \bar{x}_2 \vee x_1 \cdot x_3 \vee \bar{x}_2 \cdot x_3$	01001101	$f_{178} = \bar{x}_1 \cdot x_2 \vee \bar{x}_1 \cdot \bar{x}_3 \vee x_2 \cdot \bar{x}_3$	10110010
$f_{113} = \bar{x}_1 \cdot x_2 \vee \bar{x}_1 \cdot x_3 \vee x_2 \cdot x_3$	01110001	$f_{142} = x_1 \cdot \bar{x}_2 \vee x_1 \cdot \bar{x}_3 \vee \bar{x}_2 \cdot \bar{x}_3$	10001110

Як видно з табл. 2.1, елементарні функції операцій, керованих інформацією, поділено на дві групи: прямі елементарні функції і обернені елементарні функції. Поділ було виконано на основі результатів реалізації перетворення. Кожній прямій елементарній функції відповідає обернена елементарна функція. Розподіл на прямі і обернені елементарні функції було виконано в порядку зростання індексів елементарних функцій. В кожній парі функцій прямою вважалася та індекс якої менший [48].

Наприклад для пари елементарних функцій f_{23} і f_{232} функція f_{23} вважається прямою, а f_{232} - оберненою, так як 23<232. Для пари елементарних функцій f_{212} і f_{43} функція f_{212} вважається оберненою, а f_{43} - прямою, так як 212>43 [48].

Проте коректність розподілу на прямі і обернені елементарні функції не досліджувалась. Встановити коректність розподілу можливо лише при детальному дослідження особливостей елементарних функцій та їх поєднання в СЕТ-операції [48].

Дослідимо прямі елементарні функції. Розглянемо елементарну функцію $f_{23} = x_1 \cdot x_2 \vee x_1 \cdot x_3 \vee x_2 \cdot x_3$ [32]. Для встановлення особливостей даної елементарної функції побудуємо її таблицю істинності та синтезуємо спрощені дискретні моделі. Дані дискретні моделі не обов’язково повинні представляти собою мінімальні диз’юнктивно-нормальні форми представлення. Дані моделі в

першу чергу повинні відображати фізичну сутність даної елементарної функції. Таблиця істинності f_{23} представлена в табл. 2.2 [48].

Для побудови спрощених дискретних моделей елементарної функції використаємо карти Карно (табл. 2.3 – табл. 2.5). Карти Карно наведені в даних таблицях будуть відрізнятися лише вибраними контурами, які відрізняються різними штриховками. Якщо клітинка карти включається в різні контури, то вона буде включати декілька штриховок.

Таблиця 2.2

Таблиця істинності елементарної функції f_{23}

Вхідні дані			Результат перетворення
x_1	x_2	x_3	f_{23}
0	**0**	**0**	**0**
0	**0**	**1**	**0**
0	**1**	**0**	**0**
0	**1**	**1**	**1**
1	**0**	**0**	**0**
1	**0**	**1**	**1**
1	**1**	**0**	**1**
1	**1**	**1**	**1**

Варіант 1.1.

Таблиця 2.3

Карта Карно з виділеними контурами (варіант 1.1)

x_1	x_2	f_{23}	
0	**0**	**0**	**0**
0	**1**	**0**	**1**
1	**1**	**1**	**1**
1	**0**	**0**	**1**
		$\bar{x}_3$	x_3

На основі трьох виділених контурів отримаємо дискретну модель та перейдемо до дискретно-алгебраїчного представлення елементарної функції [7]:

$$f_{23} = x_1 \cdot x_2 \vee x_1 \cdot x_3 \vee \bar{x}_1 \cdot x_2 \cdot x_3 = \begin{cases} x_2 \cdot x_3 & якщо \quad x_1 = 0 \\ x_2 \vee x_3 & якщо \quad x_1 = 1 \end{cases} \qquad (2.1)$$

Варіант 1.2.

Таблиця 2.4

Карта Карно з виділеними контурами (варіант 1.2)

x_1	x_2	f_{23}	
0	**0**	**0**	**0**
0	**1**	**0**	**1**
1	**1**	**1**	**1**
1	**0**	**0**	**1**
		$\bar{x}_3$	x_3

На основі трьох виділених контурів отримаємо дискретно-алгебраїчне представлення елементарної функції:

$$f_{23} = x_1 \cdot x_2 \vee x_2 \cdot x_3 \vee x_1 \cdot \bar{x}_2 \cdot x_3 = \begin{cases} x_1 \cdot x_3 & якщо \quad x_2 = 0 \\ x_1 \vee x_3 & якщо \quad x_2 = 1 \end{cases} \qquad (2.2)$$

Варіант 1.3.

Таблиця 2.5

Карта Карно з виділеними контурами (варіант 1.3)

x_1	x_2	f_{23}	
0	**0**	**0**	**0**
0	**1**	**0**	**1**
1	**1**	**1**	**1**
1	**0**	**0**	**1**
		$\bar{x}_3$	x_3

На основі трьох виділених контурів отримаємо наступне дискретно-алгебраїчне представлення елементарної функції:

$$f_{23} = x_1 \cdot x_3 \vee x_2 \cdot x_3 \vee x_1 \cdot x_2 \cdot \bar{x}_3 = \begin{cases} x_1 \cdot x_2 & якщо \quad x_3 = 0 \\ x_1 \vee x_2 & якщо \quad x_3 = 1 \end{cases} \qquad (2.3)$$

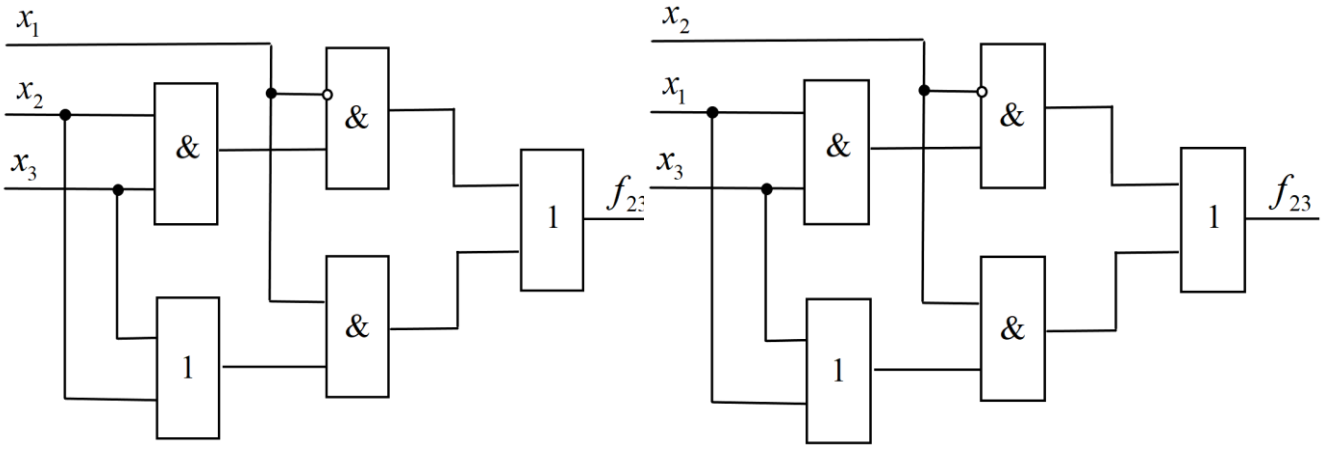
На основі отриманих дискретно-алгебраїчних представлень елементарної функції f_{23} можна зробити припущення, що дана елементарна функція для вибору операції логічного додавання ($\vee$), або логічного множення ($\cdot$) буде використовувати будь який вхідний Сі-квант (x_1, x_2, або x_3) [48].

Функціональні схеми реалізації елементарної функції в залежності від вибраного Сі-кванта управління представлені на рис. 2.1 [32].

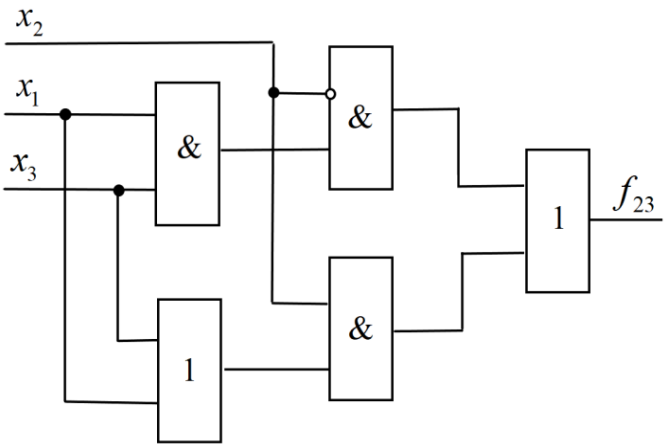
Функціональні схеми реалізації елементарної функції f_{23} відрізняються лише нумерацією вхідних Сі-квантів.

Розглянемо елементарну функцію $f_{43} = x_1 \cdot x_2 \vee x_1 \cdot \bar{x}_3 \vee x_2 \cdot \bar{x}_3$.

Таблиця істинності f_{43} представлена в табл. 2.6.



а) Управління на основі x_1 б) Управління на основі x_2



в) Управління на основі x_3

Рис. 2.1. Функціональні схеми реалізації елементарної функції f_{23}

Таблиця 2.6

Таблиця істинності елементарної функції f_{43}

Вхідні дані			Результат перетворення
x_1	x_2	x_3	f_{43}
0	**0**	**0**	**0**
0	**0**	**1**	**0**
0	**1**	**0**	**1**
0	**1**	**1**	**0**
1	**0**	**0**	**1**
1	**0**	**1**	**0**
1	**1**	**0**	**1**
1	**1**	**1**	**1**

Побудуємо дискретні моделі елементарної функції f_{43} та її дискретно-алгебраїчне представлення. Карти Карно для побудови дискретних моделей наведені в табл..2.7 – табл..2.9.

Варіант 2.1.

Таблиця 2.7

Карта Карно з виділеними контурами (варіант 2.1)

x_1	x_2	f_{43}	
0	**0**	**0**	**0**
0	**1**	**1**	**0**
1	**1**	**1**	**1**
1	**0**	**1**	**0**
		$\bar{x}_3$	x_3

Дискретну модель та дискретно-алгебраїчне представлення елементарної функції f_{43} можна представити:

$$f_{43} = x_1 \cdot x_2 \vee x_1 \cdot \bar{x}_3 \vee \bar{x}_1 \cdot x_2 \cdot \bar{x}_3 = \begin{cases} x_2 \cdot \bar{x}_3 \ \textit{якщо} \ \ x_1 = 0 \\ x_2 \vee \bar{x}_3 \ \ \textit{якщо} \ \ x_1 = 1 \end{cases} \qquad (2.4)$$

Варіант 2.2.

Таблиця 2.8

Карта Карно з виділеними контурами (варіант 2.2)

x_1	x_2	f_{43}	
0	**0**	**0**	**0**
0	**1**	**1**	**0**
1	**1**	**1**	**1**
1	**0**	**1**	**0**
		$\bar{x}_3$	x_3

Отримаємо дискретну модель та дискретно-алгебраїчне представлення елементарної функції f_{43}:

$$f_{43} = x_1 \cdot x_2 \vee x_2 \cdot \bar{x}_3 \vee x_1 \cdot \bar{x}_2 \cdot \bar{x}_3 = \begin{cases} x_1 \cdot \bar{x}_3 \ \ \textit{якщо} \ \ x_2 = 0 \\ x_1 \vee \bar{x}_3 \ \ \textit{якщо} \ \ x_2 = 1 \end{cases} \qquad (2.5)$$

Варіант 2.3.

Таблиця 2.9

Карта Карно з виділеними контурами (варіант 2.3)

x_1	x_2	f_{43}	
0	**0**	**0**	**0**
0	**1**	**1**	**0**
1	**1**	**1**	**1**
1	**0**	**1**	**0**
		$\bar{x}_3$	x_3

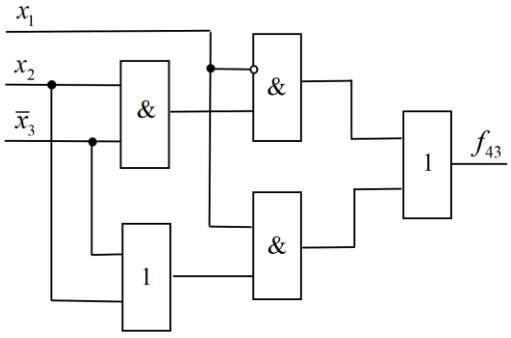
На основі трьох виділених контурів отримаємо дискретно-алгебраїчне представлення елементарної функції f_{43}:

$$f_{43} = x_1 \cdot \bar{x}_3 \vee x_2 \cdot \bar{x}_3 \vee x_1 \cdot x_2 \cdot x_3 = \begin{cases} x_1 \vee x_2 & якщо \quad x_3 = 0 \\ x_1 \cdot x_2 & якщо \quad x_3 = 1 \end{cases} \qquad (2.6)$$

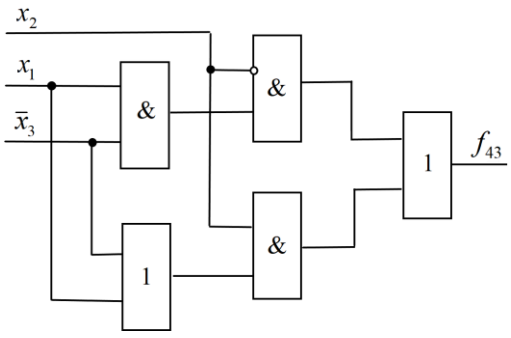
В залежності від вибраних Сі-квантів управління, на основі виразів (2.4), (2.5) і (2.6) побудуємо функціональні схеми реалізації елементарної функції f_{43}. При побудові функціональних схем спробуємо отримати максимальне співпадіння з функціональними схемами реалізації елементарної функції f_{23}, наведеними на рис. 2.1. Побудовані функціональні схеми представлені на рис. 2.2 [32].

Як видно із рис. 2.2, функціональні схеми реалізації елементарної функції f_{43} відрізняються від функціональних схем реалізації елементарної функції f_{23} лише інверсним значенням третього Сі-кванта.

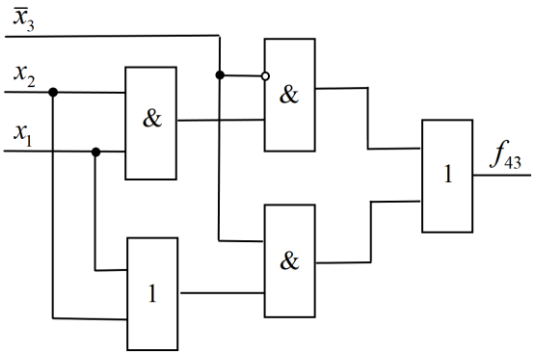
Розглянемо елементарну функцію $f_{77} = x_1 \cdot \bar{x}_2 \vee x_1 \cdot x_3 \vee \bar{x}_2 \cdot x_3$. Таблиця істинності елементарної функції f_{77} наведена в табл. 2.10.



а) Управління на основі x_1



б) Управління на основі x_2



в) Управління на основі x_3

Рис. 2.2. Функціональні схеми реалізації елементарної функції f_{43}

Таблиця 2.10

Таблиця істинності елементарної функції f_{77}

Вхідні дані			Результат перетворення
x_1	x_2	x_3	f_{77}
0	**0**	**0**	**0**
0	**0**	**1**	**1**
0	**1**	**0**	**0**
0	**1**	**1**	**0**
1	**0**	**0**	**1**
1	**0**	**1**	**1**
1	**1**	**0**	**0**
1	**1**	**1**	**1**

Карти Карно для побудови дискретних моделей елементарної функції f_{77} наведені в табл. 2.11 – табл. 2.13.

Варіант 3.1.

Таблиця 2.11

Карта Карно з виділеними контурами (варіант 3.1)

x_1	x_2	f_{77}	
0	**0**	**0**	**1**
0	**1**	**0**	**0**
1	**1**	**0**	**1**
1	**0**	**1**	**1**
		$\bar{x}_3$	x_3

Дискретну модель та дискретно-алгебраїчне представлення елементарної функції f_{77} можна представити:

$$f_{77} = x_1 \cdot \bar{x}_2 \vee x_1 \cdot x_3 \vee \bar{x}_1 \cdot \bar{x}_2 \cdot x_3 = \begin{cases} \bar{x}_2 \cdot x_3 & \textit{якщо} \quad x_1 = 0 \\ \bar{x}_2 \vee x_3 & \textit{якщо} \quad x_1 = 1 \end{cases} \qquad (2.7)$$

Варіант 3.2.

Таблиця 2.12

Карта Карно з виділеними контурами (варіант 3.2)

x_1	x_2	f_{77}	
0	**0**	**0**	**1**
0	**1**	**0**	**0**
1	**1**	**0**	**1**
1	**0**	**1**	**1**
		$\bar{x}_3$	x_3

Отримаємо дискретну модель та дискретно-алгебраїчне представлення елементарної функції f_{77}:

$$f_{77} = x_1 \cdot \bar{x}_2 \vee \bar{x}_2 \cdot x_3 \vee x_1 \cdot x_2 \cdot x_3 = \begin{cases} x_1 \vee x_3 & якщо \quad x_2 = 0 \\ x_1 \cdot x_3 & якщо \quad x_2 = 1 \end{cases} \qquad (2.8)$$

Варіант 3.3.

Таблиця 2.13

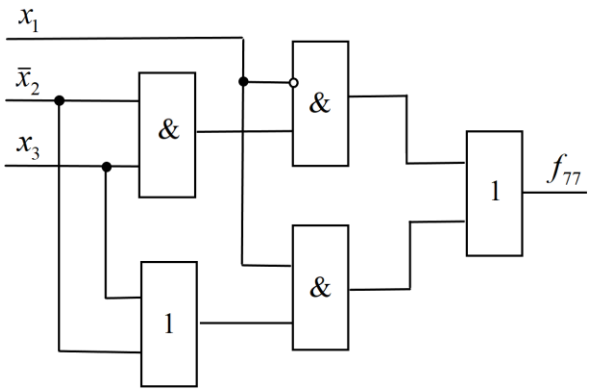
Карта Карно з виділеними контурами (варіант 3.3)

x_1	x_2	f_{77}	
0	**0**	**0**	**1**
0	**1**	**0**	**0**
1	**1**	**0**	**1**
1	**0**	**1**	**1**
		$\bar{x}_3$	x_3

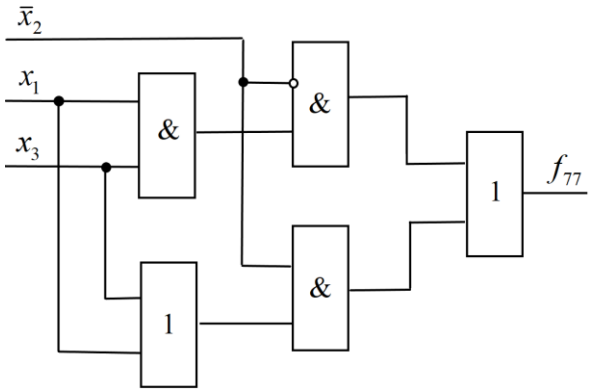
На основі трьох виділених контурів отримаємо дискретно-алгебраїчне представлення елементарної функції f_{77}:

$$f_{77} = x_1 \cdot x_3 \vee \bar{x}_2 \cdot x_3 \vee x_1 \cdot \bar{x}_2 \cdot \bar{x}_3 = \begin{cases} x_1 \cdot \bar{x}_2 & якщо \quad x_3 = 0 \\ x_1 \vee \bar{x}_2 & якщо \quad x_3 = 1 \end{cases} \qquad (2.9)$$

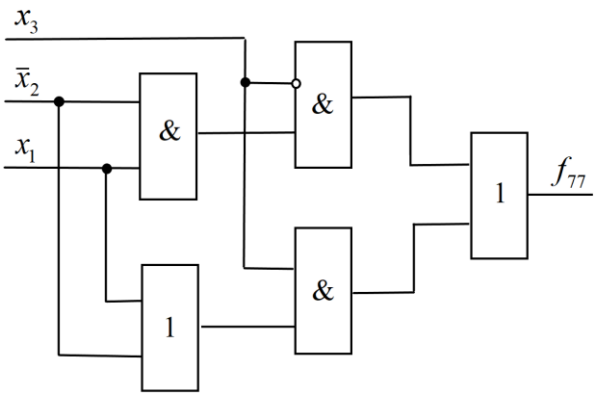
На основі виразів (2.7), (2.8) і (2.9) побудуємо функціональні схеми реалізації елементарної функції f_{77}. Дані функціональні схеми представлені на рис. 2.3.



а) Управління на основі x_1



б) Управління на основі x_2



в) Управління на основі x_3

Рис. 2.3. Функціональні схеми реалізації елементарної функції f_{77}

Як видно із рис. 2.2, функціональні схеми реалізації елементарної функції f_{77} відрізняються від функціональних схем реалізації елементарної функції f_{23} лише інверсним значенням другого Сі-кванта.

Розглянемо елементарну функцію $f_{113} = \bar{x}_1 \cdot x_2 \vee \bar{x}_1 \cdot x_3 \vee x_2 \cdot x_3$.

Таблиця істинності f_{113} представлена в табл. 2.14.

Таблиця 2.14

Таблиця істинності елементарної функції f_{43}

Вхідні дані			Результат перетворення
x_1	x_2	x_3	f_{113}
0	**0**	**0**	**0**
0	**0**	**1**	**1**
0	**1**	**0**	**1**
0	**1**	**1**	**1**
1	**0**	**0**	**0**
1	**0**	**1**	**0**
1	**1**	**0**	**0**
1	**1**	**1**	**1**

Побудуємо дискретні моделі елементарної функції f_{113} та її дискретно-алгебраїчне представлення. Карти Карно для побудови дискретних моделей наведені в табл. 2.15 – табл. 2.17.

Варіант 4.1.

Таблиця 2.15

Карта Карно з виділеними контурами (варіант 4.1)

x_1	x_2	f_{113}	
0	**0**	**0**	**1**
0	**1**	**1**	**1**
1	**1**	**0**	**1**
1	**0**	**0**	**0**
		$\bar{x}_3$	x_3

Дискретну модель та дискретно-алгебраїчне представлення елементарної функції f_{113} можна представити:

$$f_{113} = \bar{x}_1 \cdot x_2 \vee x_1 \cdot x_3 \vee x_1 \cdot x_2 \cdot x_3 = \begin{cases} x_2 \vee x_3 \ \textit{якщо} \ \ x_1 = 0 \\ x_2 \cdot x_3 \ \ \textit{якщо} \ \ x_1 = 1 \end{cases} \qquad (2.10)$$

Варіант 4.2.

Таблиця 2.16

Карта Карно з виділеними контурами (варіант 4.2)

x_1	x_2	f_{113}	
0	**0**	**0**	**1**
0	**1**	**1**	**1**
1	**1**	**0**	**1**
1	**0**	**0**	**0**
		$\bar{x}_3$	x_3

Отримаємо дискретну модель та дискретно-алгебраїчне представлення елементарної функції f_{113}:

$$f_{113} = \bar{x}_1 \cdot x_2 \vee x_2 \cdot x_3 \vee \bar{x}_1 \cdot \bar{x}_2 \cdot x_3 = \begin{cases} \bar{x}_1 \cdot x_3 \ \textit{якщо} \ \ x_2 = 0 \\ \bar{x}_1 \vee x_3 \ \ \textit{якщо} \ \ x_2 = 1 \end{cases} \qquad (2.11)$$

Варіант 4.3.

Таблиця 2.17

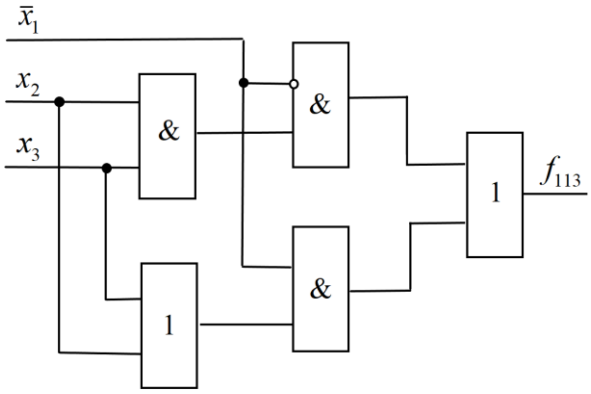
Карта Карно з виділеними контурами (варіант 4.3)

x_1	x_2	f_{113}	
0	**0**	**0**	**1**
0	**1**	**1**	**1**
1	**1**	**0**	**1**
1	**0**	**0**	**0**
		$\bar{x}_3$	x_3

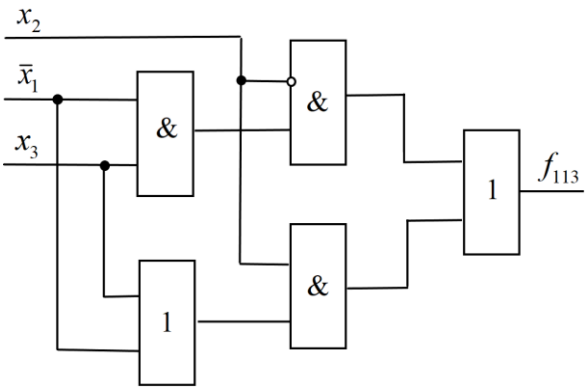
На основі трьох виділених контурів отримаємо дискретно-алгебраїчне представлення елементарної функції f_{113}:

$$f_{113} = \bar{x}_1 \cdot x_3 \vee x_2 \cdot x_3 \vee \bar{x}_1 \cdot x_2 \cdot \bar{x}_3 = \begin{cases} \bar{x}_1 \cdot x_2 \ \textit{якщо} \ \ x_3 = 0 \\ \bar{x}_1 \vee x_2 \ \ \textit{якщо} \ \ x_3 = 1 \end{cases} \qquad (2.12)$$

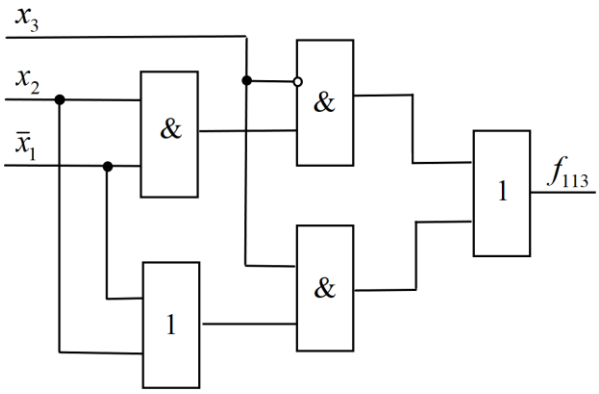
Побудуємо функціональні схеми реалізації елементарної функції f_{113} на основі виразів (2.10), (2.11) і (2.12). Дані функціональні схеми представлені на мал. 2.4 [32].



а) Управління на основі x_1



б) Управління на основі x_2



в) Управління на основі x_3

Рис. 2.4. Функціональні схеми реалізації елементарної функції f_{113}

Як видно із рис. 2.4, функціональні схеми реалізації елементарної функції f_{77} відрізняються від функціональних схем реалізації елементарної функції f_{23} лише інверсним значенням першого Сі-кванта.

2.1.1.2 Синтез дискретно-алгебраїчних моделей обернених елементарних функцій операцій, керованих інформацією

Побудуємо і проаналізуємо обернені елементарні функції. Для цього розглянемо елементарну функцію $f_{232} = \bar{x}_1 \cdot \bar{x}_2 \vee \bar{x}_1 \cdot \bar{x}_3 \vee \bar{x}_2 \cdot \bar{x}_3$.

Таблиця істинності f_{232} представлена в табл. 2.17.

Таблиця 2.17

Таблиця істинності елементарної функції f_{232}

Вхідні дані			Результат перетворення
x_1	x_2	x_3	f_{232}
0	**0**	**0**	**1**
0	**0**	**1**	**1**
0	**1**	**0**	**1**
0	**1**	**1**	**0**
1	**0**	**0**	**1**
1	**0**	**1**	**0**
1	**1**	**0**	**0**
1	**1**	**1**	**0**

Побудуємо дискретні моделі елементарної функції f_{232} та її дискретно-алгебраїчне представлення. Карти Карно для побудови дискретних моделей наведені в табл. 2.17 – табл. 2.19.

Варіант 5.1.

Таблиця 2.17

Карта Карно з виділеними контурами (варіант 5.1)

x_1	x_2	f_{232}	
0	**0**	**1**	**1**
0	**1**	**1**	**0**
1	**1**	**0**	**0**
1	**0**	**1**	**0**
		$\bar{x}_3$	x_3

Дискретну модель та дискретно-алгебраїчне представлення елементарної функції f_{232} можна представити:

$$f_{232} = \bar{x}_1 \cdot \bar{x}_2 \vee \bar{x}_1 \cdot \bar{x}_3 \vee \bar{x}_1 \cdot \bar{x}_2 \cdot \bar{x}_3 = \begin{cases} \bar{x}_2 \vee \bar{x}_3 \ \textit{якщо} \ \ x_1 = 0 \\ \bar{x}_2 \cdot \bar{x}_3 \ \ \textit{якщо} \ \ x_1 = 1 \end{cases} \qquad (2.13)$$

Варіант 5.2.

Таблиця 2.18

Карта Карно з виділеними контурами (варіант 5.2)

x_1	x_2	f_{232}	
0	**0**	**1**	**1**
0	**1**	**1**	**0**
1	**1**	**0**	**0**
1	**0**	**1**	**0**
		$\bar{x}_3$	x_3

Отримаємо дискретну модель та дискретно-алгебраїчне представлення елементарної функції f_{232}:

$$f_{232} = \bar{x}_1 \cdot \bar{x}_2 \vee \bar{x}_2 \cdot \bar{x}_3 \vee \bar{x}_1 \cdot x_2 \cdot \bar{x}_3 = \begin{cases} \bar{x}_1 \vee \bar{x}_3 \ \textit{якщо} \ \ x_2 = 0 \\ \bar{x}_1 \cdot \bar{x}_3 \ \ \textit{якщо} \ \ x_2 = 1 \end{cases} \qquad (2.14)$$

Варіант 5.3.

Таблиця 2.19

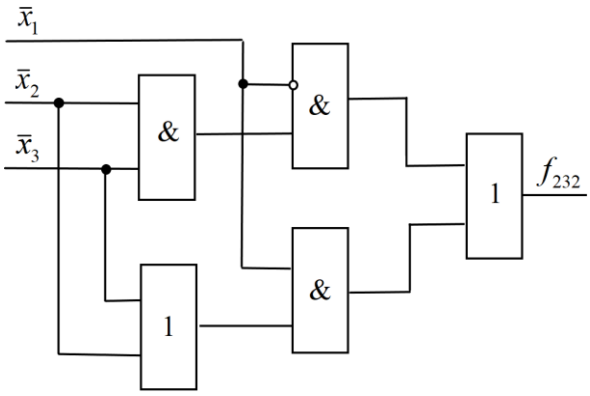
Карта Карно з виділеними контурами (варіант 5.3)

x_1	x_2	f_{232}	
0	**0**	**1**	**1**
0	**1**	**1**	**0**
1	**1**	**0**	**0**
1	**0**	**1**	**0**
		$\bar{x}_3$	x_3

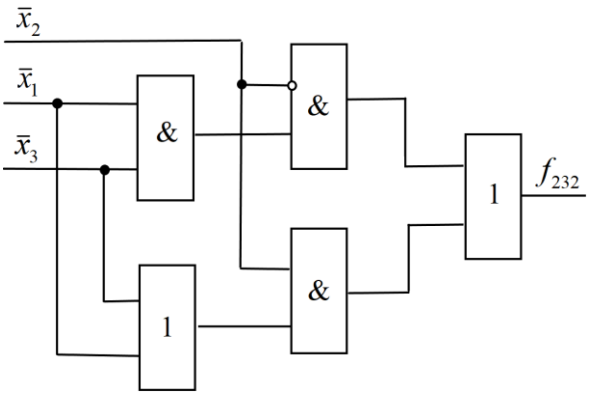
На основі трьох виділених контурів отримаємо дискретно-алгебраїчне представлення елементарної функції f_{232}:

$$f_{232} = \bar{x}_1 \cdot \bar{x}_3 \vee \bar{x}_2 \cdot \bar{x}_3 \vee \bar{x}_1 \cdot \bar{x}_2 \cdot x_3 = \begin{cases} \bar{x}_1 \vee \bar{x}_2 & якщо \quad x_3 = 0 \\ \bar{x}_1 \cdot \bar{x}_2 & якщо \quad x_3 = 1 \end{cases} \tag{2.15}$$

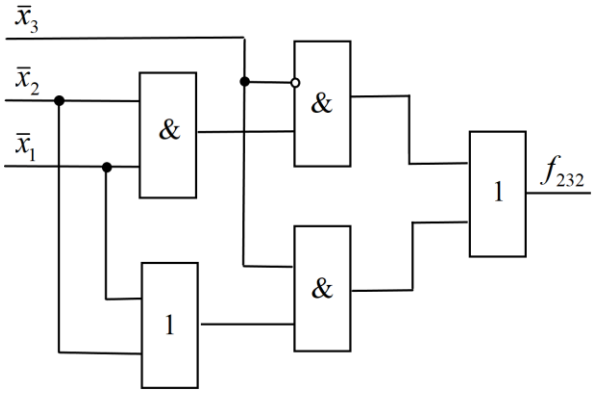
В залежності від вибраних Сі-квантів управління, на основі виразів (2.13), (2.14) і (2.15) побудуємо функціональні схеми реалізації елементарної функції f_{232}. Побудовані функціональні схеми представлені на рис. 2.5.



а) Управління на основі x_1



б) Управління на основі x_2



в) Управління на основі x_3

Рис. 2.5. Функціональні схеми реалізації елементарної функції f_{232}

Елементарна функція f_{232} є оберненою елементарною функцією до елементарної функції f_{23}. Як видно із рис. 2.5, функціональні схеми реалізації

елементарної функції f_{232} відрізняються від функціональних схем реалізації елементарної функції f_{23} інверсними значеннями всіх трьох Сі-квантів.

Розглянемо елементарну функцію $f_{212} = \bar{x}_1 \cdot \bar{x}_2 \vee \bar{x}_1 \cdot x_3 \vee \bar{x}_2 \cdot x_3$. Таблиця істинності елементарної функції f_{212} наведена в табл. 2.20.

Карти Карно для побудови дискретних моделей елементарної функції f_{212} наведені в табл. 2.21 – табл. 2.23.

Таблиця 2.20

Таблиця істинності елементарної функції f_{77}

Вхідні дані			Результат перетворення
x_1	x_2	x_3	f_{212}
0	**0**	**0**	**1**
0	**0**	**1**	**1**
0	**1**	**0**	**0**
0	**1**	**1**	**1**
1	**0**	**0**	**0**
1	**0**	**1**	**1**
1	**1**	**0**	**0**
1	**1**	**1**	**0**

Варіант 6.1.

Таблиця 2.21

Карта Карно з виділеними контурами (варіант 6.1)

x_1	x_2	f_{212}	
0	**0**	**1**	**1**
0	**1**	**0**	**1**
1	**1**	**0**	**0**
1	**0**	**0**	**1**
		$\bar{x}_3$	x_3

Дискретну модель та дискретно-алгебраїчне представлення елементарної функції f_{212} можна представити:

$$f_{212} = \bar{x}_1 \cdot \bar{x}_2 \vee \bar{x}_1 \cdot x_3 \vee x_1 \cdot \bar{x}_2 \cdot x_3 = \begin{cases} \bar{x}_2 \vee x_3 & якщо \quad x_1 = 0 \\ \bar{x}_2 \cdot x_3 & якщо \quad x_1 = 1 \end{cases} \qquad (2.16)$$

Варіант 6.2.

Таблиця 2.22

Карта Карно з виділеними контурами (варіант 6.2)

x_1	x_2	f_{212}	
0	**0**	**1**	**1**
0	**1**	**0**	**1**
1	**1**	**0**	**0**
1	**0**	**0**	**1**
		$\bar{x}_3$	x_3

Отримаємо дискретну модель та дискретно-алгебраїчне представлення елементарної функції f_{212}:

$$f_{212} = \bar{x}_1 \cdot \bar{x}_2 \vee \bar{x}_2 \cdot x_3 \vee \bar{x}_1 \cdot x_2 \cdot x_3 = \begin{cases} \bar{x}_1 \vee x_3 & якщо \quad x_2 = 0 \\ \bar{x}_1 \cdot x_3 & якщо \quad x_2 = 1 \end{cases} \qquad (2.17)$$

Варіант 6.3.

Таблиця 2.23

Карта Карно з виділеними контурами (варіант 6.3)

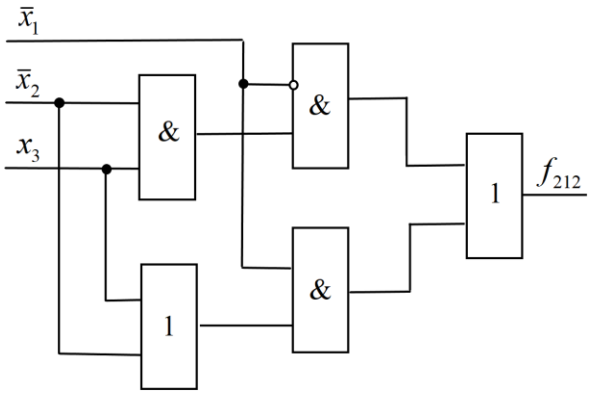
x_1	x_2	f_{212}	
0	**0**	**1**	**1**
0	**1**	**0**	**1**
1	**1**	**0**	**0**
1	**0**	**0**	**1**
		$\bar{x}_3$	x_3

На основі трьох виділених контурів отримаємо дискретно-алгебраїчне представлення елементарної функції f_{212}:

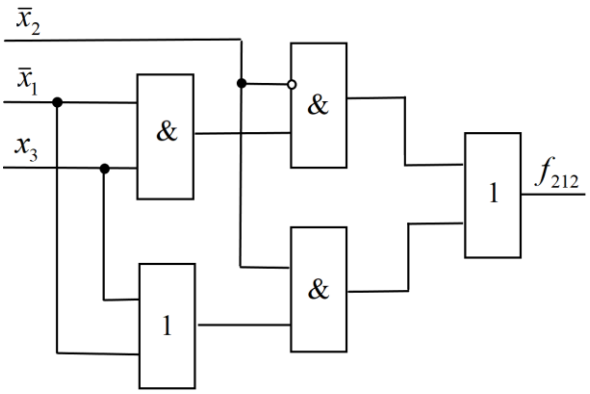
$$f_{212} = \bar{x}_1 \cdot x_3 \vee \bar{x}_2 \cdot x_3 \vee \bar{x}_1 \cdot \bar{x}_2 \cdot \bar{x}_3 = \begin{cases} \bar{x}_2 \cdot x_3 & якщо \quad x_3 = 0 \\ \bar{x}_2 \vee x_3 & якщо \quad x_3 = 1 \end{cases} \qquad (2.18)$$

На основі виразів (2.16), (2.17) і (2.18) побудуємо функціональні схеми реалізації елементарної функції f_{212} Дані функціональні схеми представлені на рис. 2.6.

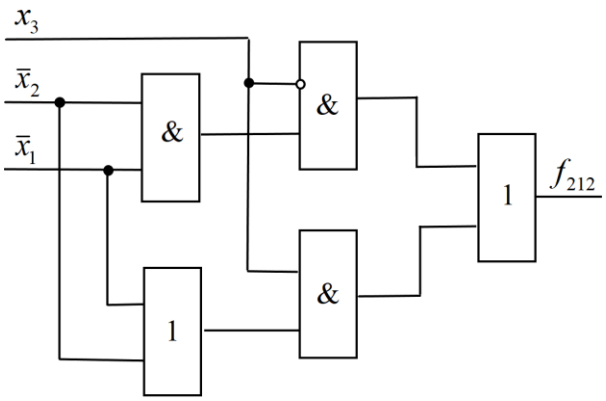
Як видно із рис. 2.6, функціональні схеми реалізації елементарної функції f_{212} відрізняються від функціональних схем реалізації елементарної функції f_{43}, представлених на рис. 2.2, інверсними значеннями всіх трьох Сі-квантів. Інверсне значення всіх трьох Сі-квантів пояснюється тим, що елементарна функція f_{232} є оберненою елементарною функцією до елементарної функції f_{43}.



а) Управління на основі x_1



б) Управління на основі x_2



в) Управління на основі x_3

Рис. 2.6. Функціональні схеми реалізації елементарної функції f_{212}

Розглянемо елементарну функцію $f_{178} = \bar{x}_1 \cdot x_2 \vee \bar{x}_1 \cdot \bar{x}_3 \vee x_2 \cdot \bar{x}_3$. Таблиця істинності елементарної функції f_{178} наведена в табл. 2.24.

Таблиця 2.24

Таблиця істинності елементарної функції f_{178}

Вхідні дані			Результат перетворення
x_1	x_2	x_3	f_{178}
0	**0**	**0**	**1**
0	**0**	**1**	**0**
0	**1**	**0**	**1**
0	**1**	**1**	**1**
1	**0**	**0**	**0**
1	**0**	**1**	**0**
1	**1**	**0**	**1**
1	**1**	**1**	**0**

Карти Карно для побудови дискретних моделей елементарної функції f_{178} наведені в табл..2.25 – табл..2.27.

Варіант 7.1.

Таблиця 2.25

Карта Карно з виділеними контурами (варіант 7.1)

x_1	x_2	f_{178}	
0	**0**	**1**	**0**
0	**1**	**1**	**1**
1	**1**	**1**	**0**
1	**0**	**0**	**0**
		$\bar{x}_3$	x_3

Дискретну модель та дискретно-алгебраїчне представлення елементарної функції f_{178} можна представити:

$$f_{178} = \bar{x}_1 \cdot x_2 \vee \bar{x}_1 \cdot \bar{x}_3 \vee x_1 \cdot x_2 \cdot \bar{x}_3 = \begin{cases} x_2 \vee \bar{x}_3 & якщо \quad x_1 = 0 \\ x_2 \cdot \bar{x}_3 & якщо \quad x_1 = 1 \end{cases} \qquad (2.19)$$

Варіант 7.2.

Таблиця 2.26

Карта Карно з виділеними контурами (варіант 7.2)

x_1	x_2	f_{178}	
0	**0**	**1**	**0**
0	**1**	**1**	**1**
1	**1**	**1**	**0**
1	**0**	**0**	**0**
		$\bar{x}_3$	x_3

Отримаємо дискретну модель та дискретно-алгебраїчне представлення елементарної функції f_{178}:

$$f_{178} = \bar{x}_1 \cdot x_2 \vee x_2 \cdot \bar{x}_3 \vee \bar{x}_1 \cdot \bar{x}_2 \cdot \bar{x}_3 = \begin{cases} \bar{x}_1 \cdot \bar{x}_3 & якщо \quad x_2 = 0 \\ \bar{x}_1 \vee \bar{x}_3 & якщо \quad x_2 = 1 \end{cases} \tag{2.20}$$

Варіант 7.3.

Таблиця 2.27

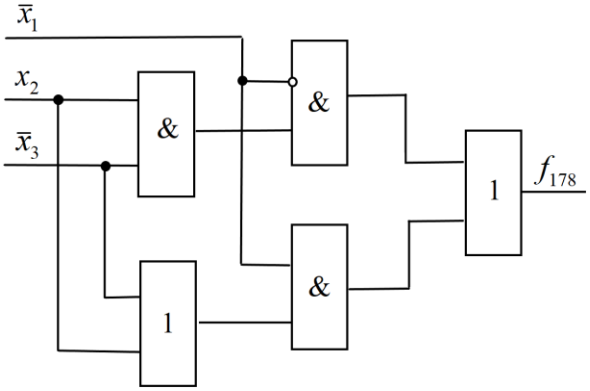
Карта Карно з виділеними контурами (варіант 7.3)

x_1	x_2	f_{178}	
0	**0**	**1**	**0**
0	**1**	**1**	**1**
1	**1**	**1**	**0**
1	**0**	**0**	**0**
		$\bar{x}_3$	x_3

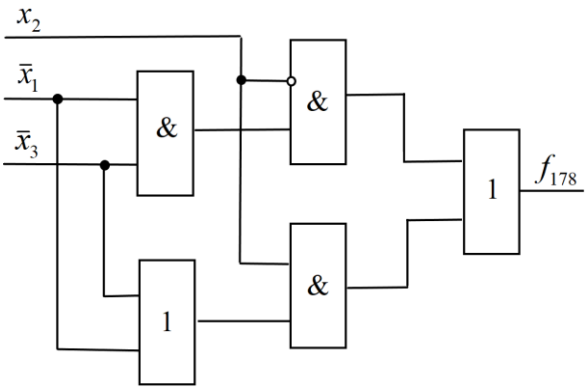
На основі трьох виділених контурів отримаємо дискретно-алгебраїчне представлення елементарної функції f_{178}:

$$f_{178} = \bar{x}_1 \cdot \bar{x}_3 \vee x_2 \cdot \bar{x}_3 \vee \bar{x}_1 \cdot x_2 \cdot x_3 = \begin{cases} \bar{x}_1 \vee x_2 & якщо \quad x_3 = 0 \\ \bar{x}_1 \cdot x_2 & якщо \quad x_3 = 1 \end{cases} \tag{2.21}$$

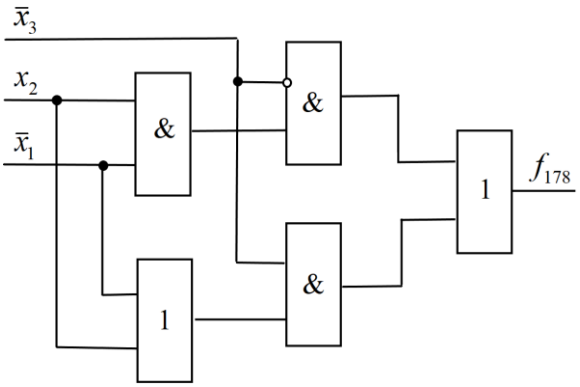
На основі виразів (2.19), (2.20) і (2.21) побудуємо функціональні схеми реалізації елементарної функції f_{178}. Дані функціональні схеми представлені на рис. 2.7.



а) Управління на основі x_1



б) Управління на основі x_2



в) Управління на основі x_3

Рис. 2.7. Функціональні схеми реалізації елементарної функції f_{178}

Як видно із рис. 2.7, функціональні схеми реалізації елементарної функції f_{178} відрізняються від функціональних схем реалізації елементарної функції f_{77}, представлених на рис. 2.3, інверсними значеннями всіх трьох Сі-квантів, тому, що елементарні функції є взаємно оберненими.

Розглянемо елементарну функцію $f_{142} = x_1 \cdot \bar{x}_2 \vee x_1 \cdot \bar{x}_3 \vee \bar{x}_2 \cdot \bar{x}_3$. Таблиця істинності елементарної функції f_{142} наведена в табл. 2.28.

Таблиця 2.28

Таблиця істинності елементарної функції f_{142}

Вхідні дані			Результат перетворення
x_1	x_2	x_3	f_{142}
0	**0**	**0**	**1**
0	**0**	**1**	**0**
0	**1**	**0**	**0**
0	**1**	**1**	**0**
1	**0**	**0**	**1**
1	**0**	**1**	**1**
1	**1**	**0**	**1**
1	**1**	**1**	**0**

Карти Карно для побудови дискретних моделей елементарної функції f_{142} наведені в табл. 2.29 – табл. 2.31.

Варіант 8.1.

Таблиця 2.29

Карта Карно з виділеними контурами (варіант 8.1)

x_1	x_2	f_{142}	
0	**0**	**1**	**0**
0	**1**	**0**	**0**
1	**1**	**1**	**0**
1	**0**	**1**	**1**
		$\bar{x}_3$	x_3

Дискретну модель та дискретно-алгебраїчне представлення елементарної функції f_{142} можна представити:

$$f_{142} = x_1 \cdot \bar{x}_2 \vee x_1 \cdot \bar{x}_3 \vee \bar{x}_1 \cdot \bar{x}_2 \cdot \bar{x}_3 = \begin{cases} \bar{x}_2 \cdot \bar{x}_3 & \textit{якщо} \quad x_1 = 0 \\ \bar{x}_2 \vee \bar{x}_3 & \textit{якщо} \quad x_1 = 1 \end{cases} \qquad (2.22)$$

Варіант 8.2.

Таблиця 2.30

Карта Карно з виділеними контурами (варіант 8.2)

x_1	x_2	f_{142}	
0	**0**	**1**	**0**
0	**1**	**0**	**0**
1	**1**	**1**	**0**
1	**0**	**1**	**1**
		$\bar{x}_3$	x_3

Отримаємо дискретну модель та дискретно-алгебраїчне представлення елементарної функції f_{142}:

$$f_{142} = x_1 \cdot \bar{x}_2 \vee \bar{x}_2 \cdot \bar{x}_3 \vee x_1 \cdot x_2 \cdot \bar{x}_3 = \begin{cases} x_1 \vee \bar{x}_3 & якщо \quad x_2 = 0 \\ x_1 \cdot \bar{x}_3 & якщо \quad x_2 = 1 \end{cases} \qquad (2.23)$$

Варіант 8.3.

Таблиця 2.31

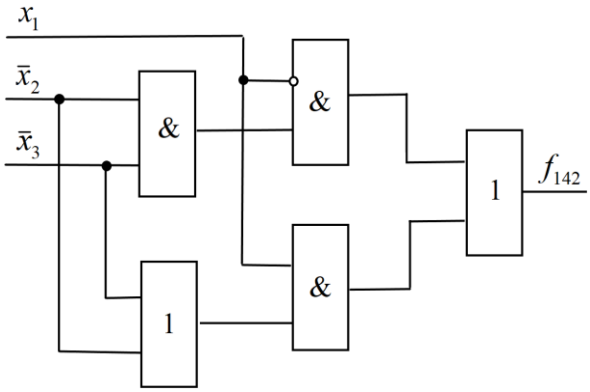
Карта Карно з виділеними контурами (варіант 8.2)

x_1	x_2	f_{142}	
0	**0**	**1**	**0**
0	**1**	**0**	**0**
1	**1**	**1**	**0**
1	**0**	**1**	**1**
		$\bar{x}_3$	x_3

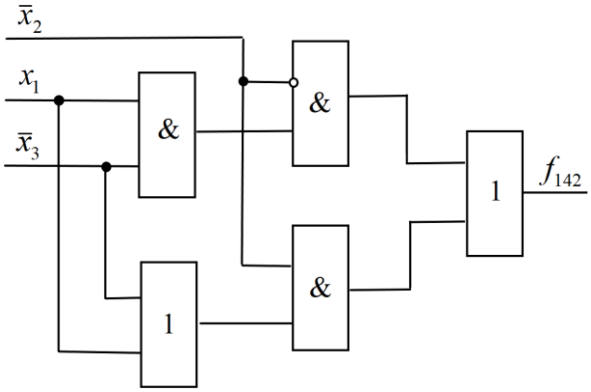
На основі трьох виділених контурів отримаємо дискретно-алгебраїчне представлення елементарної функції f_{142}:

$$f_{142} = x_1 \cdot \bar{x}_3 \vee \bar{x}_2 \cdot \bar{x}_3 \vee x_1 \cdot \bar{x}_2 \cdot x_3 = \begin{cases} x_1 \cdot \bar{x}_2 & якщо \quad x_3 = 0 \\ x_1 \vee \bar{x}_2 & якщо \quad x_3 = 1 \end{cases} \qquad (2.24)$$

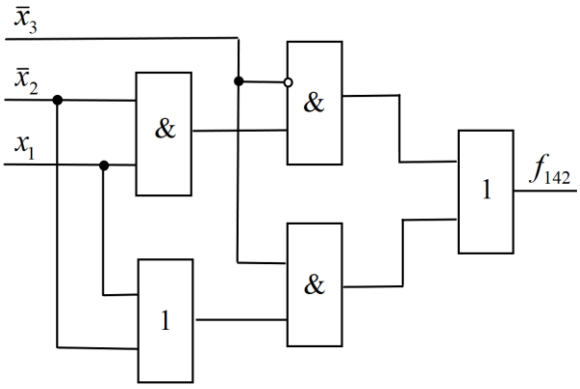
На основі виразів (2.22), (2.23) і (2.24) побудуємо функціональні схеми реалізації елементарної функції f_{142}. Дані функціональні схеми представлені на рис. 2.8.



а) Управління на основі x_1



б) Управління на основі x_2



в) Управління на основі x_3

Рис. 2.8. Функціональні схеми реалізації елементарної функції f_{142}

Елементарні функції f_{113} і f_{142} є взаємно оберненими. Так як вони взаємно обернені, то функціональні схеми їх реалізації відрізняються інверсними значеннями всіх трьох Сі-квантів, про що свідчить порівняння рис. 2.8 і рис. 2.4.

2.2 Метод синтезу моделей елементарних функцій операцій, керованих інформацією

Отримані в процесі дослідження і класифіковані дискретні і дискретно-алгебраїчні моделі елементарних функцій (2.1) – (2.24) зведені в табл. 2.32. Слід відмітити, що для класифікації дискретно-алгебраїчних моделей елементарних функцій операцій, керованих інформацією, було необхідно дослідити і порівняти крім самих моделей функціональні схеми їх реалізації [32, 48].

Таблиця 2.32

Класифікація дискретних і дискретно-алгебраїчних моделей елементарних функцій операцій, керованих інформацією

Моделі прямих елементарних функцій	Моделі обернених елементарних функцій
$f_{23} = x_1 \cdot x_2 \vee x_1 \cdot x_3 \vee \bar{x}_1 \cdot x_2 \cdot x_3 = \begin{cases} x_2 \cdot x_3 & \text{если } x_1 = 0 \\ x_2 \vee x_3 & \text{если } x_1 = 1 \end{cases}$	$f_{232} = \bar{x}_1 \cdot \bar{x}_2 \vee \bar{x}_1 \cdot \bar{x}_3 \vee \bar{x}_1 \cdot \bar{x}_2 \cdot \bar{x}_3 = \begin{cases} \bar{x}_2 \vee \bar{x}_3 & \text{якщо } x_1 = 0 \\ \bar{x}_2 \cdot \bar{x}_3 & \text{якщо } x_1 = 1 \end{cases}$
$f_{23} = x_1 \cdot x_2 \vee x_2 \cdot x_3 \vee x_1 \cdot \bar{x}_2 \cdot x_3 = \begin{cases} x_1 \cdot x_3 & \text{если } x_2 = 0 \\ x_1 \vee x_3 & \text{если } x_2 = 1 \end{cases}$	$f_{232} = \bar{x}_1 \cdot \bar{x}_2 \vee \bar{x}_2 \cdot \bar{x}_3 \vee \bar{x}_1 \cdot x_2 \cdot \bar{x}_3 = \begin{cases} \bar{x}_1 \vee \bar{x}_3 & \text{якщо } x_2 = 0 \\ \bar{x}_1 \cdot \bar{x}_3 & \text{якщо } x_2 = 1 \end{cases}$
$f_{23} = x_1 \cdot x_3 \vee x_2 \cdot x_3 \vee x_1 \cdot x_2 \cdot \bar{x}_3 = \begin{cases} x_1 \cdot x_2 & \text{если } x_3 = 0 \\ x_1 \vee x_2 & \text{если } x_3 = 1 \end{cases}$	$f_{232} = \bar{x}_1 \cdot \bar{x}_3 \vee \bar{x}_2 \cdot \bar{x}_3 \vee \bar{x}_1 \cdot \bar{x}_2 \cdot x_3 = \begin{cases} \bar{x}_1 \vee \bar{x}_2 & \text{якщо } x_3 = 0 \\ \bar{x}_1 \cdot \bar{x}_2 & \text{якщо } x_3 = 1 \end{cases}$
$f_{43} = x_1 \cdot x_2 \vee x_1 \cdot \bar{x}_3 \vee \bar{x}_1 \cdot x_2 \cdot \bar{x}_3 = \begin{cases} x_2 \cdot \bar{x}_3 & \text{если } x_1 = 0 \\ x_2 \vee \bar{x}_3 & \text{если } x_1 = 1 \end{cases}$	$f_{212} = \bar{x}_1 \cdot \bar{x}_2 \vee \bar{x}_1 \cdot x_3 \vee x_1 \cdot \bar{x}_2 \cdot x_3 = \begin{cases} \bar{x}_2 \vee x_3 & \text{якщо } x_1 = 0 \\ \bar{x}_2 \cdot x_3 & \text{якщо } x_1 = 1 \end{cases}$
$f_{43} = x_1 \cdot x_2 \vee x_2 \cdot \bar{x}_3 \vee x_1 \cdot \bar{x}_2 \cdot \bar{x}_3 = \begin{cases} x_1 \cdot \bar{x}_3 & \text{если } x_2 = 0 \\ x_1 \vee \bar{x}_3 & \text{если } x_2 = 1 \end{cases}$	$f_{212} = \bar{x}_1 \cdot \bar{x}_2 \vee \bar{x}_2 \cdot x_3 \vee \bar{x}_1 \cdot x_2 \cdot x_3 = \begin{cases} \bar{x}_1 \vee x_3 & \text{якщо } x_2 = 0 \\ \bar{x}_1 \cdot x_3 & \text{якщо } x_2 = 1 \end{cases}$
$f_{43} = x_1 \cdot \bar{x}_3 \vee x_2 \cdot \bar{x}_3 \vee x_1 \cdot x_2 \cdot x_3 = \begin{cases} x_1 \vee x_2 & \text{если } x_3 = 0 \\ x_1 \cdot x_2 & \text{если } x_3 = 1 \end{cases}$	$f_{212} = \bar{x}_1 \cdot x_3 \vee \bar{x}_2 \cdot x_3 \vee \bar{x}_1 \cdot \bar{x}_2 \cdot \bar{x}_3 = \begin{cases} \bar{x}_1 \cdot \bar{x}_2 & \text{якщо } x_3 = 0 \\ \bar{x}_1 \vee \bar{x}_2 & \text{якщо } x_3 = 1 \end{cases}$
$f_{77} = x_1 \cdot \bar{x}_2 \vee x_1 \cdot x_3 \vee \bar{x}_1 \cdot \bar{x}_2 \cdot x_3 = \begin{cases} \bar{x}_2 \cdot x_3 & \text{если } x_1 = 0 \\ \bar{x}_2 \vee x_3 & \text{если } x_1 = 1 \end{cases}$	$f_{178} = \bar{x}_1 \cdot x_2 \vee \bar{x}_1 \cdot \bar{x}_3 \vee x_1 \cdot x_2 \cdot \bar{x}_3 = \begin{cases} x_2 \vee \bar{x}_3 & \text{якщо } x_1 = 0 \\ x_2 \cdot \bar{x}_3 & \text{якщо } x_1 = 1 \end{cases}$
$f_{77} = x_1 \cdot \bar{x}_2 \vee \bar{x}_2 \cdot x_3 \vee x_1 \cdot x_2 \cdot x_3 = \begin{cases} x_1 \vee x_3 & \text{якщо } x_2 = 0 \\ x_1 \cdot x_3 & \text{якщо } x_2 = 1 \end{cases}$	$f_{178} = \bar{x}_1 \cdot x_2 \vee x_2 \cdot \bar{x}_3 \vee \bar{x}_1 \cdot \bar{x}_2 \cdot \bar{x}_3 = \begin{cases} \bar{x}_1 \cdot \bar{x}_3 & \text{якщо } x_2 = 0 \\ \bar{x}_1 \vee \bar{x}_3 & \text{якщо } x_2 = 1 \end{cases}$
$f_{77} = x_1 \cdot x_3 \vee \bar{x}_2 \cdot x_3 \vee x_1 \cdot \bar{x}_2 \cdot \bar{x}_3 = \begin{cases} x_1 \cdot \bar{x}_2 & \text{якщо } x_3 = 0 \\ x_1 \vee \bar{x}_2 & \text{якщо } x_3 = 1 \end{cases}$	$f_{178} = \bar{x}_1 \cdot \bar{x}_3 \vee x_2 \cdot \bar{x}_3 \vee \bar{x}_1 \cdot x_2 \cdot x_3 = \begin{cases} \bar{x}_1 \vee x_2 & \text{якщо } x_3 = 0 \\ \bar{x}_1 \cdot x_2 & \text{якщо } x_3 = 1 \end{cases}$
$f_{113} = \bar{x}_1 \cdot x_2 \vee x_1 \cdot x_3 \vee x_1 \cdot x_2 \cdot x_3 = \begin{cases} x_2 \vee x_3 & \text{якщо } x_1 = 0 \\ x_2 \cdot x_3 & \text{якщо } x_1 = 1 \end{cases}$	$f_{142} = x_1 \cdot \bar{x}_2 \vee x_1 \cdot \bar{x}_3 \vee \bar{x}_1 \cdot \bar{x}_2 \cdot \bar{x}_3 = \begin{cases} \bar{x}_2 \cdot \bar{x}_3 & \text{якщо } x_1 = 0 \\ \bar{x}_2 \vee \bar{x}_3 & \text{якщо } x_1 = 1 \end{cases}$
$f_{113} = \bar{x}_1 \cdot x_2 \vee x_2 \cdot x_3 \vee \bar{x}_1 \cdot \bar{x}_2 \cdot x_3 = \begin{cases} \bar{x}_1 \cdot x_3 & \text{якщо } x_2 = 0 \\ \bar{x}_1 \vee x_3 & \text{якщо } x_2 = 1 \end{cases}$	$f_{142} = x_1 \cdot \bar{x}_2 \vee \bar{x}_2 \cdot \bar{x}_3 \vee x_1 \cdot x_2 \cdot \bar{x}_3 = \begin{cases} x_1 \vee \bar{x}_3 & \text{якщо } x_2 = 0 \\ x_1 \cdot \bar{x}_3 & \text{якщо } x_2 = 1 \end{cases}$
$f_{113} = \bar{x}_1 \cdot x_3 \vee x_2 \cdot x_3 \vee \bar{x}_1 \cdot x_2 \cdot \bar{x}_3 = \begin{cases} \bar{x}_1 \cdot x_2 & \text{якщо } x_3 = 0 \\ \bar{x}_1 \vee x_2 & \text{якщо } x_3 = 1 \end{cases}$	$f_{142} = x_1 \cdot \bar{x}_3 \vee \bar{x}_2 \cdot \bar{x}_3 \vee x_1 \cdot \bar{x}_2 \cdot x_3 = \begin{cases} x_1 \cdot \bar{x}_2 & \text{якщо } x_3 = 0 \\ x_1 \vee \bar{x}_2 & \text{якщо } x_3 = 1 \end{cases}$

Отримані результати синтезу дискретно-алгебраїчних моделей елементарних функцій операцій, керованих інформацією, (табл. 2.32), а також побудовані їх функціональні схеми дозволили зробити відповідні висновки, детальний аналіз яких наведено в [32, 48]. До них належать:

1. Елементарна функція операції керованою інформацією може бути реалізована на основі однієї з трьох дискретних, або дискретно-алгебраїчних моделей.

2. Дискретно-алгебраїчні моделі елементарної функції операції керованої інформацією залежать від номера (індексу) Сі-кванта, значення якого управляє вибором операції перетворення інформації.

3. Зміна Сі-кванта, значення якого управляє вибором операції перетворення інформації елементарною функцією, приводить до перестановки Сі-квантів як в моделях елементарних функцій, так і в їх функціональних схемах реалізації.

4. Дві прямі елементарні функції, побудовані на основі одного і того ж Сі-кванта управління вибором операції інформації відрізняються інверсним значенням одного і того ж Сі-кванта вхідної інформації (включаючи Сі-квант управління вибором операції).

6. Так як елементарні функції операцій, керованих інформацією, перетворюють три вхідних Сі кванта інформації, і вони відрізняються інверсією одного з них, то група прямих елементарних функцій операцій, керованих інформацією, включає в себе чотири елементарні функції.

7. Пряма і обернена елементарні функції відрізняються інверсними значеннями всіх вхідних Сі-квантів інформації.

На основі отриманих висновків можна побудувати метод синтезу дискретно-алгебраїчних моделей елементарних функції операцій, керованих інформацією, [48]. Побудова передбачає такі етапи:

1. Побудувати дискретно-алгебраїчну модель елементарної функції операцій, керованих інформацією, яка не включає операції інверсій.

2. Побудувати на її основі три модифікації даної елементарної функції на основі перестановок вхідних Сі-квантів. Так як операції логічного додавання і логічного множення комутативні ($x_i \cdot x_j = x_j \cdot x_i;\ x_i \cdot x_j = x_j \cdot x_i;\ i \neq j \in \{1, 2, 3\}$), то буде побудовано три модифікації елементарної функції.

3. Для побудови наступної елементарної функції і її модифікацій, необхідно вибрати один із вхідних Сі-квантів інформації, і модифікувати його у всіх трьох дискретно-алгебраїчних моделях елементарної функції, які не включають операції інверсій.

4. Послідовний вибір всіх вхідних Сі-квантів інформації забезпечить побудову групи дискретно-алгебраїчних моделей прямих елементарних функції операцій, керованих інформацією, та всіх їх модифікацій.

5. Побудувати групу модифікацій дискретно-алгебраїчних моделей обернених елементарних функції операцій, керованих інформацією, на основі послідовного вибору всіх модифікацій дискретно-алгебраїчних моделей прямих елементарних функції операцій, керованих інформацією, та інверсії всіх вхідних Сі-квантів моделей .

Запропонований алгоритм реалізації методу синтезу дискретно-алгебраїчних моделей елементарних функції операцій, керованих інформацією, забезпечить автоматизацію синтезу повної групи дискретно-алгебраїчних моделей елементарних функції операцій, керованих інформацією, та їх модифікацій [48].

Перехід від дискретно-алгебраїчних до дискретних моделей елементарних функцій не представляє складності. Виходячи з цього, синтезувати повну групу дискретних моделей операцій, керованих інформацією, та їх модифікацій можна на основі синтезованої повної групи дискретно-алгебраїчних моделей операцій, керованих інформацією, [32, 48].

2.3 Синтез дискретно-казуальних моделей елементарних функцій операцій, керованих інформацією

Розглянемо застосування дискретних і дискретно-алгебраїчних моделей елементарних функцій для побудови СЕТ-операцій на їх основі.

Одноопернадна 3Сі-квантова СЕТ-операція реалізує перетворення трьох вхідних Сі-квантів інформації в три Сі-кванти результату перетворення на основі трьох елементарних функцій [3]. Перша елементарна функція реалізує перший Сі-квант результату, друга елементарна функція реалізує другий Сі-квант результату і третя елементарна функція реалізує третій Сі-квант результату

Розглянемо одну з СЕТ-операцій і їй обернену, що отримані на основі обчислювального експерименту [32].

Пряма СЕТ-операція:

$$C(x)=\begin{bmatrix} f_{43}(x) \\ f_{113}(x) \\ f_{23}(x) \end{bmatrix} \tag{2.25}$$

Обернена СЕТ-операція:

$$C'(x)=\begin{bmatrix} f_{77}(x) \\ f_{23}(x) \\ f_{113}(x) \end{bmatrix} \tag{2.26}$$

Підставимо в модель прямої (2.25) і в модель оберненої (2.26) СЕТ-операції моделі дискретних елементарних функцій операцій, керованих інформацією, відповідно до табл. 2.1. Після підстановки отримаємо:

- дискретна модель прямої СЕТ-операції:

$$C(x)=\begin{bmatrix} x_1 \cdot x_2 \vee x_1 \cdot \bar{x}_3 \vee x_2 \cdot \bar{x}_3 \\ \bar{x}_1 \cdot x_2 \vee \bar{x}_1 \cdot x_3 \vee x_2 \cdot x_3 \\ x_1 \cdot x_2 \vee x_1 \cdot x_3 \vee x_2 \cdot x_3 \end{bmatrix} \tag{2.27}$$

- дискретна модель оберненої СЕТ-операції:

$$C'(x)=\begin{bmatrix} x_1 \cdot \bar{x}_2 \vee x_1 \cdot x_3 \vee \bar{x}_2 \cdot x_3 \\ x_1 \cdot x_2 \vee x_1 \cdot x_3 \vee x_2 \cdot x_3 \\ \bar{x}_1 \cdot x_2 \vee \bar{x}_1 \cdot x_3 \vee x_2 \cdot x_3 \end{bmatrix} \tag{2.28}$$

Дискретні моделі СЕТ-операцій (2.27) і (2.28) роблять задачу встановлення взаємозв'язків між елементарними функціями в СЕТ-операціях і між прямими та оберненими СЕТ-операціями достатньо складними.

Підставивши в моделі СЕТ-операції (2.25) і (2.26) моделі дискретно-алгебраїчних елементарних функцій операцій, керованих інформацією, відповідно до табл. 2.32 отримаємо:

- дискретно-алгебраїчна модель прямої СЕТ-операції:

$$C(x)=\begin{bmatrix} \begin{cases} x_2 \cdot \bar{x}_3 & если \quad x_1 = 0 \\ x_2 \vee \bar{x}_3 & если \quad x_1 = 1 \end{cases} \\ \begin{cases} \bar{x}_1 \cdot x_3 & якщо \quad x_2 = 0 \\ \bar{x}_1 \vee x_3 & якщо \quad x_2 = 1 \end{cases} \\ \begin{cases} x_1 \cdot x_2 & если \quad x_3 = 0 \\ x_1 \vee x_2 & если \quad x_3 = 1 \end{cases} \end{bmatrix} \tag{2.29}$$

- дискретно-алгебраїчна модель оберненої СЕТ-операції:

$$C'(x)=\begin{bmatrix} \begin{cases} \bar{x}_2 \cdot x_3 & если \quad x_1 = 0 \\ \bar{x}_2 \vee x_3 & если \quad x_1 = 1 \end{cases} \\ \begin{cases} x_1 \cdot x_3 & если \quad x_2 = 0 \\ x_1 \vee x_3 & если \quad x_2 = 1 \end{cases} \\ \begin{cases} \bar{x}_1 \cdot x_2 & якщо \quad x_3 = 0 \\ \bar{x}_1 \vee x_2 & якщо \quad x_3 = 1 \end{cases} \end{bmatrix} \tag{2.30}$$

Дискретно-алгебраїчні моделі СЕТ-операцій (2.29) і (2.30) спрощують задачу встановлення взаємозв'язків між елементарними функціями в СЕТ-операціях і між прямими та оберненими СЕТ-операціями порівняно з дискретними моделями СЕТ-операцій (2.27) і (2.28). Проте дані моделі мають громіздке представлення, яке не сприяє простоті їх сприйняття.

Слід відмітити що вибраний опис моделей повинен забезпечити можливість представлення всього різноманіття СЕТ-операцій, а не тільки СЕТ-операцій побудованих на основі елементарних функцій операцій, керованих інформацією, [48].

В теорії ситуаційного управління стан системи описується трьома подіями $(A; B; C)$, де *B* – подія яка реалізується; *A* – подія яка передувала події *B* і без реалізації якої подія *B* неможлива; *C* – подія якій передувала подія *B*, і реалізації якої неможлива до завершення події *B*. На основі даного опису подій в [40] запропоновано уніфікований опис дискретних елементарних функцій. Сутність даного опису полягає в дискретному представленні елементарної функції як трьох взаємно пов'язаних подій, при цьому кожна з подій описується дискретною моделлю:

$$f = (f_1)(f_2)(f_3). \tag{2.31}$$

В залежності від результату реалізації події f_2 буде виконуватися подія f_1, або f_3. Якщо $f_2 = 0$, то буде реалізовуватися подія f_1, інакше буде реалізована подія f_3. Фіксований вибір подій забезпечує простоту представлення дискретної моделі [47].

Так як розглянутий опис дискретних подій відображає логіку причинних зв'язків між дискретними моделями, то доцільно його назвати казуальним описом. Отримані за допомогою даного опису дискретні моделі будемо називати дискретно-казуальними моделями.

Спираючись на [48], використаємо опис (2.31) для представлення моделей елементарних функцій операцій, керованих інформацією, та розглянемо перехід від дискретно-алгебраїчного опису моделей елементарних функцій до дискретно-казуального опису елементарних функцій.

Дискретно-алгебраїчні моделі елементарної функції f_{23}, які описані (2.1), (2.2) і (2.3), можна представити як:

$$f_{23} = \begin{cases} x_2 \cdot x_3 & якщо \quad x_1 = 0 \\ x_2 \vee x_3 & якщо \quad x_1 = 1 \end{cases} = (x_2 \cdot x_3)(x_1)(x_2 \vee x_3) \tag{2.32}$$

$$f_{23} = \begin{cases} x_1 \cdot x_3 & якщо \quad x_2 = 0 \\ x_1 \vee x_3 & якщо \quad x_2 = 1 \end{cases} = (x_1 \cdot x_3)(x_2)(x_1 \vee x_3) \tag{2.33}$$

$$f_{23} = \begin{cases} x_1 \cdot x_2 & якщо \quad x_3 = 0 \\ x_1 \vee x_2 & якщо \quad x_3 = 1 \end{cases} = (x_1 \cdot x_2)(x_3)(x_1 \vee x_2) \tag{2.34}$$

Дискретно дискретно-алгебраїчні моделі елементарної функції f_{43}, які описані (2.4), (2.5) і (2.6), можна представити як:

$$f_{43}=\begin{cases} x_2 \cdot \bar{x}_3 \ \textit{якщо} \ \ x_1=0 \\ x_2 \vee \bar{x}_3 \ \ \textit{якщо} \ \ x_1=1 \end{cases} = (x_2 \cdot \bar{x}_3\ )(x_1)(x_2 \vee \bar{x}_3) \qquad (2.35)$$

$$f_{43}=\begin{cases} x_1 \cdot \bar{x}_3 \ \ \textit{якщо} \ \ x_2=0 \\ x_1 \vee \bar{x}_3 \ \ \textit{якщо} \ \ x_2=1 \end{cases} = (x_1 \cdot \bar{x}_3\ )(x_2)(x_1 \vee \bar{x}_3) \qquad (2.36)$$

$$f_{43}=\begin{cases} x_1 \vee x_2 \ \ \textit{якщо} \ \ x_3=0 \\ x_1 \cdot x_2 \ \ \textit{якщо} \ \ x_3=1 \end{cases} = (x_1 \vee x_2\ )(x_3)(x_1 \cdot x_2\ ) \qquad (2.37)$$

Як видно з наведених прикладів (2.32) – (2.37), дискретно-казуальний опис моделей дозволяє спростити запис елементарних функцій, зберігаючи переваги дискретно-алгебраїчного опису моделей.

Розглянемо дискретно-казуальні моделі обернених елементарних функцій:

$$f_{232}=\begin{cases} \bar{x}_2 \vee \bar{x}_3 \ \textit{якщо} \ \ x_1=0 \\ \bar{x}_2 \cdot \bar{x}_3 \ \ \textit{якщо} \ \ x_1=1 \end{cases} = (\bar{x}_2 \vee \bar{x}_3\ )(x_1)(\bar{x}_2 \cdot \bar{x}_3) = (\bar{x}_2 \cdot \bar{x}_3\ )(\bar{x}_1)(\bar{x}_2 \vee \bar{x}_3) \qquad (2.38)$$

$$f_{232}=\begin{cases} \bar{x}_1 \vee \bar{x}_3 \ \textit{якщо} \ \ x_2=0 \\ \bar{x}_1 \cdot \bar{x}_3 \ \ \textit{якщо} \ \ x_2=1 \end{cases} = (\bar{x}_1 \vee \bar{x}_3\ )(x_2)(\bar{x}_1 \cdot \bar{x}_3) = (\ \bar{x}_1 \cdot \bar{x}_3)(\bar{x}_2)(\bar{x}_1 \vee \bar{x}_{33}) \qquad (2.39)$$

$$f_{232}=\begin{cases} \bar{x}_1 \vee \bar{x}_2 \ \textit{якщо} \ \ x_3=0 \\ \bar{x}_1 \cdot \bar{x}_2 \ \ \textit{якщо} \ \ x_3=1 \end{cases} = (\bar{x}_1 \vee \bar{x}_2)(\ x_3)(\bar{x}_1 \cdot \bar{x}_2) = (\bar{x}_1 \cdot \bar{x}_2)(\ \bar{x}_3)(\bar{x}_1 \vee \bar{x}_2\ ) \qquad (2.40)$$

Як видно, дискретно-казуальні моделі прямих елементарних функцій (2.32) – (2.37) відрізняються від дискретно-казуальних моделей обернених елементарних функцій (2.38) – (2.40) інверсією вхідних Сі-квантів.

Побудуємо і класифікуємо дискретно-казуальні моделі елементарних функцій операцій, керованих інформацією, по аналогії з класифікацією

дискретно-алгебраїчних моделей [58]. Результати класифікації представлені в табл. 2.33 [32].

Таблиця 2.33

Класифікація дискретно-казуальних моделей елементарних функцій операцій, керованих інформацією

Моделі прямих елементарних функцій	**Моделі обернених елементарних функцій**
$f_{23} = (x_2 \cdot x_3)(x_1)(x_2 \vee x_3)$	$f_{232} = (\bar{x}_2 \vee \bar{x}_3)(x_1)(\bar{x}_2 \cdot \bar{x}_3)$
$f_{23} = (x_1 \cdot x_3)(x_2)(x_1 \vee x_3)$	$f_{232} = (\bar{x}_1 \vee \bar{x}_3)(x_2)(\bar{x}_1 \cdot \bar{x}_3)$
$f_{23} = (x_1 \cdot x_2)(x_3)(x_1 \vee x_2)$	$f_{232} = (\bar{x}_1 \vee \bar{x}_2)(x_3)(\bar{x}_1 \cdot \bar{x}_2)$
$f_{43} = (x_2 \cdot \bar{x}_3)(x_1)(x_2 \vee \bar{x}_3)$	$f_{212} = (\bar{x}_2 \vee x_3)(x_1)(\bar{x}_2 \cdot x_3)$
$f_{43} = (x_1 \cdot \bar{x}_3)(x_2)(x_1 \vee \bar{x}_3)$	$f_{212} = (\bar{x}_1 \vee x_3)(x_2)(\bar{x}_1 \cdot x_3)$
$f_{43} = (x_1 \vee x_2)(x_3)(x_1 \cdot x_2)$	$f_{212} = (\bar{x}_1 \cdot \bar{x}_2)(x_3)(\bar{x}_1 \vee \bar{x}_2)$
$f_{77} = (\bar{x}_2 \cdot x_3)(x_1)(\bar{x}_2 \vee x_3)$	$f_{178} = (x_2 \vee \bar{x}_3)(x_1)(x_2 \cdot \bar{x}_3)$
$f_{77} = (x_1 \vee x_3)(x_2)(x_1 \cdot x_3)$	$f_{178} = (\bar{x}_1 \cdot \bar{x}_3)(x_2)(\bar{x}_1 \vee \bar{x}_3)$
$f_{77} = (x_1 \cdot \bar{x}_2)(x_3)(x_1 \vee \bar{x}_2)$	$f_{178} = (\bar{x}_1 \vee x_2)(x_3)(\bar{x}_1 \cdot x_2)$
$f_{113} = (x_2 \vee x_3)(x_1)(x_2 \cdot x_3)$	$f_{142} = (\bar{x}_2 \cdot \bar{x}_3)(x_1)(\bar{x}_2 \vee \bar{x}_3)$
$f_{113} = (\bar{x}_1 \cdot x_3)(x_2)(\bar{x}_1 \vee x_3)$	$f_{142} = (x_1 \vee \bar{x}_3)(x_2)(x_1 \cdot \bar{x}_3)$
$f_{113} = (\bar{x}_1 \cdot x_2)(x_3)(\bar{x}_1 \vee x_2)$	$f_{142} = (x_1 \vee \bar{x}_2)(x_3)(x_1 \cdot \bar{x}_2)$

Отримані результати синтезу дискретно-казуальних моделей елементарних функцій операцій, керованих інформацією, дозволяють без дослідження функціональних схем зробити аналогічні висновки як і по класифікації дискретно-алгебраїчних моделей операцій. Виходячи з цього можна стверджувати, що метод синтезу дискретно-казуальних моделей елементарних функцій операцій, керованих інформацією, буде відрізнятися від методу синтезу дискретно-казуальних моделей елементарних функцій операцій, керованих інформацією, лише формою запису функцій. Отже можна констатувати, що дискретно-алгебраїчні і дискретно-казуальні моделі операцій, керованих інформацією, будуються за одним методом синтезу з відмінностями в представленні отриманих моделей [48].

Розглянемо моделі СЕТ-операцій (2.25) і (2.26), представлених на основі дискретно-казуальних моделей елементарних функцій операцій, керованих інформацією, [32].

- дискретно-казуальна модель прямої СЕТ-операції

$$C(x)=\begin{bmatrix}(x_2\cdot\bar{x}_3)(x_1)(x_2\vee\bar{x}_3)\\(\bar{x}_1\cdot x_3)(x_2)(\bar{x}_1\vee x_3)\\(x_1\cdot x_2)(x_3)(x_1\vee x_2)\end{bmatrix} \tag{2.41}$$

- дискретно-казуальна модель оберненої СЕТ-операції

$$C'(x)=\begin{bmatrix}(\bar{x}_2\cdot x_3)(x_1)(\bar{x}_2\vee x_3)\\(x_1\cdot x_3)(x_2)(x_1\vee x_3)\\(\bar{x}_1\cdot x_2)(x_3)(\bar{x}_1\vee x_2)\end{bmatrix} \tag{2.42}$$

На основі дискретно-казуальних моделей СЕТ-операцій (2.41) і (2.42) можна зробити висновок, що їх запис дозволяє спростити дослідження і побудову методів синтезу СЕТ-операцій, порівняно з дискретними моделями операцій (2.27) і (2.28), та дискретно-алгебраїчними моделями операцій (2.29) і (2.30).

Висновки до розділу 2.

В розділі вперше запропоновано метод синтезу елементарних функцій операцій, керованих інформацією, на основі відомих дискретних моделей елементарних функцій, отриманих за результатами обчислювального експерименту, за допомогою встановлення і формалізації взаємозв’язків між дискретними змінними, що забезпечило можливість побудови повних множин дискретно-алгебраїчних і дискретно-казуальних моделей елементарних функцій операцій, керованих інформацією, для спрощення подальшого дослідження синтезу СЕТ-операцій на основі елементарних функцій операцій, керованих інформацією.

1. На основі дискретних моделей елементарних функцій операцій, керованих інформацією, отриманих за результатами обчислювального експерименту, побудовані дискретно-алгебраїчні моделі елементарних функцій операцій, керованих інформацією.

2. Визначена основна властивість елементарних функцій операцій, керованих інформацією, яка полягає в тому, що вибір операції логічного додавання або логічного множення двох вхідних Сі-квантів інформації визначається значенням третього управляючого Сі-кванта вхідної інформації.

3. Встановлено, що для управлінні вибором логічної операції, яка визначає результат перетворення вхідної інформації елементарною функцією операції керованою інформацією, може бути використано будь який вхідний Сі-квант інформації.

4. На основі зміни управляючих Сі-квантів інформації запропоновано технологію багатоваріантного синтезу дискретно-алгебраїчних моделей елементарних функцій операцій, керованих інформацією.

5. На прикладі дискретно-алгебраїчного опису елементарних функцій розроблено багатоваріантний метод синтезу моделей елементарних функцій операцій, керованих інформацією.

6 Для спрощення процесів подальшого дослідження синтезу і аналізу СЕТ-операцій, побудованих на основі елементарних функцій операцій, керованих інформацією, запропоновано використання дискретно-казуальних моделей елементарних функцій.

7. Встановлено, що використання дискретно-казуального опису дозволяє будувати багатоваріантні дискретно-казуальні моделі елементарних функцій на основі розробленого методу синтезу моделей елементарних функцій операцій, керованих інформацією.

Результати розділу опубліковані в [3, 32, 47, 48, 58].

РОЗДІЛ 3. ДОСЛІДЖЕННЯ І СИНТЕЗ СЕТ-ОПЕРАЦІЙ НА ОСНОВІ ЕЛЕМЕНТАРНИХ ФУНКЦІЙ ОПЕРАЦІЙ, КЕРОВАНИХ ІНФОРМАЦІЄЮ,

3.1. Дослідження моделі СЕТ-операції на основі елементарних функцій операцій, керованих інформацією

Методологія синтезу і дослідження груп СЕТ-операцій для зменшення складності наукових досліджень передбачає поділ груп операцій на підгрупи [32]: підгрупу базових операцій, підгрупу операцій перестановки і підгрупу операцій інверсії. Повна група СЕТ-операцій включає поєднання всіх трьох підгруп, крім того можуть поєднуватися підгрупа базових операцій з підгрупою операцій перестановки, підгрупа базових операцій з підгрупою операцій інверсії. Для визначення властивостей групи операцій достатньо визначити властивості базової операцій, дослідити механізми їх синтезу.

В результаті проведених досліджень базових груп трьохрозрядних операцій було встановлено наступне:

- для синтезу і дослідження групи СЕТ-операцій бажано знайти базову групу операцій, в якій прямі і обернені операції співпадають. Бажано, щоб базова група операцій включала максимально можливу кількість симетричних СЕТ-операцій;
- послідовність ключових елементів елементарних функцій повинна співпадати з послідовністю вхідних і вихідних Сі-квантів інформації. Ключовим елементом елементарної функції в межах цієї роботи є змінна, що відображає відповідний Сі-квант вхідної інформації, наявна в елементарній функції, і може розглядатися як управляюча. Управляюча змінна суттєво впливає на реалізацію елементарної функції. Наприклад:

- для моделі елементарної функції $f_{29} = x_1 \cdot \bar{x}_2 \vee x_2 \cdot x_3 = (x_1)(x_2)(x_3)$ управляючою змінною є змінна x_2;
- для моделі елементарної функції $f_{39} = x_2 \cdot \bar{x}_3 \vee x_1 \cdot x_3 = (x_2)(x_3)(x_1)$ управляючою змінною є змінна x_3;
- для моделі елементарної функції $f_{197} = \bar{x}_1 \cdot \bar{x}_2 \vee x_1 \cdot x_3 = (\bar{x}_2)(x_1)(x_3)$ управляючою змінною є змінна x_1;

Елементарні функції операцій, керованих інформацією, на відміну від інших елементарних функцій мають свої особливості, які полягають в тому, що в даних елементарних функціях будь яка змінна може розглядатися як ключовий елемент. Підтвердженням цього факту можуть служити моделі елементарних функцій операцій, керованих інформацією, що наведені в табл. 2.32 і табл. 2.33. Варіативність представлення елементарних функцій із-за визначення ключового елементу приводить до суттєвого збільшення варіацій моделі СЕТ-операції. Розглянемо варіанти математичного опису вже побудованої моделі прямої СЕТ-операції (2.41) і оберненої до неї СЕТ- операції (2.42) [47].

Дослідження моделей СЕТ-операцій, побудованих на основі елементарних функцій операцій, керованих інформацією, будемо проводити на основі дискретно-казуального представлення. Так як кожна елементарна функція операції керованої інформацією відповідно до табл. 2.33 має три дискретно-казуальні представлення, а СЕТ-операція поєднує три елементарні функції, то кожну СЕТ-операцію можна представити однією з 27 моделей [31]. Дискретно казуальні моделі СЕТ-операції, побудованої на основі елементарних функцій операцій, керованих інформацією, наведені в табл..3.1 [47].

Так як СЕТ-операції на основі елементарних функцій операцій, керованих інформацією, представляють собою математичну групу операцій, то для кожної прямої СЕТ-операції існує лише одна обернена СЕТ-операція [47].

Таблиця 3.1.

Дискретно казуальні моделі СЕТ-операції, побудованої на основі елементарних функцій операцій, керованих інформацією

№ п/п	Дискретно-казуальна модель СЕТ-операції	
	Пряме перетворення	Обернене перетворення
	$C(x)=\begin{bmatrix} f_{43}(x) \\ f_{113}(x) \\ f_{23}(x) \end{bmatrix}$	$C'(x)=\begin{bmatrix} f_{77}(x) \\ f_{23}(x) \\ f_{113}(x) \end{bmatrix}$
1	$C(x)=\begin{bmatrix} (x_2 \cdot \bar{x}_3)(x_1)(x_2 \vee \bar{x}_3) \\ (x_2 \vee x_3)(x_1)(x_2 \cdot x_3) \\ (x_2 \cdot x_3)(x_1)(x_2 \vee x_3) \end{bmatrix}$	$C'(x)=\begin{bmatrix} (\bar{x}_2 \cdot x_3)(x_1)(\bar{x}_2 \vee x_3) \\ (x_2 \cdot x_3)(x_1)(x_2 \vee x_3) \\ (x_2 \vee x_3)(x_1)(x_2 \cdot x_3) \end{bmatrix}$
2	$C(x)=\begin{bmatrix} (x_2 \cdot \bar{x}_3)(x_1)(x_2 \vee \bar{x}_3) \\ (x_2 \vee x_3)(x_1)(x_2 \cdot x_3) \\ (x_1 \cdot x_3)(x_2)(x_1 \vee x_3) \end{bmatrix}$	$C'(x)=\begin{bmatrix} (\bar{x}_2 \cdot x_3)(x_1)(\bar{x}_2 \vee x_3) \\ (x_2 \cdot x_3)(x_1)(x_2 \vee x_3) \\ (\bar{x}_1 \cdot x_3)(x_2)(\bar{x}_1 \vee x_3) \end{bmatrix}$
3	$C(x)=\begin{bmatrix} (x_2 \cdot \bar{x}_3)(x_1)(x_2 \vee \bar{x}_3) \\ (x_2 \vee x_3)(x_1)(x_2 \cdot x_3) \\ (x_1 \cdot x_2)(x_3)(x_1 \vee x_2) \end{bmatrix}$	$C'(x)=\begin{bmatrix} (\bar{x}_2 \cdot x_3)(x_1)(\bar{x}_2 \vee x_3) \\ (x_2 \cdot x_3)(x_1)(x_2 \vee x_3) \\ (\bar{x}_1 \cdot x_2)(x_3)(\bar{x}_1 \vee x_2) \end{bmatrix}$
4	$C(x)=\begin{bmatrix} (x_2 \cdot \bar{x}_3)(x_1)(x_2 \vee \bar{x}_3) \\ (\bar{x}_1 \cdot x_3)(x_2)(\bar{x}_1 \vee x_3) \\ (x_2 \cdot x_3)(x_1)(x_2 \vee x_3) \end{bmatrix}$	$C'(x)=\begin{bmatrix} (\bar{x}_2 \cdot x_3)(x_1)(\bar{x}_2 \vee x_3) \\ (x_1 \cdot x_3)(x_2)(x_1 \vee x_3) \\ (x_2 \vee x_3)(x_1)(x_2 \cdot x_3) \end{bmatrix}$
5	$C(x)=\begin{bmatrix} (x_2 \cdot \bar{x}_3)(x_1)(x_2 \vee \bar{x}_3) \\ (\bar{x}_1 \cdot x_3)(x_2)(\bar{x}_1 \vee x_3) \\ (x_1 \cdot x_3)(x_2)(x_1 \vee x_3) \end{bmatrix}$	$C'(x)=\begin{bmatrix} (\bar{x}_2 \cdot x_3)(x_1)(\bar{x}_2 \vee x_3) \\ (x_1 \cdot x_3)(x_2)(x_1 \vee x_3) \\ (\bar{x}_1 \cdot x_3)(x_2)(\bar{x}_1 \vee x_3) \end{bmatrix}$
6	$C(x)=\begin{bmatrix} (x_2 \cdot \bar{x}_3)(x_1)(x_2 \vee \bar{x}_3) \\ (\bar{x}_1 \cdot x_3)(x_2)(\bar{x}_1 \vee x_3) \\ (x_1 \cdot x_2)(x_3)(x_1 \vee x_2) \end{bmatrix}$	$C'(x)=\begin{bmatrix} (\bar{x}_2 \cdot x_3)(x_1)(\bar{x}_2 \vee x_3) \\ (x_1 \cdot x_3)(x_2)(x_1 \vee x_3) \\ (\bar{x}_1 \cdot x_2)(x_3)(\bar{x}_1 \vee x_2) \end{bmatrix}$
7	$C(x)=\begin{bmatrix} (x_2 \cdot \bar{x}_3)(x_1)(x_2 \vee \bar{x}_3) \\ (\bar{x}_1 \cdot x_2)(x_3)(\bar{x}_1 \vee x_2) \\ (x_2 \cdot x_3)(x_1)(x_2 \vee x_3) \end{bmatrix}$	$C'(x)=\begin{bmatrix} (\bar{x}_2 \cdot x_3)(x_1)(\bar{x}_2 \vee x_3) \\ (x_1 \cdot x_2)(x_3)(x_1 \vee x_2) \\ (x_2 \vee x_3)(x_1)(x_2 \cdot x_3) \end{bmatrix}$

8	$C(x)=\begin{bmatrix}(x_2\cdot\bar{x}_3)(x_1)(x_2\vee\bar{x}_3)\\(\bar{x}_1\cdot x_2)(x_3)(\bar{x}_1\vee x_2)\\(x_1\cdot x_3)(x_2)(x_1\vee x_3)\end{bmatrix}$	$C'(x)=\begin{bmatrix}(\bar{x}_2\cdot x_3)(x_1)(\bar{x}_2\vee x_3)\\(x_1\cdot x_2)(x_3)(x_1\vee x_2)\\(\bar{x}_1\cdot x_3)(x_2)(\bar{x}_1\vee x_3)\end{bmatrix}$
9	$C(x)=\begin{bmatrix}(x_2\cdot\bar{x}_3)(x_1)(x_2\vee\bar{x}_3)\\(\bar{x}_1\cdot x_2)(x_3)(\bar{x}_1\vee x_2)\\(x_1\cdot x_2)(x_3)(x_1\vee x_2)\end{bmatrix}$	$C'(x)=\begin{bmatrix}(\bar{x}_2\cdot x_3)(x_1)(\bar{x}_2\vee x_3)\\(x_1\cdot x_2)(x_3)(x_1\vee x_2)\\(\bar{x}_1\cdot x_2)(x_3)(\bar{x}_1\vee x_2)\end{bmatrix}$
10	$C(x)=\begin{bmatrix}(x_1\cdot\bar{x}_3)(x_2)(x_1\vee\bar{x}_3)\\(x_2\vee x_3)(x_1)(x_2\cdot x_3)\\(x_2\cdot x_3)(x_1)(x_2\vee x_3)\end{bmatrix}$	$C'(x)=\begin{bmatrix}(x_1\vee x_3)(x_2)(x_1\cdot x_3)\\(x_2\cdot x_3)(x_1)(x_2\vee x_3)\\(x_2\vee x_3)(x_1)(x_2\cdot x_3)\end{bmatrix}$
11	$C(x)=\begin{bmatrix}(x_1\cdot\bar{x}_3)(x_2)(x_1\vee\bar{x}_3)\\(x_2\vee x_3)(x_1)(x_2\cdot x_3)\\(x_1\cdot x_3)(x_2)(x_1\vee x_3)\end{bmatrix}$	$C'(x)=\begin{bmatrix}(x_1\vee x_3)(x_2)(x_1\cdot x_3)\\(x_2\cdot x_3)(x_1)(x_2\vee x_3)\\(\bar{x}_1\cdot x_3)(x_2)(\bar{x}_1\vee x_3)\end{bmatrix}$
12	$C(x)=\begin{bmatrix}(x_1\cdot\bar{x}_3)(x_2)(x_1\vee\bar{x}_3)\\(x_2\vee x_3)(x_1)(x_2\cdot x_3)\\(x_1\cdot x_2)(x_3)(x_1\vee x_2)\end{bmatrix}$	$C'(x)=\begin{bmatrix}(x_1\vee x_3)(x_2)(x_1\cdot x_3)\\(x_2\cdot x_3)(x_1)(x_2\vee x_3)\\(\bar{x}_1\cdot x_2)(x_3)(\bar{x}_1\vee x_2)\end{bmatrix}$
13	$C(x)=\begin{bmatrix}(x_1\cdot\bar{x}_3)(x_2)(x_1\vee\bar{x}_3)\\(\bar{x}_1\cdot x_3)(x_2)(\bar{x}_1\vee x_3)\\(x_2\cdot x_3)(x_1)(x_2\vee x_3)\end{bmatrix}$	$C'(x)=\begin{bmatrix}(x_1\vee x_3)(x_2)(x_1\cdot x_3)\\(x_1\cdot x_3)(x_2)(x_1\vee x_3)\\(x_2\vee x_3)(x_1)(x_2\cdot x_3)\end{bmatrix}$
14	$C(x)=\begin{bmatrix}(x_1\cdot\bar{x}_3)(x_2)(x_1\vee\bar{x}_3)\\(\bar{x}_1\cdot x_3)(x_2)(\bar{x}_1\vee x_3)\\(x_1\cdot x_3)(x_2)(x_1\vee x_3)\end{bmatrix}$	$C'(x)=\begin{bmatrix}(x_1\vee x_3)(x_2)(x_1\cdot x_3)\\(x_1\cdot x_3)(x_2)(x_1\vee x_3)\\(\bar{x}_1\cdot x_3)(x_2)(\bar{x}_1\vee x_3)\end{bmatrix}$
15	$C(x)=\begin{bmatrix}(x_1\cdot\bar{x}_3)(x_2)(x_1\vee\bar{x}_3)\\(\bar{x}_1\cdot x_3)(x_2)(\bar{x}_1\vee x_3)\\(x_1\cdot x_2)(x_3)(x_1\vee x_2)\end{bmatrix}$	$C'(x)=\begin{bmatrix}(x_1\vee x_3)(x_2)(x_1\cdot x_3)\\(x_1\cdot x_3)(x_2)(x_1\vee x_3)\\(\bar{x}_1\cdot x_2)(x_3)(\bar{x}_1\vee x_2)\end{bmatrix}$
16	$C(x)=\begin{bmatrix}(x_1\cdot\bar{x}_3)(x_2)(x_1\vee\bar{x}_3)\\(\bar{x}_1\cdot x_2)(x_3)(\bar{x}_1\vee x_2)\\(x_2\cdot x_3)(x_1)(x_2\vee x_3)\end{bmatrix}$	$C'(x)=\begin{bmatrix}(x_1\vee x_3)(x_2)(x_1\cdot x_3)\\(x_1\cdot x_2)(x_3)(x_1\vee x_2)\\(x_2\vee x_3)(x_1)(x_2\cdot x_3)\end{bmatrix}$
17	$C(x)=\begin{bmatrix}(x_1\cdot\bar{x}_3)(x_2)(x_1\vee\bar{x}_3)\\(\bar{x}_1\cdot x_2)(x_3)(\bar{x}_1\vee x_2)\\(x_1\cdot x_3)(x_2)(x_1\vee x_3)\end{bmatrix}$	$C'(x)=\begin{bmatrix}(x_1\vee x_3)(x_2)(x_1\cdot x_3)\\(x_1\cdot x_2)(x_3)(x_1\vee x_2)\\(\bar{x}_1\cdot x_3)(x_2)(\bar{x}_1\vee x_3)\end{bmatrix}$

18	$C(x)=\begin{bmatrix}(x_1\cdot\bar{x}_3\,)(\,x_2)(x_1\vee\bar{x}_3\,)\\(\bar{x}_1\cdot x_2\,)(\,x_3)(\bar{x}_1\vee x_2)\\(x_1\cdot x_2\,)(\,x_3)(x_1\vee x_2)\end{bmatrix}$	$C'(x)=\begin{bmatrix}(x_1\vee x_3\,)(\,x_2)(x_1\cdot x_3)\\(x_1\cdot x_2\,)(\,x_3)(x_1\vee x_2)\\(\bar{x}_1\cdot x_2\,)(\,x_3)(\bar{x}_1\vee x_2)\end{bmatrix}$
19	$C(x)=\begin{bmatrix}(x_1\vee x_2\,)(\,x_3)(x_1\cdot x_2)\\(x_2\vee x_3\,)(x_1)(x_2\cdot x_3)\\(x_2\cdot x_3\,)(x_1)(x_2\vee x_3)\end{bmatrix}$	$C'(x)=\begin{bmatrix}(x_1\cdot\bar{x}_2\,)(\,x_3)(x_1\vee\bar{x}_2)\\(x_2\cdot x_3\,)(x_1)(x_2\vee x_3)\\(x_2\vee x_3\,)(x_1)(x_2\cdot x_3)\end{bmatrix}$
20	$C(x)=\begin{bmatrix}(x_1\vee x_2\,)(\,x_3)(x_1\cdot x_2)\\(x_2\vee x_3\,)(x_1)(x_2\cdot x_3)\\(x_1\cdot x_3\,)(\,x_2)(x_1\vee x_3)\end{bmatrix}$	$C'(x)=\begin{bmatrix}(x_1\cdot\bar{x}_2\,)(\,x_3)(x_1\vee\bar{x}_2)\\(x_2\cdot x_3\,)(x_1)(x_2\vee x_3)\\(\bar{x}_1\cdot x_3\,)(\,x_2)(\bar{x}_1\vee x_3)\end{bmatrix}$
21	$C(x)=\begin{bmatrix}(x_1\vee x_2\,)(\,x_3)(x_1\cdot x_2)\\(x_2\vee x_3\,)(x_1)(x_2\cdot x_3)\\(x_1\cdot x_2\,)(\,x_3)(x_1\vee x_2)\end{bmatrix}$	$C'(x)=\begin{bmatrix}(x_1\cdot\bar{x}_2\,)(\,x_3)(x_1\vee\bar{x}_2)\\(x_2\cdot x_3\,)(x_1)(x_2\vee x_3)\\(\bar{x}_1\cdot x_2\,)(\,x_3)(\bar{x}_1\vee x_2)\end{bmatrix}$
22	$C(x)=\begin{bmatrix}(x_1\vee x_2\,)(\,x_3)(x_1\cdot x_2)\\(\bar{x}_1\cdot x_3\,)(\,x_2)(\bar{x}_1\vee x_3)\\(x_2\cdot x_3\,)(x_1)(x_2\vee x_3)\end{bmatrix}$	$C'(x)=\begin{bmatrix}(x_1\cdot\bar{x}_2\,)(\,x_3)(x_1\vee\bar{x}_2)\\(x_1\cdot x_3\,)(\,x_2)(x_1\vee x_3)\\(x_2\vee x_3\,)(x_1)(x_2\cdot x_3)\end{bmatrix}$
23	$C(x)=\begin{bmatrix}(x_1\vee x_2\,)(\,x_3)(x_1\cdot x_2)\\(\bar{x}_1\cdot x_3\,)(\,x_2)(\bar{x}_1\vee x_3)\\(x_1\cdot x_3\,)(\,x_2)(x_1\vee x_3)\end{bmatrix}$	$C'(x)=\begin{bmatrix}(x_1\cdot\bar{x}_2\,)(\,x_3)(x_1\vee\bar{x}_2)\\(x_1\cdot x_3\,)(\,x_2)(x_1\vee x_3)\\(\bar{x}_1\cdot x_3\,)(\,x_2)(\bar{x}_1\vee x_3)\end{bmatrix}$
24	$C(x)=\begin{bmatrix}(x_1\vee x_2\,)(\,x_3)(x_1\cdot x_2)\\(\bar{x}_1\cdot x_3\,)(\,x_2)(\bar{x}_1\vee x_3)\\(x_1\cdot x_2\,)(\,x_3)(x_1\vee x_2)\end{bmatrix}$	$C'(x)=\begin{bmatrix}(x_1\cdot\bar{x}_2\,)(\,x_3)(x_1\vee\bar{x}_2)\\(x_1\cdot x_3\,)(\,x_2)(x_1\vee x_3)\\(\bar{x}_1\cdot x_2\,)(\,x_3)(\bar{x}_1\vee x_2)\end{bmatrix}$
25	$C(x)=\begin{bmatrix}(x_1\vee x_2\,)(\,x_3)(x_1\cdot x_2)\\(\bar{x}_1\cdot x_2\,)(\,x_3)(\bar{x}_1\vee x_2)\\(x_2\cdot x_3\,)(x_1)(x_2\vee x_3)\end{bmatrix}$	$C'(x)=\begin{bmatrix}(x_1\cdot\bar{x}_2\,)(\,x_3)(x_1\vee\bar{x}_2)\\(x_1\cdot x_2\,)(\,x_3)(x_1\vee x_2)\\(x_2\vee x_3\,)(x_1)(x_2\cdot x_3)\end{bmatrix}$
26	$C(x)=\begin{bmatrix}(x_1\vee x_2\,)(\,x_3)(x_1\cdot x_2)\\(\bar{x}_1\cdot x_2\,)(\,x_3)(\bar{x}_1\vee x_2)\\(x_1\cdot x_3\,)(\,x_2)(x_1\vee x_3)\end{bmatrix}$	$C'(x)=\begin{bmatrix}(x_1\cdot\bar{x}_2\,)(\,x_3)(x_1\vee\bar{x}_2)\\(x_1\cdot x_2\,)(\,x_3)(x_1\vee x_2)\\(\bar{x}_1\cdot x_3\,)(\,x_2)(\bar{x}_1\vee x_3)\end{bmatrix}$
27	$C(x)=\begin{bmatrix}(x_1\vee x_2\,)(\,x_3)(x_1\cdot x_2)\\(\bar{x}_1\cdot x_2\,)(\,x_3)(\bar{x}_1\vee x_2)\\(x_1\cdot x_2\,)(\,x_3)(x_1\vee x_2)\end{bmatrix}$	$C'(x)=\begin{bmatrix}(x_1\cdot\bar{x}_2\,)(\,x_3)(x_1\vee\bar{x}_2)\\(x_1\cdot x_2\,)(\,x_3)(x_1\vee x_2)\\(\bar{x}_1\cdot x_2\,)(\,x_3)(\bar{x}_1\vee x_2)\end{bmatrix}$

Так як пряму СЕТ-операцію на основі елементарних функцій операцій, керованих інформацією, можна представити 27 варіантами її моделі, то і обернену до неї СЕТ-операцію також можна представити 27 варіантами її моделі (табл. 3.1). Виходячи з цього, при знаходженні самих простих взаємозв'язків між прямою і оберненою моделями СЕТ-операцій необхідно аналізувати 729 ($27 \cdot 27$) пар моделей. Проте знаходження взаємозв'язку між однією прямою і однією оберненою СЕТ-операціями не гарантує коректність даного взаємозв'язку для іншої пари взаємно обернених СЕТ-операцій.

В процесі подальшого дослідження, виходячи з результатів моделювання (табл. 3.1) обмежимося лише двома підходами в побудові моделей СЕТ-операцій на основі елементарних функцій операцій, керованих інформацією.

Перший підхід полягає в побудові моделей СЕТ-операцій на основі елементарних функцій, порядковий номер керуючої функції якої співпадає з порядковим номером самої елементарної функції в операції. Даному підходу відповідають лише по одній моделі прямої і оберненої СЕТ-операції:

$$C(x)=\begin{bmatrix}(x_2 \cdot \bar{x}_3)(x_1)(x_2 \vee \bar{x}_3)\\(\bar{x}_1 \cdot x_3)(x_2)(\bar{x}_1 \vee x_3)\\(x_1 \cdot x_2)(x_3)(x_1 \vee x_2)\end{bmatrix}, \qquad C'(x)=\begin{bmatrix}(\bar{x}_2 \cdot x_3)(x_1)(\bar{x}_2 \vee x_3)\\(x_1 \cdot x_3)(x_2)(x_1 \vee x_3)\\(\bar{x}_1 \cdot x_2)(x_3)(\bar{x}_1 \vee x_2)\end{bmatrix}.$$

Другий підхід полягає в побудові моделей СЕТ-операцій на основі елементарних функцій, побудованих на основі однієї і тієї ж керуючої функції. Даному підходу відповідають три набори моделей з прямої і оберненої СЕТ-операцій:

$$C(x)=\begin{bmatrix}(x_2 \cdot \bar{x}_3)(x_1)(x_2 \vee \bar{x}_3)\\(x_2 \vee x_3)(x_1)(x_2 \cdot x_3)\\(x_2 \cdot x_3)(x_1)(x_2 \vee x_3)\end{bmatrix}, \qquad C'(x)=\begin{bmatrix}(\bar{x}_2 \cdot x_3)(x_1)(\bar{x}_2 \vee x_3)\\(x_2 \cdot x_3)(x_1)(x_2 \vee x_3)\\(x_2 \vee x_3)(x_1)(x_2 \cdot x_3)\end{bmatrix};$$

$$C(x)=\begin{bmatrix}(x_1 \cdot \bar{x}_3)(x_2)(x_1 \vee \bar{x}_3)\\(\bar{x}_1 \cdot x_3)(x_2)(\bar{x}_1 \vee x_3)\\(x_1 \cdot x_3)(x_2)(x_1 \vee x_3)\end{bmatrix}, \qquad C'(x)=\begin{bmatrix}(x_1 \vee x_3)(x_2)(x_1 \cdot x_3)\\(x_1 \cdot x_3)(x_2)(x_1 \vee x_3)\\(\bar{x}_1 \cdot x_3)(x_2)(\bar{x}_1 \vee x_3)\end{bmatrix};$$

$$C(x)=\begin{bmatrix}(x_1 \vee x_2)(x_3)(x_1 \cdot x_2)\\(\bar{x}_1 \cdot x_2)(x_3)(\bar{x}_1 \vee x_2)\\(x_1 \cdot x_2)(x_3)(x_1 \vee x_2)\end{bmatrix}, \qquad C'(x)=\begin{bmatrix}(x_1 \cdot \bar{x}_2)(x_3)(x_1 \vee \bar{x}_2)\\(x_1 \cdot x_2)(x_3)(x_1 \vee x_2)\\(\bar{x}_1 \cdot x_2)(x_3)(\bar{x}_1 \vee x_2)\end{bmatrix}.$$

Як видно з наведених прикладів, кожен з підходів має свої переваги і недоліки. Наприклад, в наведеному прикладі першого підходу у всіх моделях елементарних функцій операція логічного множення буде виконуватись при нульовому значенні функції керування. Проте у всіх елементарних функціях в операції логічного множення використовуються різні вхідні Сі-кванти вхідної інформації.

Перевага другого підходу полягає у використанні одних і тих самих Сі-квантів вхідної інформації всіма елементарними функціями. Недолік полягає в реалізації логічного множення, або логічного додавання при нульовому значенні функції керування.

Проведений аналіз наведених прикладів показує, що при побудові моделей СЕТ-операцій на основі елементарних функцій операцій, керованих інформацією, доцільно використовувати елементарні функції в яких наперед відома умова виконання логічного додавання чи логічного множення. Досягти даного результату можливо на основі використання властивостей дискретно-казуальних моделей.

Для спрощення сприйняття властивостей дискретно-казуальної моделі як системи трьох взаємопов’язаних дискретних складових, представимо її в загальному вигляді [41]:

$$f(x) = (f_1(x))(f_2(x))(f_3(x)) \qquad (3.1)$$

Модель (3.1) трактується наступним чином: в залежності від результату виконання функції $f_2(x)$ буде реалізована або функція $f_1(x)$, або $f_3(x)$. Для однозначного представлення моделі (3.1) будемо вважати, що за умови $f_2(x) = 0$ буде виконуватися функція $f_1(x)$, інакше буде виконуватися функція $f_3(x)$ [41]. В даній моделі функцію $f_2(x)$ будемо називати функцією керування, а функції $f_1(x)$ і $f_3(x)$ будемо називати функціями перетворення.

В дискретно-казуальній моделі (3.1) функції $f_1(x)$, $f_2(x)$ і $f_3(x)$ можуть бути представлені дискретними і дискретно-казуальними моделями.

Властивості дискретно казуальної моделі полягають в наступному [58]:

- Інверсія функції керування приведе до перестановки місцями функцій перетворення:

$$f(x) = [(f_1(x))(f_2(x))(f_3(x))] = [(f_3(x))\overline{(f_2(x))}(f_1(x))]. \quad (3.2)$$

- Інверсія результату функції приведе до інверсії функцій перетворення:

$$\overline{f(x)} = \overline{[(f_1(x))(f_2(x))(f_3(x))]} = [\overline{(f_1(x))}(f_2(x))\overline{(f_3(x))}]. \quad (3.3)$$

Відповідно до властивостей (3.2) і (3.3), моделі СЕТ-операцій побудованих на основі елементарних функцій операцій, керованих інформацією, можна представити наступним чином:

$$C(x) = \begin{bmatrix} (x_2 \cdot \bar{x}_3)(x_1)(x_2 \vee \bar{x}_3) \\ (x_2 \vee x_3)(x_1)(x_2 \cdot x_3) \\ (x_2 \cdot x_3)(x_1)(x_2 \vee x_3) \end{bmatrix} = \begin{bmatrix} (x_2 \cdot \bar{x}_3)(x_1)(x_2 \vee \bar{x}_3) \\ (x_2 \cdot x_3)(\bar{x}_1)(x_2 \vee x_3) \\ (x_2 \cdot x_3)(x_1)(x_2 \vee x_3) \end{bmatrix};$$

$$C'(x) = \begin{bmatrix} (\bar{x}_2 \cdot x_3)(x_1)(\bar{x}_2 \vee x_3) \\ (x_2 \cdot x_3)(x_1)(x_2 \vee x_3) \\ (x_2 \vee x_3)(x_1)(x_2 \cdot x_3) \end{bmatrix} = \begin{bmatrix} (\bar{x}_2 \cdot x_3)(x_1)(\bar{x}_2 \vee x_3) \\ (x_2 \cdot x_3)(x_1)(x_2 \vee x_3) \\ (x_2 \cdot x_3)(\bar{x}_1)(x_2 \vee x_3) \end{bmatrix};$$

$$C(x) = \begin{bmatrix} (x_1 \vee x_2)(x_3)(x_1 \cdot x_2) \\ (\bar{x}_1 \cdot x_2)(x_3)(\bar{x}_1 \vee x_2) \\ (x_1 \cdot x_2)(x_3)(x_1 \vee x_2) \end{bmatrix} = \begin{bmatrix} (x_1 \cdot x_2)(\bar{x}_3)(x_1 \vee x_2) \\ (\bar{x}_1 \cdot x_2)(x_3)(\bar{x}_1 \vee x_2) \\ (x_1 \cdot x_2)(x_3)(x_1 \vee x_2) \end{bmatrix}.$$

Приймати рішення про доцільність використання розглянутих підходів до представлення моделей СЕТ-операцій побудованих на основі елементарних функцій операцій, керованих інформацією, на основі аналізу лише однієї операції не доцільно. Тому необхідно дослідити всю групу СЕТ-операцій.

3.2. Аналіз результатів обчислювального експерименту з моделювання СЕТ-операцій на основі елементарних функцій операцій, керованих інформацією

Для дослідження одноопераднних СЕТ-операцій на основі елементарних функцій операцій, керованих інформацією, необхідно мати множину даних операцій. Наявність даної множини і буде набором вхідних даних для проведення дослідження. Одноопераднді СЕТ-операції на основі елементарних функцій операцій, керованих інформацією, належать до групи 3Сі-квантових СЕТ-операції. Повна група 3Сі-квантових СЕТ-операції представляє собою всі підстановки з поля перестановок G_8 і включає в себе 40320 СЕТ-операцій. Всі 3Сі-квантові СЕТ-операції будуються на основі 70 3Сі-квантових елементарних функцій. Одноопераднді 3Сі-квантові СЕТ-операції на основі елементарних функцій операцій, керованих інформацією, будуються на основі 8 елементарних функцій операцій, керованих інформацією, [41, 47, 48]. Так як елементарних функцій всього 8, то кількість СЕТ-операцій, які потрібно знайти для проведення дослідження, буде значно меншою за 40320. Виходячи з незначної кількості елементарних функцій на основі яких будуються одноопераднді 3Сі-квантові СЕТ-операції на основі елементарних функцій операцій, керованих інформацією, доцільно для автоматизованого синтезу операцій використати повний перебір варіантів розміщення елементарних функцій в операціях. Даний підхід і було використано при проведенні обчислювального експерименту [47].

За результатами обчислювального експерименту було отримано 192 СЕТ-операції на основі елементарних функцій операцій, керованих інформацією. Результати обчислювального експерименту наведені в додатку А.

Будь яку СЕТ-операцію можна модифікувати шляхом перестановки елементарних функцій, а також шляхом інверсії результатів виконання елементарної функції. Якщо СЕТ-операція на основі елементарних функцій операцій, керованих інформацією, є ЗСі-квантовою, то вона виконує криптографічне перетворення ЗСі-квантів вхідної інформації і формує ЗСі-кванти результату перетворення [68, 79]. Виходячи з цього, її можна модифікувати за допомогою 6 операцій перестановки елементарних функцій і 8 операцій інверсії результатів. Відповідно на основі будь якої СЕТ-операції можна отримати 48 її модифікацій.

Так як група СЕТ-операції на основі елементарних функцій операцій, керованих інформацією, включає в себе 192 операції, то вона включає в себе модифікації 4 унікальних базових операцій (192:48=4). Дані 4 унікальні базові операції складають базову групу СЕТ-операції на основі елементарних функцій операцій, керованих інформацією. З будь якої операції базової групи шляхом перестановок і інверсій будується множина модифікованих СЕТ-операцій. Кожна побудована операція з даної множини буде унікальною (не буде повторюватись), а побудовані множини операцій не будуть перетинатися. Так як множина модифікованих СЕТ-операцій будується шляхом перестановок і інверсій елементарних функцій базової операції, то базова група операцій на основі елементарних функцій операцій, керованих інформацією, включає в себе будь які 4 операції, які належать до 4 різних множин модифікованих операцій [47].

В процесі дослідження одноопераднних СЕТ-операцій на основі елементарних функцій операцій, керованих інформацією, необхідно встановити правила побудови прямих і обернених СЕТ-операцій. Також ми вважаємо, що в межах цієї роботи доцільно дослідити правила побудови СЕТ-операцій базової групи, так як правила їх модифікації на основі перестановки і інверсії елементарних функцій відомі [22, 52].

Таблиця 3.2.

Підмножини симетричних СЕТ-операції на основі елементарних функцій операцій, керованих інформацією, [52].

	Множина 1	Множина 2	Множина 3	Множина 4
1	$C_{23,43,77}(x)$	$C_{23,43,142}(x)$	$C_{23,142,77}(x)$	$C_{43,77,113}(x)$
2	$C_{23,77,43}(x)$	$C_{43,23,113}(x)$	$C_{77,113,23}(x)$	$C_{77,113,43}(x)$
3	$C_{43,23,178}(x)$	$C_{43,142,232}(x)$	$C_{77,232,142}(x)$	$C_{113,43,77}(x)$
4	$C_{77,212,23}(x)$	$C_{113,23,43}(x)$	$C_{113,77,23}(x)$	$C_{113,77,43}(x)$
5	$C_{178,43,232}(x)$	$C_{142,232,212}(x)$	$C_{142,178,232}(x)$	$C_{142,178,212}(x)$
6	$C_{212,232,77}(x)$	$C_{212,113,23}(x)$	$C_{178,23,113}(x)$	$C_{142,212,178}(x)$
7	$C_{232,178,212}(x)$	$C_{212,232,142}(x)$	$C_{178,142,232}(x)$	$C_{178,142,212}(x)$
8	$C_{232,212,178}(x)$	$C_{232,212,113}(x)$	$C_{232,113,178}(x)$	$C_{212,178,142}(x)$

Нижні індекси в моделях СЕТ-операцій, наведених в табл. 3.2, відображають індекси елементарних функцій з яких побудовано дані операції. Наприклад:

$$C_{77,212,23}(x)=\begin{bmatrix} f_{77}(x) \\ f_{212}(x) \\ f_{23}(x) \end{bmatrix}.$$

Базова група СЕТ-операцій на основі елементарних функцій операцій, керованих інформацією, яка складається лише з симетричних операцій, включає в себе по одній модифікованій операції з кожної множини. Наприклад:

- $C_{23,43,77}(x)$, $C_{23,43,142}(x)$, $C_{23,142,77}(x)$, $C_{43,77,113}(x)$;
- $C_{23,43,77}(x)$, $C_{43,23,113}(x)$, $C_{178,23,113}(x)$, $C_{142,178,212}(x)$;
- $C_{178,43,232}(x)$, $C_{142,232,212}(x)$, $C_{77,232,142}(x)$, $C_{178,142,212}(x)$.

Відповідно до табл. 3.2, кількість операцій в групі, що складається з симетричних операцій буде визначатися як $8\cdot 8\cdot 8\cdot 8=8^4=4096$.

Вибір базової групи для побудови методу синтезу СЕТ-операцій на основі елементарних функцій операцій, керованих інформацією, необхідно проводити на основі двох вимог [52]:

1. Мінімальна простота синтезу 4 симетричних СЕТ-операцій базової групи. Дана вимога базується на необхідності зменшення обчислювальних ресурсів для моделювання систем захисту інформацій на основі СЕТ-шифрування.
2. Максимальна відмінність відповідних елементарних функцій в 4 симетричних СЕТ-операціях базової групи для реалізації вихідних Сі-квантів інформації. Дана вимога базується на бажанні максимального ускладнення криптографічного аналізу, для визначення правил формування послідовності криптографічних перетворень.

Наведені вимоги достатньо суперечливі і вимагають різних підходів до пошуку СЕТ-операцій базової групи. Необхідно відмітити, що незалежно від того, яка базова група СЕТ-операцій буде взята за основу, це забезпечить побудову повної групи операцій на основі перестановок і інверсій елементарних функцій. Вибір базової групи буде впливати лише на послідовність синтезу СЕТ-операцій.

Виходячи з цього, доцільно розглядати вимоги до СЕТ-операцій базової групи незалежно одна від одної, а вже на основі отриманих результатів, та, за необхідності, спробувати знайти компроміс.

3.3. Синтез базової групи СЕТ-операцій на основі елементарних функцій операцій, керованих інформацією, за критерієм простоти їх побудови

В процесі аналізу підмножини симетричних СЕТ-операції на основі елементарних функцій операцій, керованих інформацією, констатовано, що наведеній в табл. 3.2 першій вимозі відповідає базова група, яка включає в себе такі СЕТ-операції [47]:

$$C_{23,43,77}(x), \quad C_{23,43,142}(x), \quad C_{23,142,77}(x), \quad C_{113,43,77}(x).$$

Обґрунтуємо вибір даних СЕТ-операцій в склад базової групи і сформулюємо підхід на основі якого було реалізовано даний вибір.

Основу вибраної базової групи складає така СЕТ-операція:

$$C_{23,43,77}(x) = \begin{bmatrix} f_{23}(x) \\ f_{43}(x) \\ f_{77}(x) \end{bmatrix}. \tag{3.4}$$

Дана СЕТ-операція належить до першої множини симетричних операцій (табл. 3.2). Вона включає в себе першу $f_{23}(x)$, другу $f_{43}(x)$ і третю $f_{77}(x)$ елементарні функції з чотирьох прямих елементарних функцій (табл. 2.1), відсортованих в порядку зростання порядкового номеру. Четверта пряма елементарна функція $f_{113}(x)$ в даній СЕТ-операції не використовується.

Побудова другої СЕТ-операції полягає в заміні першої елементарної функції. Спочатку першу елементарну функцію в СЕТ-операції (3.4) слід замінити четвертою елементарною функцією:

$$f_{23}(x) \rightarrow f_{113}(x) \tag{3.5}$$

Виконавши заміну отримаємо:

$$C_{113,43,77}(x)=\begin{bmatrix} f_{113}(x) \\ f_{43}(x) \\ f_{77}(x) \end{bmatrix}. \tag{3.6}$$

СЕТ-операція (3.6) належить до першої множини симетричних операцій (табл. 3.2).

Побудова третьої СЕТ-операції полягає в заміні другої елементарної функції. Другу елементарну функцію в СЕТ-операції (3.4) слід замінити оберненою четвертою елементарною функцією:

$$f_{43}(x) \rightarrow \bar{f}_{113}(x) = f_{142}(x) \tag{3.7}$$

Виконавши заміну отримаємо:

$$C_{23,142,77}(x)=\begin{bmatrix} f_{23}(x) \\ f_{142}(x) \\ f_{77}(x) \end{bmatrix}. \tag{3.8}$$

Дана СЕТ-операція належить до третьої множини симетричних операцій (табл. 3.2).

Побудова четвертої СЕТ-операції полягає в заміні третьої елементарної функції. Третю елементарну функцію в СЕТ-операції (3.4) слід замінити оберненою четвертою елементарною функцією:

$$f_{77}(x) \rightarrow \bar{f}_{113}(x) = f_{142}(x) \tag{3.9}$$

Виконавши заміну отримаємо:

$$C_{23,43,142}(x)=\begin{bmatrix} f_{23}(x) \\ f_{43}(x) \\ f_{142}(x) \end{bmatrix}. \tag{3.10}$$

Дана СЕТ-операція належить до другої множини симетричних операцій (табл. 3.2).

За результатами побудови отримано по одній симетричній СЕТ-операції з кожної із чотирьох множин симетричних СЕТ-операцій. Це означає, що була побудована базова група СЕТ-операцій на основі елементарних функцій операцій, керованих інформацією.

Для оцінки відповідності синтезованої базової групи СЕТ-операцій другій вимозі до побудови базових груп, введемо коефіцієнт зміни кількості елементарних функцій при криптографічному перетворенні блоків інформації.

Визначимо коефіцієнт зміни кількості елементарних функцій при криптографічному перетворенні блоків інформації ($K_{\to f(x)}$) як відношення сумарної кількості змін елементарних функцій до кількості варіантів перетворення блоків:

$$K_{\to f(x)} = \frac{\sum_{i=1}^{n}\sum_{j=1}^{n} k_{ij}}{n^2} \qquad (3.11)$$

де n - кількість СЕТ-операцій в криптографічній системі, k_{ij} - зміна кількості елементарних функцій при переході від СЕТ-операції $C_i(x)$ до СЕТ-операції $C_j(x)$.

Даний коефіцієнт показує середнє значення зміни елементарних функцій між операціями криптографічного перетворення двох сусідніх блоків інформації на заданому наборі СЕТ-операцій. Незважаючи на те, що коефіцієнт вводився для оцінки варіативності перетворення двох сусідніх блоків інформації, їм можна оцінювати варіативність перетворення будь яких двох блоків шифрограми.

Точна оцінка варіативності криптографічного перетворення проводиться аналогічно з використанням таблиць істинності моделей елементарних функцій і СЕТ-операцій.

Побудуємо таблицю відмінностей елементарних функцій в СЕТ-операціях синтезованої базової групи (табл. 3.3) для попередньої оцінки результатів застосування синтезованої базової групи СЕТ-операцій.

На основі табл. 3.3 визначимо $K_{\to f(x)}$ в криптографічному алгоритмі, який використовує операції базової групи $C_{23,43,77}(x)$, $C_{113,43,77}(x)$, $C_{23,142,77}(x)$, $C_{23,43,142}(x)$.

$$K_{\to f(x)} = \frac{18}{16} = 1{,}125.$$

Таблиця 3.3.

Таблиця відмінностей елементарних функцій в СЕТ-операціях базової групи

	$C_{23,43,77}(x)$	$C_{113,43,77}(x)$	$C_{23,142,77}(x)$	$C_{23,43,142}(x)$
$C_{23,43,77}(x)$	**0**	**1**	**1**	**1**
$C_{113,43,77}(x)$	**1**	**0**	**2**	**2**
$C_{23,142,77}(x)$	**1**	**2**	**0**	**2**
$C_{23,43,142}(x)$	**1**	**2**	**2**	**0**

Для уточнення і практичної реалізації розглянутого алгоритму побудови базової групи з симетричних СЕТ-операцій на основі елементарних функцій операцій, керованих інформацією, необхідно перейти від СЕТ-операцій, побудованих на основі набору елементарних функцій, до дискретно-казуальних моделей СЕТ-операцій [41, 47].

Відповідно до табл. 3.1, синтез дискретно-казуальних моделей можна будувати на основі 27 варіантів, які відрізняються порядком використання ключових елементів в елементарних функціях.

Під ключовим елементом будемо розуміти порядковий номер Сі-кванта вхідної інформації, на основі якого реалізовано казуальне управління вибором операції перетворення для побудови вихідного Сі-кванта інформації.

Всі дискретно-казуальні моделі СЕТ-операцій базової групи повинні будуватися на основі одного варіанту розміщення ключових елементів. В процесі дослідження обмежимося чотирма варіантами вибору послідовностей ключових елементів.

Варіант 1 послідовності ключових елементів:

$$\begin{bmatrix} x_1 \rightarrow f_{1^*}(x) \\ x_2 \rightarrow f_{2^*}(x) \\ x_3 \rightarrow f_{3^*}(x) \end{bmatrix} \tag{3.12}$$

де $f_{j^*}(x)$ – j-та елементарна функція в кортежі одноопераднної СЕТ-операції.

Варіант 2 послідовності ключових елементів:

$$\begin{bmatrix} x_1 \rightarrow f_{1^*}(x) \\ x_1 \rightarrow f_{2^*}(x). \\ x_1 \rightarrow f_{3^*}(x) \end{bmatrix} \tag{3.13}$$

Варіант 3 послідовності ключових елементів:

$$\begin{bmatrix} x_2 \rightarrow f_{1^*}(x) \\ x_2 \rightarrow f_{2^*}(x). \\ x_2 \rightarrow f_{3^*}(x) \end{bmatrix} \tag{3.14}$$

Варіант 4 послідовності ключових елементів:

$$\begin{bmatrix} x_3 \rightarrow f_{1^*}(x) \\ x_3 \rightarrow f_{2^*}(x). \\ x_3 \rightarrow f_{3^*}(x) \end{bmatrix} \tag{3.15}$$

Побудуємо СЕТ-операції базової групи (3.4), (3.6), (3.8) і (3.10) на основі першого варіанту послідовності ключових елементів (3.12):

$$C_{23,43,77}(x)=\begin{bmatrix}(x_2\cdot x_3\ )(x_1)(x_2\vee x_3)\\(x_1\cdot \bar{x}_3\ )(\ x_2)(x_1\vee \bar{x}_3\ )\\(x_1\cdot \bar{x}_2\ )(\ x_3)(x_1\vee \bar{x}_2)\end{bmatrix}; \qquad (3.16)$$

$$C_{113,43,77}(x)=\begin{bmatrix}(x_2\vee x_3\ )(x_1)(x_2\cdot x_3)\\(x_1\cdot \bar{x}_3\ )(\ x_2)(x_1\vee \bar{x}_3\ )\\(x_1\cdot \bar{x}_2\ )(\ x_3)(x_1\vee \bar{x}_2)\end{bmatrix}=\begin{bmatrix}(x_2\cdot x_3\ )(\bar{x}_1)(x_2\vee x_3)\\(x_1\cdot \bar{x}_3\ )(\ x_2)(x_1\vee \bar{x}_3\ )\\(x_1\cdot \bar{x}_2\ )(\ x_3)(x_1\vee \bar{x}_2)\end{bmatrix}; \qquad (3.17)$$

$$C_{23,142,77}(x)=\begin{bmatrix}(x_2\cdot x_3\ )(x_1)(x_2\vee x_3\\(x_1\vee \bar{x}_3\ )(x_2)(x_1\cdot \bar{x}_3)\\(x_1\cdot \bar{x}_2\ )(\ x_3)(x_1\vee \bar{x}_2)\end{bmatrix}=\begin{bmatrix}(x_2\cdot x_3\ )(x_1)(x_2\vee x_3\\(x_1\cdot \bar{x}_3\ )(\ \bar{x}_2)(x_1\vee \bar{x}_3\ )\\(x_1\cdot \bar{x}_2\ )(\ x_3)(x_1\vee \bar{x}_2)\end{bmatrix}; \qquad (3.18)$$

$$C_{23,43,142}(x)=\begin{bmatrix}(x_2\cdot x_3\ )(x_1)(x_2\vee x_3)\\(x_1\cdot \bar{x}_3\ )(\ x_2)(x_1\vee \bar{x}_3\ )\\(x_1\vee \bar{x}_2)(\ x_3)(x_1\cdot \bar{x}_2)\end{bmatrix}=\begin{bmatrix}(x_2\cdot x_3\ )(x_1)(x_2\vee x_3)\\(x_1\cdot \bar{x}_3\ )(\ x_2)(x_1\vee \bar{x}_3\ )\\(x_1\cdot \bar{x}_2\ )(\ \bar{x}_3)(x_1\vee \bar{x}_2)\end{bmatrix}. \qquad (3.19)$$

На основі побудованих дискретно-казуальних моделей СЕТ-операції базової групи (3.16) – (3.19) згідно першого варіанту послідовності ключових елементів можна формалізувати наступний алгоритм їх синтезу:

1. В основу синтезу базової групи СЕТ-операцій на основі елементарних функцій операцій, керованих інформацією, береться СЕТ-операція $C_{23,43,77}(x)$. Дана СЕТ-операція є першою СЕТ-операцією базової групи;

2. Для побудови другої СЕТ-операції базової групи необхідно інвертувати ключовий елемент x_1 першої елементарної функції $f_{23}(x)$. Дане інвертування забезпечить перетворення $f_{23}(x)$ в $f_{113}(x)$;

3. Для побудови третьої СЕТ-операції базової групи необхідно інвертувати ключовий елемент x_2 першої елементарної функції $f_{43}(x)$. Дане інвертування забезпечить перетворення $f_{43}(x)$ в $f_{142}(x)$;

4. Для побудови четвертої СЕТ-операції базової групи необхідно інвертувати ключовий елемент x_3 першої елементарної функції $f_{77}(x)$. Дане інвертування забезпечить перетворення $f_{77}(x)$ в $f_{142}(x)$;

Синтезу базової групи СЕТ-операцій на основі елементарних функцій операцій, керованих інформацією, реалізується при виборі СЕТ-операції $C_{23,43,77}(x)$ з послідовною нумерацією ключових елементів шляхом інверсії ключових елементів.

Формально алгоритм синтезу можна представити так:

Алгоритм 1:

1.1. $C_{1*}(x) = C_{23,43,77}(x)$;

1.2. $f_{1*}(x) : (x_1) \to (\bar{x}_1)$; $f_{23}(x) \to f_{113}(x)$; $C_{23,43,77}(x) \to C_{13,43,77}(x)$; $C_{2*}(x) = C_{113,43,77}(x)$;

1.3. $f_{2*}(x) : (x_2) \to (\bar{x}_2)$; $f_{43}(x) \to f_{142}(x)$; $C_{23,43,77}(x) \to C_{13,142,77}(x)$; $C_{3*}(x) = C_{23,142,77}(x)$;

1.4. $f_{3*}(x) : (x_3) \to (\bar{x}_3)$; $f_{77}(x) \to f_{142}(x)$; $C_{23,43,77}(x) \to C_{13,43,142}(x)$; $C_{2*}(x) = C_{23,43,142}(x)$.

Побудуємо СЕТ-операції базової групи на основі другого варіанту послідовності ключових елементів (3.13):

$$C_{23,43,77}(x)=\begin{bmatrix}(x_2\cdot x_3\ )(x_1)(x_2\vee x_3)\\(x_2\cdot \bar{x}_3\ )(x_1)(x_2\vee \bar{x}_3)\\(\bar{x}_2\cdot x_3\ )(x_1)(\bar{x}_2\vee x_3)\end{bmatrix};\qquad (3.20)$$

$$C_{113,43,77}(x)=\begin{bmatrix}(x_2\vee x_3\ )(x_1)(x_2\cdot x_3)\\(x_2\cdot \bar{x}_3\ )(x_1)(x_2\vee \bar{x}_3)\\(\bar{x}_2\cdot x_3\ )(x_1)(\bar{x}_2\vee x_3)\end{bmatrix}=\begin{bmatrix}(x_2\cdot x_3\ )(\bar{x}_1)(x_2\vee x_3)\\(x_2\cdot \bar{x}_3\ )(x_1)(x_2\vee \bar{x}_3)\\(\bar{x}_2\cdot x_3\ )(x_1)(\bar{x}_2\vee x_3)\end{bmatrix};\qquad (3.21)$$

$$C_{23,142,77}(x)=\begin{bmatrix}(x_2\cdot x_3\ )(x_1)(x_2\vee x_3)\\(\bar{x}_2\cdot \bar{x}_3\ )(x_1)(\bar{x}_2\vee \bar{x}_3)\\(\bar{x}_2\cdot x_3\ )(\ x_1)(\bar{x}_2\vee x_3)\end{bmatrix};\qquad (3.22)$$

$$f_{77}=(\bar{x}_2\cdot x_3\ )(x_1)(\bar{x}_2\vee x_3)$$

$$C_{23,43,142}(x)=\begin{bmatrix}(x_2\cdot x_3\ )(x_1)(x_2\vee x_3)\\(x_2\cdot \bar{x}_3\ )(x_1)(x_2\vee \bar{x}_3)\\(\bar{x}_2\cdot \bar{x}_3\ )(x_1)(\bar{x}_2\vee \bar{x}_3)\end{bmatrix}.\qquad (3.23)$$

На основі побудованих дискретно-казуальних моделей СЕТ-операції базової групи (3.20) – (3.23) згідно другого варіанту послідовності ключових елементів можна формалізувати наступний алгоритм їх синтезу:

Алгоритм 2:

2.1. $C_{1^*}(x)=C_{23,43,77}(x);$

2.2. $f_{1^*}(x):x_1\to\bar{x}_1;\ f_{23}(x)\to f_{113}(x);\ C_{23,43,77}(x)\to C_{13,43,77}(x);\ C_{2^*}(x)=C_{113,43,77}(x);$

2.3. $f_{2^*}(x):x_2\to\bar{x}_2;\ f_{43}(x)\to f_{142}(x);\ C_{23,43,77}(x)\to C_{13,142,77}(x);\ C_{3^*}(x)=C_{23,142,77}(x);$

2.4. $f_{3^*}(x):x_3\to\bar{x}_3;\ f_{77}(x)\to f_{142}(x);\ C_{23,43,77}(x)\to C_{13,43,142}(x);\ C_{2^*}(x)=C_{23,43,142}(x).$

Побудуємо СЕТ-операції базової групи на основі третього варіанту послідовності ключових елементів (3.14):

$$C_{23,43,77}(x)=\begin{bmatrix}(x_1\cdot x_3\ )(x_2)(x_1\vee x_3)\\(x_1\cdot \bar{x}_3\ )(\ x_2)(x_1\vee \bar{x}_3\ )\\(x_1\vee x_3\ )(\ x_2)(x_1\cdot x_3)\end{bmatrix}=\begin{bmatrix}(x_1\cdot x_3\ )(x_2)(x_1\vee x_3)\\(x_1\cdot \bar{x}_3\ )(\ x_2)(x_1\vee \bar{x}_3\ )\\(x_1\cdot x_3\ )(\ \bar{x}_2)(x_1\vee x_3)\end{bmatrix};\qquad (3.24)$$

$$C_{113,43,77}(x)=\begin{bmatrix}(\bar{x}_1\cdot x_3\ )(\ x_2)(\bar{x}_1\vee x_3)\\(x_1\cdot \bar{x}_3\ )(x_2)(x_1\vee \bar{x}_3)\\(x_1\cdot x_3\ )(\bar{x}_2)(x_2\vee x_3)\end{bmatrix};\qquad (3.25)$$

$$C_{23,142,77}(x)=\begin{bmatrix}(x_1\cdot x_3\ )(x_2)(x_1\vee x_3)\\(x_1\vee \bar{x}_3\ )(x_2)(x_1\cdot \bar{x}_3)\\(x_1\cdot x_3\ )(\ \bar{x}_2)(x_1\vee x_3)\end{bmatrix}=\begin{bmatrix}(x_1\cdot x_3\ )(x_2)(x_1\vee x_3)\\(x_1\cdot \bar{x}_3\ )(\bar{x}_2)(x_1\vee \bar{x}_3)\\(x_1\cdot x_3\ )(\ \bar{x}_2)(x_1\vee x_3)\end{bmatrix};\qquad (3.26)$$

$$C_{23,43,142}(x)=\begin{bmatrix}(x_1\cdot x_3\ )(x_2)(x_1\vee x_3)\\(x_1\cdot \bar{x}_3\ )(\ x_2)(x_1\vee \bar{x}_3)\\(x_1\vee \bar{x}_3\ )(x_2)(x_1\cdot \bar{x}_3)\end{bmatrix}=\begin{bmatrix}(x_1\cdot x_3\ )(x_2)(x_1\vee x_3)\\(x_1\cdot \bar{x}_3\ )(\ x_2)(x_1\vee \bar{x}_3)\\(x_1\cdot \bar{x}_3\ )(\bar{x}_2)(x_1\vee \bar{x}_3)\end{bmatrix}.\qquad (3.27)$$

На основі побудованих дискретно-казуальних моделей СЕТ-операції базової групи (3.24) – (3.27) згідно третього варіанту послідовності ключових елементів можна формалізувати наступний алгоритм їх синтезу:

Алгоритм 3:

3.1. $C_{1^*}(x)=C_{23,43,77}(x)$;

3.2. $f_{1^*}(x)\colon x_1\to\bar{x}_1;\ \bar{x}_1\to x_1;\quad f_{23}(x)\to f_{113}(x);\quad C_{23,43,77}(x)\to C_{13,43,77}(x);$
$C_{2^*}(x)=C_{113,43,77}(x)$;

3.3. $f_{2^*}(x)\colon x_2\to\bar{x}_2;\ \bar{x}_2\to x_2;\quad f_{43}(x)\to f_{142}(x);\quad C_{23,43,77}(x)\to C_{13,142,77}(x);$
$C_{3^*}(x)=C_{23,142,77}(x)$;

3.4. $f_{3^*}(x)\colon x_3\to\bar{x}_3;\ \bar{x}_3\to x_2;\quad f_{77}(x)\to f_{142}(x);\quad C_{23,43,77}(x)\to C_{13,43,142}(x);$
$C_{2^*}(x)=C_{23,43,142}(x)$.

Побудуємо СЕТ-операції базової групи на основі четвертого варіанту послідовності ключових елементів (3.15):

$$C_{23,43,77}(x)=\begin{bmatrix}(x_1\cdot x_2\ )(\ x_3)(x_1\vee x_2)\\(x_1\vee x_2\ )(\ x_3)(x_1\cdot x_2)\\(x_1\cdot \bar{x}_2\ )(\ x_3)(x_1\vee \bar{x}_2)\end{bmatrix}=\begin{bmatrix}(x_1\cdot x_2\ )(\ x_3)(x_1\vee x_2)\\(x_1\cdot x_2\ )(\ \bar{x}_3)(x_1\vee x_2)\\(x_1\cdot \bar{x}_2\ )(\ x_3)(x_1\vee \bar{x}_2)\end{bmatrix}; \tag{3.28}$$

$$C_{113,43,77}(x)=\begin{bmatrix}(\bar{x}_1\cdot x_2\ )(\ x_3)(\bar{x}_1\vee x_2)\\(x_1\cdot x_2\ )(\ \bar{x}_3)(x_1\vee x_2)\\(x_1\cdot \bar{x}_2\ )(\ x_3)(x_1\vee \bar{x}_2)\end{bmatrix}; \tag{3.29}$$

$$C_{23,142,77}(x)=\begin{bmatrix}(x_1\cdot x_2\ )(\ x_3)(x_1\vee x_2)\\(x_1\vee \bar{x}_2)(\ x_3)(x_1\cdot \bar{x}_2)\\(x_1\cdot \bar{x}_2\ )(\ x_3)(x_1\vee \bar{x}_2)\end{bmatrix}=\begin{bmatrix}(x_1\cdot x_2\ )(\ x_3)(x_1\vee x_2)\\(x_1\cdot \bar{x}_2\ )(\bar{x}_3)(x_1\vee \bar{x}_2)\\(x_1\cdot \bar{x}_2\ )(\ x_3)(x_1\vee \bar{x}_2)\end{bmatrix}; \tag{3.30}$$

$$C_{23,43,142}(x)=\begin{bmatrix}(x_1\cdot x_2\ )(\ x_3)(x_1\vee x_2)\\(x_1\cdot x_2\ )(\ \bar{x}_3)(x_1\vee x_2)\\(x_1\vee \bar{x}_2)(\ x_3)(x_1\cdot \bar{x}_2)\end{bmatrix}=\begin{bmatrix}x_1\cdot x_2\ )(\ x_3)(x_1\vee x_2)\\(x_1\cdot x_2\ )(\ \bar{x}_3)(x_1\vee x_2)\\(x_1\cdot \bar{x}_2\ )(\bar{x}_3)(x_1\vee \bar{x}_2)\end{bmatrix}. \tag{3.31}$$

На основі побудованих дискретно-казуальних моделей СЕТ-операції базової групи (3.28) – (3.31) згідно четвертого варіанту послідовності ключових елементів можна формалізувати наступний алгоритм їх синтезу:

Алгоритм 4:

4.1. $C_{1^*}(x)=C_{23,43,77}(x)$;

4.2. $f_{1^*}(x): x_1\to\bar{x}_1;\ \bar{x}_1\to x_1$; $f_{23}(x)\to f_{113}(x)$; $C_{23,43,77}(x)\to C_{13,43,77}(x)$;
$C_{2^*}(x)=C_{113,43,77}(x)$;

4.3. $f_{2^*}(x): x_2\to\bar{x}_2;\ \bar{x}_2\to x_2$; $f_{43}(x)\to f_{142}(x)$; $C_{23,43,77}(x)\to C_{13,142,77}(x)$;
$C_{3^*}(x)=C_{23,142,77}(x)$;

4.4. $f_{3^*}(x): x_3\to\bar{x}_3;\ \bar{x}_3\to x_2$; $f_{77}(x)\to f_{142}(x)$; $C_{23,43,77}(x)\to C_{13,43,142}(x)$;
$C_{2^*}(x)=C_{23,43,142}(x)$.

Аналіз наведених алгоритмів показав, що всі чотири алгоритми мають однакову складність реалізації і відрізняються лише вибраними моделями

елементарних функцій. Слід відмітити, що алгоритми 2, 3 і 4 співпадають, а алгоритм 1 є обмеженими випадком алгоритмів 2 – 4. Заміна алгоритму 1 на інший алгоритм при збереженні правил вибору моделей елементарних функцій не приведе до зміни результату моделювання СЕТ-операцій базової групи.

Недоліком запропонованих алгоритмів є значення коефіцієнту зміни кількості елементарних функцій при криптографічному перетворенні блоків інформації операціями базової групи СЕТ-операцій на основі елементарних функцій операцій, керованих інформацією.

3.4. Синтез базової групи СЕТ-операцій на основі елементарних функцій операцій, керованих інформацією, за критерієм відмінності відповідних елементарних функцій

Для забезпечення максимальної відмінності відповідних елементарних функцій в 4 симетричних СЕТ-операціях базової групи та для реалізації вихідних Сі-квантів інформації було додатково проаналізовано підмножини симетричних СЕТ-операції, наведених в табл. 3.2.

За результатами аналізу визначена базова група, яка включає в себе наступні СЕТ-операції:

$$C_{23,43,77}(x), \quad C_{113,77,43}(x), \quad C_{77,113,23}(x), \quad C_{43,23,113}(x).$$

Побудуємо таблицю відмінностей елементарних функцій в СЕТ-операціях встановленої базової групи (табл. 3.4).

Таблиця 3.4.

Таблиця відмінностей елементарних функцій в СЕТ-операціях базової групи

	$C_{23,43,77}(x)$	$C_{113,77,43}(x)$	$C_{77,113,23}(x)$	$C_{43,23,113}(x)$
$C_{23,43,77}(x)$	**0**	**3**	**3**	**3**
$C_{113,77,43}(x)$	**3**	**0**	**3**	**3**
$C_{77,113,23}(x)$	**3**	**3**	**0**	**3**
$C_{43,23,113}(x)$	**3**	**3**	**3**	**0**

На основі табл. 3.4 визначимо $K_{\to f(x)}$ в криптографічному алгоритмі, який використовує операції базової групи $C_{23,43,77}(x)$, $C_{113,77,43}(x)$, $C_{77,113,23}(x)$, $C_{43,23,113}(x)$:

$$K_{\to f(x)} = \frac{36}{16} = 2{,}25.$$

Отримане значення коефіцієнта 2,25 буде максимальним для базових груп з чотирьох ЗСі-квантових СЕТ-операцій. Дане максимальне значення трактується на основі того, що при порівнянні всіх СЕТ-операцій жодна елементарна функція формування вихідного Сі-кванта інформації не повторилася.

Розглянемо побудову базової групи СЕТ-операцій на основі елементарних функцій операцій, керованих інформацією. Алгоритм побудови базової групи СЕТ-операцій, який реалізується на рівні елементарних функцій, має таке представлення:

1. Основу вибраної базової групи складає СЕТ-операція $C_{23,43,77}(x)$ (3.4): $C_{1^*}(x) = C_{23,43,77}(x)$;
2. Друга СЕТ-операція базової групи будується шляхом заміни першої елементарної функції та перестановки місцями другої і третьої елементарних функцій:

$$C_{2^*}(x):\ f_{1^*}(x) = f_{23}(x) \to f_{1^*}(x) = f_{113}(x);$$
$$(f_{2^*}(x) \to f_{3^*}(x)) = (f_{43}(x) \to f_{77}(x));$$
$$(f_{3^*}(x) \to f_{2^*}(x)) = (f_{77}(x) \to f_{43}(x));$$

$$C_{113,77,43}(x) = \begin{bmatrix} f_{113}(x) \\ f_{77}(x) \\ f_{43}(x) \end{bmatrix}; \qquad (3.32)$$

3. Третя СЕТ-операція базової групи будується шляхом заміни другої елементарної функції та перестановки місцями першої і третьої елементарних функцій:

$$C_{3^*}(x):\ f_{2^*}(x)=f_{43}(x)\to f_{2^*}(x)=f_{113}(x);$$
$$(f_{1^*}(x)\to f_{3^*}(x))=(f_{23}(x)\to f_{77}(x));$$
$$(f_{3^*}(x)\to f_{1^*}(x))=(f_{77}(x)\to f_{23}(x));$$
$$C_{77,113,23}(x)=\begin{bmatrix} f_{77}(x) \\ f_{113}(x) \\ f_{23}(x) \end{bmatrix}; \qquad (3.33)$$

4. Четверта СЕТ-операція базової групи будується шляхом заміни третьої елементарної функції та перестановки місцями першої і другої елементарних функцій:

$$C_{4^*}(x):\ f_{3^*}(x)=f_{77}(x)\to f_{3^*}(x)=f_{113}(x);$$
$$(f_{1^*}(x)\to f_{2^*}(x))=(f_{23}(x)\to f_{43}(x));$$
$$(f_{2^*}(x)\to f_{1^*}(x))=(f_{43}(x)\to f_{23}(x));$$
$$C_{43,23,113}(x)=\begin{bmatrix} f_{43}(x) \\ f_{23}(x) \\ f_{113}(x) \end{bmatrix}. \qquad (3.34)$$

Для практичного застосування простий синтез базових груп СЕТ-операцій на рівні елементарних функцій з наступним переходом до моделей елементарних функцій та СЕТ-операцій недостатньо ефективний. За можливості, доцільно розробити алгоритм синтезу базових операцій на рівні моделей елементарних функцій. Даний перехід дозволить перейти з рівня елементарних функцій до рівня Сі-квантів інформації, що забезпечить простоту технічної реалізації синтезу операцій.

Побудуємо СЕТ-операції базової групи (3.4), (3.32), (3.33) і (3.34) на основі першого варіанту послідовності ключових елементів (3.12):

$C_{23,43,77}(x)$ описана моделлю (3.16);

$$C_{113,77,43}(x)=\begin{bmatrix}(x_2\vee x_3\ )(x_1)(x_2\cdot x_3)\\(x_1\vee x_3\ )(\ x_2)(x_1\cdot x_3)\\(x_1\vee x_2\ )(\ x_3)(x_1\cdot x_2)\end{bmatrix}=\begin{bmatrix}(x_2\cdot x_3\ )(\bar{x}_1)(x_2\vee x_3)\\(x_1\cdot x_3\ )(\ \bar{x}_2)(x_1\vee x_3)\\(x_1\cdot x_2\ )(\ \bar{x}_3)(x_1\vee x_2)\end{bmatrix};\qquad(3.35)$$

$$C_{77,113,23}(x)=\begin{bmatrix}(\bar{x}_2\cdot x_3\ )(x_1)(\bar{x}_2\vee x_3)\\(\bar{x}_1\cdot x_3\ )(\ x_2)(\bar{x}_1\vee x_3)\\(x_1\cdot x_2\ )(\ x_3)(x_1\vee x_2)\end{bmatrix};\qquad(3.36)$$

$$C_{43,23,113}(x)=\begin{bmatrix}(x_2\cdot \bar{x}_3\ )(x_1)(x_2\vee \bar{x}_3)\\(x_1\cdot x_3\ )(\ x_2)(x_1\vee x_3\ )\\(\bar{x}_1\cdot x_2\ )(\ x_3)(\bar{x}_1\vee x_2)\end{bmatrix}.\qquad(3.37)$$

На основі побудованих дискретно-казуальних моделей СЕТ-операції базової групи (3.16), (3.35) – (3.37) згідно першого варіанту послідовності ключових елементів (3.12) можна формалізувати наступний алгоритм їх синтезу:

Алгоритм 5:

5.1. $C_{1*}(x)=C_{23,43,77}(x)$;

5.2. $f_{1*}(x):(x_1)\to(\bar{x}_1);\ f_{23}(x)\to f_{113}(x)$;

$f_{2*}(x):(x_2)\to(\bar{x}_2);\ \bar{x}_3\to x_3;\ \ f_{43}(x)\to f_{77}(x)$;

$f_{3*}(x):(x_3)\to(\bar{x}_3);\ \bar{x}_2\to x_2;\ \ f_{77}(x)\to f_{43}(x)$;

$C_{23,43,77}(x)\to C_{113,77,43}(x);\ C_{2*}(x)=C_{113,77,43}(x)$;

5.3. $f_{2*}(x):\ x_1\to\bar{x}_1;\ \bar{x}_3\to x_3;\ \ f_{43}(x)\to f_{113}(x)$;

$f_{1*}(x):x_2\to\bar{x}_2;\ f_{23}(x)\to f_{77}(x)$;

$f_{3*}(x):\ \bar{x}_2\to x_2;\ \ f_{77}(x)\to f_{23}(x)$;

$C_{23,43,77}(x)\to C_{77,113,23}(x);\ C_{3*}(x)=C_{77,113,23}(x)$;

5.4. $f_{3*}(x):\ x_1\to\bar{x}_1;\ \bar{x}_2\to x_2;\ \ f_{77}(x)\to f_{23}(x)$;

$f_{1*}(x):x_3\to\bar{x}_3;\ f_{23}(x)\to f_{43}(x)$;

$f_{2*}(x):\ \bar{x}_3\to x_3;\ \ f_{43}(x)\to f_{23}(x)$;

$$C_{23,43,77}(x) \to C_{43,23,113}(x);\ C_{3^*}(x) = C_{43,23,113}(x);$$

Побудуємо СЕТ-операції базової групи на основі другого варіанту послідовності ключових елементів (3.13):

$C_{23,43,77}(x)$ описана моделлю (3.20);

$$C_{113,77,43}(x) = \begin{bmatrix} (x_2 \vee x_3)(x_1)(x_2 \cdot x_3) \\ (\bar{x}_2 \cdot x_3)(x_1)(\bar{x}_2 \vee x_3) \\ (x_2 \cdot \bar{x}_3)(x_1)(x_2 \vee \bar{x}_3) \end{bmatrix} = \begin{bmatrix} (x_2 \cdot x_3)(\bar{x}_1)(x_2 \vee x_3) \\ (\bar{x}_2 \cdot x_3)(x_1)(\bar{x}_2 \vee x_3) \\ (x_2 \cdot \bar{x}_3)(x_1)(x_2 \vee \bar{x}_3) \end{bmatrix}; \quad (3.38)$$

$$C_{77,113,23}(x) = \begin{bmatrix} (\bar{x}_2 \cdot x_3)(x_1)(\bar{x}_2 \vee x_3) \\ (x_2 \cdot x_3)(\bar{x}_1)(x_2 \vee x_3) \\ (x_2 \cdot x_3)(x_1)(x_2 \vee x_3) \end{bmatrix}; \quad (3.39)$$

$$C_{43,23,113}(x) = \begin{bmatrix} (x_2 \cdot \bar{x}_3)(x_1)(x_2 \vee \bar{x}_3) \\ (x_2 \cdot x_3)(x_1)(x_2 \vee x_3) \\ (x_2 \cdot x_3)(\bar{x}_1)(x_2 \vee x_3) \end{bmatrix}. \quad (3.40)$$

На основі побудованих дискретно-казуальних моделей СЕТ-операції базової групи (3.20), (3.38) – (3.40) згідно другого варіанту послідовності ключових елементів (3.13) можна формалізувати наступний алгоритм їх синтезу:

Алгоритм 6:

6.1. $C_{1^*}(x) = C_{23,43,77}(x);$

6.2. $f_{1^*}(x): x_1 \to \bar{x}_1;\ f_{23}(x) \to f_{113}(x);$

$f_{2^*}(x):\ x_2 \to \bar{x}_2;\ \bar{x}_3 \to x_3;\ \ f_{43}(x) \to f_{77}(x);$

$f_{3^*}(x):\ \bar{x}_2 \to x_2;\ x_3 \to \bar{x}_3;\ f_{77}(x) \to f_{43}(x);$

$C_{23,43,77}(x) \to C_{113,77,43}(x);\ C_{2^*}(x) = C_{113,77,43}(x);$

6.3. $f_{2^*}(x):\ x_1 \to \bar{x}_1;\ \bar{x}_3 \to x_3;\ \ f_{43}(x) \to f_{113}(x)$

$f_{1^*}(x): x_2 \to \bar{x}_2;\ f_{23}(x) \to f_{77}(x)\ ;$

$f_{3^*}(x):\ \bar{x}_2 \to x_2;\ \ f_{77}(x) \to f_{23}(x)$

$C_{23,43,77}(x) \to C_{77,113,23}(x);\ C_{3^*}(x) = C_{77,113,23}(x);$

6.4. $f_{3^*}(x): x_1 \to \bar{x}_1;\ \bar{x}_2 \to x_2;\ \ f_{77}(x) \to f_{23}(x);\ f_{1^*}(x): x_3 \to \bar{x}_3;\ f_{23}(x) \to f_{43}(x)\ ;$

$f_{2^*}(x):\ \bar{x}_3 \to x_3;\ \ f_{43}(x) \to f_{23}(x)$

$C_{23,43,77}(x) \to C_{43,23,113}(x);\ C_{3^*}(x) = C_{43,23,113}(x);$

Побудуємо СЕТ-операції базової групи на основі третього варіанту послідовності ключових елементів (3.14):

$C_{23,43,77}(x)$ описана моделлю (3.24);

$$C_{113,77,43}(x)=\begin{bmatrix}(\bar{x}_1\cdot x_3)(\,x_2)(\bar{x}_1\vee x_3)\\(x_1\vee x_3)(\,x_2)(x_1\cdot x_3)\\(x_1\cdot\bar{x}_3)(\,x_2)(x_1\vee\bar{x}_3)\end{bmatrix}=\begin{bmatrix}(\bar{x}_1\cdot x_3)(\,x_2)(\bar{x}_1\vee x_3)\\(x_1\cdot x_3)(\,\bar{x}_2)(x_1\vee x_3)\\(x_1\cdot\bar{x}_3)(\,x_2)(x_1\vee\bar{x}_3)\end{bmatrix};\qquad(3.41)$$

$$C_{77,113,23}(x)=\begin{bmatrix}(x_1\cdot x_3\,)(\,\bar{x}_2)(x_1\vee x_3)\\(\bar{x}_1\cdot x_3)(\,x_2)(\bar{x}_1\vee x_3)\\(x_1\cdot x_3)(x_2)(x_1\vee x_3)\end{bmatrix};\qquad(3.42)$$

$$C_{43,23,113}(x)=\begin{bmatrix}(x_1\cdot\bar{x}_3)(\,x_2)(x_1\vee\bar{x}_3)\\(x_1\cdot x_3)(x_2)(x_1\vee x_3)\\(\bar{x}_1\cdot x_3)(\,x_2)(\bar{x}_1\vee x_3)\end{bmatrix}.\qquad(3.43)$$

На основі побудованих дискретно-казуальних моделей СЕТ-операції базової групи (3.24), (3.41) – (3.43) згідно третього варіанту послідовності ключових елементів (3.14) можна формалізувати наступний алгоритм їх синтезу:

Алгоритм 7:

7.1. $C_{1^*}(x)=C_{23,43,77}(x)$;

7.2. $f_{1^*}(x)\colon x_1\to\bar{x}_1;\ f_{23}(x)\to f_{113}(x)$;
$f_{2^*}(x)\colon x_2\to\bar{x}_2;\ \bar{x}_3\to x_3;\ f_{43}(x)\to f_{77}(x)$;
$f_{3^*}(x)\colon \bar{x}_2\to x_2;\ x_3\to\bar{x}_3;\ f_{77}(x)\to f_{43}(x)$;
$C_{23,43,77}(x)\to C_{113,77,43}(x);\ C_{2^*}(x)=C_{113,77,43}(x)$;

7.3. $f_{2^*}(x)\colon x_1\to\bar{x}_1;\ \bar{x}_3\to x_3;\ f_{43}(x)\to f_{113}(x)$
$f_{1^*}(x)\colon x_2\to\bar{x}_2;\ f_{23}(x)\to f_{77}(x)$;
$f_{3^*}(x)\colon \bar{x}_2\to x_2;\ f_{77}(x)\to f_{23}(x)$
$C_{23,43,77}(x)\to C_{77,113,23}(x);\ C_{3^*}(x)=C_{77,113,23}(x)$;

7.4. $f_{3^*}(x)\colon x_1\to\bar{x}_1;\ \bar{x}_2\to x_2;\ f_{77}(x)\to f_{23}(x);\ f_{1^*}(x)\colon x_3\to\bar{x}_3;\ f_{23}(x)\to f_{43}(x)$;
$f_{2^*}(x)\colon \bar{x}_3\to x_3;\ f_{43}(x)\to f_{23}(x)$
$C_{23,43,77}(x)\to C_{43,23,113}(x);\ C_{3^*}(x)=C_{43,23,113}(x)$;

Побудуємо СЕТ-операції базової групи на основі четвертого варіанту послідовності ключових елементів (3.15):

$C_{23,43,77}(x)$ описана моделлю (3.28);

$$C_{113,77,43}(x)=\begin{bmatrix}(\bar{x}_1\cdot x_2\ )(\ x_3)(\bar{x}_1\vee x_2)\\(x_1\cdot \bar{x}_2\ )(\ x_3)(x_1\vee \bar{x}_2)\\(x_1\cdot x_2\ )(\ \bar{x}_3)(x_1\vee x_2)\end{bmatrix}; \tag{3.44}$$

$$C_{77,113,23}(x)=\begin{bmatrix}(x_1\cdot \bar{x}_2\ )(\ x_3)(x_1\vee \bar{x}_2)\\(\bar{x}_1\cdot x_2\ )(\ x_3)(\bar{x}_1\vee x_2)\\(x_1\cdot x_2\ )(\ x_3)(x_1\vee x_2)\end{bmatrix}; \tag{3.45}$$

$$C_{43,23,113}(x)=\begin{bmatrix}(x_1\cdot x_2\ )(\ \bar{x}_3)(x_1\vee x_2)\\(x_1\cdot x_2\ )(\ x_3)(x_1\vee x_2)\\(\bar{x}_1\cdot x_2\ )(\ x_3)(\bar{x}_1\vee x_2)\end{bmatrix}. \tag{3.46}$$

На основі побудованих дискретно-казуальних моделей СЕТ-операції базової групи (3.28), (3.41) – (3.43) згідно четвертого варіанту послідовності ключових елементів (3.15) можна формалізувати наступний алгоритм їх синтезу:

Алгоритм 8:

8.1. $C_{1^*}(x)=C_{23,43,77}(x)$;

8.2. $f_{1^*}(x): x_1\to\bar{x}_1;\ f_{23}(x)\to f_{113}(x)$;
$f_{2^*}(x):\ x_2\to\bar{x}_2;\ \bar{x}_3\to x_3;\ \ f_{43}(x)\to f_{77}(x)$;
$f_{3^*}(x):\ \bar{x}_2\to x_2;\ x_3\to\bar{x}_3;\ f_{77}(x)\to f_{43}(x)$;
$C_{23,43,77}(x)\to C_{113,77,43}(x);\ C_{2^*}(x)=C_{113,77,43}(x)$;

8.3. $f_{2^*}(x):\ x_1\to\bar{x}_1;\ \bar{x}_3\to x_3;\ \ f_{43}(x)\to f_{113}(x)$
$f_{1^*}(x): x_2\to\bar{x}_2;\ f_{23}(x)\to f_{77}(x)$;
$f_{3^*}(x):\ \bar{x}_2\to x_2;\ \ f_{77}(x)\to f_{23}(x)$
$C_{23,43,77}(x)\to C_{77,113,23}(x);\ C_{3^*}(x)=C_{77,113,23}(x)$;

8.4. $f_{3^*}(x): x_1\to\bar{x}_1;\ \bar{x}_2\to x_2;\ \ f_{77}(x)\to f_{23}(x);\ f_{1^*}(x): x_3\to\bar{x}_3;\ f_{23}(x)\to f_{43}(x)$;
$f_{2^*}(x):\ \bar{x}_3\to x_3;\ \ f_{43}(x)\to f_{23}(x)$
$C_{23,43,77}(x)\to C_{43,23,113}(x);\ C_{3^*}(x)=C_{43,23,113}(x)$;

Аналіз алгоритмів з 5 по 8 показав, що всі вони мають однакову складність реалізації і відрізняються лише вибраними моделями елементарних функцій. Проте їх представлення ускладнюється переходами від прямих Сі-квантів інформації до обернених і навпаки. Спростити даний алгоритм можна на основі використання законів дискретної математики ($\bar{\bar{x}}_i = x_i$). Слід відмітити, що в дискретно-казуальних моделях елементарних функцій операцій, керованих інформацією, управляюча перемінна використовується всього один раз, а тому при зменшенні складності алгоритму немає необхідності виділяти управляючі перемінні дужками.

Алгоритм 9:

9.1. $C_{1*}(x) = C_{23,43,77}(x)$;

9.2. $f_{1*}(x): x_1 \to \bar{x}_1$;

$f_{2*}(x)$; $f_{3*}(x)$: $x_2 \to \bar{x}_2$; $x_3 \to \bar{x}_3$;

$C_{23,43,77}(x) \to C_{113,77,43}(x)$; $C_{2*}(x) = C_{113,77,43}(x)$;

9.3. $f_{2*}(x)$: $x_1 \to \bar{x}_1$; $x_3 \to \bar{x}_3$;

$f_{1*}(x)$; $f_{3*}(x): x_2 \to \bar{x}_2$;

$C_{23,43,77}(x) \to C_{77,113,23}(x)$; $C_{3*}(x) = C_{77,113,23}(x)$;

9.4. $f_{3*}(x): x_1 \to \bar{x}_1$; $x_2 \to \bar{x}_2$;

$f_{1*}(x)$; $f_{2*}(x): x_3 \to \bar{x}_3$;

$C_{23,43,77}(x) \to C_{43,23,113}(x)$; $C_{3*}(x) = C_{43,23,113}(x)$.

Запропонований алгоритм придатний для моделювання базової групи СЕТ-операцій на основі елементарних функцій операцій, керованих інформацією, яка включає в себе симетричні операції та забезпечує максимальне значення критерію відмінності відповідних елементарних функцій (2.25).

3.5. Синтез групи СЕТ-операцій на основі елементарних функцій операцій, керованих інформацією.

Синтез будь якої групи СЕТ-операцій реалізується на основі операцій базової групи ($C_b(x)$), операцій перестановки елементарних функцій ($C_p(f(x))$), і операцій інверсії елементарних функцій ($C_\gamma(f(x)) = f(x) \oplus \gamma_m$) [48, 52]. Процес синтезу на основі даного підходу дозволяє будувати групи на основі поєднання операцій базової групи з операціями перестановки елементарних функцій, або на основі поєднання операцій базової групи з операціями інверсії елементарних функцій, або на основі поєднання операцій базової групи з операціями перестановки елементарних функцій і операціями інверсії елементарних функцій. На основі даного підходу було побудовано метод синтезу груп елементарних функцій [48, 52].

На практиці реалізувати даний метод можна за допомогою таких варіантів моделей синтезу прямих і обернених СЕТ-операцій:

Варіант 1.

Якщо

$$C_{b.i,p.j,m.h}(x) = C_{p.j}(C_{b.i}(x)) \oplus \gamma_{m.h} = y \qquad (3.47),$$

тоді

$$C'_{b.i,p.j,m.h}(y) = C'_{b.i}(C'_{p.j}(y \oplus \gamma_{m.h})) = x. \qquad (3.48)$$

Модель (3.47) формалізує правила побудови моделі СЕТ-операції на основі трьохетапного криптографічного перетворення:

1. На першому етапі реалізується криптографічне перетворення інформації СЕТ-операцією базової групи $C_{b.i}(x)$. Дана операція базової групи буде основою модифікованої СЕТ-операції;

2. На другому етапі криптографічного перетворення інформації результат реалізації базової СЕТ-операції модифікується шляхом додаткової перестановки Сі-квантів інформації. При побудові модифікованої моделі,

елементарні функції СЕТ-операції $C_{b.\mathrm{i}}(x)$ будуть переставлені місцями за допомогою СЕТ-операції $C_{p.j}(f(x))$. В результаті додаткового перетворення отримаємо: $C_{p.j}(C_{b.i}(x))$;

3. На третьому етапі криптографічного перетворення над результатом реалізації другого етапу проводиться додаткове гамування шляхом додавання по модулю два псевдовипадкової послідовності. При побудові моделі, даний етап відображається додатковою модифікацією елементарних функцій СЕТ-операції шляхом їх псевдовипадкових інверсій на основі додавання по модулю два з маскою, яка задається гамуючою послідовністю.

Послідовність нижніх індексів в модифікованій СЕТ-операції $C_{b.i,p.j,m.h}(x)$ відображає порядок її побудови: над i - ю операцією базової групи виконується j - а операція перестановки елементарних функцій, і виконується інвертування переставлених елементарних функції h -м вектором гамуючої послідовності.

Модель (3.48) формалізує правила побудови моделі оберненої СЕТ-операції до моделі (3.47) на основі трьохетапного криптографічного перетворення:

1. На першому етапі оберненого криптографічного перетворення з шифрограми видаляється гамуюча послідовність, яка була додатково введена на третьому етапі прямого криптографічного перетворення. При побудові моделі, даний етап відображається модифікацією результату шифрування (вхідних Сі-квантів для моделі оберненого перетворення) y шляхом їх псевдовипадкових інверсій на основі додавання по модулю два з маскою, яка задається гамуючою послідовністю і використовувалася при шифруванні.

2. На другому етапі оберненого криптографічного перетворення, застосувавши обернену перестановку Сі-квантів інформації, після першого етапу розшифрування отримаємо результат шифрування базовою СЕТ-операцією. При побудові модифікованої моделі оберненої СЕТ-операції,

застосувавши обернену перестановку елементарних функцій $C^{/}_{p.j}\left(f(x)\right)$, отримаємо пряму СЕТ-операцію;

3. На третьому етапі реалізується обернене криптографічне перетворення оберненою СЕТ-операцією базової групи $C^{/}_{b.\mathrm{i}}(x)$.

Необхідно відмітити, що в моделях (3.47) і (3.48) послідовності коефіцієнтів для прямого і оберненого перетворення однакові. Це введено для однозначності сприйняття процесів синтезу. В процесі синтезу прямих модифікованих операцій порядок перетворень відповідає порядку позначених коефіцієнтів зліва направо (традиційний порядок), а для синтезу операцій оберненого перетворення порядок операцій буде зворотній (з права на ліво).

Продемонструємо побудову прямої і модифікованої моделі на прикладі. Для спрощення сприйняття процесу побудови використаємо СЕТ-операцію базової групи $C_{23,43,77}(x)$ (3.16), побудованої на основі першого варіанту послідовності ключовий елементів (3.12).

Групу операцій перестановки елементарних функцій 3Сі-квантових СЕТ-операцій задаємо таблицею 3.5.

Таблиця 3.5.

Групу операцій перестановки елементарних функцій 3Сі-квантових СЕТ-операцій

СЕТ-операції інверсії		**СЕТ-операції**	
Пряма СЕТ-операція	**Обернена СЕТ-операція**	**Пряма СЕТ-операція**	**Обернена СЕТ-операція**
$C_{p.1}\left(f(x)\right)=\begin{bmatrix} f_{1^*}(x) \\ f_{2^*}(x) \\ f_{3^*}(x) \end{bmatrix}$	$C^{/}_{p.1}\left(f(x)\right)=\begin{bmatrix} f_{1^*}(x) \\ f_{2^*}(x) \\ f_{3^*}(x) \end{bmatrix}$	$C_{p.2}\left(f(x)\right)=\begin{bmatrix} f_{2^*}(x) \\ f_{1^*}(x) \\ f_{3^*}(x) \end{bmatrix}$	$C^{/}_{p.2}\left(f(x)\right)=\begin{bmatrix} f_{2^*}(x) \\ f_{1^*}(x) \\ f_{3^*}(x) \end{bmatrix}$
$C_{p.3}\left(f(x)\right)=\begin{bmatrix} f_{3^*}(x) \\ f_{2^*}(x) \\ f_{1^*}(x) \end{bmatrix}$	$C^{/}_{p.3}\left(f(x)\right)=\begin{bmatrix} f_{3^*}(x) \\ f_{2^*}(x) \\ f_{1^*}(x) \end{bmatrix}$	$C_{p.4}\left(f(x)\right)=\begin{bmatrix} f_{1^*}(x) \\ f_{3^*}(x) \\ f_{2^*}(x) \end{bmatrix}$	$C^{/}_{p.4}\left(f(x)\right)=\begin{bmatrix} f_{1^*}(x) \\ f_{3^*}(x) \\ f_{2^*}(x) \end{bmatrix}$
$C_{p.5}\left(f(x)\right)=\begin{bmatrix} f_{2^*}(x) \\ f_{3^*}(x) \\ f_{1^*}(x) \end{bmatrix}$	$C^{/}_{p.5}\left(f(x)\right)=\begin{bmatrix} f_{3^*}(x) \\ f_{1^*}(x) \\ f_{2^*}(x) \end{bmatrix}$	$C_{p.6}\left(f(x)\right)=\begin{bmatrix} f_{3^*}(x) \\ f_{1^*}(x) \\ f_{2^*}(x) \end{bmatrix}$	$C^{/}_{p.6}\left(f(x)\right)=\begin{bmatrix} f_{2^*}(x) \\ f_{3^*}(x) \\ f_{1^*}(x) \end{bmatrix}$

Групу операцій інверсії елементарних функцій 3Сі-квантових СЕТ-операцій задаємо таблицею векторів 3.6.

Таблиця 3.6.

Групу операцій інверсії елементарних функцій ЗСі-квантових СЕТ-операцій

Вектори інверсії			
$\gamma_{m.1}=\begin{bmatrix}0\\0\\0\end{bmatrix}$	$\gamma_{m.2}=\begin{bmatrix}0\\0\\1\end{bmatrix}$	$\gamma_{m.3}=\begin{bmatrix}0\\1\\0\end{bmatrix}$	$\gamma_{m.4}=\begin{bmatrix}0\\1\\1\end{bmatrix}$
$\gamma_{m.5}=\begin{bmatrix}1\\0\\0\end{bmatrix}$	$\gamma_{m.6}=\begin{bmatrix}1\\0\\1\end{bmatrix}$	$\gamma_{m.7}=\begin{bmatrix}1\\1\\0\end{bmatrix}$	$\gamma_{m.8}=\begin{bmatrix}1\\1\\1\end{bmatrix}$

Виконавши над СЕТ-операцією базової групи $C_{23,43,77}(x)$ (3.16) операцію перестановки елементарних функцій, наприклад $C_{p.5}(f(x))$, отримаємо:

$$C_{p.5}(C_{b.1}(x))=\begin{bmatrix}(x_1\cdot\bar{x}_3)(x_2)(x_1\vee\bar{x}_3)\\(x_1\cdot\bar{x}_2)(x_3)(x_1\vee\bar{x}_2)\\(x_2\cdot x_3)(x_1)(x_2\vee x_3)\end{bmatrix}. \qquad (3.49)$$

За результатами додаткового гамування елементарних функцій моделі (3.49), наприклад маскою $\gamma_{m.7}$, побудуємо модифіковану СЕТ-операцію по аналогії з [10]:

$$C_{p.5}(C_{b.1}(x))\oplus\gamma_{m.7}=\begin{bmatrix}(x_1\cdot\bar{x}_3)(x_2)(x_1\vee\bar{x}_3)\\(x_1\cdot\bar{x}_2)(x_3)(x_1\vee\bar{x}_2\\(x_2\cdot x_3)(x_1)(x_2\vee x_3)\end{bmatrix}\oplus\begin{bmatrix}1\\1\\0\end{bmatrix}=$$

$$=\begin{bmatrix}(x_1\cdot\bar{x}_3)(x_2)(x_1\vee\bar{x}_3)\oplus 1\\(x_1\cdot\bar{x}_2)(x_3)(x_1\vee\bar{x}_2)\oplus 1\\(x_2\cdot x_3)(x_1)(x_2\vee x_3)\oplus 0\end{bmatrix}=\begin{bmatrix}\overline{(x_1\cdot\bar{x}_3)}(x_2)(\overline{x_1\vee\bar{x}_3})\\\overline{(x_1\cdot\bar{x}_2)}(x_3)(\overline{x_1\vee\bar{x}_2})\\(x_2\cdot x_3)(x_1)(x_2\vee x_3)\end{bmatrix}=$$

$$=\begin{bmatrix}(\bar{x}_1\vee x_3)(x_2)(\bar{x}_1\cdot x_3)\\(\bar{x}_1\vee x_2)(x_3)(\bar{x}_1\cdot x_2)\\(x_2\cdot x_3)(x_1)(x_2\vee x_3)\end{bmatrix}=\begin{bmatrix}(\bar{x}_1\cdot x_3)(\bar{x}_2)(\bar{x}_1\vee x_3)\\(\bar{x}_1\cdot x_2)(\bar{x}_3)(\bar{x}_1\vee\bar{x}_2)\\(x_2\cdot x_3)(x_1)(x_2\vee x_3)\end{bmatrix};$$

$$C_{b.1,p.5,m.7}(x)=\begin{bmatrix}(\bar{x}_1\cdot x_3)(\bar{x}_2)(\bar{x}_1\vee x_3)\\(\bar{x}_1\cdot x_2)(\bar{x}_3)(\bar{x}_1\vee x_2)\\(x_2\cdot x_3)(x_1)(x_2\vee x_3)\end{bmatrix}=y. \qquad (3.49)$$

Знайдемо обернену СЕТ-операцію шляхом перевірки послідовності дій по алгоритму оберненого криптографічного перетворення.

$$y \oplus \gamma_{m.7} = \begin{bmatrix} (\bar{x}_1 \cdot x_3)(\bar{x}_2)(\bar{x}_1 \vee x_3) \\ (\bar{x}_1 \cdot x_2)(\bar{x}_3)(\bar{x}_1 \vee x_2) \\ (x_2 \cdot x_3)(x_1)(x_2 \vee x_3) \end{bmatrix} \oplus \begin{bmatrix} 1 \\ 1 \\ 0 \end{bmatrix} = \begin{bmatrix} (\bar{x}_1 \cdot x_3)(\bar{x}_2)(\bar{x}_1 \vee x_3) \oplus 1 \\ (\bar{x}_1 \cdot x_2)(\bar{x}_3)(\bar{x}_1 \vee x_2) \oplus 1 \\ (x_2 \cdot x_3)(x_1)(x_2 \vee x_3) \oplus 0 \end{bmatrix} =$$

$$= \begin{bmatrix} (\overline{\bar{x}_1 \cdot x_3})(\bar{x}_2)(\overline{\bar{x}_1 \vee x_3}) \\ (\overline{\bar{x}_1 \cdot x_2})(\bar{x}_3)(\overline{\bar{x}_1 \vee x_2}) \\ (x_2 \cdot x_3)(x_1)(x_2 \vee x_3) \end{bmatrix} = \begin{bmatrix} (x_1 \vee \bar{x}_3)(\bar{x}_2)(x_1 \cdot \bar{x}_3) \\ (x_1 \vee \bar{x}_2)(\bar{x}_3)(x_1 \cdot \bar{x}_2) \\ (x_2 \cdot x_3)(x_1)(x_2 \vee x_3) \end{bmatrix} = \begin{bmatrix} (x_1 \cdot \bar{x}_3)(x_2)(x_1 \vee \bar{x}_3) \\ (x_1 \cdot \bar{x}_2)(x_3)(x_1 \vee \bar{x}_2) \\ (x_2 \cdot x_3)(x_1)(x_2 \vee x_3) \end{bmatrix} \quad (3.50)$$

Над отриманою моделлю (3.50) виконаємо обернену перестановку елементарних функцій $C'_{p.5}(f(x))$

$$C'_{p.5}(y \oplus \gamma_{m.7}) = \begin{bmatrix} (x_1 \cdot \bar{x}_3)(x_2)(x_1 \vee \bar{x}_3) \\ (x_1 \cdot \bar{x}_2)(x_3)(x_1 \vee \bar{x}_2) \\ (x_2 \cdot x_3)(x_1)(x_2 \vee x_3) \end{bmatrix} = \begin{bmatrix} (x_2 \cdot x_3)(x_1)(x_2 \vee x_3) \\ (x_1 \cdot \bar{x}_3)(x_2)(x_1 \vee \bar{x}_3) \\ (x_1 \cdot \bar{x}_2)(x_3)(x_1 \vee \bar{x}_2) \end{bmatrix} = C_{b.1}(x) \quad (3.51)$$

Отримана модель операції оберненого криптографічного перетворення співпала з моделлю прямого криптографічного перетворення. Так як за умови синтезу операцій базової групи, до якої входить СЕТ-операція $C_{b.1}(x)$, всі операцій були симетричними, то алгоритм оберненого криптографічного перетворення коректний. Коректність даного алгоритму перевірена на синтезі повної групи СЕТ-операцій на основі елементарних функцій операцій, керованих інформацією. На основі перетворень (3.50) і (3.51), модель оберненого криптографічного перетворення можна представити так:

$$y \oplus \gamma_{m.7} = \begin{bmatrix} y_1 \oplus 1 \\ y_2 \oplus 1 \\ y_3 \oplus 0 \end{bmatrix}$$

$$C'_{p.5}(y \oplus \gamma_{m.7}) = \begin{bmatrix} y_3 \oplus 0 \\ y_1 \oplus 1 \\ y_2 \oplus 1 \end{bmatrix} = \begin{bmatrix} y_3 \\ \bar{y}_1 \\ \bar{y}_2 \end{bmatrix} \quad (3.52)$$

Підставивши значення (3.52) в модель (3.16), отримаємо:

$$C^{/}_{b.1}\left(C^{/}_{p.5}\left(y \oplus \gamma_{m.7}\right)\right) = \begin{bmatrix} (\bar{y}_1 \cdot \bar{y}_2\ )(y_3)(\bar{y}_1 \vee \bar{y}_2) \\ (y_2 \cdot y_3\ )(\ \bar{y}_1)(y_2 \vee y_3\ ) \\ (y_1 \cdot y_3\ )(\ \bar{y}_2)(y_1 \vee y_3) \end{bmatrix} = C^{/}_{b.1,p.5,m.7}(y) = x. \quad (3.53);$$

Моделі прямого криптографічного перетворення (3.49) і оберненого криптографічного перетворення (3.53) не співпали. Тому можна констатувати, що за результатами модифікації симетричної СЕТ-операції $C_{b.1}(x)$ за допомогою перестановки $C_{p.5}(f(x))$ і інверсії $\gamma_{m.7}$ буде побудована несиметрична СЕТ-операція $C_{b.1,p.5,m.7}(x)$.

Варіант 2.

Якщо

$$C_{b.i,m.h,p.j}(x) = C_{p.j}\left(C_{b.i}(x) \oplus \gamma_{m.h}\right) = y \quad (3.54),$$

тоді

$$C^{/}_{b.i,m.h,p.j}(y) = C^{/}_{b.i}\left(C^{/}_{p.j}(y) \oplus \gamma_{m.h}\right) = x\,. \quad (3.55)$$

Відповідно до (3.53), реалізація СЕТ-операції виконується в наступній послідовності:

1. На першому етапі реалізується криптографічне перетворення інформації СЕТ-операцією базової групи $C_{b.i}(x)$;

2. На другому етапі проводиться додаткове гамування результату виконання базової операції $C_{b.i}(x)$: $C_{b.i}(x) \oplus \gamma_{m.h}$;

3. На третьому етапі проводиться перестановка елементарних функцій операцією $C_{p.j}(f(x))$: $C_{p.j}\left(C_{b.i}(x) \oplus \gamma_{m.h}\right)$.

Для коректності висновків щодо побудови модифікованої СЕТ операції по другому варіанту синтезу, використаємо, як і в першому варіанті синтезу, операції перетворення інформації $C_{b.1}(x)$, $C_{p.5}(f(x))$, і $\gamma_{m.7}$.

Відповідно до моделі (3.54) і алгоритму її реалізації, отримаємо модифіковану СЕТ-операцію прямого криптографічного перетворення:

$$C_{b.i}(x)\oplus\gamma_{m.h}=\begin{bmatrix}(x_2\cdot x_3)(x_1)(x_2\vee x_3)\\(x_1\cdot\bar{x}_3)(x_2)(x_1\vee\bar{x}_3)\\(x_1\cdot\bar{x}_2)(x_3)(x_1\vee\bar{x}_2)\end{bmatrix}\oplus\begin{bmatrix}1\\1\\0\end{bmatrix}=\begin{bmatrix}(x_2\cdot x_3)(x_1)(x_2\vee x_3)\oplus1\\(x_1\cdot\bar{x}_3)(x_2)(x_1\vee\bar{x}_3)\oplus1\\(x_1\cdot\bar{x}_2)(x_3)(x_1\vee\bar{x}_2)\oplus0\end{bmatrix}=$$

$$=\begin{bmatrix}\overline{(x_2\cdot x_3)}(x_1)(\overline{x_2\vee x_3})\\\overline{(x_1\cdot\bar{x}_3)}(x_2)(\overline{x_1\vee\bar{x}_3})\\(x_1\cdot\bar{x}_2)(x_3)(x_1\vee\bar{x}_2)\end{bmatrix}=\begin{bmatrix}(\bar{x}_2\vee\bar{x}_3)(x_1)(\bar{x}_2\cdot\bar{x}_3)\\(\bar{x}_1\vee x_3)(x_2)(\bar{x}_1\cdot x_3)\\(x_1\cdot\bar{x}_2)(x_3)(x_1\vee\bar{x}_2)\end{bmatrix}=\begin{bmatrix}(\bar{x}_2\cdot\bar{x}_3)(\bar{x}_1)(\bar{x}_2\vee\bar{x}_3)\\(\bar{x}_1\cdot x_3)(\bar{x}_2)(\bar{x}_1\vee x_3)\\(x_1\cdot\bar{x}_2)(x_3)(x_1\vee\bar{x}_2)\end{bmatrix}$$

$$C_{p.5}(C_{b.1}(x)\oplus\gamma_{m.7})=\begin{bmatrix}(\bar{x}_1\cdot x_3)(\bar{x}_2)(\bar{x}_1\vee x_3)\\(x_1\cdot\bar{x}_2)(x_3)(x_1\vee\bar{x}_2)\\(\bar{x}_2\cdot\bar{x}_3)(\bar{x}_1)(\bar{x}_2\vee\bar{x}_3)\end{bmatrix}=C_{b.1,m.7,p.5}(x)\qquad(3.56)$$

Відповідно до (3.55), реалізація оберненої СЕТ-операції виконується в такій послідовності:

1. На першому етапі проводиться перестановка елементарних функцій операцією оберненої перестановки $C^{/}_{p.j}(y)$;

2. На другому етапі проводиться додаткове гамування результату виконання базової операції оберненої перестановки: $C^{/}_{p.j}(y)\oplus\gamma_{m.h}$;

3. На третьому реалізується криптографічне перетворення інформації СЕТ-операцією базової групи $C^{/}_{b.i}(y)$. $C^{/}_{b.i}\left(C^{/}_{p.j}(y)\oplus\gamma_{m.h}\right)$.

Відповідно до моделі (3.55) і алгоритму її реалізації, отримаємо модифіковану СЕТ-операцію оберненого криптографічного перетворення:

$$C^{/}_{p.5}(y)\oplus\gamma_{m.7}=\begin{bmatrix}y_3\\y_1\\y_2\end{bmatrix}\oplus\begin{bmatrix}1\\1\\0\end{bmatrix}=\begin{bmatrix}y_3\oplus1\\y_1\oplus1\\y_2\end{bmatrix}=\begin{bmatrix}\bar{y}_3\\\bar{y}_1\\y_2\end{bmatrix}\qquad(3.57)$$

Підставивши значення (3.57) в модель (3.16), отримаємо:

$$C^{/}_{b.1}\left(C^{/}_{p.5}(y)\oplus\gamma_{m.7}\right)=\begin{bmatrix}(\bar{y}_1\cdot y_2\ )(\bar{y}_3)(\bar{y}_1\vee y_2)\\(\bar{y}_3\cdot\bar{y}_2\ )(\ \bar{y}_1)(\bar{y}_3\vee\bar{y}_2\ )\\(\bar{y}_3\cdot y_1\ )(\ y_2)(\bar{y}_3\vee y_1)\end{bmatrix}=C^{/}_{b.1,m.7,p.5}(y)=x. \quad (3.58)$$

Так як моделі (3.56) і (3.58) не співпали, то за результатом модифікації буде отримано несиметричну СЕТ-операцію.

Необхідно відмітити, що СЕТ-операції (3.51) і (3.56) не співпали. На основі даного результату можна сформулювати припущення, що різні варіанти модифікації СЕТ-операцій при однакових умовах дозволяють отримати різні СЕТ-операції.

Перевіримо дане припущення на наступному варіанті моделі синтезу модифікованих СЕТ-операцій.

Варіант 3.

Якщо

$$C_{m.h,b.i,p.j}(x)=C_{p.j}\left(C_{b.i}(x\oplus\gamma_{m.h})\right)=y \quad (3.59),$$

тоді

$$C^{/}_{m.h,b.i,p.j}(y)=C^{/}_{b.i}\left(C^{/}_{p.j}(y)\right)\oplus\gamma_{m.h}=x. \quad (3.60)$$

Відповідно до (3.59), реалізація СЕТ-операції виконується в наступній послідовності:

1. На першому етапі реалізується гамування Сі-квантів вхідних даних: $x\oplus\gamma_{m.h}$;

2. На другому етапі реалізується криптографічне перетворення модифікованої вхідної інформації СЕТ-операцією базової групи $C_{b.\mathrm{i}}(x)$: $C_{b.i}\left(x\oplus\gamma_{m.h}\right)$;

3. На третьому етапі проводиться перестановка елементарних функцій операцією $C_{p.j}(f(x))$: $C_{p.j}\left(C_{b.i}\left(x \oplus \gamma_{m.h}\right)\right)$.

Отримаємо модифіковану СЕТ-операцію прямого криптографічного перетворення відповідно до моделі (3.59):

$$x \oplus \gamma_{m.7} = \begin{bmatrix} x_1 \\ x_2 \\ x_3 \end{bmatrix} \oplus \begin{bmatrix} 1 \\ 1 \\ 0 \end{bmatrix} = \begin{bmatrix} x_1 \oplus 1 \\ x_2 \oplus 1 \\ x_3 \end{bmatrix} = \begin{bmatrix} \bar{x}_1 \\ \bar{x}_2 \\ x_3 \end{bmatrix}. \qquad (3.61)$$

Підставивши значення (3.61) в модель (3.16), отримаємо:

$$C_{b.1}\left(x \oplus \gamma_{m.7}\right) = \begin{bmatrix} (\bar{x}_2 \cdot x_3)(\bar{x}_1)(\bar{x}_2 \vee x_3) \\ (\bar{x}_1 \cdot \bar{x}_3)(\bar{x}_2)(\bar{x}_1 \vee \bar{x}_3) \\ (\bar{x}_1 \cdot x_2)(x_3)(\bar{x}_1 \vee x_2) \end{bmatrix}. \qquad (3.62)$$

Виконавши перестановку елементарних функцій в моделі (3.62), отримаємо:

$$C_{p.5}\left(C_{b.1}\left(x \oplus \gamma_{m.7}\right)\right) = \begin{bmatrix} (\bar{x}_1 \cdot \bar{x}_3)(\bar{x}_2)(\bar{x}_1 \vee \bar{x}_3) \\ (\bar{x}_1 \cdot x_2)(x_3)(\bar{x}_1 \vee x_2) \\ (\bar{x}_2 \cdot x_3)(\bar{x}_1)(\bar{x}_2 \vee x_3) \end{bmatrix} = C_{m.7,b.1,p.5}(x) = y. \qquad (3.63)$$

Отримана модель модифікованої СЕТ-операції (3.63) відрізняється від моделей СЕТ-операцій (3.49) і (3.56), а це свідчить про справедливість припущення про побудову різних послідовностей СЕТ-операцій в процесі генерації груп операцій при використанні різних варіантів синтезу.

Проаналізуємо можливу кількість варіантів побудови групи СЕТ-операцій на основі перестановок і інверсій операцій базової групи. Для цього використаємо перестановки індексів в позначеннях моделей модифікації СЕТ-операцій. Було досліджено коректність і унікальність моделей модифікації СЕТ-операцій та отримано такі варіанти:

$C_{b.i,p.j,m.h}(x)$ – перший варіант модифікації

$C_{b.i,m.h,p.j}(x)$ – другий варіант модифікації

$C_{m.h,b.i,p.j}(x)$ – третій варіант модифікації

Враховуючи наявність в кожній моделі послідовності трьох перетворень, можна допустити, що кількість варіантів модифікації може досягати шести. Дане припущення базується на значенні перестановок з трьох елементів: $3! = 1 \cdot 2 \cdot 3 = 6$. Розглянемо інші можливі варіанти перестановки індексів:

$C_{p.j,b.i,m.h}(x)$. Так як при однакових перестановках результатів виконання елементарних функцій і перестановці вхідних Сі-квантів елементарний функцій результати криптографічного перетворення не співпадають ($C_{p.j,b.i}(x) \neq C_{b.i,p.j}(x)$), то $C_{p.j,b.i,m.h}(x) \neq C_{b.i,p.j,m.h}(x)$.

Перевіримо даний результат на прикладі:

$$C_{p.5,b.1}(x) = C_{b.1}\left(C_{p.5}(x)\right) = \begin{bmatrix} (x_1 \cdot x_3)(x_2)(x_1 \vee x_3) \\ (\bar{x}_1 \cdot x_2)(x_3)(\bar{x}_1 \vee x_2) \\ (x_2 \cdot \bar{x}_3)(x_1)(x_2 \vee \bar{x}_3) \end{bmatrix}$$

$$C_{b.1}\left(C_{p.5}(x)\right) \oplus \gamma_{m.7} = \begin{bmatrix} (x_1 \cdot x_3)(x_2)(x_1 \vee x_3) \\ (\bar{x}_1 \cdot x_2)(x_3)(\bar{x}_1 \vee x_2) \\ (x_2 \cdot \bar{x}_3)(x_1)(x_2 \vee \bar{x}_3) \end{bmatrix} \oplus \begin{bmatrix} 1 \\ 1 \\ 0 \end{bmatrix} = \begin{bmatrix} (\overline{x_1 \cdot x_3})(x_2)(\overline{x_1 \vee x_3}) \\ (\overline{\bar{x}_1 \cdot x_2})(x_3)(\overline{\bar{x}_1 \vee x_2}) \\ (x_2 \cdot \bar{x}_3)(x_1)(x_2 \vee \bar{x}_3) \end{bmatrix} =$$

$$= \begin{bmatrix} (\bar{x}_1 \vee \bar{x}_3)(x_2)(\bar{x}_1 \cdot \bar{x}_3) \\ (x_1 \vee \bar{x}_2)(x_3)(x_1 \cdot \bar{x}_2) \\ (x_2 \cdot \bar{x}_3)(x_1)(x_2 \vee \bar{x}_3) \end{bmatrix} = \begin{bmatrix} (\bar{x}_1 \cdot \bar{x}_3)(\bar{x}_2)(\bar{x}_1 \vee \bar{x}_3) \\ (x_1 \cdot \bar{x}_2)(\bar{x}_3)(x_1 \vee \bar{x}_2) \\ (x_2 \cdot \bar{x}_3)(x_1)(x_2 \vee \bar{x}_3) \end{bmatrix}$$

$$C_{p.5,b.1,m.7}(x) = \begin{bmatrix} (\bar{x}_1 \cdot \bar{x}_3)(\bar{x}_2)(\bar{x}_1 \vee \bar{x}_3) \\ (x_1 \cdot \bar{x}_2)(\bar{x}_3)(x_1 \vee \bar{x}_2) \\ (x_2 \cdot \bar{x}_3)(x_1)(x_2 \vee \bar{x}_3) \end{bmatrix}. \qquad (3.64)$$

Так як моделі СЕТ-операцій (3,49), (3,56), (3,63) і (3,64) не співпали, то існує четвертий варіант модифікації СЕТ-операцій

Варіант 4.

Якщо

$$C_{p.j,b.i,m.h}(x) = C_{b.i}\left(C_{p.j}(x)\right) \oplus \gamma_{m.h} = y \qquad (3.65),$$

тоді

$$C'_{p.j,b.i,m.h}(y) = C'_{p.j}\left(C'_{b.i}\left(y \oplus \gamma_{m.h}\right)\right) = x\,. \qquad (3.66)$$

Розглянемо наступну перестановку індексів в позначеннях моделей модифікації СЕТ-операцій.

$C_{p.j,m.h,b.i}(x)$. Виходячи з того, що $C_{p.j,m.h}(x) \neq C_{m.h,p.j}(x)$, а $C_{m.h,b.i}(x) \neq C_{b.i,m.h}(x)$, будуть справедливі нерівності: $C_{p.j,m.h,b.i}(x) \neq C_{b.i,m.h,p.j}(x) \neq C_{b.i,p.j,m.h}(x) \neq C_{m.h,b.i,p.j}(x) \neq C_{p.j,b.i,m.h}(x)$.

Виходячи з цього, дану модель можна розглядати як четвертий варіант побудови модифікованих СЕТ-операцій.

Варіант 5.

Якщо

$$C_{p.j,m.h,b.i}(x) = C_{b.i}\left(C_{p.j}(x) \oplus \gamma_{m.h}\right) = y \qquad (3.67),$$

тоді

$$C'_{p.j,m.h,b.i}(y) = C'_{p.j}\left(C'_{b.i}(y) \oplus \gamma_{m.h}\right) = x\,. \qquad (3.68)$$

Отримаємо модифіковану СЕТ-операцію прямого криптографічного перетворення відповідно до моделі (3.67):

$$C_{p.5}(x)\oplus\gamma_{m.7}=\begin{bmatrix}x_2\\x_3\\x_1\end{bmatrix}\oplus\begin{bmatrix}1\\1\\0\end{bmatrix}=\begin{bmatrix}x_2\oplus 1\\x_3\oplus 1\\x_1\end{bmatrix}=\begin{bmatrix}\bar{x}_2\\\bar{x}_3\\x_1\end{bmatrix} \quad (3.69)$$

Підставивши в $C_{b.1}(x)$ модель (3.69), отримаємо:

$$C_{b.1}\left(C_{p.5}(x)\oplus\gamma_{m.7}\right)=\begin{bmatrix}(x_1\cdot\bar{x}_3)(\bar{x}_2)(x_1\vee\bar{x}_3)\\(\bar{x}_1\cdot\bar{x}_2)(\bar{x}_3)(\bar{x}_1\vee\bar{x}_2)\\(\bar{x}_2\cdot x_3)(x_1)(\bar{x}_2\vee x_3)\end{bmatrix}=C_{p.7,m.7,b.1}(x)=y \quad (3.70)$$

Так як моделі СЕТ-операцій (3,49), (3,56), (3,63), (3,64) і (3.70) не співпали, то п’ятий варіант модифікації СЕТ-операцій буде коректним.

Розглянемо останню перестановку індексів в позначеннях моделей модифікації СЕТ-операцій $C_{m.h,p.j,b.i}(x)$.

Варіант 6.

Якщо

$$C_{m.h,p.j,b.i}(x)=C_{b.i}\left(C_{p.j}\left(x\oplus\gamma_{m.h}\right)\right)=y \quad (3.71),$$

тоді

$$C'_{m.h,p.j,b.i}(y)=C'_{p.j}\left(C'_{b.i}(y)\right)\oplus\gamma_{m.h}=x. \quad (3.72)$$

Отримаємо модифіковану СЕТ-операцію прямого криптографічного перетворення відповідно до моделі (3.71):

$$x\oplus\gamma_{m.7}=\begin{bmatrix}x_1\\x_2\\x_3\end{bmatrix}\oplus\begin{bmatrix}1\\1\\0\end{bmatrix}=\begin{bmatrix}\bar{x}_1\\\bar{x}_2\\x_3\end{bmatrix};\qquad C_{p.5}\left(x\oplus\gamma_{m.7}\right)=\begin{bmatrix}\bar{x}_2\\x_3\\\bar{x}_1\end{bmatrix};$$

$$C_{b.i}\left(C_{p.j}\left(x\oplus\gamma_{m.h}\right)\right)=\begin{bmatrix}(\bar{x}_1\cdot x_3)(\bar{x}_2)(\bar{x}_1\vee x_3)\\(x_1\cdot\bar{x}_2)(x_3)(x_1\vee\bar{x}_2)\\(x_2\cdot\bar{x}_3)(\bar{x}_1)(x_2\vee\bar{x}_3)\end{bmatrix}=C_{m.h,p.j,b.i}(x)=y \quad (3.72)$$

Так як моделі СЕТ-операцій (3.72), (3,49), (3,56), (3,63) і (3,64) не співпали, то існує шостий варіант модифікації СЕТ-операцій.

Всі розглянуті шість варіантів модифікації СЕТ-операцій на основі використання чотирьох базових операцій забезпечують побудову повної групи СЕТ-операцій на основі елементарних функцій керованих інформацією. В процесі дослідження було встановлено, що при однакових послідовностях вибору операцій базової групи, операцій перестановки і операцій інверсії буде побудовано шість послідовностей модифікованих операцій, які відрізняються послідовністю їх синтезу. Даний результат дозволяє збільшувати період генераторів псевдовипадкових послідовностей СЕТ-операцій за рахунок додаткової псевдовипадкової вибірки варіантів модифікації операцій.

Висновки до розділу 3

За результатами досліджень, описаних в розділі, удосконалено метод синтезу ЗСі-квантових одноопераднних СЕТ-операцій на основі базової групи СЕТ-операцій шляхом розширення набору моделей модифікації СЕТ-операцій і встановлення нових взаємозв’язків між операціями прямого і оберненого криптографічного перетворення, що забезпечило багатоваріантність побудову групи СЕТ-операцій. Як наслідок, це підвищує складність процесів криптографічного аналізу.

1. В процесі дослідження встановлено, що кожну СЕТ-операцію, побудовану на основі елементарних функцій операцій, керованих інформацією, можна представити за допомогою 27 моделей операції при використанні 27 варіантів послідовності ключових елементів.

2. Аналіз результатів обчислювального експерименту з моделювання СЕТ-операцій на основі елементарних функцій операцій, керованих інформацією, дозволив запропонувати підхід до побудови базової групи СЕТ-операцій, яка містить лише симетричні операції. Побудова відповідної базової

групи суттєво зменшує обсяг дослідження, так як нівелює задачу пошуку обернених СЕТ-операцій, адже прямі і обернені операції співпадають.

3.Запропоновано використовувати критерій простоти побудови і критерій відмінності відповідних елементарних функцій в СЕТ-операціях для оцінки різних варіантів побудови базової групи і результатів їх реалізації.

4. Запропоновано моделі синтезу базової групи СЕТ-операцій на основі елементарних функцій операцій, керованих інформацією, за критерієм простоти їх побудови.

5. Запропоновано моделі синтезу базової групи СЕТ-операцій на основі елементарних функцій операцій, керованих інформацією, за критерієм відмінності відповідних елементарних функцій

6. Запропоновано моделі синтезу групи СЕТ-операцій на основі варіантів поєднання операцій базової групи з операціями перестановки елементарних функцій і операціями інверсії елементарних функцій. Отримані моделі і стали основою для удосконалення метод синтезу ЗСі-квантових одноопераднних СЕТ-операцій.

7. Результати розділу опубліковані в [3, 31, 41, 47, 48, 52, 58, 61, 79].

РОЗДІЛ 4. СИНТЕЗ ДВОХОПЕРАНДНИХ СЕТ-ОПЕРАЦІЙ І КРИПТОГРАФІЧНИХ СИСТЕМ НА ОСНОВІ ЕЛЕМЕНТАРНИХ ФУНКЦІЙ ОПЕРАЦІЙ, КЕРОВАНИХ ІНФОРМАЦІЄЮ

4.1. Дискретно-казуальне моделювання двохоперандних СЕТ-операцій, керованих інформацією

Одним і перспективних напрямів використання СЕТ-операцій в криптографії є побудова на їх основі криптографічних систем потокового шифрування [3]. Особливості архітектури СЕТ-операцій дозволяють адаптувати їх властивості до якісного виконання задач захисту інформації і визначених умов використання. В монографії [3] показано, що двохоперандні операції криптографічного перетворення дозволяють будувати криптографічні системи з більшими (розширеними) можливостями.

Криптографічна система, побудована на основі одноопераднних СЕТ-операцій, в процесі шифрування повинна псевдовипадково генерувати послідовність одноопераднних СЕТ-операцій, або вибирати їх із наперед заданої множини. Одноопераднa СЕТ-операція реалізує дискретну модель однієї таблиці підстановки. Тому застосування одноопераднних СЕТ-операцій можна розглядати як варіант реалізації простих підстановочних шифрів; однозвучних підстановочних шифрів, поліграмних підстановочних шифрів, поліалфавітних підстановочних шифрів. [3, 125]. Проте наведені варіанти побудови підстановочних шифрів по своїй ефективності поступаються шифрам, побудованим на основі додавання по модулю два інформації і псевдовипадкової послідовності.

Потокові криптографічні системи на основі двохоперандних СЕТ-операцій можна розглядати як вдосконалені аналоги потокових

криптографічних систем, побудованих на основі додавання по модулю два. На відміну від потокових криптографічних систем на основі додавання по модулю два, дані криптографічні системи забезпечують зчеплення і розсіювання Сі-квантів вхідної інформації, розсіювання Сі-квантів псевдовипадкової послідовності, в також реалізують шифрування з плаваючим блоком криптографічного перетворення [3]. Застосування взаємообернених СЕТ-операцій [68] і СЕТ-операцій, які допускають перестановку операндів [80], дозволяють будувати криптографічні системи на нових принципах прямого і оберненого криптографічного перетворення інформації.

Відповідно до огляду наведених наукових результатів, необхідно і доцільно перейти від побудови одноопераднних СЕТ-операцій до двохоперандних СЕТ-операцій.

Будувати двохоперандні СЕТ-операції на основі елементарних функцій операцій, керованих інформацією, представлених дискретно-алгебраїчними моделями складне через необхідність реалізації громіздких перетворень [48]. Тому доцільно будувати двохоперандні СЕТ-операції на основі елементарних функцій операцій, керованих інформацією, які представлені дискретно-казуальними моделями [42].

На сьогоднішній день проводилось лише дискретно-казуальне моделювання двохоперандних СЕТ-операцій перестановок керованих інформацією, [58]. Сутність процесу дискретно-казуального моделювання двохоперандних СЕТ операцій полягає в таких етапах:

1. Визначити кількість одноопераднних СЕТ-операцій, які буде реалізовувати двохоперандна СЕТ-операція;

2. Визначити набір одноопераднних СЕТ-операцій, які буде реалізовувати двохоперандна СЕТ-операція;

3. Побудувати дискретно-казуальні моделі одноопераднних СЕТ-операцій, які буде реалізовувати двохоперандна СЕТ-операція;

4. Визначити підхід до синтезу двохоперапндної СЕТ-операції [9]. Під підходом до синтезу будемо розуміти набір параметрів моделі двохоперандної СЕТ-операції, які необхідно мінімізувати в процесі об’єднання одннооперандних моделей операцій;

5. Для спрощення моделі двохоперандної СЕТ-операції, на основі вибраних параметрів моделі, визначити орієнтовну послідовність одноопераидних СЕТ-операцій в кортежі двохоперандної СЕТ-операції. Це необхідно, оскільки послідовність одноопераидних СЕТ-операцій в кортежі двохоперандної СЕТ-операції впливає на складність дискретно-казуальної моделі [58];

6. Побудувати таблицю істинності визначених параметрів дискретно-казуальної моделі на основі об’єднання однойменних елементарних функцій кортежу одноопераидних СЕТ-операцій;

7. На основі таблиці істинності побудувати мінімальні діз’юнктивно-кон’юнктивні моделі визначених параметрів;

8. За потреби, зокрема для спрощення схемотехнічної реалізації, представити мінімальні діз’юнктивно-кон’юнктивні моделі параметрів дискретно-казуальними моделями;

9. Побудувати узагальнену модель двохоперандної СЕТ-операції;

10. Повторивши пункти 4-9 і 5-9, побудувати декілька інших варіантів моделі двохоперандної СЕТ-операції;

11. Визначити серед побудованих варіантів моделі дискретно-казуальну модель двохоперандної СЕТ-операції, яка має найменшу складність реалізації. Дана дискретно-казуальна модель і буде вважатися результатом синтезу двохоперандної СЕТ-операції.

Синтез дискретно-казуальних моделей двохоперандних СЕТ-операцій на основі елементарних функцій операцій, керованих інформацією,

відрізняється від синтезу дискретно-казуальних моделей двохоперандних СЕТ-операцій перестановок керованих інформацією. Це пов’язано з багатоваріантністю дискретно-казуальної моделі СЕТ-операції. Як було зазначено, будь яку одноопераднду СЕТ-операцію на основі елементарних функцій операцій, керованих інформацією, можна представити за допомогою 27 моделей (табл. 3.1) [31]. Описаний процес синтезу можна використати для синтезу двохоперандних СЕТ-операцій на основі елементарних функцій операцій, керованих інформацією, лише за умови використання першого варіанту послідовності ключовий елементів (3.12) і лише одного варіанту набору одноперандних СЕТ-операцій в кортежі двохоперандної операції. Це обмеження суттєво спрощує процес синтезу двохоперандної СЕТ-операції на основі елементарних функцій операцій, керованих інформацією, проте не може забезпечити простоти побудовано моделі [42].

При побудові двохоперандної СЕТ-операції, використання одноопераднди СЕТ-операцій базової групи забезпечить максимальну варіативність алгоритму криптографічного перетворення. Це пов’язано з тим, що модифікація двохоперандних операцій базується на модифікації одноопераднди операцій, а множини модифікованих одноопераднди операцій, що побудовані на основі різних СЕТ-операцій базової групи, не перетинаються.

Виходячи з цього, для побудови двохоперандної СЕТ-операції необхідно вибрати всі чотири одноопераднді СЕТ-операцій на основі елементарних функцій операцій, керованих інформацією, які складають базову групу операцій [42].

В процесі дослідження синтезу двохоперандних СЕТ-операцій обмежимося чотирма варіантами послідовності ключовий елементів, представлених залежностями (3.12) – (3.15), які використовувались при побудові базових груп одноопераднди СЕТ-операцій.

При дослідженні процесу синтезу двохоперандної СЕТ-операції на основі елементарних функцій операцій, керованих інформацією, необхідно побудувати і порівняти варіанти дискретно-казуальних моделей операцій, отриманих шляхом поєднання одноопераднних операцій базових груп, синтезованих за критерієм простоти їх побудови і за критерієм відмінності відповідних елементарних функцій [42].

4.2. Дискретно-казуальне моделювання двохоперандних СЕТ-операцій на основі елементарних функцій операцій, керованих інформацією, за критерієм простоти побудови базової групи одноопераднних СЕТ-операцій.

За результатами дослідження одноопераднних СЕТ-операцій на основі елементарних функцій операцій, керованих інформацією, за критерієм простоти їх побудови (підрозділ 3.3) були синтезовані чотири варіанти представлення моделей синтезованої базової групи СЕТ-операцій [42, 52].

1. Перша базова група включає в себе двохоперандні СЕТ-операції (3.16) – (3.19);
2. Друга базова група включає в себе двохоперандні СЕТ-операції (3.20) – (3.23);
3. Третя базова група включає в себе двохоперандні СЕТ-операції (3.24) – (3.27);
4. Друга базова група включає в себе двохоперандні СЕТ-операції (3.28) – (3.31).

Побудуємо двохоперандну СЕТ-операцію на основі елементарних функцій операцій, керованих інформацією, включно з операцією, яка реалізує

кортеж із чотирьох одноопераднних СЕТ-операцій першої базової групи $C_{23,43,77}(x)$, $C_{113,43,77}(x)$, $C_{23,142,77}(x)$ і $C_{23,43,142}(x)$.

$$C(x,y)=C(C_{23,43,77}(x),C_{113,43,77}(x),C_{23,142,77}(x),C_{23,43,142}(x)). \qquad (4.1)$$

Модель (4.1) можна представити так:

$$C(x,\,y)=\begin{cases} C_{23,43,77}(x),\ якщо\ y_1=0;\ y_2=0 \\ C_{113,43,77}(x),\ якщо\ y_1=0;\ y_2=1 \\ C_{23,142,77}(x),\ якщо\ y_1=1;\ y_2=0 \\ C_{23,43,142}(x),\ якщо\ y_1=1;\ y_2=1 \end{cases}. \qquad (4.2)$$

Підставивши в модель (4.2) моделі одноопераднних СЕТ-операцій, (3.16) – (3.19) отримаємо:

$$C(x,\,y)\ =\ \begin{cases} \begin{bmatrix} (x_2\cdot x_3)(x_1)(x_2\vee x_3) \\ (x_1\cdot \bar{x}_3)(x_2)(x_1\vee \bar{x}_3) \\ (x_1\cdot \bar{x}_2)(x_3)(x_1\vee \bar{x}_2) \end{bmatrix},\ якщо\ y_1=0;\ y_2=0 \\ \begin{bmatrix} (x_2\cdot x_3)(\bar{x}_1)(x_2\vee x_3) \\ (x_1\cdot \bar{x}_3)(x_2)(x_1\vee \bar{x}_3) \\ (x_1\cdot \bar{x}_2)(x_3)(x_1\vee \bar{x}_2) \end{bmatrix},\ якщо\ y_1=0;\ y_2=1 \\ \begin{bmatrix} (x_2\cdot x_3)(x_1)(x_2\vee x_3) \\ (x_1\cdot \bar{x}_3)(\bar{x}_2)(x_1\vee \bar{x}_3) \\ (x_1\cdot \bar{x}_2)(x_3)(x_1\vee \bar{x}_2) \end{bmatrix},\ якщо\ y_1=1;\ y_2=0 \\ \begin{bmatrix} (x_2\cdot x_3)(x_1)(x_2\vee x_3) \\ (x_1\cdot \bar{x}_3)(x_2)(x_1\vee \bar{x}_3) \\ (x_1\cdot \bar{x}_2)(\bar{x}_3)(x_1\vee \bar{x}_2) \end{bmatrix},\ якщо\ y_1=1;\ y_2=1 \end{cases}. \qquad (4.3)$$

Практичне використання моделі СЕТ-операції (4.3) обмежується складністю її реалізації. Для зменшення складності кортежної дискретно-казуальної моделі необхідно її модифікувати по аналогії з [58]. Модифікація СЕТ-операції виконується на основі об’єднання однойменних елементарних функцій. Це забезпечує спрощення кортежної моделі. Опис дискретно-казуальної моделі двохоперандної СЕТ-операції (4.3) на основі елементарних

функцій операцій, керованих інформацією, відрізняється від опису моделей двохоперандних СЕТ-операцій перестановок керованих інформацією.

Об’єднаємо перші елементарні функції для дискретно-казуальної моделі (4.3) щоб побудувати першу елементарну функцію двохоперандної СЕТ-операції:

$$f_1(x) = \begin{cases} (x_2 \cdot x_3)(x_1)(x_2 \vee x_3), \ якщо \ y_1 = 0; \ y_2 = 0 \\ (x_2 \cdot x_3)(\bar{x}_1)(x_2 \vee x_3), \ якщо \ y_1 = 0; \ y_2 = 1 \\ (x_2 \cdot x_3)(x_1)(x_2 \vee x_3), \ якщо \ y_1 = 1; \ y_2 = 0 \\ (x_2 \cdot x_3)(x_1)(x_2 \vee x_3), \ якщо \ y_1 = 1; \ y_2 = 1 \end{cases}. \quad (4.4)$$

В загальному вигляді першу елементарну функцію двохоперандної СЕТ-операції можна представити так:

$$f_1(x) = ((a_{1.1} \oplus x_2) \cdot (a_{1.2} \oplus x_3))(a_{1.3} \oplus x_1)((a_{1.4} \oplus x_2) \vee (a_{1.5} \oplus x_3)) \quad (4.5)$$

Так як $a_{1.1} = a_{1.4}$ і $a_{1.2} = a_{1.5}$, то модель (4.5) можна представити:

$$f_1(x) = ((a_{1.1} \oplus x_2) \cdot (a_{1.2} \oplus x_3))(a_{1.3} \oplus x_1)((a_{1.2} \oplus x_2) \vee (a_{1.3} \oplus x_3)) \quad (4.6)$$

де $a_{1.1} = f(y_1, y_2)$ – коефіцієнт управління інверсією змінної x_2 в першій елементарній функції двохоперандної СЕТ-операції; $a_{1.2} = f(y_1, y_2)$ – коефіцієнт управління інверсією змінної x_3 в першій елементарній функції двохоперандної СЕТ-операції; $a_{1.3} = f(y_1, y_2)$ – коефіцієнт управління інверсією змінної x_1 в першій елементарній функції двохоперандної СЕТ-операції.

Опис об’єднаної елементарної функції (4.4) відрізняється від опису об’єднаних елементарних функцій перестановок керованих інформацією, [58], тому побудова таблиці істинності для мінімізації моделі (4.4) має свої особливості і реалізується відповідно до моделі (4.6). Дана таблиця істинності наведена в табл. 4.1.

Таблиця 4.1

Таблиця істинності побудови елементарної функції $f_1(x)$ моделі СЕТ-операції (4.3)

$C(x,y)$	Значення y		Наявність інверсії в моделі $f_1(x)$		
	y_1	y_2	$a_{1.1}$	$a_{1.2}$	$a_{1.3}$
$C_1(x)$	**0**	**0**	**0**	**0**	**0**
$C_2(x)$	**0**	**1**	**0**	**0**	**1**
$C_3(x)$	**1**	**0**	**0**	**0**	**0**
$C_4(x)$	**1**	**1**	**0**	**0**	**0**

За результатами мінімізації отримаємо коефіцієнти управління інверсією змінних $a_{1.1}=0$, $a_{1.2}=0$ і $a_{1.3}=\bar{y}_1\cdot y_2$. Підставивши отримані коефіцієнти в модель (4.6), отримаємо:

$$f_1(x) = (x_2\cdot x_3)((\bar{y}_1\cdot y_2)\oplus x_1)(x_2\vee x_3) \qquad (4.7)$$

Об’єднаємо другі елементарні функції для дискретно-казуальної моделі (4.3) для побудови другої елементарної функції двохоперандної СЕТ-операції:

$$f_2(x) = \begin{cases} (x_1\cdot\bar{x}_3)(x_2)(x_1\vee\bar{x}_3), \text{ якщо } y_1=0;\ y_2=0 \\ (x_1\cdot\bar{x}_3)(x_2)(x_1\vee\bar{x}_3), \text{ якщо } y_1=0;\ y_2=1 \\ (x_1\cdot\bar{x}_3)(\bar{x}_2)(x_1\vee\bar{x}_3), \text{ якщо } y_1=1;\ y_2=0 \\ (x_1\cdot\bar{x}_3)(x_2)(x_1\vee\bar{x}_3), \text{ якщо } y_1=1;\ y_2=1 \end{cases}. \qquad (4.8)$$

В загальному вигляді другу елементарну функцію двохоперандної СЕТ-операції можна представити так:

$$f_2(x) = ((a_{1.1}\oplus x_1)\cdot(a_{1.2}\oplus x_3))(a_{1.3}\oplus x_2)((a_{1.4}\oplus x_1)\vee(a_{1.5}\oplus x_3)) \qquad (4.9)$$

Так як $a_{1.1}=a_{1.4}$ і $a_{1.2}=a_{1.5}$, то модель (4.9) можна представити:

$$f_2(x) = ((a_{1.1}\oplus x_1)\cdot(a_{1.2}\oplus x_3))(a_{1.3}\oplus x_2)((a_{1.2}\oplus x_1)\vee(a_{1.3}\oplus x_3)) \qquad (4.10)$$

де $a_{1.1}=f(y_1,y_2)$ – коефіцієнт управління інверсією змінної x_1 в другій елементарній функції двохоперандної СЕТ-операції; $a_{1.2}=f(y_1,y_2)$ – коефіцієнт

управління інверсією змінної x_3 в другій елементарній функції двохоперандної СЕТ-операції; $a_{1.3} = f(y_1, y_2)$ – коефіцієнт управління інверсією змінної x_2 в другій елементарній функції двохоперандної СЕТ-операції.

Таблиця істинності побудови елементарної функції $f_2(x)$ моделі СЕТ-операції (4.3) наведена в табл. 4.2.

Таблиця 4.2

Таблиця істинності побудови елементарної функції $f_2(x)$ моделі СЕТ-операції (4.3)

$C(x, y)$	Значення y		Наявність інверсії в моделі $f_2(x)$		
	y_1	y_2	$a_{1.1}$	$a_{1.2}$	$a_{1.3}$
$C_1(x)$	**0**	**0**	**0**	**1**	**0**
$C_2(x)$	**0**	**1**	**0**	**1**	**0**
$C_3(x)$	**1**	**0**	**0**	**1**	**1**
$C_4(x)$	**1**	**1**	**0**	**1**	**0**

За результатами мінімізації отримаємо коефіцієнти управління інверсією змінних $a_{1.1} = 0$, $a_{1.2} = 1$ і $a_{1.3} = y_1 \cdot \bar{y}_2$. Підставивши отримані коефіцієнти в модель (4.10) отримаємо:

$$f_2(x) = (x_1 \cdot \bar{x}_3)((y_1 \cdot \bar{y}_2) \oplus x_2)(x_1 \vee \bar{x}_3) \qquad (4.11)$$

Об’єднаємо треті елементарні функції для дискретно-казуальної моделі (4.3), для побудови третьої елементарної функції двохоперандної СЕТ-операції:

$$f_3(x) = \begin{cases} (x_1 \cdot \bar{x}_2)(x_3)(x_1 \vee \bar{x}_2), \ якщо \ y_1 = 0; \ y_2 = 0 \\ (x_1 \cdot \bar{x}_2)(x_3)(x_1 \vee \bar{x}_2), \ якщо \ y_1 = 0; \ y_2 = 1 \\ (x_1 \cdot \bar{x}_2)(x_3)(x_1 \vee \bar{x}_2), \ якщо \ y_1 = 1; \ y_2 = 0 \\ (x_1 \cdot \bar{x}_2)(\bar{x}_3)(x_1 \vee \bar{x}_2), \ якщо \ y_1 = 1; \ y_2 = 1 \end{cases}. \qquad (4.12)$$

В загальному вигляді третю елементарну функцію двохоперандної СЕТ-операції можна представити так:

$$f_3(x) = ((a_{1.1} \oplus x_1) \cdot (a_{1.2} \oplus x_2))(a_{1.3} \oplus x_3)((a_{1.4} \oplus x_1) \vee (a_{1.5} \oplus x_2)) \qquad (4.13)$$

Так як $a_{1.1} = a_{1.4}$ і $a_{1.2} = a_{1.5}$, то модель (4.9) можна представити:

$$f_3(x) = ((a_{1.1} \oplus x_1) \cdot (a_{1.2} \oplus x_2))(a_{1.3} \oplus x_3)((a_{1.2} \oplus x_1) \vee (a_{1.3} \oplus x_2)) \quad (4.14)$$

де $a_{1.1} = f(y_1, y_2)$ – коефіцієнт управління інверсією змінної x_1 в третій елементарній функції двохоперандної СЕТ-операції; $a_{1.2} = f(y_1, y_2)$ – коефіцієнт управління інверсією змінної x_2 в третій елементарній функції двохоперандної СЕТ-операції; $a_{1.3} = f(y_1, y_2)$ – коефіцієнт управління інверсією змінної x_3 в третій елементарній функції двохоперандної СЕТ-операції.

Таблиця істинності побудови елементарної функції $f_3(x)$ моделі СЕТ-операції (4.3) наведена в табл. 4.3.

Таблиця 4.3

Таблиця істинності побудови елементарної функції $f_3(x)$ моделі СЕТ-операції (4.3)

$C(x, y)$	Значення y		Наявність інверсії в моделі $f_2(x)$		
	y_1	y_2	$a_{1.1}$	$a_{1.2}$	$a_{1.3}$
$C_1(x)$	**0**	**0**	**0**	**1**	**0**
$C_2(x)$	**0**	**1**	**0**	**1**	**0**
$C_3(x)$	**1**	**0**	**0**	**1**	**0**
$C_4(x)$	**1**	**1**	**0**	**1**	**1**

За результатами мінімізації отримаємо коефіцієнти управління інверсією змінних $a_{1.1} = 0$, $a_{1.2} = 1$ і $a_{1.3} = y_1 \cdot y_2$. Підставивши отримані коефіцієнти в модель (4.10), отримаємо:

$$f_3(x) = (x_1 \cdot \bar{x}_2)((y_1 \cdot y_2) \oplus x_3)(x_1 \vee \bar{x}_2) \quad (4.15)$$

Об’єднавши елементарні функції (4.7), (4.11) і (4.15), отримаємо удосконалену дискретно-казуальну модель двохоперандної СЕТ-операції на основі елементарних функцій операцій, керованих інформацією, (4.3):

$$C(x, y) = \begin{bmatrix} (x_2 \cdot x_3)((\bar{y}_1 \cdot y_2) \oplus x_1)(x_2 \vee x_3) \\ (x_1 \cdot \bar{x}_3)((y_1 \cdot \bar{y}_2) \oplus x_2)(x_1 \vee \bar{x}_3) \\ (x_1 \cdot \bar{x}_2)((y_1 \cdot y_2) \oplus x_3)(x_1 \vee \bar{x}_2) \end{bmatrix} \quad (4.16)$$

Побудуємо дискретно-казуальну модель двохоперандної СЕТ-операції (4.2) на основі другого варіанту послідовності ключовий елементів (3.13). Підставивши в модель (4.2) моделі одноопераднних СЕТ-операцій (3.20) – (3.23) отримаємо:

$$C(x, y) = \begin{cases} \begin{bmatrix} (x_2 \cdot x_3)(x_1)(x_2 \vee x_3) \\ (x_2 \cdot \bar{x}_3)(x_1)(x_2 \vee \bar{x}_3) \\ (\bar{x}_2 \cdot x_3)(x_1)(\bar{x}_2 \vee x_3) \end{bmatrix}, \text{ якщо } y_1 = 0;\ y_2 = 0 \\ \begin{bmatrix} (x_2 \cdot x_3)(\bar{x}_1)(x_2 \vee x_3) \\ (x_2 \cdot \bar{x}_3)(x_1)(x_2 \vee \bar{x}_3) \\ (\bar{x}_2 \cdot x_3)(x_1)(\bar{x}_2 \vee x_3) \end{bmatrix}, \text{ якщо } y_1 = 0;\ y_2 = 1 \\ \begin{bmatrix} (x_2 \cdot x_3)(x_1)(x_2 \vee x_3) \\ (\bar{x}_2 \cdot \bar{x}_3)(x_1)(\bar{x}_2 \vee \bar{x}_3) \\ (\bar{x}_2 \cdot x_3)(x_1)(\bar{x}_2 \vee x_3) \end{bmatrix}, \text{ якщо } y_1 = 1;\ y_2 = 0 \\ \begin{bmatrix} (x_2 \cdot x_3)(x_1)(x_2 \vee x_3) \\ (x_2 \cdot \bar{x}_3)(x_1)(x_2 \vee \bar{x}_3) \\ (\bar{x}_2 \cdot \bar{x}_3)(x_1)(\bar{x}_2 \vee \bar{x}_3) \end{bmatrix}, \text{ якщо } y_1 = 1;\ y_2 = 1 \end{cases}. \quad (4.17)$$

Так як у всіх елементарних функціях всіх одноопераднних операцій моделі (4.17) ключовий елемент буде x_1, то узагальнену модель елементарної функції можна представити так:

$$f_i(x) = ((a_{i.1} \oplus x_2) \cdot (a_{i.2} \oplus x_3))(a_{i.3} \oplus x_1)((a_{i.2} \oplus x_2) \vee (a_{i.3} \oplus x_3)) \quad (4.18)$$

де i - порядковий номер елементарної функції ($i \in \{1, 2, 3\}$); $a_{i.1} = f(y_1, y_2)$ – коефіцієнт управління інверсією змінної x_2 i-ї елементарної функції двохоперандної СЕТ-операції; $a_{i.2} = f(y_1, y_2)$ – коефіцієнт управління інверсією змінної x_3 i-ї елементарної функції двохоперандної СЕТ-операції; $a_{i.3} = f(y_1, y_2)$ – коефіцієнт управління інверсією змінної x_1 i-ї елементарної функції двохоперандної СЕТ-операції.

Побудуємо першу елементарну функцію двохоперандної СЕТ-операції. Об’єднавши перші елементарні функції двохоперандної СЕТ-операції (4.17), отримаємо:

$$f_1(x) = \begin{cases} (x_2 \cdot x_3)(x_1)(x_2 \vee x_3), \text{ якщо } y_1 = 0;\ y_2 = 0 \\ (x_2 \cdot x_3)(\bar{x}_1)(x_2 \vee x_3), \text{ якщо } y_1 = 0;\ y_2 = 1 \\ (x_2 \cdot x_3)(x_1)(x_2 \vee x_3), \text{ якщо } y_1 = 1;\ y_2 = 0 \\ (x_2 \cdot x_3)(x_1)(x_2 \vee x_3), \text{ якщо } y_1 = 1;\ y_2 = 1 \end{cases} \quad (4.19)$$

Таблиця істинності для удосконалення елементарної функції (4.19) наведена в табл. 4.4.

Таблиця 4.4

Таблиця істинності побудови елементарної функції $f_1(x)$ моделі СЕТ-операції (4.17)

$C(x, y)$	Значення y		Наявність інверсії в моделі $f_1(x)$		
	y_1	y_2	$a_{1.1}$	$a_{1.2}$	$a_{1.3}$
$C_1(x)$	**0**	**0**	**0**	**0**	**0**
$C_2(x)$	**0**	**1**	**0**	**0**	**1**
$C_3(x)$	**1**	**0**	**0**	**0**	**0**
$C_4(x)$	**1**	**1**	**0**	**0**	**0**

Мінімізувавши коефіцієнти управління інверсією змінних для першої елементарної функції і підставивши їх в модель (4.18), отримаємо:

$$f_1(x) = (x_2 \cdot x_3)((\bar{y}_1 \cdot y_2) \oplus x_1)(x_2 \vee x_3). \quad (4.20)$$

Необхідно відмітити, що отримана модель елементарної функції двохоперандної СЕТ-операції (4.20) повністю співпала з моделлю елементарної функції двохоперандної СЕТ-операції (4.7).

Об’єднавши другі елементарні функції двохоперандної СЕТ-операції (4.17), побудуємо $f_2(x)$

$$f_2(x) = \begin{cases} (x_2 \cdot \bar{x}_3)(x_1)(x_2 \vee \bar{x}_3), \text{ якщо } y_1 = 0;\ y_2 = 0 \\ (x_2 \cdot x_3)(\bar{x}_1)(x_2 \vee x_3), \text{ якщо } y_1 = 0;\ y_2 = 1 \\ (\bar{x}_2 \cdot \bar{x}_3)(x_1)(\bar{x}_2 \vee \bar{x}_3), \text{ якщо } y_1 = 1;\ y_2 = 0 \\ (x_2 \cdot \bar{x}_3)(x_1)(x_2 \vee \bar{x}_3), \text{ якщо } y_1 = 1;\ y_2 = 1 \end{cases} \quad (4.21)$$

Побудуємо таблицю істинності для удосконалення моделі елементарної функції $f_2(x)$ (табл. 4.5).

Таблиця 4.5

Таблиця істинності побудови елементарної функції $f_2(x)$ моделі СЕТ-операції (4.17)

$C(x, y)$	Значення y		Наявність інверсії в моделі $f_2(x)$		
	y_1	y_2	$a_{1.1}$	$a_{1.2}$	$a_{1.3}$
$C_1(x)$	**0**	**0**	**0**	**1**	**0**
$C_2(x)$	**0**	**1**	**0**	**0**	**1**
$C_3(x)$	**1**	**0**	**1**	**1**	**0**
$C_4(x)$	**1**	**1**	**0**	**1**	**0**

Побудувавши на основі табл. 4.5 коефіцієнти управління інверсією змінних для другої елементарної функції і підставивши їх в модель (4.18) отримаємо:

$$f_2(x) = ((y_1 \cdot \bar{y}_2) \oplus x_2) \cdot (\bar{y}_1 \vee y_2) \oplus x_3)((\bar{y}_1 \cdot y_2) \oplus x_1)((y_1 \cdot \bar{y}_2) \oplus x_2) \vee (\bar{y}_1 \vee y_2) \oplus x_3)). \quad (4.22)$$

Об’єднавши треті елементарні функції двохоперандної СЕТ-операції (4.17) побудуємо $f_3(x)$:

$$f_1(x) = \begin{cases} (\bar{x}_2 \cdot x_3)(x_1)(\bar{x}_2 \vee x_3), \text{ якщо } y_1 = 0;\ y_2 = 0 \\ (\bar{x}_2 \cdot x_3)(x_1)(\bar{x}_2 \vee x_3), \text{ якщо } y_1 = 0;\ y_2 = 1 \\ (\bar{x}_2 \cdot x_3)(\ x_1)(\bar{x}_2 \vee x_3), \text{ якщо } y_1 = 1;\ y_2 = 0 \\ (x_2 \cdot \bar{x}_3)(x_1)(x_2 \vee \bar{x}_3), \text{ якщо } y_1 = 1;\ y_2 = 1 \end{cases} \quad (4.23)$$

Побудуємо таблицю істинності для удосконалення моделі елементарної функції $f_3(x)$ (табл. 4.6).

Таблиця 4.6

Таблиця істинності побудови елементарної функції $f_3(x)$ моделі СЕТ-операції (4.17)

$C(x, y)$	Значення y		Наявність інверсії в моделі $f_3(x)$		
	y_1	y_2	$a_{1.1}$	$a_{1.2}$	$a_{1.3}$
$C_1(x)$	**0**	**0**	**1**	**0**	**0**
$C_2(x)$	**0**	**1**	**1**	**0**	**0**
$C_3(x)$	**1**	**0**	**1**	**0**	**0**
$C_4(x)$	**1**	**1**	**0**	**1**	**0**

Побудувавши на основі табл. 4.6 коефіцієнти управління інверсією змінних для третьої елементарної функції і підставивши їх в модель (4.18), отримаємо:

$$f_3(x) = ((\bar{y}_1 \vee \bar{y}_2) \oplus x_2) \cdot (y_1 \cdot y_2) \oplus x_3)(x_1)((\bar{y}_1 \vee \bar{y}_2) \oplus x_2) \vee (y_1 \cdot y_2) \oplus x_3)) . \quad (4.24)$$

Об’єднавши елементарні функції (4.20), (4.22) і (4.24), отримаємо удосконалену дискретно-казуальну модель двохоперандної СЕТ-операції на основі елементарних функцій операцій, керованих інформацією, (4.3), побудовану при використанні другого варіанту послідовності ключових елементів (3.13):

$$C(x, y) = \begin{bmatrix} (x_2 \cdot x_3)((\bar{y}_1 \cdot y_2) \oplus x_1)(x_2 \vee x_3) \\ ((y_1 \cdot \bar{y}_2) \oplus x_2) \cdot (\bar{y}_1 \vee y_2) \oplus x_3)((\bar{y}_1 \cdot y_2) \oplus x_1)((y_1 \cdot \bar{y}_2) \oplus x_2) \vee (\bar{y}_1 \vee y_2) \oplus x_3)) \\ ((\bar{y}_1 \vee \bar{y}_2) \oplus x_2) \cdot (y_1 \cdot y_2) \oplus x_3)(x_1)((\bar{y}_1 \vee \bar{y}_2) \oplus x_2) \vee (y_1 \cdot y_2) \oplus x_3)) \end{bmatrix} \quad (4.25)$$

Порівняльний аналіз моделей показав, що дискретно казуальна модель двохоперандної СЕТ-операції, побудована при використанні першого варіанту послідовності ключових елементів (4.16), має меншу складність порівняно з аналогічною моделлю, побудованою при використанні другого варіанту послідовності ключових елементів (4.25).

Побудуємо дискретно-казуальну модель двохоперандної СЕТ-операції (4.2) на основі третього варіанту послідовності ключових елементів (3.14). Підставивши в модель (4.2) моделі одноопераднних СЕТ-операцій (3.24) – (3.27), отримаємо:

$$C(x, y) = \begin{cases} \begin{bmatrix} (x_1 \cdot x_3)(x_2)(x_1 \vee x_3) \\ (x_1 \cdot \bar{x}_3)(x_2)(x_1 \vee \bar{x}_3) \\ (x_1 \cdot x_3)(\bar{x}_2)(x_1 \vee x_3) \end{bmatrix}, \text{ якщо } y_1 = 0;\ y_2 = 0 \\ \begin{bmatrix} (\bar{x}_1 \cdot x_3)(x_2)(\bar{x}_1 \vee x_3) \\ (x_1 \cdot \bar{x}_3)(x_2)(x_1 \vee \bar{x}_3) \\ (x_1 \cdot x_3)(\bar{x}_2)(x_2 \vee x_3) \end{bmatrix}, \text{ якщо } y_1 = 0;\ y_2 = 1 \\ \begin{bmatrix} (x_1 \cdot x_3)(x_2)(x_1 \vee x_3) \\ (x_1 \cdot \bar{x}_3)(\bar{x}_2)(x_1 \vee \bar{x}_3) \\ (x_1 \cdot x_3)(\bar{x}_2)(x_1 \vee x_3) \end{bmatrix}, \text{ якщо } y_1 = 1;\ y_2 = 0 \\ \begin{bmatrix} (x_1 \cdot x_3)(x_2)(x_1 \vee x_3) \\ (x_1 \cdot \bar{x}_3)(x_2)(x_1 \vee \bar{x}_3) \\ (x_1 \cdot \bar{x}_3)(\bar{x}_2)(x_1 \vee \bar{x}_3) \end{bmatrix}, \text{ якщо } y_1 = 1;\ y_2 = 1 \end{cases}. \quad (4.26)$$

В моделі двохоперандної СЕТ-операції (4.26) ключовий елемент всіх елементарних функцій буде x_2. Виходячи з цього, узагальнену модель елементарних функцій двохоперандної СЕТ-операції можна представити:

$$f_i(x) = ((a_{i.1} \oplus x_1) \cdot (a_{i.2} \oplus x_3))(a_{i.3} \oplus x_2)((a_{i.2} \oplus x_1) \vee (a_{i.3} \oplus x_3)) \quad (4.27)$$

де $a_{i.1}$, $a_{i.2}$ і $a_{i.3}$– коефіцієнти управління інверсією змінних i-ї елементарної функції двохоперандної СЕТ-операції x_1, x_3 та x_2.

По аналогії з побудовою удосконаленої моделі СЕТ-операції (4.25), на основі моделі (4.17) побудуємо модель СЕТ-операції (4.26).

За результатами побудови таблиць істинності і їх мінімізації були отримані коефіцієнти управління інверсією змінних і моделі елементарних функцій:

Для першої узагальненої елементарної функції: $a_{1.1} = \bar{y}_1 \cdot y_2$; $a_{1.2} = 0$; $a_{1.3} = 0$.

$$f_1(x) = ((\bar{y}_1 \cdot y_2) \oplus x_1) \cdot x_3)(x_2)((\bar{y}_1 \cdot y_2) \oplus x_1) \vee x_3). \quad (4.27)$$

Для другої узагальненої елементарної функції: $a_{2.1} = 0$; $a_{2.2} = 0$; $a_{2.3} = y_1 \cdot \bar{y}_2$.

$$f_2(x) = (x_1 \cdot x_3)((y_1 \cdot \bar{y}_2) \oplus x_2)(x_1 \vee x_3). \quad (4.28)$$

Для третьої узагальненої елементарної функції: $a_{3.1} = 0$; $a_{3.2} = \bar{y}_1 \cdot \bar{y}_2$; $a_{3.3} = 1$.

$$f_3(x) = (x_1 \cdot ((\bar{y}_1 \cdot \bar{y}_2) \oplus x_3))(\bar{x}_2)(x_1 \vee ((\bar{y}_1 \cdot \bar{y}_2) \oplus x_3)). \quad (4.29)$$

Об’єднавши моделі елементарних функцій (4.27)-(4.29), отримаємо:

$$C(x, y) = \begin{bmatrix} ((\bar{y}_1 \cdot y_2) \oplus x_1) \cdot x_3)(x_2)((\bar{y}_1 \cdot y_2) \oplus x_1) \vee x_3) \\ (x_1 \cdot x_3)((y_1 \cdot \bar{y}_2) \oplus x_2)(x_1 \vee x_3) \\ (x_1 \cdot ((\bar{y}_1 \cdot \bar{y}_2) \oplus x_3))(\bar{x}_2)(x_1 \vee ((\bar{y}_1 \cdot \bar{y}_2) \oplus x_3)) \end{bmatrix}. \qquad (4.30)$$

Отримана дискретно-казуальна модель двохоперандної СЕТ-операції (4.30) простіша, ніж (4.25), але складніша, ніж (4.16).

Побудуємо дискретно-казуальну модель двохоперандної СЕТ-операції (4.2) на основі четвертого варіанту послідовності ключових елементів (3.15). Підставивши в модель (4.2) моделі одноопераднних СЕТ-операцій (3.28) – (3.31), отримаємо:

$$C(x, y) = \begin{cases} \begin{bmatrix} (x_1 \cdot x_2)(x_3)(x_1 \vee x_2) \\ (x_1 \cdot x_2)(\bar{x}_3)(x_1 \vee x_2) \\ (x_1 \cdot \bar{x}_2)(x_3)(x_1 \vee \bar{x}_2) \end{bmatrix}, \text{ якщо } y_1 = 0;\ y_2 = 0 \\ \begin{bmatrix} (\bar{x}_1 \cdot x_2)(x_3)(\bar{x}_1 \vee x_2) \\ (x_1 \cdot x_2)(\bar{x}_3)(x_1 \vee x_2) \\ (x_1 \cdot \bar{x}_2)(x_3)(x_1 \vee \bar{x}_2) \end{bmatrix}, \text{ якщо } y_1 = 0;\ y_2 = 1 \\ \begin{bmatrix} (x_1 \cdot x_2)(x_3)(x_1 \vee x_2) \\ (x_1 \cdot \bar{x}_2)(\bar{x}_3)(x_1 \vee \bar{x}_2) \\ (x_1 \cdot \bar{x}_2)(x_3)(x_1 \vee \bar{x}_2) \end{bmatrix}, \text{ якщо } y_1 = 1;\ y_2 = 0 \\ \begin{bmatrix} (x_1 \cdot x_2)(x_3)(x_1 \vee x_2) \\ (x_1 \cdot x_2)(\bar{x}_3)(x_1 \vee x_2) \\ (x_1 \cdot \bar{x}_2)(\bar{x}_3)(x_1 \vee \bar{x}_2) \end{bmatrix}, \text{ якщо } y_1 = 1;\ y_2 = 1 \end{cases}. \qquad (4.31)$$

Ключовий елемент всіх елементарних в моделі двохоперандної СЕТ-операції (4.31) функцій буде x_3. Виходячи з цього, узагальнену модель елементарних функцій двохоперандної СЕТ-операції можна представити так:

$$f_i(x) = ((a_{i.1} \oplus x_1) \cdot (a_{i.2} \oplus x_2))(a_{i.3} \oplus x_3)((a_{i.2} \oplus x_1) \vee (a_{i.3} \oplus x_2)) \qquad (4.32)$$

де $a_{i.1}$, $a_{i.2}$ і $a_{i.3}$– коефіцієнти управління інверсією змінних i-ї елементарної функції двохоперандної СЕТ-операції x_1, x_2 і x_3.

Побудуємо удосконалену модель СЕТ-операції (4.31):

Для першої узагальненої елементарної функції: $a_{1.1} = \bar{y}_1 \cdot y_2$; $a_{1.2} = 0$; $a_{1.3} = 0$.

$$f_1(x) = ((\bar{y}_1 \cdot y_2) \oplus x_1) \cdot x_2)(x_3)((\bar{y}_1 \cdot y_2) \oplus x_1) \vee x_2). \quad (4.33)$$

Для другої узагальненої елементарної функції: $a_{2.1} = 0$; $a_{2.2} = y_1 \cdot \bar{y}_2$; $a_{2.3} = 1$.

$$f_2(x) = (x_1 \cdot ((y_1 \cdot \bar{y}_2) \oplus x_2))(\bar{x}_3)(x_1 \vee ((y_1 \cdot \bar{y}_2) \oplus x_2)). \quad (4.34)$$

Для третьої узагальненої елементарної функції: $a_{3.1} = 0$; $a_{3.2} = 1$; $a_{3.3} = \bar{y}_1 \cdot \bar{y}_2$.

$$f_3(x) = (x_1 \cdot \bar{x}_2)((\bar{y}_1 \cdot \bar{y}_2) \oplus x_3)(x_1 \vee \bar{x}_2). \quad (4.35)$$

Об’єднавши моделі елементарних функцій (4.33)-(4.35), отримаємо:

$$C(x, y) = \begin{bmatrix} ((\bar{y}_1 \cdot y_2) \oplus x_1) \cdot x_2)(x_3)((\bar{y}_1 \cdot y_2) \oplus x_1) \vee x_2) \\ (x_1 \cdot ((y_1 \cdot \bar{y}_2) \oplus x_2))(\bar{x}_3)(x_1 \vee ((y_1 \cdot \bar{y}_2) \oplus x_2)) \\ (x_1 \cdot \bar{x}_2)((\bar{y}_1 \cdot \bar{y}_2) \oplus x_3)(x_1 \vee \bar{x}_2) \end{bmatrix}. \quad (4.36)$$

Порівняльний аналіз отриманих дискретно-казуальних моделей двохоперандних СЕТ-операцій на основі елементарних функцій операцій, керованих інформацією, за критерієм простоти побудови базової групи одноопераднних СЕТ-операцій показав:

1. Серед моделей (4.16), (4.25), (4.30) і (4.36), найменш складною є модель (4.16), побудована на основі першого варіанту послідовності ключових елементів, коли індекс змінної ключового елементу співпадає з індексом елементарної функції.

2. Так як модель (4.16) має найменшу складність, то її практична реалізація найпростіша в технічній реалізації, що є одним із основних факторів малоресурсної криптографії.

4.3. Дискретно-казуальне моделювання двохоперандних СЕТ-операцій на основі елементарних функцій операцій, керованих інформацією, за критерієм відмінності відповідних елементарних функцій

В підрозділі 3.4. була синтезована базова група СЕТ-операцій на основі елементарних функцій операцій, керованих інформацією, за критерієм відмінності відповідних елементарних функцій. Дана група включає в себе чотири симетричні СЕТ-операції: $C_{23,43,77}(x)$, $C_{113,77,43}(x)$, $C_{77,113,23}(x)$, $C_{43,23,113}(x)$. СЕТ-операції даної базової групи можуть бути представлені основними чотирма варіантами дискретно-казуальних моделей: (3.16), (3.35) – (3.37); (3.20), (3.38) – (3.40); (3.24), (3.41) – (3.43); (3.28), (3.44) –(3.46).

Побудуємо і дослідимо двохоперандні СЕТ-операції на основі елементарних функцій операцій, керованих інформацією, шляхом об’єднання одноопераднних СЕТ-операцій, які відповідають критерію відмінності відповідних елементарних функцій.

В загальному вигляді, модель двохоперандної СЕТ-операції на основі елементарних функцій операцій, керованих інформацією, побудовану з симетричних одноопередних операцій, синтезованих за критерієм відмінності відповідних елементарних функцій, можна представити так:

$$C(x,\, y) = \begin{cases} C_{23,43,77}(x), \ \textit{якщо}\ y_1 = 0;\ y_2 = 0 \\ C_{113,77,43}(x), \ \textit{якщо}\ y_1 = 0;\ y_2 = 1 \\ C_{77,113,23}(x), \ \textit{якщо}\ y_1 = 1;\ y_2 = 0 \\ C_{43,23,113}(x), \ \textit{якщо}\ y_1 = 1;\ y_2 = 1 \end{cases}. \qquad (4.37)$$

Підставимо в модель (4.37) дискретно-казуальні моделі одноопераднних СЕТ-операцій, які побудовані на основі першого варіанту послідовності ключових елементів (3.16), (3.35) – (3.37):

$$C(x, y) = \begin{cases} \begin{bmatrix} (x_2 \cdot x_3)(x_1)(x_2 \vee x_3) \\ (x_1 \cdot \bar{x}_3)(x_2)(x_1 \vee \bar{x}_3) \\ (x_1 \cdot \bar{x}_2)(x_3)(x_1 \vee \bar{x}_2) \end{bmatrix}, \text{ якщо } y_1 = 0;\ y_2 = 0 \\ \begin{bmatrix} (x_2 \cdot x_3)(\bar{x}_1)(x_2 \vee x_3) \\ (x_1 \cdot x_3)(\bar{x}_2)(x_1 \vee x_3) \\ (x_1 \cdot x_2)(\bar{x}_3)(x_1 \vee x_2) \end{bmatrix}, \text{ якщо } y_1 = 0;\ y_2 = 1 \\ \begin{bmatrix} (\bar{x}_2 \cdot x_3)(x_1)(\bar{x}_2 \vee x_3) \\ (\bar{x}_1 \cdot x_3)(x_2)(\bar{x}_1 \vee x_3) \\ (x_1 \cdot x_2)(x_3)(x_1 \vee x_2) \end{bmatrix}, \text{ якщо } y_1 = 1;\ y_2 = 0 \\ \begin{bmatrix} (x_2 \cdot \bar{x}_3)(x_1)(x_2 \vee \bar{x}_3) \\ (x_1 \cdot x_3)(\ x_2)(x_1 \vee x_3) \\ (\bar{x}_1 \cdot x_2)(\ x_3)(\bar{x}_1 \vee x_2) \end{bmatrix}, \text{ якщо } y_1 = 1;\ y_2 = 1 \end{cases} . \quad (4.38)$$

Побудуємо удосконалену дискретно-казуальну модель двохоперандної СЕТ-операції (4.37) по аналогії з побудовою моделі (4.16). Для першої узагальненої елементарної функції отримаємо: $a_{1.1} = y_1 \cdot \bar{y}_2$; $a_{1.2} = y_1 \cdot y_2$; $a_{1.3} = \bar{y}_1 \cdot y_2$.

$$f_1(x) = (((y_1 \cdot \bar{y}_2) \oplus x_2) \cdot ((y_1 \cdot y_2) \oplus x_3))((\bar{y}_1 \cdot y_2) \oplus x_1)(((y_1 \cdot \bar{y}_2) \oplus x_2) \vee ((y_1 \cdot y_2) \oplus x_3))$$

Для другої узагальненої елементарної функції отримаємо: $a_{2.1} = y_1 \cdot \bar{y}_2$; $a_{2.2} = \bar{y}_1 \cdot \bar{y}_2$; $a_{2.3} = \bar{y}_1 \cdot y_2$.

$$f_2(x) = (((y_1 \cdot \bar{y}_2) \oplus x_1) \cdot ((\bar{y}_1 \cdot \bar{y}_2) \oplus x_3))((\bar{y}_1 \cdot y_2) \oplus x_2)(((y_1 \cdot \bar{y}_2) \oplus x_1) \vee ((\bar{y}_1 \cdot \bar{y}_2) \oplus x_3)).$$

Для третьої узагальненої елементарної функції отримаємо: $a_{3.1} = y_1 \cdot y_2$; $a_{3.2} = \bar{y}_1 \cdot \bar{y}_2$; $a_{3.3} = y_1 \cdot \bar{y}_2$.

$$f_3(x) = (((y_1 \cdot y_2) \oplus x_1) \cdot ((\bar{y}_1 \cdot \bar{y}_2) \oplus x_2))((y_1 \cdot \bar{y}_2) \oplus x_3)(((y_1 \cdot y_2) \oplus x_1) \vee ((\bar{y}_1 \cdot \bar{y}_2) \oplus x_2)).$$

На основі отриманих елементарних функцій побудуємо удосконалену дискретно-казуальну модель двохоперандної СЕТ-операції:

$$C(x, y) = \begin{bmatrix} (((y_1 \cdot \bar{y}_2) \oplus x_2) \cdot ((y_1 \cdot y_2) \oplus x_3))((\bar{y}_1 \cdot y_2) \oplus x_1)(((y_1 \cdot \bar{y}_2) \oplus x_2) \vee ((y_1 \cdot y_2) \oplus x_3)) \\ (((y_1 \cdot \bar{y}_1) \oplus x_1) \cdot ((\bar{y}_1 \cdot \bar{y}_2) \oplus x_3))((\bar{y}_1 \cdot y_2) \oplus x_2)(((y_1 \cdot \bar{y}_2) \oplus x_1) \vee ((\bar{y}_1 \cdot \bar{y}_2) \oplus x_3)) \\ (((y_1 \cdot y_2) \oplus x_1) \cdot ((\bar{y}_1 \cdot \bar{y}_2) \oplus x_2))((y_1 \cdot \bar{y}_2) \oplus x_3)(((y_1 \cdot y_2) \oplus x_1) \vee ((\bar{y}_1 \cdot \bar{y}_2) \oplus x_2)) \end{bmatrix} \quad (4.39)$$

Модель СЕТ-операції (4.39) забезпечує значення критерію відмінності відповідних елементарних функцій $K_{\to f(x)} = 2{,}25$. Твердження ґрунтується на тому, що одноопераднді операції забезпечують дане значення критерію.

Дискретно-казуальну модель двохоперандної СЕТ-операції (4.37) на основі другого варіанту послідовності ключових елементів можна побудувати через об'єднання одноопераднних операцій (3.20), (3.38) – (3.40).

$$C(x,y) = \begin{cases} \begin{bmatrix} (x_2 \cdot x_3)(x_1)(x_2 \vee x_3) \\ (x_2 \cdot \bar{x}_3)(x_1)(x_2 \vee \bar{x}_3) \\ (\bar{x}_2 \cdot x_3)(x_1)(\bar{x}_2 \vee x_3) \end{bmatrix}, \textit{якщо } y_1 = 0;\ y_2 = 0 \\ \begin{bmatrix} (x_2 \cdot x_3)(\bar{x}_1)(x_2 \vee x_3) \\ (\bar{x}_2 \cdot x_3)(x_1)(\bar{x}_2 \vee x_3) \\ (x_2 \cdot \bar{x}_3)(x_1)(x_2 \vee \bar{x}_3) \end{bmatrix}, \textit{якщо } y_1 = 0;\ y_2 = 1 \\ \begin{bmatrix} (\bar{x}_2 \cdot x_3)(x_1)(\bar{x}_2 \vee x_3) \\ (x_2 \cdot x_3)(\bar{x}_1)(x_2 \vee x_3) \\ (x_2 \cdot x_3)(x_1)(x_2 \vee x_3) \end{bmatrix}, \textit{якщо } y_1 = 1;\ y_2 = 0 \\ \begin{bmatrix} (x_2 \cdot \bar{x}_3)(x_1)(x_2 \vee \bar{x}_3) \\ (x_2 \cdot x_3)(x_1)(x_2 \vee x_3) \\ (x_2 \cdot x_3)(\bar{x}_1)(x_2 \vee x_3) \end{bmatrix}, \textit{якщо } y_1 = 1;\ y_2 = 1 \end{cases} \quad (4.40)$$

Побудуємо удосконалену модель СЕТ-операції (4.40) по аналогії з побудовою моделі (4.25). Для першої узагальненої елементарної функції отримаємо: $a_{1.1} = y_1 \cdot \bar{y}_2$; $a_{1.2} = y_1 \cdot y_2$; $a_{1.3} = \bar{y}_1 \cdot y_2$.

$$f_1(x) = (((y_1 \cdot \bar{y}_2) \oplus x_2) \cdot ((y_1 \cdot y_2) \oplus x_3))((\bar{y}_1 \cdot y_2) \oplus x_1)(((y_1 \cdot \bar{y}_2) \oplus x_2) \vee ((y_1 \cdot y_2) \oplus x_3))$$

Для другої узагальненої елементарної функції отримаємо: $a_{2.1} = \bar{y}_1 \cdot y_2$; $a_{2.2} = \bar{y}_1 \cdot \bar{y}_2$; $a_{2.3} = y_1 \cdot \bar{y}_2$.

$$f_2(x) = (((\bar{y}_1 \cdot y_2) \oplus x_2) \cdot ((\bar{y}_1 \cdot \bar{y}_2) \oplus x_3))((y_1 \cdot \bar{y}_2) \oplus x_1)(((\bar{y}_1 \cdot y_2) \oplus x_2) \vee ((\bar{y}_1 \cdot \bar{y}_2) \oplus x_3)).$$

Для третьої узагальненої елементарної функції отримаємо: $a_{3.1} = \bar{y}_1 \cdot \bar{y}_2$; $a_{3.2} = \bar{y}_1 \cdot y_2$; $a_{3.3} = y_1 \cdot y_2$.

$$f_3(x) = (((\bar{y}_1 \cdot \bar{y}_2) \oplus x_2) \cdot ((\bar{y}_1 \cdot y_2) \oplus x_3))((y_1 \cdot y_2) \oplus x_1)(((\bar{y}_1 \cdot \bar{y}_2) \oplus x_2) \vee ((\bar{y}_1 \cdot y_2) \oplus x_3)).$$

На основі отриманих елементарних функцій побудуємо удосконалену дискретно-казуальну модель двохоперандної СЕТ-операції.

$$C(x,y) = \begin{bmatrix} (((y_1 \cdot \bar{y}_2) \oplus x_2) \cdot ((y_1 \cdot y_2) \oplus x_3))((\bar{y}_1 \cdot y_2) \oplus x_1)(((y_1 \cdot \bar{y}_2) \oplus x_2) \vee ((y_1 \cdot y_2) \oplus x_3)) \\ (((\bar{y}_1 \cdot y_2) \oplus x_2) \cdot ((\bar{y}_1 \cdot \bar{y}_2) \oplus x_3))((y_1 \cdot \bar{y}_2) \oplus x_1)(((\bar{y}_1 \cdot y_2) \oplus x_2) \vee ((\bar{y}_1 \cdot \bar{y}_2) \oplus x_3)) \\ (((\bar{y}_1 \cdot \bar{y}_2) \oplus x_2) \cdot ((\bar{y}_1 \cdot y_2) \oplus x_3))((y_1 \cdot y_2) \oplus x_1)(((\bar{y}_1 \cdot \bar{y}_2) \oplus x_2) \vee ((\bar{y}_1 \cdot y_2) \oplus x_3)) \end{bmatrix} \quad (4.41)$$

Складність отриманої моделі співпадає з складністю моделі (4.39).

Побудувати дискретно-казуальну модель двохоперандної СЕТ-операції (4.37) на основі третього варіанту послідовності ключових елементів можна через об'єднання одноопераднних операцій (3.24), (3.41) – (3.43).

$$C(x,y) = \begin{cases} \begin{bmatrix} (x_1 \cdot x_3)(x_2)(x_1 \vee x_3) \\ (x_1 \cdot \bar{x}_3)(x_2)(x_1 \vee \bar{x}_3) \\ (x_1 \cdot x_3)(\bar{x}_2)(x_1 \vee x_3) \end{bmatrix}, \text{ якщо } y_1 = 0;\ y_2 = 0 \\ \begin{bmatrix} (\bar{x}_1 \cdot x_3)(x_2)(\bar{x}_1 \vee x_3) \\ (x_1 \cdot x_3)(\bar{x}_2)(x_1 \vee x_3) \\ (x_1 \cdot \bar{x}_3)(x_2)(x_1 \vee \bar{x}_3) \end{bmatrix}, \text{ якщо } y_1 = 0;\ y_2 = 1 \\ \begin{bmatrix} (x_1 \cdot x_3)(\bar{x}_2)(x_1 \vee x_3) \\ (\bar{x}_1 \cdot x_3)(x_2)(\bar{x}_1 \vee x_3) \\ (x_1 \cdot x_3)(x_2)(x_1 \vee x_3) \end{bmatrix}, \text{ якщо } y_1 = 1;\ y_2 = 0 \\ \begin{bmatrix} (x_1 \cdot \bar{x}_3)(x_2)(x_1 \vee \bar{x}_3) \\ (x_1 \cdot x_3)(x_2)(x_1 \vee x_3) \\ (\bar{x}_1 \cdot x_3)(x_2)(\bar{x}_1 \vee x_3) \end{bmatrix}, \text{ якщо } y_1 = 1;\ y_2 = 1 \end{cases} \quad (4.42)$$

Побудуємо удосконалену модель СЕТ-операції (4.42) по аналогії з побудовою моделі (4.30). Для першої узагальненої елементарної функції отримаємо: $a_{1.1} = \bar{y}_1 \cdot y_2$; $a_{1.2} = y_1 \cdot y_2$; $a_{1.3} = y_1 \cdot \bar{y}_2$.

$$f_1(x) = (((\bar{y}_1 \cdot y_2) \oplus x_1) \cdot ((y_1 \cdot y_2) \oplus x_3))((y_1 \cdot \bar{y}_2) \oplus x_2)(((\bar{y}_1 \cdot y_2) \oplus x_1) \vee ((y_1 \cdot y_2) \oplus x_3))$$

Для другої узагальненої елементарної функції отримаємо: $a_{2.1} = y_1 \cdot \bar{y}_2$; $a_{2.2} = \bar{y}_1 \cdot \bar{y}_2$; $a_{2.3} = \bar{y}_1 \cdot y_2$.

$$f_2(x) = (((y_1 \cdot \bar{y}_2) \oplus x_1) \cdot ((\bar{y}_1 \cdot \bar{y}_2) \oplus x_3))((\bar{y}_1 \cdot y_2) \oplus x_2)(((y_1 \cdot \bar{y}_2) \oplus x_1) \vee ((\bar{y}_1 \cdot \bar{y}_2) \oplus x_3)).$$

Для третьої узагальненої елементарної функції отримаємо: $a_{3.1} = y_1 \cdot y_2$; $a_{3.2} = \bar{y}_1 \cdot y_2$; $a_{3.3} = \bar{y}_1 \cdot \bar{y}_2$.

$$f_3(x) = (((y_1 \cdot y_2) \oplus x_1) \cdot ((\bar{y}_1 \cdot y_2) \oplus x_3))((\bar{y}_1 \cdot \bar{y}_2) \oplus x_2)(((y_1 \cdot y_2) \oplus x_1) \vee ((\bar{y}_1 \cdot y_2) \oplus x_3)).$$

На основі отриманих елементарних функцій побудуємо удосконалену дискретно-казуальну модель двохоперандної СЕТ-операції.

$$C(x,y) = \begin{bmatrix} (((\bar{y}_1 \cdot y_2) \oplus x_1) \cdot ((y_1 \cdot y_2) \oplus x_3))((y_1 \cdot \bar{y}_2) \oplus x_2)(((\bar{y}_1 \cdot y_2) \oplus x_1) \vee ((y_1 \cdot y_2) \oplus x_3)) \\ (((y_1 \cdot \bar{y}_2) \oplus x_1) \cdot ((\bar{y}_1 \cdot \bar{y}_2) \oplus x_3))((\bar{y}_1 \cdot y_2) \oplus x_2)(((y_1 \cdot \bar{y}_2) \oplus x_1) \vee ((\bar{y}_1 \cdot \bar{y}_2) \oplus x_3)) \\ (((y_1 \cdot y_2) \oplus x_1) \cdot ((\bar{y}_1 \cdot y_2) \oplus x_3))((\bar{y}_1 \cdot \bar{y}_2) \oplus x_2)(((y_1 \cdot y_2) \oplus x_1) \vee ((\bar{y}_1 \cdot y_2) \oplus x_3)) \end{bmatrix} \quad (4.43)$$

Складність отриманої моделі співпадає з складністю моделі (4.30).

Побудуємо дискретно-казуальну модель двохоперандної СЕТ-операції (4.37) на основі четвертого варіанту послідовності ключових елементів через об'єднання одноопераднних операцій ((3.28), (3.44) –(3.46).

$$C(x, y) = \begin{cases} \begin{bmatrix} (x_1 \cdot x_2)(x_3)(x_1 \vee x_2) \\ (x_1 \cdot x_2)(\bar{x}_3)(x_1 \vee x_2) \\ (x_1 \cdot \bar{x}_2)(x_3)(x_1 \vee \bar{x}_2) \end{bmatrix}, \text{ якщо } y_1 = 0;\ y_2 = 0 \\ \begin{bmatrix} (\bar{x}_1 \cdot x_2)(x_3)(\bar{x}_1 \vee x_2) \\ (x_1 \cdot \bar{x}_2)(x_3)(x_1 \vee \bar{x}_2) \\ (x_1 \cdot x_2)(\bar{x}_3)(x_1 \vee x_2) \end{bmatrix}, \text{ якщо } y_1 = 0;\ y_2 = 1 \\ \begin{bmatrix} (x_1 \cdot \bar{x}_2)(x_3)(x_1 \vee \bar{x}_2) \\ (\bar{x}_1 \cdot x_2)(x_3)(\bar{x}_1 \vee x_2) \\ (x_1 \cdot x_2)(x_3)(x_1 \vee x_2) \end{bmatrix}, \text{ якщо } y_1 = 1;\ y_2 = 0 \\ \begin{bmatrix} (x_1 \cdot x_2)(\bar{x}_3)(x_1 \vee x_2) \\ (x_1 \cdot x_2)(x_3)(x_1 \vee x_2) \\ (\bar{x}_1 \cdot x_2)(x_3)(\bar{x}_1 \vee x_2) \end{bmatrix}, \text{ якщо } y_1 = 1;\ y_2 = 1 \end{cases} \quad (4.44)$$

Побудуємо удосконалену модель СЕТ-операції (4.44) по аналогії з побудовою моделі (4.36). Для першої узагальненої елементарної функції отримаємо: $a_{1.1} = y_1 \cdot \bar{y}_2$; $a_{1.2} = \bar{y}_1 \cdot y_2$; $a_{1.3} = y_1 \cdot y_2$.

$$f_1(x) = (((y_1 \cdot \bar{y}_2) \oplus x_1) \cdot ((\bar{y}_1 \cdot y_2) \oplus x_2))((y_1 \cdot y_2) \oplus x_3)(((y_1 \cdot \bar{y}_2) \oplus x_1) \vee ((\bar{y}_1 \cdot y_2) \oplus x_2))$$

Для другої узагальненої елементарної функції отримаємо: $a_{2.1} = y_1 \cdot \bar{y}_2$; $a_{2.2} = \bar{y}_1 \cdot y_2$; $a_{2.3} = \bar{y}_1 \cdot \bar{y}_2$.

$$f_2(x) = (((y_1 \cdot \bar{y}_2) \oplus x_1) \cdot ((\bar{y}_1 \cdot y_2) \oplus x_2))((\bar{y}_1 \cdot \bar{y}_2) \oplus x_3)(((y_1 \cdot \bar{y}_2) \oplus x_1) \vee ((\bar{y}_1 \cdot y_2) \oplus x_2)).$$

Для третьої узагальненої елементарної функції отримаємо: $a_{3.1} = y_1 \cdot y_2$; $a_{3.2} = \bar{y}_1 \cdot \bar{y}_2$; $a_{3.3} = \bar{y}_1 \cdot y_2$.

$$f_3(x) = (((y_1 \cdot y_2) \oplus x_1) \cdot ((\bar{y}_1 \cdot \bar{y}_2) \oplus x_2))((\bar{y}_1 \cdot y_2) \oplus x_3)(((y_1 \cdot y_2) \oplus x_1) \vee ((\bar{y}_1 \cdot \bar{y}_2) \oplus x_2)).$$

На основі отриманих елементарних функцій побудуємо удосконалену дискретно-казуальну модель двохоперандної СЕТ-операції.

$$C(x,y)=\begin{bmatrix} (((y_1\cdot\bar{y}_2)\oplus x_1)\cdot((\bar{y}_1\cdot y_2)\oplus x_2))((y_1\cdot y_2)\oplus x_3)(((y_1\cdot\bar{y}_2)\oplus x_1)\vee((\bar{y}_1\cdot y_2)\oplus x_2)) \\ (((y_1\cdot\bar{y}_2)\oplus x_1)\cdot((\bar{y}_1\cdot y_2)\oplus x_2))((\bar{y}_1\cdot\bar{y}_2)\oplus x_3)(((y_1\cdot\bar{y}_2)\oplus x_1)\vee((\bar{y}_1\cdot y_2)\oplus x_2)) \\ (((y_1\cdot y_2)\oplus x_1)\cdot((\bar{y}_1\cdot\bar{y}_2)\oplus x_2))((\bar{y}_1\cdot y_2)\oplus x_3)(((y_1\cdot y_2)\oplus x_1)\vee((\bar{y}_1\cdot\bar{y}_2)\oplus x_2)) \end{bmatrix} \quad (4.45)$$

Складність отриманої моделі співпадає з складністю моделі (4.39).

Проведений аналіз показав, що складності дискретно-казуальних моделей СЕТ-операцій на основі елементарних функцій операцій, керованих інформацією, за критерієм відмінності відповідних елементарних функцій (4.39) (4.41), (4.43) і (4.45) однакові. Складність моделей не залежить від варіантів розміщення ключових елементів в моделях. Виходячи з цього можна стверджувати, що практичне застосування отриманих моделей вимагає однакових ресурсів при побудові систем малоресурсної криптографії.

Проте при практичному моделюванні СЕТ-операцій для систем захисту інформації доцільно використовувати однакові підходи для побудови операцій криптографічного перетворення. Результати дослідження двохоперандних СЕТ-операцій на основі елементарних функцій операцій, керованих інформацією, за критерієм простоти їх побудови показали перспективність застосування першого варіанту розміщення ключових елементів. Виходячи з цього, доцільно синтезувати СЕТ-операції, в яких номера ключових елементів співпадають з номерами елементарних функцій.

4.4. Побудова криптографічних систем, які реалізують СЕТ-операції на основі елементарних функцій операцій, керованих інформацією.

Теорія СЕТ-шифрування і архітектура СЕТ-операцій передбачає декілька технологій побудови криптографічних систем [48]:

- криптографічні системи на основі одноопераднної СЕТ-операції;

- криптографічні системи на основі декількох одноопераднних СЕТ-операцій;
- криптографічні системи на основі двохоперандної СЕТ-операції;
- криптографічні системи на основі групи двохоперандних СЕТ-операції.

Проте використання СЕТ-операції на основі елементарних функцій операцій, керованих інформацією, при побудові криптографічних систем має свої особливості. Це пов’язане з тим, що алгоритм реалізації даних СЕТ-операцій змінюється в залежності від вхідних даних, над якими здійснюється криптографічне перетворення. Синтезовані СЕТ-операції на основі елементарних функцій операцій, керованих інформацією, можуть бути використані як при побудові криптографічних систем, так і криптографічних мереж. Підходи до вибору кортежей одноопераднних СЕТ-операцій, на основі яких будуються моделі криптографічних мереж з використанням двохоперандних СЕТ-операцій, наведені в [67].

Розглянемо варіанти побудови криптографічних систем з використанням СЕТ-операції на основі елементарних функцій операцій, керованих інформацією.

4.4.1. Криптографічна система, яка реалізує одноопераднду СЕТ-операцію на основі елементарних функцій операцій, керованих інформацією.

При побудові криптографічних систем на основі одноопераднних СЕТ-операцій необхідно враховувати їх симетричність. Структура криптографічної системи обміну конфіденціальною інформацією між абонентами з

застосуванням одноопераднних симетричних СЕТ-операцій наведена на рис. 4.1 [48].

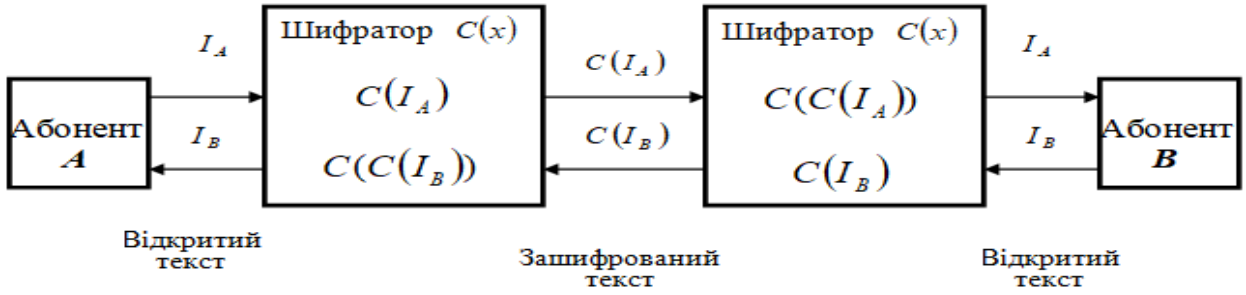


Рис. 4.1. Криптографічна система обміну конфіденціальною інформацією між абонентами з застосуванням одноопераднних симетричних СЕТ-операцій [3].

Детальний опис функціонування криптографічної системи, представленої на рис. 4.1, наведено в [48].

Якщо в криптографічній системі буде використано в якості $C(x)$ СЕТ-операції на основі елементарних функцій операцій, керованих інформацією, то це забезпечить додаткове управління процесом шифрування і розшифрування інформації.

Структура криптографічної системи обміну конфіденціальною інформацією між абонентами з застосуванням одноопераднних симетричних СЕТ-операцій операції на основі елементарних функцій операцій керованих інформацією наведена на рис. 4.2.

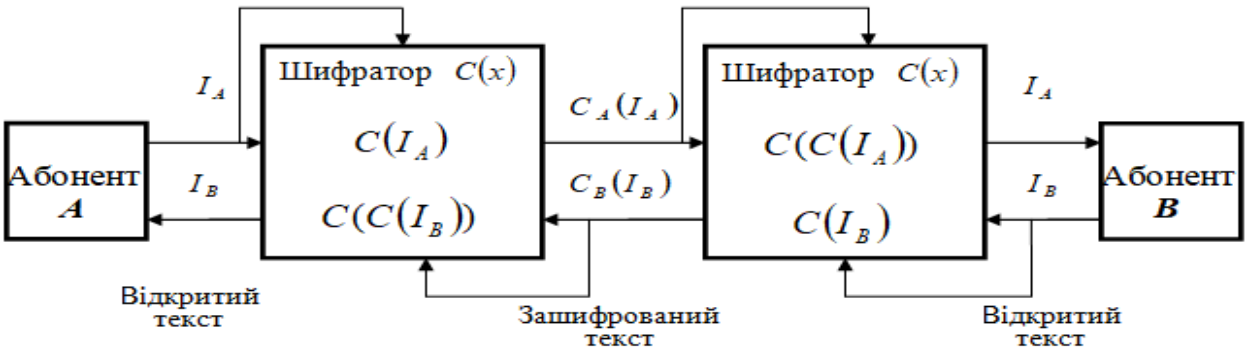


Рис. 4.2. Криптографічна система обміну конфіденціальною інформацією між абонентами з застосуванням одноопераднних симетричних СЕТ-операцій на основі елементарних функцій операцій, керованих інформацією.

Так як криптографічна система використовує одну одноопераднду СЕТ-операцію, то вона реалізує лише одну таблицю підстановки. Проте одноопераднда СЕТ-операція на основі елементарних функцій операцій, керованих інформацією, перетворює 3Сі-кванти вхідного відкритого тексту в 3Сі-кванти зашифрованого тексту. Дана операція перетворює або 3 біти інформації, або 3 байти інформації, або три слова інформації. Розмірність Сі-кванта інформації залежить від реалізації криптосистеми.

Якщо криптосистема реалізує перетворення інформації по три біти, то кількість біт, які перетворюються, менша розрядності символів, які необхідно зашифрувати. В даному випадку криптографічна система, представлена на рис. 4.2, забезпечує як підстановку біт символу, так і міжсимвольне перемішування. Сутність процесу підстановки і перемішування в загальному вигляді представлена на рис. 4.3 [48], де m - кількість біт для відображення символу відкритого тексту, n - кількість біт які перетворює одноопераднда СЕТ-операція.

Якщо криптосистема реалізує перетворення інформації по три байти або по три слова, то вона реалізує перетворення на основі підстановки однойменних біт між байтами. В даному випадку буде реалізоване міжбайтове перетворенням біт з міжбайтовим перемішуванням.

Рис. 4.3. Умовна реалізація процесу шифрування з перестановками і розсіюванням символів ($n < m$) [48].

Основний недолік даної криптосистеми полягає в тому, що при обміні абонентами однаковими відкритими текстами по каналу зв’язку будуть

передаватись однакові зашифровані тексти [3]. Даний недолік можна усунути шляхом використання несиметричних одноопераднних СЕТ-операцій.

Структура криптографічної системи обміну конфіденціальною інформацією між абонентами з застосуванням одноопераднних несиметричних СЕТ-операцій наведена на рис. 4.4 і описана в [48].

Застосування в криптографічних системах як симетричних, так і несиметричних СЕТ-операції на основі елементарних функцій операцій, керованих інформацією, забезпечує додаткове управління процесом шифрування і розшифрування інформації.

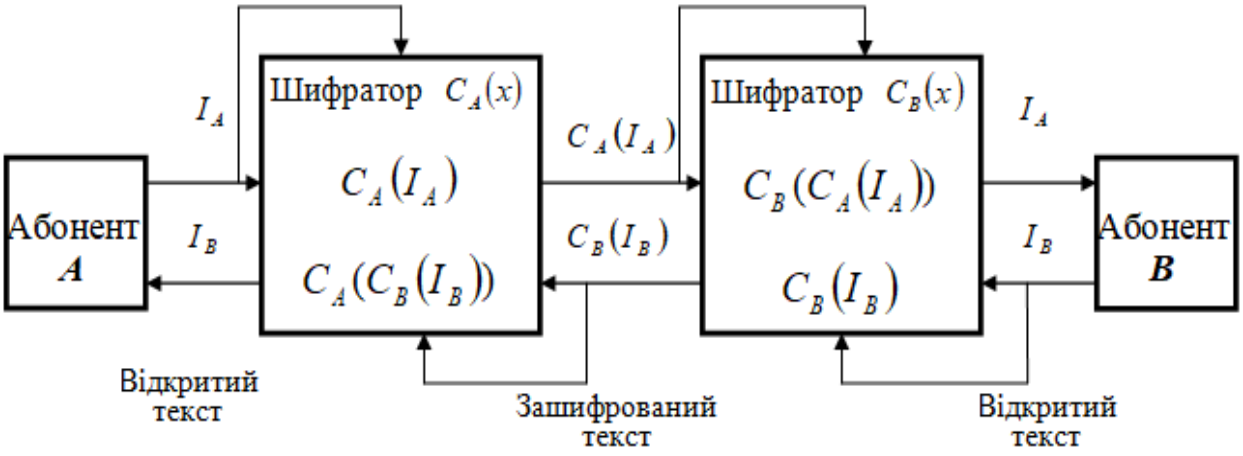


Рис. 4.4. Криптографічна система обміну конфіденціальною інформацією між абонентами з застосуванням несиметричних одноопераднних СЕТ-операцій на основі елементарних функцій операцій, керованих інформацією, [48].

В подальшому будемо розглядати криптосистеми з використанням лише несиметричних СЕТ операцій. Це пов’язано з тим, що симетричні СЕТ-операції є частковим випадком несиметричних СЕТ-операцій.

4.4.2. Криптографічна система, яка реалізує декілька одноопераднних СЕТ-операцій на основі елементарних функцій операцій, керованих інформацією.

До недоліків криптографічних систем на основі використання однієї одноопераднної СЕТ-операції на основі елементарних функцій операцій, керованих інформацією, можна віднести реалізацію лише однієї таблиці підстановки. Тому доцільно при побудові криптографічних систем використовувати декілька одноопераднних СЕТ-операцій.

Криптографічна система двостороннього обміну конфіденціальною інформацією між абонентами з застосуванням декількох одноопераднних несиметричних СЕТ-операцій наведена на рис. 4.5 і описана в [48].

Якщо в криптографічній системі (рис. 4.5) використати множину одноопераднних несиметричних СЕТ-операції на основі елементарних функцій операцій, керованих інформацією, то це забезпечить можливість реалізації подвійного управління процесом крипто перетворення.

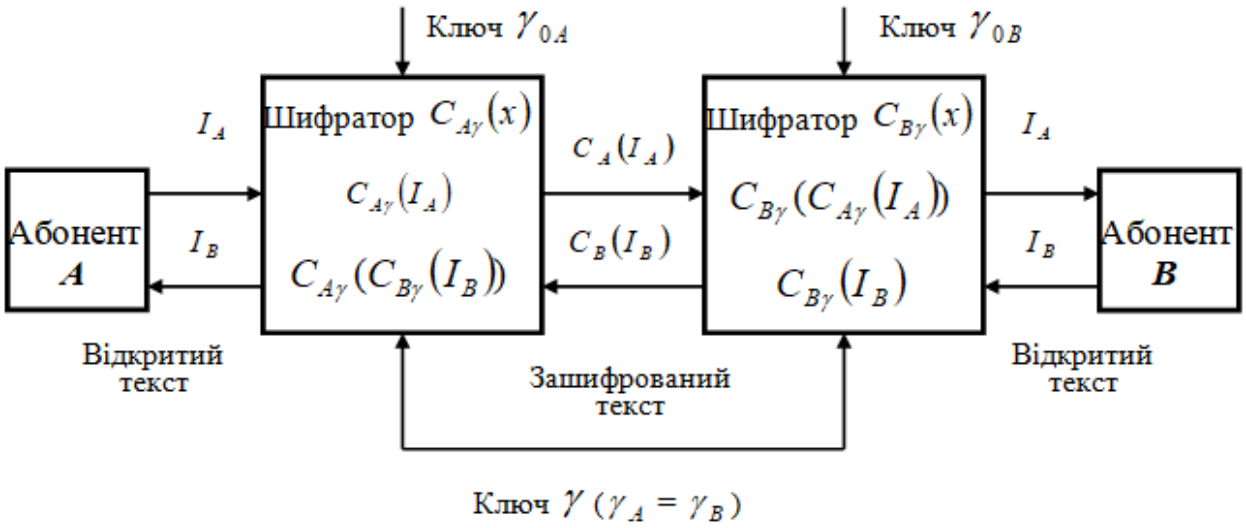


Рис. 4.5. Криптографічна система двостороннього обміну конфіденціальною інформацією між абонентами з застосуванням декількох одноопераднних несиметричних СЕТ-операцій [48].

Криптографічна система двостороннього обміну конфіденціальною інформацією між абонентами з застосуванням декількох одноопераднних несиметричних СЕТ-операцій на основі елементарних функцій операцій, керованих інформацією, представлена на рис 4.6.

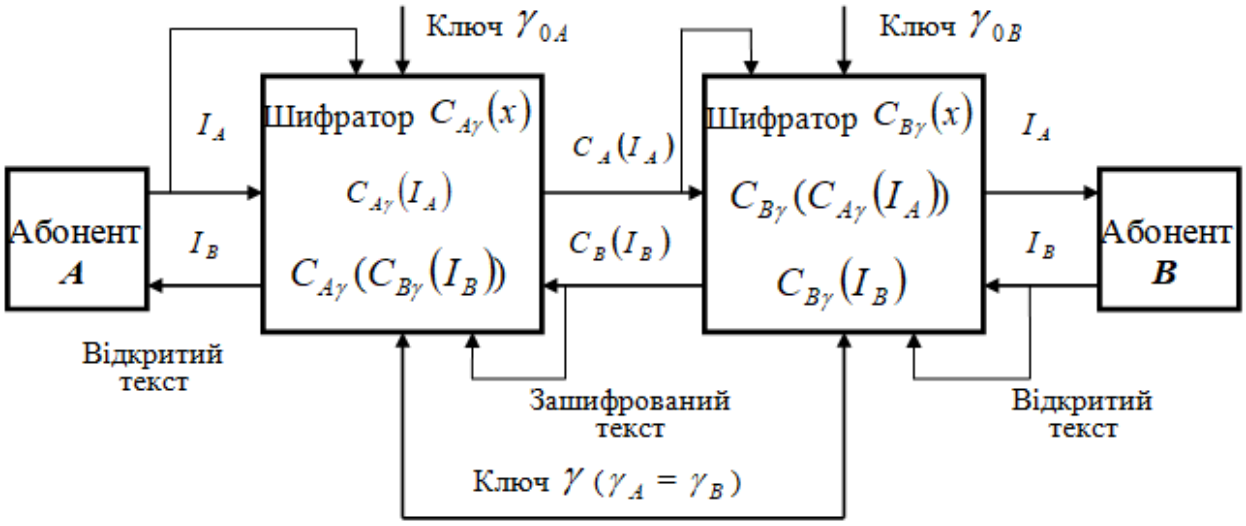


Рис. 4.6. Криптографічна система двостороннього обміну конфіденціальною інформацією між абонентами з застосуванням декількох одноопераднних несиметричних СЕТ-операцій на основі елементарних функцій операцій, керованих інформацією.

Реалізація в криптографічній системі, представленій на рис. 4.6, декількох одноопераднних СЕТ-операцій приводить до пропорціонального збільшення складності шифраторів $C_{A\gamma}(x)$ і $C_{B\gamma}(x)$ в декілька разів.

Самим простим варіантом збільшення кількості таблиць підстановки, які реалізує криптографічна система, є використання множини модифікованих СЕТ-операцій на основі перестановок і інверсій елементарних функцій.

В підрозділі 3.5 розроблено метод синтезу групи СЕТ-операцій на основі елементарних функцій операцій, керованих інформацією, і запропоновано 6 варіантів його реалізації. Даний метод базується на модифікації всіх операцій базової групи шляхом перестановок і інверсій елементарних функцій. Так як будь яку операції з групи СЕТ-операцій на основі елементарних функцій

операцій, керованих інформацією, можна трактувати як першу операцію базової групи, яка будується, то її модифікації можна описати шістьома варіантами моделей прямого і оберненого модифікованого криптографічного перетворення.

Розглянемо перший варіант побудови моделей модифікації СЕТ-операції, описаний завдяки (3.47) і (3.48). Обмежившись використання лише першої (будь якої) СЕТ-операції базової групи, отримаємо співвідношення між прямим і оберненим крипто перетворенням.

Якщо модифікація СЕТ-операції задана перетворенням

$$C_{b.1,p.j,m.h}(x) = C_{p.j}(C_{b.1}(x)) \oplus \gamma_{m.h} = y, \qquad (4.45),$$

тоді модифікувати обернену СЕТ-операцію необхідно так:

$$C'_{b.1,p.j,m.h}(y) = C'_{b.1}(C'_{p.j}(y \oplus \gamma_{m.h})) = x. \qquad (4.46)$$

де $C_{b.1}(x)$ - одноопераднда СЕТ-операція на основі елементарних функцій операцій, керованих інформацією, завдяки якій реалізована криптографічна система, наведена на рис.4.4.

Моделі (4.45) і (4.46) забезпечують побудову 48 модифікацій прямих і обернених СЕТ-операцій до операції $C_{b.1}(x)$.

Криптографічна система двостороннього обміну конфіденціальною інформацією між абонентами з застосуванням множини модифікованих одноопераднх СЕТ-операцій на основі елементарних функцій операцій, керованих інформацією, наведена на рис. 4.7.

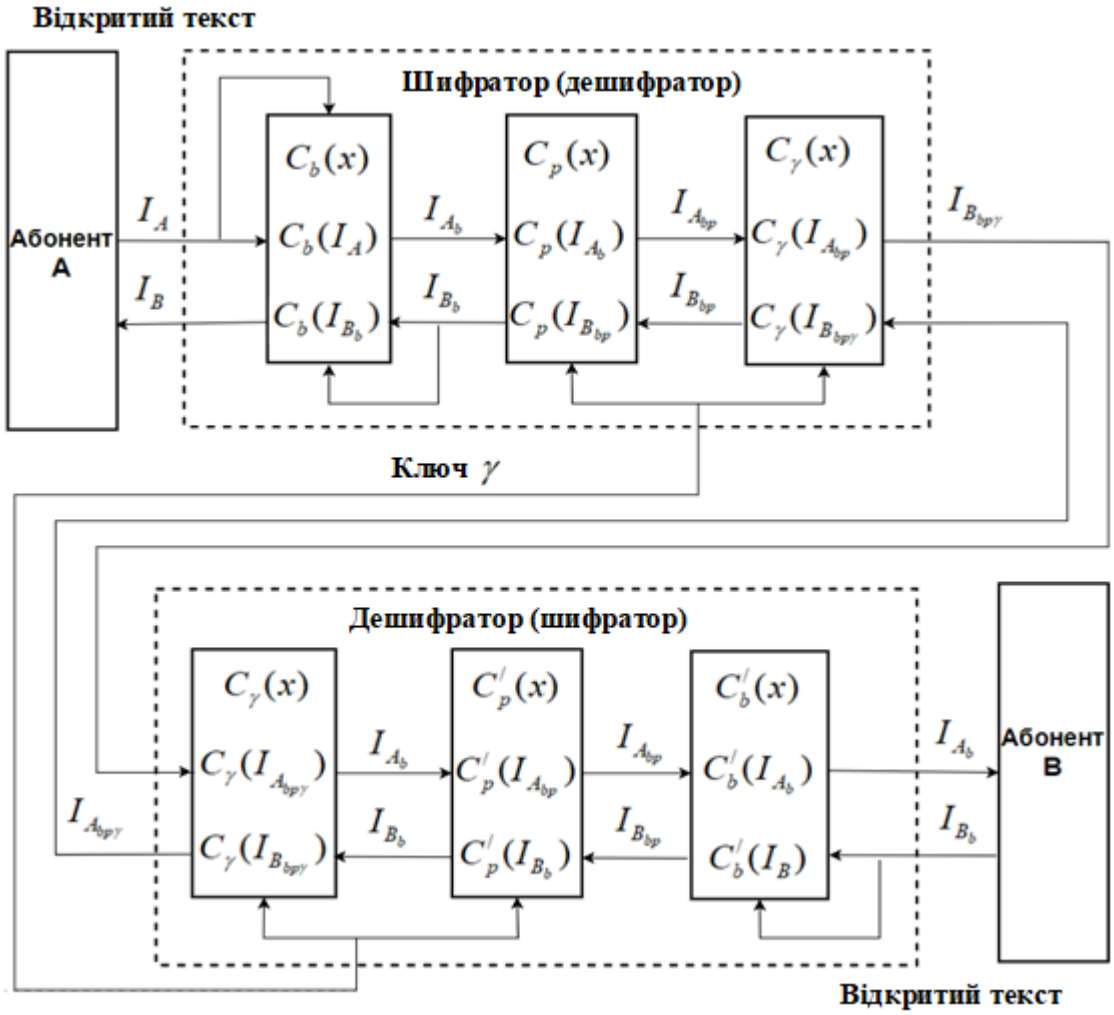


Рис. 4.7. Криптографічна система двостороннього обміну конфіденціальною інформацією між абонентами з застосуванням множини модифікованих одноопераднних СЕТ-операцій на основі елементарних функцій операцій, керованих інформацією, (моделі (4.45) і (4.46)).

Криптографічна система (рис.4.7) працює так:

1. Передача повідомлення від абонента А до абонента В.

1.1. Від абонента А відкритий текст I_A поступає на вхід шифратора, який зв'язаний з першим блоком криптографічного перетворення. Перший блок криптографічного перетворення $C_b(x)$ реалізує перший етап шифрування $C_b(I_A)$. Отримана шифрограма I_{Ab} поступає на вхід другого блоку шифрування, який реалізує СЕТ-операцію $C_p(x)$ і забезпечує перестановку Сі-

квантів вхідної інформації $C_p(I_{Ab})$. Модифікована шифрограма I_{Abp} поступає на вхід третього блоку шифрування, який реалізує СЕТ-операцію $C_\gamma(x)$ і забезпечує модифікацію шифрограми на основі додаткового гамування $C_\gamma(I_{Abp})$. Вибір СЕТ-операцій $C_p(x)$ і $C_\gamma(x)$ реалізується на основі ключової послідовності γ. Зашифрований текст $I_{Abp\gamma}$ з виходу третього блоку шифрування через вихід шифратора передається в відкритий канал зв'язку.

1.2. Зашифрований текст $I_{Abp\gamma}$ поступає на вхід дешифратора, який зв'язаний з третім блоком оберненого криптографічного перетворення. Третій блок оберненого криптографічного перетворення $C_\gamma(x)$ видаляє з шифрограми $I_{Abp\gamma}$ гамуючи послідовність $C_\gamma(I_{Abp\gamma})$. Результат першого етапу розшифрування I_{Abp} поступає на вхід другого блоку оберненого криптографічного перетворення $C_p^{/}(x)$, який забезпечує обернену перестановку вхідних Сі-квантів зашифрованого тексту $C_p^{/}(I_{Abp})$. З виходу другого блоку оберненого криптографічного перетворення зашифрована інформація I_{Ab} поступає на вхід першого блоку розшифрування $C_b^{/}(x)$, який забезпечує обернене базове криптографічне перетворення $C_b^{/}(I_{Ab})$. Вибір СЕТ-операцій $C_p^{/}(x)$ і $C_\gamma(x)$ реалізується на основі ключової послідовності γ. При шифруванні і розшифруванні використовуються одна ключова послідовність. З виходу першого блоку розшифрування розшифроване повідомлення I_A через вихід дешифратора передається абоненту А.

2. Передача повідомлення від абонента В до абонента А.

Базові СЕТ-операції належать до групи СЕТ-операцій і для них справедливі рівності [48]:

$$\begin{cases} C_b^{/}(C_b(x)) = x; \\ C_b(C_b^{/}(x)) = x. \end{cases} \tag{4.47}$$

Аналогічно, СЕТ-операції перестановки також належать до однієї групи і для них будуть справедливі рівності [48]:

$$\begin{cases} C_p^{/}(C_p(x)) = x; \\ C_p(C_p^{/}(x)) = x. \end{cases} \quad (4.48)$$

Системи рівностей (4.47) і (4.48) забезпечують можливість використовувати операції розшифрування для шифрування інформації, а розшифрування зашифрованої інформації реалізувати на основі операцій шифрування.

Виходячи з цього, для забезпечення малоресурсності криптографічної системи, вирази (4.47) і (4.48) було покладено в основу реалізації каналу оберненого захищеного зв'язку.

2.1. Від абонента В відкритий текст I_B поступає на вхід дешифратора, який буде реалізувати функцію шифратора. Вхід дешифратора є входом першого блоку розшифрування $C_b^{/}(x)$ для абонента А, а для абонента В є першим блоком шифрування, який зашифрує відкритий текст $C_b^{/}(I_B)$. Отримана шифрограма I_{Bb} поступає на вхід другого блоку розшифрування, який реалізує СЕТ-операцію $C_p^{/}(x)$ для абонента А, а для абонента В він є першим блоком шифрування, і забезпечує перестановку Сі-квантів вхідної інформації $C_p^{/}(I_{Bb})$. Модифікована шифрограма I_{Bbp} поступає на вхід третього блоку розшифрування для абонента А, а для абонента В є першим блоком шифрування, який реалізує СЕТ-операцію $C_\gamma(x)$. Даний блок забезпечує модифікацію шифрограми на основі додаткового гамування $C_\gamma(I_{Bbp})$. Зашифрований текст $I_{Bbp\gamma}$ з виходу третього блоку через вихід шифратора передається у відкритий канал зв'язку.

2.2. Зашифрований текст $I_{Bbp\gamma}$ поступає на вхід шифратора, який буде реалізувати функцію дешифратора. Вхід дешифратора є входом третього блоку

розшифрування $C_\gamma(x)$ для абонента В, а для абонента А третім блоком шифрування, який перетворює шифрограму $C_\gamma(I_{Bbp\gamma})$ шляхом видалення з неї додаткового гамування.

Результат першого етапу розшифрування I_{Bbp} поступає на вхід другого блоку криптографічного перетворення $C_p(x)$, який забезпечує для абонента А пряму перестановку, а для абонента В обернену перестановку $C_p(I_{Bbp})$. Модифікована другим блоком перетворення шифрограма I_{Bb} поступає в перший блок криптографічного перетворення $C_b(x)$, який для абонента В розшифровує шифрограму $C_b(I_{Bb})$ у відкритий текст I_B. Вибір СЕТ-операцій при шифруванні і розшифруванні повідомлення від абонента В до абонента А реалізується на основі однієї ключової послідовності γ.

Криптографічна система, представлена на рис. 4.7, реалізує всі переваги криптосистеми побудованої при використанні СЕТ-операцій на основі елементарних функцій операцій, керованих інформацією. Розглянута криптографічна система (рис. 4.7) використовує 48 модифікованих СЕТ-операцій і реалізує 48 таблиць підстановки. Збільшення кількості таблиць підстановки в 48 раз порівняно з криптографічною системою, представленою на рис. 4.6, вимагає додаткове використання 6 прямих і 6 обернених СЕТ-операцій перестановок, а також 8 СЕТ-операцій інверсії (гамування).

Додатково збільшення кількості таблиць підстановок в криптографічній системі без додаткового використання СЕТ-операцій перестановок і інверсій можливе шляхом застосування двохоперандних СЕТ-операцій на основі елементарних функцій операцій, керованих інформацією.

4.4.3. Криптографічні системи, які реалізують симетричні двохоперандні СЕТ-операції на основі елементарних функцій операцій, керованих інформацією.

Криптографічну систему на основі використання декількох одноопераднних СЕТ-операції на основі елементарних функцій операцій, керованих інформацією, можна модифікувати в криптографічну систему на основі використання однієї двохоперандної СЕТ-операції. При цьому слід відмітити, що складність практичної реалізації однієї двохоперандної СЕТ-операції менше сумарної складності кортежу одноопераднних операцій, адже в процесі об’єднання операцій здійснюється мінімізація таблиці істинності набору операцій.

Криптографічна система двостороннього обміну конфіденціальною інформацією між абонентами з застосуванням двохоперандної симетричної СЕТ-операцій на основі елементарних функцій операцій, керованих інформацією, представлена на рис 4.8.

Результати проведених досліджень показали, що при побудові криптографічних систем на основі двохоперандної СЕТ-операції необхідно використовувати симетричні двохоперандні СЕТ-операції на основі елементарних функцій операцій, керованих інформацією, синтезовані за критерієм відмінності відповідних елементарних функцій. Наприклад, спробуємо побудувати криптографічну систему на основі моделі СЕТ-операції (4.43), яка синтезована за критерієм відмінності відповідних елементарних функцій.

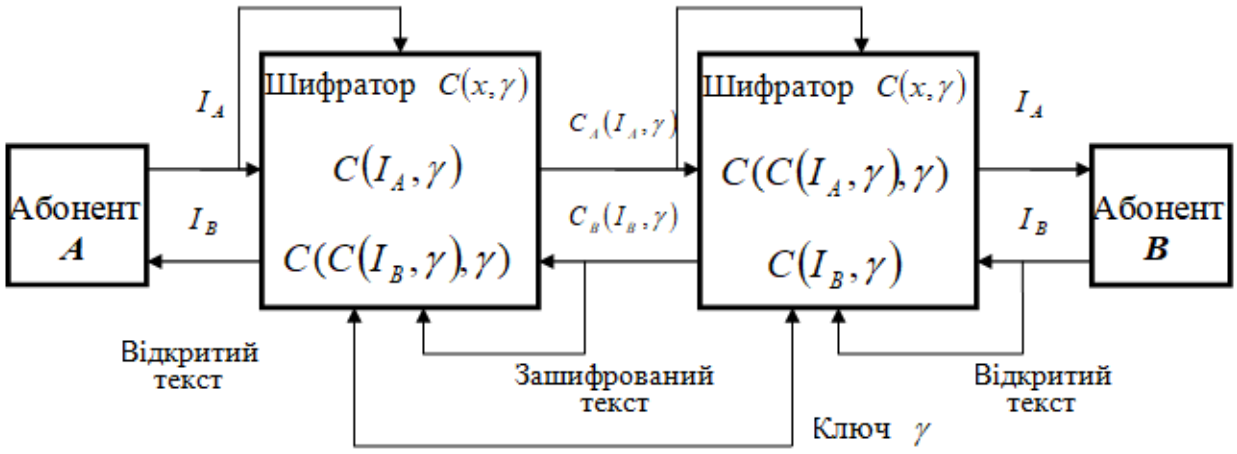


Рис. 4.8. Криптографічна система двостороннього обміну конфіденціальною інформацією між абонентами з застосуванням двохоперандної симетричної СЕТ-операції на основі елементарних функцій операцій, керованих інформацією.

Криптографічна система (рис.4.8) працює аналогічно криптографічній системі, побудованій на основі однієї симетричної двохоперандної СЕТ-операції, наведеній в [48], з урахуванням додаткових зв'язків управління СЕТ-операцією від вхідної інформації.

По аналогії з криптографічною системою двостороннього обміну конфіденціальною інформацією між абонентами з застосуванням множини модифікованих одноопераднних СЕТ-операцій на основі елементарних функцій операцій, керованих інформацією, побудуємо криптографічну систему з застосуванням множини модифікованих двохоперандних СЕТ-операцій. Дана криптографічна системи представлена на рис.4.9.

Криптосистема, представлена на рис. 4.9 працює аналогічно криптосистемі, представленій на рис. 4.7. Основна відмінність полягає в тому, що на основі ключової послідовності γ реалізується модифікація двохоперандної СЕТ-операції.

В результаті проведених досліджень встановлено, що при використанні модифікації двохоперандної СЕТ-операції шляхом перестановки елементарних функцій та інверсії результатів перетворення доцільно використовувати кортеж з операцій, які синтезовано за критерієм простоти побудови базової групи одноопераднних СЕТ-операцій. Наприклад, спробуємо побудувати криптографічну систему на основі моделі СЕТ-операції (4.36), яка синтезована за критерієм простоти побудови базової групи одноопераднних СЕТ-операцій.

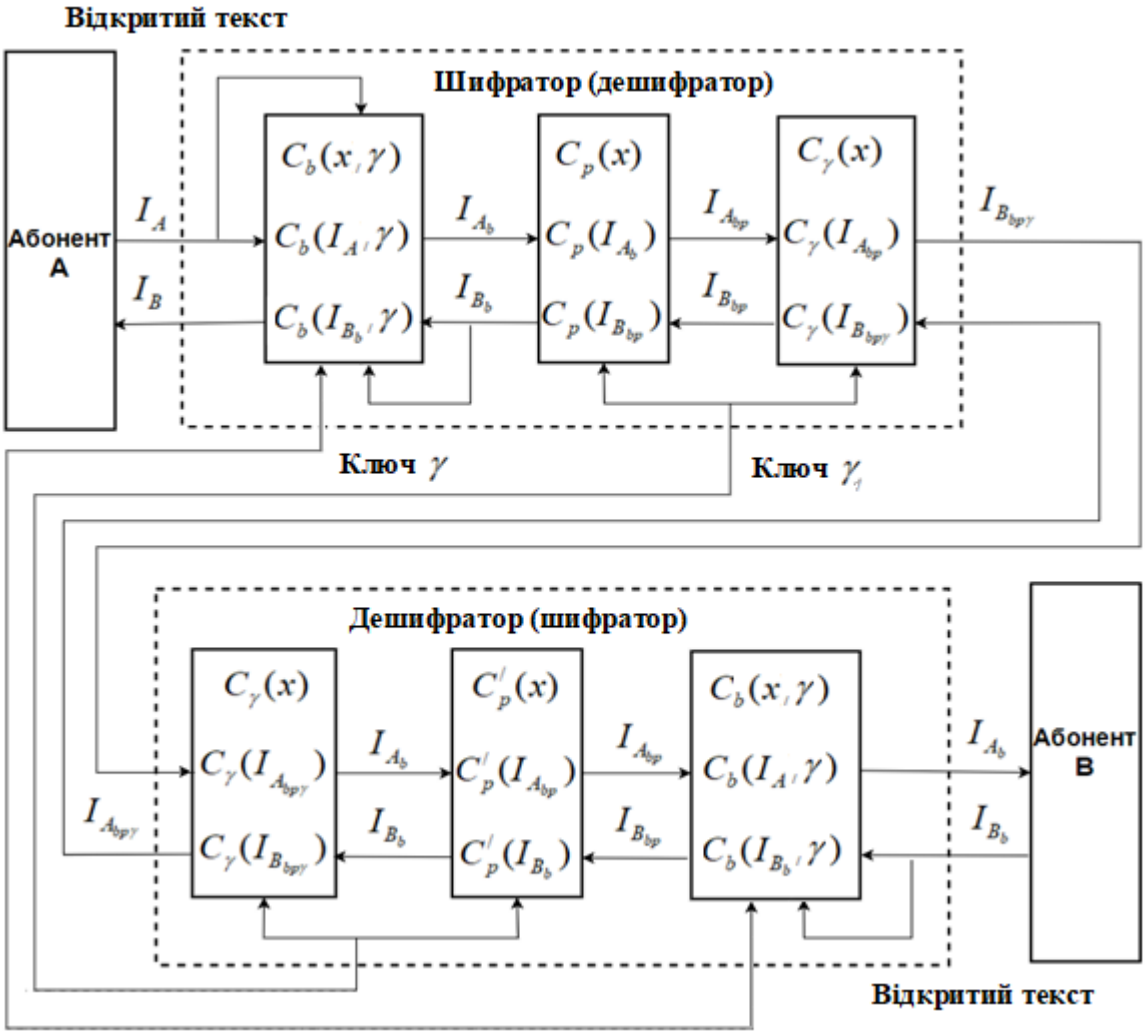


Рис. 4.9. Криптографічна система двостороннього обміну конфіденціальною інформацією між абонентами з застосуванням множини модифікованих двохоперандних СЕТ-операцій на основі елементарних функцій операцій, керованих інформацією.

На основі моделі СЕТ-операції (4.36), яка реалізує базову групу одноопераднних СЕТ-операцій шляхом перестановки елементарних функцій та інверсії результатів перетворення, буде синтезована повна група СЕТ-операцій на основі елементарних функцій операцій, керованих інформацією, яка включає 192 операції. Так як двохоперандна СЕТ-операція симетрична, то пряме і обернене перетворення співпадають. Дана криптографічна система для перетворення 3Сі-квантів інформації буде використовувати 192 таблиці підстановок, а це максимальна кількість таблиць підстановок, які можуть реалізувати СЕТ-операцій на основі елементарних функцій операцій, керованих інформацією. Тому подальше ускладнення криптографічної системи шляхом використання трьохоперандних СЕТ-операцій не доцільне, так як не забезпечить збільшення кількості таблиць підстановок, які реалізуються в криптографічному алгоритмі.

Оцінимо криптографічні системи двостороннього обміну конфіденціальною інформацією між абонентами з застосуванням двохоперандної симетричної СЕТ-операції на основі елементарних функцій операцій, керованих інформацією, (рис. 4.8), та з застосуванням множини модифікованих двохоперандних СЕТ-операцій на основі елементарних функцій операцій, керованих інформацією, (рис.4.9).

Для проведення оцінювання використаємо набір статистичних тестів «NIST STS» (NIST Statistical Test Suite) і методику проведення статистичного тестування генераторів псевдовипадкових чисел, орієнтованих на використання в задачах криптографічного захисту інформації [8, 33]. Опис пакету статичних тестів NIST STS наведено в додатку А.

Представимо шифрограми, побудовані криптографічними системами (рис. 4.8 і рис. 4.9), в якості вихідних даних генератора псевдовипадкових чисел. Для реалізації тестування на основі пакету NIST STS згенеруємо шифрограму довжиною не менше 10 м/біт. В якості вхідних даних для побудови шифрограми використаємо художні і технічні тексти із мережі Internet, в якості

генератора ключової послідовності (ключових послідовностей) використаєм вбудований генератор випадкових послідовностей Random [28].

Результати тестування шифрограм, згенерованих на основі текстової інформації криптографічними системами, представленими на рис. 4.8 і рис. 4.9, наведені в додатку Б.

Статистичний портрет за результатами тестування криптографічної системи обміну конфіденціальною інформацією між абонентами з застосуванням двохоперандної симетричної СЕТ-операції на основі елементарних функцій операцій, керованих інформацією, наведено на рис. 4.10.

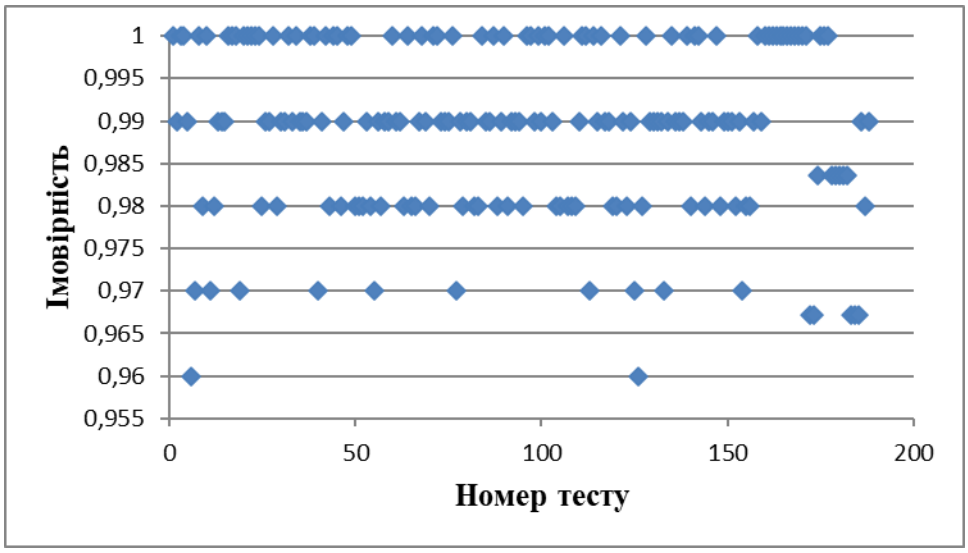


Рис. 4.10. Статистичний портрет за результатами тестування криптографічної системи двостороннього обміну конфіденціальною інформацією між абонентами з застосуванням двохоперандної симетричної СЕТ-операції на основі елементарних функцій операцій, керованих інформацією

Статистичний портрет за результатами тестування криптографічної системи двостороннього обміну конфіденціальною інформацією між абонентами з застосуванням множини модифікованих двохоперандних СЕТ-

операцій на основі елементарних функцій операцій, керованих інформацією, наведено на рис. 4.11.

Узагальнені результати тестування криптографічних систем наведені в табл..4.7.

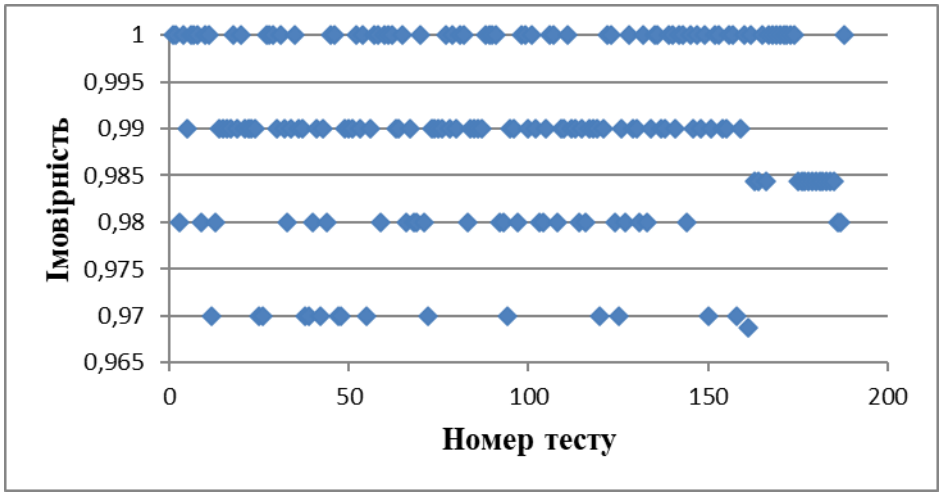


Рис. 4.11. Статистичний портрет за результатами тестування криптографічної системи двостороннього обміну конфіденціальною інформацією між абонентами з застосуванням множини модифікованих двохоперандних СЕТ-операцій на основі елементарних функцій операцій, керованих інформацією

Таблиця 4.7

Результати тестування криптографічних систем

Генератор	**Кількість тестів, у яких тестування пройшли більше 99 % послідовностей**	**Кількість тестів, у яких тестування пройшли більше 96 % послідовностей**
Криптографічна система двостороннього обміну конфіденціальною інформацією між абонентами з застосуванням двохоперандної симетричної СЕТ-операції на основі елементарних функцій операцій, керованих інформацією.	129 (68,2 %)	189 (100 %)
Криптографічна система двостороннього обміну конфіденціальною інформацією між абонентами з застосуванням множини модифікованих	136 (73,5 %)	189 (100 %)

двохоперандних СЕТ-операцій на основі елементарних функцій операцій, керованих інформацією		

Результати тестування криптографічних систем, які побудовані з застосуванням двохоперандних симетричних СЕТ-операції на основі елементарних функцій операцій, керованих інформацією, задовольняють вимогам стійкості до статистичного крипто аналізу відповідно до методики NIST STS. Виходячи з цього можна стверджувати, що дані малоресурсні криптосистеми можна використовувати для захисту конфіденційної інформації в комп'ютерних системах і мережах.

Висновки до розділу 4

За результатами досліджень: удосконалено системи малоресурсного потокового шифрування на основі випадкових підстановок, які реалізуються двохоперандними СЕТ-операціями шляхом розробки дискретно-казуальних моделей двохоперандних СЕТ-операції на основі елементарних функцій операцій, керованих інформацією, і моделей модифікації СЕТ-операцій, що забезпечило можливість подвійного управління процесом криптографічного перетворення від ключової послідовності і від вхідної інформації; збільшено кількість таблиць підстановки до 192 (кількість СЕТ-операцій в групі операцій на основі елементарних функцій операцій, керованих інформацією) для перетворення 3 Сі-квантів інформації (3 біт інформації); визначено, що стійкість результатів шифрування до статистичного криптоаналізу відповідає вимогам методики NIST STS.

1. На основі узагальнення особливостей дискретно-казуального моделювання двохоперандних СЕТ-операції перестановок керованих інформацією, запропоновано реалізовувати моделювання двохоперандних СЕТ-

операції на основі елементарних функцій операцій, керованих інформацією, шляхом поєднання в кортежі симетричних одноопераднних операцій.

2. Для побудови систем потокового шифрування на основі однієї двохоперандної СЕТ-операції і групи модифікованих СЕТ-операцій доцільно синтезувати двохоперандні СЕТ-операції на основі елементарних функцій операцій, керованих інформацією, на основі критерію відмінності відповідних елементарних функцій та простоти побудови базової групи одноопераднних СЕТ-операцій.

3. Запропоновано послідовність перетворень кортежу одноопераднних СЕТ-операцій, реалізація якої забезпечила синтез дискретно-казуальної моделі двохоперандної СЕТ-операції на основі елементарних функцій операцій, керованих інформацією, за критерієм простоти побудови базової групи одноопераднних СЕТ-операцій.

4. Побудовано дискретно-казуальну модель двохоперандної СЕТ-операції на основі елементарних функцій операцій, керованих інформацією, за критерієм відмінності відповідних елементарних функцій. Встановлено особливості синтезу даних моделей СЕТ-операцій.

5. Досліджено особливості побудови криптографічних систем, які реалізують СЕТ-операції на основі елементарних функцій операцій, керованих інформацією. Через неспівпадіння розрядностей відображення алфавіту і розрядності блоку перетворення, ці СЕТ-операції забезпечують міжсимвольне перемішування та розсіювання біт вхідної інформації. Реалізація даних СЕТ-операцій забезпечила можливість подвійного управління процесом криптографічного перетворення від ключової послідовності і від вхідної інформації.

6. Побудовані криптографічні системи, які реалізують симетричні двохоперандні СЕТ-операції на основі елементарних функцій операцій, керованих інформацією, для перетворення 3Сі-кванта інформації (3 біт

інформації), забезпечують можливість збільшення кількості використаних в процесі шифрування модифікованих таблиць підстановок до 192. За результатами тестування побудованих криптографічних систем, стійкість шифрограм до статистичного криптоаналізу відповідає вимогам методики NIST STS.

7. Результати розділу опубліковані в [3, 28, 31, 48, 52, 58, 68, 79].

ВИСНОВКИ

У дисертаційному дослідженні вирішено важливу науково-технічну задачу підвищення варіативності малоресурсних потокових шифрів випадкової підстановки за рахунок розробки і впровадження методу синтезу СЕТ-операцій на основі елементарних функцій операцій, керованих інформацією, які забезпечили можливість подвійного управління процесом криптографічного перетворення, як від ключової послідовності, так і від вхідної інформації, а також збільшили кількості таблиць підстановки, що реалізуються в криптоалгоритмі.

1. Розроблено метод синтезу елементарних функцій операцій, керованих інформацією, на основі відомих дискретних моделей елементарних функцій, отриманих за результатами обчислювального експерименту, за допомогою побудови множин варіантів мінімізованих дискретних моделей та їх функціональних схем, встановлено і формалізовано взаємозв'язки між дискретними змінними, що забезпечило можливість побудови повних множин дискретно-алгебраїчних і дискретно-казуальних моделей елементарних функцій операцій, керованих інформацією. Багатоваріантність представлення елементарних функцій на основі різних управляючих змінних забезпечило спрощення подальшого дослідження синтезу СЕТ-операцій на основі елементарних функцій операцій, керованих інформацією.

2. Побудовано метод синтезу ЗСі-квантових СЕТ-операцій на основі елементарних функцій операцій, керованих інформацією, шляхом визначення множин симетричних одноопераднних СЕТ-операцій для побудови базових груп за результатами обчислювального експерименту, синтезу базових груп симетричних одноопераднних СЕТ-операцій за критерієм простоти їх побудови та критерієм відмінності відповідних елементарних функцій, багатоваріантного представлення СЕТ-операцій дискретно-казуальними моделями, мінімізації взаємозв'язків в кортежі одноопераднних СЕТ-операцій при побудові двохоперандних СЕТ-операцій за критерієм простоти побудови та критерієм відмінності відповідних елементарних функцій, що забезпечило можливість

подвійного управління процесом криптографічного перетворення і знизило складність реалізації СЕТ-операцій в малоресурсних системах потокового шифрування.

3. Удосконалено системи потокового шифрування на основі випадкових підстановок шляхом застосування двохоперандних СЕТ-операції на основі елементарних функцій операцій, керованих інформацією, синтезованих за критерієм відмінності відповідних елементарних функцій і генераторів модифікованих двохоперандних СЕТ-операцій, синтезованих за критерієм простоти їх побудови, що забезпечило можливість подвійного управління процесом криптографічного перетворення від ключової послідовності і від вхідної інформації, збільшило кількість таблиць підстановки до 192 (кількість СЕТ-операцій в групі операцій на основі елементарних функцій операцій, керованих інформацією) для перетворення 3 Сі-квантів інформації (3 біт інформації). Стійкість результатів шифрування до статистичного криптоаналізу відповідає вимогам методики NIST STS.

4. Практична цінність роботи полягає в отриманні придатних в практиці побудови комп’ютерних криптографічних систем з нових моделей і операцій криптографічного перетворення їх функціональних схем і криптографічних алгоритмів для реалізації СЕТ-операцій на основі елементарних функцій операцій, керованих інформацією. Отримані практичні результати в сукупності забезпечують побудову криптографічних систем з подвійним управлінням процесом криптографічного перетворення, збільшують варіативність криптографічних алгоритмів шляхом використання 192 таблиць підстановки для перетворення 3 Сі-квантів інформації (трьох біт інформації). Для побудови симетричних двохоперандних СЕТ-операцій може бути виконистано 4096 варіантів базових групп, котрі містять лише симетричні одноопернадні СЕТ-операції. Будувати криптографічні системи з використанням однієї двохоперандної СЕТ-операції на основі елементарних функцій операцій, керованих інформацією, доцільно, якщо коефіцієнт відмінності відповідних елементарних функцій в СЕТ-операціях базової групи становить 2,25. Якщо цей коефіцієнт становить 1,125, то цю базову групу доцільно використовувати при

побудові двохоперандної СЕТ-операції для криптографічних перетворень, яка реалізує модифікацію таблиць підстановки. На основі реалізації побудованими двохоперандними СЕТ-операціями псевдовипадкових міжсимвольних перетворень і розсіювання символів досягається стійкість результатів шифрування до статистичного криптоаналізу відповідно до методики NIST STS.

Результати дисертаційного дослідження Підласого Дмитра Андрійовича, а саме удосконалена система комп'ютерного потокового шифрування на основі випадкових підстановок операцій, керованих інформацією, використані при розробці макету захищеної системи дистанційного управління наземним самохідним роботизованим комплексом. Впроваджена система потокового шифрування реалізована на рівні програмного модуля системи управління роботизованим комплексом "MOROZ-02L".

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. ДСТУ ISO/IEC 18033-4:2015 (ISO/IEC 18033-4:2011, IDT)/Зміна № 1:2023 (ISO/IEC 18033-4:2011/Amd 1:2020, IDT) «Інформаційні технології. Методи захисту. Алгоритми шифрування Частина 4. Потокові шифри». URL : http://uas.org.ua/ua/services/standartizatsiya (дата звернення: 03.05.2024).
2. ДСТУ ISO/IEC 18033-3:2015 (ISO/IEC 18033-3:2010, IDT)/Зміна № 1:2023 (ISO/IEC 18033-3:2010/Amd 1:2021, IDT) «Інформаційні технології. Методи захисту. Алгоритми шифрування. Частина 3. Блокові шифри». URL : http://uas.org.ua/ua/services/standartizatsiya (дата звернення: 03.05.2024).
3. Рудницький В. М., Лада Н. В., Кучук Г. А., Підласий Д. А. Архітектура СЕТ-операцій і технології потокового шифрування = Architecture of CET-operations and stream encryption technologies : монографія / Черкаси : видавець Пономаренко Р. В., 2024. 374 с. ISBN 978-966-2554-81-6. URL : https://dndivsovt.com/index.php/monograph/issue/view/22/22 (дата звернення: 13.09.2024).
4. 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.
5. Бабенко В. Г., Мельник О. Г., Стабецька Т. А. Синтез нелінійних операцій криптографічного перетворення. *Безпека інформації*. 2014. Т. 20, № 2. С. 143–147.
6. Бабенко В., Мельник О., Мельник Р. Класифікація трьохрозрядних елементарних функцій для криптографічного перетворення інформації. *Безпека інформації*. 2013. Т. 19, № 1. С. 56–59.
7. Бабенко В. Г., Мельник Р. П., Рудницький С. В. Дослідження способів запису трьохрозрядних криптографічних операцій. *Системи управління, навігації та зв'язку*. 2012. С. 170–173.

8. Богданов В. В., Паламарчук Н. А. Навчальний комплекс статистичної оцінки псевдовипадкових і текстових послідовностей. *Збірник наукових праць Військового інституту телекомунікацій та інформатизації Національного технічного університету України «Київський політехнічний інститут»*. 2007. Вип. 3. С. 17–26.
9. Бреус С., Цимбаленко О., Глухов М. Інформаційні технології: їх роль у зміні бізнес-парадигми компаній. *Економіка та суспільство*. 2024. Вип. 63. URL : https://doi.org/10.32782/2524-0072/2024-63-15 (дата звернення: 28.11.2025).
10. Лужецький В. А., Остапенко А. В. Блочний шифр на основі псевдонедетермінованої послідовності криптопримітивів. *Наукові праці Вінницького національного технічного університету*. 2010. Вип. 4. URL : https://praci.vntu.edu.ua/index.php/praci/article/view/234 (дата звернення: 15.02.2024).
11. Лужецький В. А. Дмитришин О. В. *Наукові праці Вінницького національного технічного університету*. 2011. Вип. 1. URL : http://praci.vntu.edu.ua/index.php/praci/article/view/245/243 (дата звернення: 15.02.2024).
12. Лужецький В. А. Баришев Ю. В. Методи та засоби паралельного керованого хешування. *Наукові праці Вінницького національного технічного університету*. 2011. Вип. 2. URL : http://praci.vntu.edu.ua/index.php/praci/article/view/257/255 (дата звернення: 15.02.2024).
13. Лужецький В. А., Михалевич В. М., Михалевич О. В., Каплун В. А. Оцінка кількості унікальних лінійних рекурентних послідовностей другого порядку. *Наукові праці Вінницького національного технічного університету*. 2011. Вип. 2. URL : http://praci.vntu.edu.ua/index.php/praci/article/ view/267/265 (дата звернення: 15.02.2024).
14. Голуб С. В., Бабенко В. Г., Рудницький С. В. Метод синтезу операцій криптографічного перетворення на основі додавання за модулем два. *Системи обробки інформації*. 2012. Вип. 3. Т. 1. С. 119–122.

15. Дахно Т. В., Рудницький В. М. Класифікація трьохрозрядних спеціалізованих логічних функцій за складністю реалізації. *Системи обробки інформації.* 2010. С. 39–41.
16. Деменко Є. Є. Дослідження застосування алгоритмів малоресурсної криптографії у децентралізованих середовищах : поясн. записка до кваліф. роботи магістра : спец. 125 – Кібербезпека, освітня програма «Безпека інформаційних і комунікаційних систем». Х. : Харківський національний університет імені В. Н. Каразіна, 2022. 93 с.
17. Деменко Є., Нарєжній О. Дослідження застосування алгоритмів малоресурсної криптографії у децентралізованих середовищах. Х. : Харківський національний університет імені В. Н. Каразіна, 2022. С. 21–29.
18. Дудикевич В. Б., Опірський І. Р. Аналіз моделей захисту інформації в інформаційних мережах держави. *Системи обробки інформації.* 2016. Вип. 4. С. 86–89.
19. Ковальчук І. І., Саркісян Л. Г. Визначення трендів розвитку світового ринку ІКТ під впливом цифровізації. *Вісник студентського наукового товариства Донецького національного університету імені Василя Стуса*. 2019. С. 199–203.
20. Козловська С. Г. Синтез груп двохоперандних операцій криптоперетворення на основі перестановочних схем. *Сучасна спеціальна техніка.* 2018. Вип. 4 (55). С. 44–50.
21. Корецька В. О., Корецький О. В., Шлянчак С. О. Інформаційні технології як сучасна індустрія в світовій економіці. *Телекомунікаційні та інформаційні технології.* 2022. Вип. 2. С. 13–23.
22. Рудницький В. М., Мильчевіч В. Я., Бабенко В. Г. [та ін.]. Криптографічне кодування: методи і засоби реалізації (частина 2) : монографія / Харків : видавець Щедрая усадьба плюс, 2014. 224 с.

23. Рудницький В. М., Півнева С. В., Бабенко В. Г. [та ін.]. Криптографічне кодування: методи і засоби реалізації : монографія / Тольятті : видавець Тольят. держ. ун-т, 2013. 196 с.
24. Криптографічне кодування: обробка та захист інформації : кол. монографія / під ред. В. М. Рудницького. Х. : ДІСА ПЛЮС, 2018. 139 с.
25. Рудницький В. М., Лада Н. В., Бабенко В. Г. Криптографічне кодування: синтез операцій потокового шифрування з точністю до перестановки : монографія / Харків : видавець ДІСА ПЛЮС, 2018. 184 с.
26. Криптографічне кодування : кол. монографія / під ред. В. М. Рудницького, В. Я. Мильчевіча / Харків : видавець Щедрая усадьба плюс, 2014. 240 с.
27. Ларін В. В., Рудницький В. М., Гусак М. Ю. Дослідження сучасних криптографічних систем захисту інформації. *Протидія загрозам з повітря: актуальні питання та шляхи їх вирішення : матеріали Міжнародної науково-практичної конференції, (м. Київ, 2 жовтня 2024 р.)* / ред. П. В. Опенька. 2024. 220 с.
28. Ларін В. В., Рудницький В. М., Підласий Д. А. Оцінка статистичних властивостей результатів шифрування на основі операцій, керованих інформацією. *Наукові праці Державного науково-дослідного інституту випробування і сертифікації озброєння та військової техніки*. 2024. Т. 22. № 4. С. 121–127. DOI : https://doi.org/10.37701/dndivsovt.22.2024.15 (дата звернення: 09.04.2025).
29. Лужецький В. А. Селезньов В. І. Огляд підходів та методів малоресурсного гешування даних. *Вісник Вінницького політехнічного інституту.* 2025. Вип. 6. С. 99–112. URL : https://doi.org/10.31649/1997-9266-2025-183-6-99-112 (дата звернення: 19.01.2026).
30. Миронюк Т. В., Мельник О. Г. Синтез елементарних функцій перестановок, керованих інформацією. *Інформаційні технології в освіті, науці і техніці (ІТОНТ – 2014)* : *тези доповідей II Міжнародної науково-практичної конференції (м. Черкаси, 24–26 квіт. 2014 р.).* Черкаси : ЧДТУ, 2014. Т. 1. С. 147–148.

31. Підласий Д. А. Мультиваріантне представлення СЕТ-операцій на основі елементарних функцій операцій, керованих інформацією. *Сучасні напрями розвитку інформаційно-комунікаційних технологій та засобів управління* : *тези доповідей шістнадцятої міжнародної науково-технічної конференції (м. Баку – Харків – Жиліна, 29–30 квітня 2026 р.)* : зб. наукових праць. Т 3. 2026. С. 14. DOI : https://doi.org/10.32620/ICT.26.t3 (дата звернення: 05.05.2026).

32. Підласий Д. А. Дослідження і синтез елементарних функцій операцій, керованих інформацією / *Технології розвитку безпілотних систем* : кол. монографія. Т. 2. Безекіпажні системи, розд. / [В. Г. Бабенко та ін. ; під ред. В. М. Рудницького]. Черкаси : видавець Третяков О. М., 2025. 207 с. С. 55–90. ISBN 978-617-8725-03-7. DOI : https://doi.org/10.5281/zenodo.19191122 (дата звернення: 28.03.2026).

33. Потій А. В., Орлова С. Ю., Гриненко Т. А. Статистичне тестування генераторів випадкових і псевдовипадкових чисел з використанням набору статистичних тестів NIST STS. URL : www.kiev-security.org.ua (дата звернення: 07.03.2026).

34. Рудницька Ю. В., Короткий Т. К. Інформаційна технологія моделювання та дослідження симетричних СЕТ-операцій. *Проблеми інформатизації : тези доповідей Десятої міжнародної науково-технічної конференції (м. Черкаси – Баку – Бельсько-Бяла – Харків, 24–25 листоп. 2022 р.)*. 2022. Т. 1. С. 40.

35. Рудницький В. М., Ларін В. В., Гусак М. Ю. Проблеми малоресурсного шифрування для управління безпілотними комплексами. *Випробування та сертифікація*. 2024. Вип. 3 (5). С. 64– 69.

36. Рудницький В. М., Ларін В. В. , Підласий Д. А. Дискретно-казуальне моделювання двохоперандних СЕТ-операцій для потокового шифрування. *Новітні технології – для захисту повітряного простору : матеріали XXII міжнародної наукової конференції Харківського національного. університету Повітряних Сил імені Івана Кожедуба (м. Харків, 08–09 квітня 2026 р.)* : зб. наукових праць. 2026. С. 556. URL :

https://hups.mil.gov.ua/wp-content/uploads/admission-university/naukovij_centr/XXI%D0%86_mizhnarodna_naukova_konferencia_KhNUPS_2026_V2.pdf (дата звернення: 15.05.2026).

37. Рудницький В. М., Бабенко В. Г. Модель уніфікованого пристрою криптографічного перетворення інформації. *Системи обробки інформації*. 2009. С. 173–177.
38. Рудницький В. М., Бабенко В. Г. , Рудницький С. В. [та ін.]. Особливості груп несиметричних СЕТ-операцій, синтезованих з точністю до перестановки першого операнда. *Вчені записки ТНУ імені В. І. Вернадського. Серія : Технічні науки.* 2025. Т. 36 (75), вип. 4. С. 265–271.
39. Рудницький В. М., Безменов С. О., Підласий Д. А. Аналіз елементарних функцій операцій, керованих інформацією. *Безпілотна авіація у сучасній збройній боротьбі* : *матеріали науково-практичної конференції інженерно-авіаційного факультету Харківського національного. Університету Повітряних Сил імені Івана Кожедуба. (м. Харків, 7 грудня 2023 року.)* : зб. наукових праць. 2023. С. 25. URL : https://www.hups.mil.gov.ua/assets/doc/science/stud-conf/bpla-hnups-konf.pdf (дата звернення: 16.04.2024).
40. Рудницький В. М., Ларін В. В., Мельник О. Г. Уніфікація опису моделей операцій для СЕТ-шифрування. *Проблеми інформатизації* : *тези доповідей одинадцятої міжнародної науково-технічної конференції (м. Черкаси – Баку – Бельсько-Бяла – Харків, 16–17 листопада 2023 р.).* 2023. Т. 2. С. 36.
41. Рудницький В. М., Ларін В. В., Мельник О. Г., Підласий Д. А. Дискретно-казуальне представлення моделей елементарних функцій і СЕТ-операцій. *Системи управління, навігації та зв'язку.* 2023. № 4. С. 96–101. DOI : https://doi.org/10.26906/SUNZ.2023.4.096 (дата звернення: 15.02.2024).
42. Рудницький В. М., Тарасенко Я. В., Лада Н. В. [та ін.]. Аналіз результатів моделювання СЕТ-операцій на основі елементарних функцій операцій,

керованих інформацією. *Системи та технології (правонаступник наукового журналу «Вісник Академії митної служби України. Серія: Технічні науки»)*. 2025. Вип. 2 (70). С. 258–264.

43. Рудницький В. М., Тишко С. О., Ларін В. В., Піонтківський П. М. Дослідження захищеної системи управління на основі СЕТ-операцій, керованих інформацією. *Випробування і сертифікація озброєння та військової техніки* : *тези доповідей XXV науково-технічної конференції Державного науково-дослідного інституту випробувань і сертифікації озброєння та військової техніки (м. Черкаси, 25 вересня 2025р.*) Черкаси: ДНДІ ВС ОВТ, 2025. С. 360.
44. Рудницький В. М., Бабенко В. Г., Жиляєв Д. А. Алгебраїчна структура множини логічних операцій кодування. *Наука і техніка Повітряних Сил Збройних Сил України*. 2011. Вип. 2 (6). С. 112–114.
45. Рудницький В. М., Бабенко В. Г., Стабецька Т. А. Узагальнений метод синтезу обернених нелінійних операцій розширеного матричного криптографічного перетворення. *Системи обробки інформації* . 2014. Вип. 6 (122). С. 118–121.
46. Рудницький В. М., Миронюк Т. В., Мельник О. Г., Щербина В. П. Синтез елементарних функцій перестановок, керованих інформацією *Безпека інформації*. 2014. Т. 20, вип. 3. С. 242–247.
47. Рудницький В. М., Лада Н. В., Ларін В. В., Підласий Д. А. Дискретно-казуальне моделювання елементарних функцій операцій, керованих інформацією. *Системи управління, навігації та зв'язку.* 2024. С. 139–142. DOI : https://doi.org/10.26906/SUNZ.2024.4.139 (дата звернення: 11.02.2025).
48. Рудницький В. М. , Лада Н. В., Підласий Д. А., Мельник О. Г. Синтез дискретно-алгебраїчних моделей елементарних функцій операцій, керованих інформацією. Кібербезпека: освіта, наука, техніка. 2024. Т. 3, вип. 23. С. 6–16. DOI : https://doi.org/ 10.28925/2663-4023.2024.23.616 (дата звернення: 25.06.2025).

49. Сучасні інформаційні технології в кібербезпеці : монографія / Довбиш А. С. , Ободяк В. К., Шелехов І. В. [та ін.] ; за ред. В. К. Ободяка, І. В. Шелехова. 2021. 348 с.
50. Технології розвитку безпілотних систем : кол. монографія / під ред. В. М. Рудницького. Т. 1. Малоресурсний захист інформації в безпілотних системах. Черкаси : видавець Вовчок О. Ю., 2025. 324 с. ISBN 978-617-7508-50-1.
51. Технології розвитку безпілотних систем : кол. монографія / під ред. В. М. Рудницького. Т. 2. Безекіпажні системи. Черкаси : видавець Третяков О. М., 2025. 208 с. ISBN 978-617-8725-03-7.
52. Рудницький, В. М., Тарасенко, Я. В., Лада, Н. В., Бабенко, В. Г., & Підласий, Д. А. (2025). АНАЛІЗ РЕЗУЛЬТАТІВ МОДЕЛЮВАННЯ СЕТ-ОПЕРАЦІЙ НА ОСНОВІ ЕЛЕМЕНТАРНИХ ФУНКЦІЙ ОПЕРАЦІЙ КЕРОВАНИХ ІНФОРМАЦІЄЮ. *Системи та технології*, *70*(2), 258-263. DOI: https://doi.org/10.32782/2521-6643-2025-2-70.29 (дата звернення: 11.01.2026).
53. Lada N. V. [et al.]. Analyzing a group of two-operand symmetric cryptographic transformation operations. *Problems of Informatization* : *Proceedings of the 7th International Scientific and Technical Conference (Cherkasy – Kharkiv – Baku – Bielsko-Biala, 13–15 November, 2019).* Cherkasy : Cherkasy State Technological University; Baku : Military Academy of the Armed Forces of the Republic of Azerbaijan, Bielsko-Biała : Academy of Technology and Humanities, Kharkiv : National Technical University “Kharkiv Polytechnic Institute”. 2019. Vol. 1. P. 85.
54. Rudnytskyi V. M. [et al.]. Constructing symmetric operations of cryptographic information encoding. *Workshop on Cybersecurity Providing in Information and Telecommunication Systems (CPITS II 2021).* Kyiv, Ukraine : CEUR Workshop Proceedings, 2022. Vol. 3187. P. 182–194. ISSN 1613-0073.

55. Rudnytskyi V. M. [et al.]. Construction of two-digit two-operand operations of strict and stable cryptographic coding. *Control, Navigation and Communication Systems.* 2018. Vol. 6, no. 52. P. 113–115.
56. Rudnytskyi V. M. [et al.]. Cryptographic encoding in modern symmetric and asymmetric encryption. *26th International Conference on Knowledge-Based and Intelligent Information & Engineering* Systems *(KES 2022). Procedia Computer Science.* 2022. Vol. 207. P. 54–63.
57. Rudnytskyi V. M. [et al.]. Current state and prospects for the development of CET-encryption. *Military Innovation in Contemporary Warfare* : *Abstracts'collection*. Kyiv, 18–19 April , 2024.
58. V. Rudnytskyi, N. Lada, V. Larin, D. Holovniak, H. Haponenko, D. Pidlasyi and T. Stabetska. Discrete and casual modeling of CET-operations of data-controlled permutations. *Journal of Xidian University.* 2024. Vol. 18, iss. 6. P. 747–767. URL : https://drive.google.com/file/d/1iYOUKC7OuDlVXW81GDrhx09VkM9dQZz_/view (дата звернення: 08.02.2025).
59. Rudnytskyi V. M. [et al.]. Features of modeling two-operand operations of cryptographic transformation of information. *Unmanned Aircraft in the Modern Armed Struggle* : *Proceedings of the Scientific and Practical Conference (Kharkiv, 7 December, 2023).* Kharkiv : Ivan Kozhedub Kharkiv National Air Force University, 2023. P. 45.
60. Rudnytskyi V. M. [et al.]. Increasing the cryptographic strength of CET-encryption by ensuring the transformation quality of the information block. *13th International Conference on Dependable Systems, Services and Technologies (DESSERT).* Athens, Greece, 2023. P. 1–6.
61. V. Rudnytskyi, N. Lada, V. Larin, V. Tkachenko, T. Korotkyi, D. Pidlasyi and D. Tarasenko. Information system for modeling and research of pseudorandom sequences of CET-operations for post quantum stream encryption. *Journal of Xidian University.* 2024. Vol. 18, iss. 7. P. 1284–

1298. DOI : https://doi.org/10.5281/Zenodo.13096683 (дата звернення: 09.02.2025).

62. Holovniak D. V., Sapozhnikov S. K., Lada N. V., Mechanisms of practical implementation of asymmetric two-operand CET-operations. *Problems of Informatization : Proceedings of the 11th International Scientific and Technical Conference (Baku – Kharkiv – Bielsko-Biala, 16–17 November, 2023).* Baku : Military Academy of the Armed Forces of the Republic of Azerbaijan, Bielsko-Biala : Academy of Technology and Humanities, Kharkiv : National Technical University “Kharkiv Polytechnic Institute”, 2023. Vol. 2, sect. 3, 6. P. 34.
63. Lada N. V., Kozlovska S. G. Applying cryptographic addition operations by module two with accuracy of permutation in stream ciphers.*Control, Navigation and Communication Systems*. 2018. Vol. 1, №. 47. P. 127–130.
64. 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.* 2022. Vol. 2, «. 20. P. 35–43.
65. Lada N. V., Kozlovska S. G. Synthesis and analysis of permutation schemes for constructing two-operand cryptographic transformation operations. *Problems of Informatization : Proceedings of the 6th International Scientific and Technical Conference (Cherkasy – Baku – Bielsko-Biala – Kharkiv, 14–16 November, 2018).* Cherkasy : Cherkasy State Technological University; Baku : Military Academy of the Armed Forces of the Republic of Azerbaijan, Bielsko-Biała : Academy of Technology and Humanities, Kharkiv : National Technical University “Kharkiv Polytechnic Institute”, 2018. P. 11.
66. Lada N. V., Rudnytska Yu. V. Classifying groups of asymmetric two-operand operations of information cryptographic transformation basing on permutation schemes of their synthesis. *Problems of Informatization : : Proceedings of the 6th International Scientific and Technical Conference (Cherkasy – Baku – Bielsko-Biala – Kharkiv, 14–16 November, 2018).* Cherkasy : Cherkasy State Technological University; Baku : Military Academy of the Armed Forces of the

Republic of Azerbaijan, Bielsko-Biała : Academy of Technology and Humanities, Kharkiv : National Technical University “Kharkiv Polytechnic Institute”, 2018. P. 11.

67. V. Rudnytskyi1, V. Babenko, N. Lada, T. Stabetska, D. Pidlasyi, L. Parkhuts. Modeling of a cryptographic network based on application of CET-operations. *Workshop on Cyber Security and Data Protection II, CSDP-II.* Lviv, 2025. Vol. 4042. P. 64–79. URL : https://ceur-ws.org/Vol-4042/paper5.pdf (дата звернення: 15.02.2026).
68. V. Rudnytskyi, N. Lada, V. Babenko, H. Kuchuk, D. Pidlasyi, D. Kamak and Ye. Ivashchenko. Modeling of groups of dual-cycle non-commutative two-operand CET-operations. *Journal of Xidian University.* 2024. Vol. 18, iss. 10. P. 916–958. DOI : https://doi.org/10.5281/Zenodo.13992956 (дата звернення: 11.02.2025).
69. Rudnytskyi V. M. [et al.]. Modeling relationships in non-commutative two-operand two-bit CET-operations of a double cycle when permuting the operands. *Technology Audit and Production Reserves*. 2024. Vol. 3, №. 2 (77). P. 30–35.
70. Prokopenko T. A., Rudnytska Yu. V. Automation of design of crypto primitives. *Problems of Informatization* : *Proceedings of the 9th International Scientific and Technical Conference (Cherkasy – Kharkiv – Baku – Bielsko-Biala, 16–18 November, 2021).* Cherkasy : Cherkasy State Technological University; Baku : Military Academy of the Armed Forces of the Republic of Azerbaijan; Bielsko-Biała : Academy of Technology and Humanities; Kharkiv : National Technical University “Kharkiv Polytechnic Institute”, 2021. Vol. 1. P. 85.
71. Rudnytska Yu. V., Korotkyi T. K. Information technology of modeling and research of symmetric SET-operations. Problems of Informatization : *Proceedings of the 10th International Scientific and Technical Conference (Cherkasy – Baku – Bielsko-Biala – Kharkiv, 24–25 November, 2022).* Cherkasy : Cherkasy State Technological University; Baku : Military Academy of the Armed Forces of the Republic of Azerbaijan; Bielsko-Biała : Academy of

Technology and Humanities; Kharkiv : National Technical University “Kharkiv Polytechnic Institute”, 2022. Vol. 1. P. 40.

72. Rudnytska Yu. V., Rudnytskyi S. V. Simulation of symmetric cryptographic encoding operations. *Problems of Informatization* : *Proceedings of the 10th International Scientific and Technical Conference (Cherkasy – Baku – Bielsko-Biala – Kharkiv, 24–25 November, 2022).* Cherkasy : Cherkasy State Technological University; Baku : Military Academy of the Armed Forces of the Republic of Azerbaijan; Bielsko-Biała : Academy of Technology and Humanities; Kharkiv : National Technical University “Kharkiv Polytechnic Institute”, 2022. Vol. 2. P. 10.

73. Rudnytskyi V. M., Lada N. V., Lada S. V. Investigating the sets of asymmetric two-operand operations with double transformation cycle. *Sensors, devices and systems* : *Proceedings of the 9th International Scientific and Technical Conference (Cherkasy – Kherson – Lazurne, 2021).* 2021 P. 78–80.

74. Rudnytskyi V. M., Lada N. V., Melnyk O. G. Classification of CET operations *Problems of Informatization* : *Proceedings of the 11th International Scientific and Technical Conference (Baku – Kharkiv – Bielsko-Biala, 16–17 November, 2023.).* Baku : Military Academy of the Armed Forces of the Republic of Azerbaijan; Bielsko-Biała : Academy of Technology and Humanities; Kharkiv : National Technical University “Kharkiv Polytechnic Institute”, 2023. Vol. 2, sect. 3, 6. P. 35.

75. Rudnytskyi V. M., Lada N. V., Lada S. V. Analyzing the methods of cryptographic coding operations synthesis for constructing groups of asymmetric two-operand double-cycle operations. *Problems of Informatization* : *Proceedings of the 9th International Scientific and Technical Conference (Cherkasy – Kharkiv – Baku – Bielsko-Biala, 18–19 November, 2021).* Cherkasy : Cherkasy State Technological University; Baku : Military Academy of the Armed Forces of the Republic of Azerbaijan, Bielsko-Biała : Academy of Technology and Humanities, Kharkiv : National Technical University “Kharkiv Polytechnic Institute”, 2021. Vol. 1. P. 80.

76. Rudnytskyi V. M., Larin V. V., Melnyk O. G. Unification of the description of operation models for CET-encryption. *Problems of Informatization* : *Proceedings of the 11th International Scientific and Technical Conference, Baku – Kharkiv – Bielsko-Biala, 16–17 November, 2023).* Baku : Military Academy of the Armed Forces of the Republic of Azerbaijan, Bielsko-Biala : Academy of Technology and Humanities, Kharkiv : National Technical University “Kharkiv Polytechnic Institute”, 2023. Vol. 2, sections 3, 6. P. 36.
77. Rudnytskyi V., Lada N., Dashkovskyi V. Protection of the information network of a medical institution. *Medical and Technical Cooperation for the Sake of Victory: Current Tasks of Medical, Biological Physics and Informatics : Proceedings of the 3rd All-Ukrainian Scientific and Practical Conference with International Participation (Vinnytsya, 5–6 April, 2024).* Vinnytsya, National Pirogov Memorial Medical University. 2024. P. 140–141.
78. Rudnytskyi V. M., Pidlasyi D. A. [et al.]. Synthesis of discrete and algebraic models of elementary functions of data-controlled operations. *Cybersecurity: Education, Science, Technique.* 2024. Vol. 3. P. 6–16.
79. V. Rudnytskyi, N. Lada, V. Larin, O. Melnyk, T. Stebetska, T. Korotkyi, D. Pidlasyi. Usage of non-commutative two-operand CET-operations in limited resources stream ciphers. *Journal of Xidian University*. 2024. Vol. 18, iss. 5. P. 1105–1120. DOI : https://doi.org/10.5281/Zenodo.11253625 (дата звернення: 03.06.2025).
80. ISO/IEC 29192-1:2019. Information Technology – Security Techniques – Lightweight Cryptography. Part 1: General. 2012.
81. ISO/IEC 29192-2:2019. Information Technology – Security Techniques – Lightweight Cryptography. Part 2: Block Ciphers. 2012.
82. ISO/IEC 29192-3:2019. Information Technology – Security Techniques – Lightweight Cryptography. Part 3: Stream Ciphers. 2012.
83. Hatzivasilis G. [et al.]. A review of lightweight block ciphers. *Journal of Cryptographic Engineering.* 2018. Vol. 8, no. 2. P. 141–184.

84. Manifavas Ch. [et al.]. A survey of lightweight stream ciphers for embedded systems. *Security and Communication Networks.* 2016. Vol. 9, no. 10. P. 1226–1246.

85. Mileva A., Dimitrova V., Kara O., Mihaljević M. J. Catalog and illustrative examples of lightweight cryptographic primitives. *Security of Ubiquitous Computing Systems Selected Topics.* Cham : Springer Int. Publishing, 2021. P. 21–49. ISBN 978-3-030-10590-7.

86. Amy Demetra Geae Vennos. Security of lightweight cryptographic primitives : Ph.D. Dissertation. Virginia Tech., 2021.

87. 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 (дата звернення: 01.06.2024).

88. Gupta B. B., Quamara M. An overview of Internet of Things (IoT): Architectural aspects, challenges, and protocols. *Concurrency and Computation*: Practice and Experience. 2020. Vol. 32, sect. 21.

89. Ekwueme C. P. , Adam I. H., Dwivedi A. [et al.]. Lightweight cryptography for Internet of Things: A review. *EAI Endorsed Transactions on Internet of Things.* 2024. Vol. 10, sect. 1. P. 1–9.

90. Pei C., Xiao Y., Han X. Trade-off of security and performance of lightweight block ciphers in Industrial Wireless Sensor Networks. *EURASIP Journal on Wireless Communications and Networking.* 2018. Vol. 1. P. 117. URL : https://doi.org/10.1186/s13638-018-1121-6 (дата звернення: 03.06.2024).

91. Huang C. AquaMZ: New lightweight authenticated encryption with generalized feistel network based primitive for IoT protocols. *Proceedings of the 2022 6th International Conference on Computer Science and Artificial Intelligence.* 2022. P. 327–332.

92. Eisenbarth T. [et al.]. Compact implementation and performance evaluation of block ciphers in ATtiny devices. *AFRICACRYPT*. 2012. P. 172–187.

93. CRYPTREC Cryptographic Technology Guideline - Lightweight Cryptography - 2023 Edition. CRYPTREC Lightweight Cryptography Working Group. 2023. 112 p.

94. Diehl W., Farahmand F., Yalla P. [et al.]. Comparison of hardware and software implementations of selected lightweight block ciphers. *27th International Conference on Field Programmable Logic and Applications (FPL).* Ghent, Belgium, 2017. P. 1–4. URL : https://doi.org/10.23919/FPL.2017.8056808 (дата звернення: 07.07.2024).

95. Dutta I. K., Ghosh B., Bayoumi M. Lightweight cryptography for internet of insecure things: A survey. *Proceedings of the 2019 IEEE 9th Annual Computing and Communication Workshop and Conference (CCWC).* Las Vegas, NV, USA, 2019. P. 475–481. URL : https://doi.org/10.1109/CCWC.2019.8666557 (дата звернення: 07.07.2024).

96. Xia Y., Teng C., Zeng Z. [et al.]. Energy-efficient cache content placement strategy for electric Internet of Things. *Wireless Networks.* 2026. URL : https://doi.org/10.1007/s11276-026-04138-y (дата звернення: 29.06.2024).

97. Bucci M., Giancane L., Luzzi R. [et al.]. Enhancing power analysis attacks against cryptographic devices. *IET Circuits, Devices & Systems*. 2008. Vol. 2, no. 3. P. 298–305.

98. Berger T. P. [et al.]. Extended generalized feistel networks using matrix representation to propose a new lightweight block cipher: Lilliput. *IEEE Transactions on Computers*. 2016. Vol. 65, no. 7. P. 2074–2089.

99. Dinu D.-D., Biryukov A., Großschädl J. [et al.]. FELICS – fair evaluation of lightweight cryptographic systems. *NIST Workshop on Lightweight Cryptography 2015*. National Institute of Standards and Technology (NIST), 2015.

100. Engels D., Fan X., Gong G. [et al.]. Hummingbird: ultra-lightweight cryptography for resource-constrained devices. *Financial Cryptography and Data Security (FC 2010).* Springer, 2010. Vol. 6054. P. 3–18.

101. Rahman Nazil A. [et al.]. Information technology perspective on business. *International Journal for Multidisciplinary Research*. 2026. Vol. 7. P. 1–14. URL : https://doi.org/10.36948/ijfmr.2025.v07i04.53765. (дата звернення: 25.05.2026).

102. Gubbi J. [et al.]. Internet of Things (IoT): A vision, architectural elements, and future directions. *Future Generation Computer Systems*. 2013. Vol. 29. P. 1645–1660.

103. Xia F. [et al.]. Internet of Things. *International Journal of Communication Systems.* 2012. Vol. 25. P. 1101–1102.

104. Bothos J. M. A., Vlachos V. Cybersecurity vulnerability and risk of industrial control systems / A Hybrid Threats, Cyberterrorism and Cyberwarfare / ed by M. A. Ferrag [et al.]. Boca Raton : CRC Press, 2023. P. 148–165.

105. Journault A. , Standaert F., Varici K. Improving the security and efficiency of block ciphers based on ls-designs. *Designs, Codes and Cryptography*. 2017. Vol. 82, no. 1–2. P. 495–509.

106. Kiernan B. G. Analysis of lightweight cryptographic primitives : Ph.D. Dissertation. Kiernan Virginia Tech., 2021.

107. Diedrich L., Murati L. , Wiesmaier A. Stream ciphers in the IoT: Grain and Trivium. *First Workshop on Security and Privacy for Internet of Things and Cyber-Physical Systems (SPIC'15).* 2015. P. 1–19.

108. Hasan M. K. [et al.] Lightweight cryptographic algorithms for guessing attack protection in complex Internet of Things applications. *Complexity*. 2021. Vol. 1. 13 p.

109. 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.

110. Ammar M. Russello G., Crispo B. Internet of things: A survey on the security of IoT frameworks. *Journal of Information Security and Applications.* 2018. Vol. 38, sect. 2. P. 8–27.

111. Rana M., Mamun Q., Islam R. Lightweight cryptography in IoT networks: A survey. *Future Generation Computer Systems*. 2022. Vol. 129. P. 77–89.

112. Meng Th. X., Buchanan W. Lightweight cryptographic algorithms on resource-constrained devices. 2020. 42 p. (Preprints).

113. Banik S. [et al.]. Midori: A block cipher for low energy. Advances in cryptology. A*dvances in Cryptology – ASIACRYPT 2015 :* Proceedings of the 21st Int. Conf. 2015. Part II, vol. 9453. P. 411–436.

114. Mohammad Shah I. N. [et al.]. Modified generalized feistel network block cipher for the Internet of Things. *Symmetry*. 2023. Vol. 15, no. 4. P. 900.

115. Moradi A., Poschmann A. , Ling S. [et al.]. Pushing the limits: A very compact and a threshold implementation of AES / *Advances in Cryptology – EUROCRYPT*, May 15–19, 2011 / ed. by K. G. Paterson. Tallinn, Estonia : Springer, 2011. Vol. 6632. P. 69–88.

116. Boesgaard M. , Vesterager M. , Pedersen T. [et al.]. Rabbit: A new high-performance stream cipher. *Fast Software Encryption (FSE 2003)*, Febr. 24–26, 2003 / ed. by T. Johansson. Lund, Sweden : Springer, 2003. Vol. 2887. P. 307–329.

117. Garg Seema R. Role of artificial intelligence in stock market: A literature review. *Conference: Role of Multidisciplinary and Technology-Led Approach: An Inch Closer of Attainment of Viksit Bharat 2047*. Landran, Mohali : Chandigarh Business School of Administration, 2026. P. 230–236.

118. McKay K. [et al.]. Report on lightweight cryptography : Technical report. National Institute of Standards and Technology, 2016. 21 p. URL : https://doi.org/10.6028/NIST.IR.8114 (дата звернення: 15.09.2024).

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

120. Jia X. [et al.]. RFID technology and its applications in Internet of Things (IoT). *2nd International Conference on Consumer Electronics, Communications and Networks (CECNet)*. Yichang, China, 2012. P. 1282–

1285. URL : https://doi.org/10.1109/CECNet.2012.6201508 (дата звернення: 29.09.2024).

121. 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, no. 3. P. 365–403.

122. Ruijia Z., Wenling L., Xuemei Z. The impact of Information and Communication Technology (ICT) on learning outcomes in early childhood and primary education: A meta-analysis of moderating factors. *Frontiers in Psychology*. 2025. Vol. 16. P. 297–315. URL : https://doi.org/10.1007/978-3-032-09098-0_15.

123. Awang A. [et al.]. Security in the Internet of Things: A review. *IEEE Access*. 2022. Vol. 10. P. 649–670. URL : https://doi.org/10.1109/ACCESS.2022.3209355 (дата звернення: 30.11.2024).

124. Shannon C. Communication theory of secrecy systems. *Bell System Technical Journal*. 1949. Vol. 28, no. 4. P. 656–715.

125. Singh S. The code book: The secret history of codes and code-breaking. HarperCollins Publishers, 2011. 402 p.

126. Stein A. Digitalization in agricultural production. *Bioeconomy. Advancing the Transition to a Sustainable, Biobased Economy*. Second Ed. / ed. by I. Lewandowski, L. Mayorga-Duarte, P. Scheurich [et al.]. Cham : Springer, 2026. P. 297–315.

ДОДАТОК А
Опис пакету статичних тестів NIST STS

№	Назва статистичного тесту	Статистика тесту c(S)	Дефект, що виявляється у тесті
1.	Частотний або монобітний тест.	Нормалізована абсолютна сума значень елементів послідовності.	Досить велика кількість нулів або одиниць у згенерованій послідовності.
2.	Частотний тест в середині блоку.	Міра узгодженості одиниць, що виявляються в ході тесту із теоретичним сподіванням.	Відхилення частоти появи одиниць у блоці (локальне) від ідеального значення $1/2$.
3.	Перевірка накопичених сум.	Максимальне відхилення значень накопиченої суми елементів послідовності від початкової точки відліку .	Велика кількість одиниць або нулів на початку, чи в кінці послідовності.
4.	Перевірка серій.	Загальна кількість серій на всій послідовності.	Занадто швидка або повільна зміна знаку під час генерації досліджуваної послідовності.
5.	Перевірка максимальної довжини серії в блоці.	Міра узгодження значень максимальної довжини, що виявляються в ході тесту із теоретичним сподіванням.	Відхилення від теоретичного закону розподілу максимальної довжини серій одиниць.
6.	Перевірка рангу двійкової матриці.	Міра узгодження значень рангів різноманітних порядків, що виявляються в ході тесту із теоретичним сподіванням.	Відхилення емпіричного закону розподілу рангів матриць від теоретичного, що вказує на залежність елементів згенерованої послідовності.
7.	Спектральний аналіз на основі дискретного перетворення Фур'є.	Нормалізована різниця кількості частотних компонент, що виявляються із теоретичним сподіванням за умови перевищення граничного рівня 95%.	Виявлення трендів у двійковій послідовності.
8.	Перевірка шаблонів, які перекриваються.	Міра узгодженості кількості шаблонів, що перекриваються у ході виконання тесту із теоретичними значеннями	Велика кількість m-бітових серій одиниць у послідовності.
9.	Універсальний тест Маурера.	Сума логарифма відстаней між l-бітними шаблонами.	Можливість стиснення послідовності.
10.	Ентропійний тест.	Міра узгодженості значення джерела ентропії, що отримується в ході виконання тесту із таким, що теоретично очікується від випадкового.	Нерівномірність розподілу m-бітових слів у послідовності (регулярність властивостей джерела).
11.	Перевірка випадкових відхилень.	Міра узгодженості спостережуваної кількості візитів при випадковому блуканні у заданий стан в середині циклу із тим, що теоретично очікується.	Відхилення від теоретичного закону розподілу візитів в конкретний стан при випадковому блуканні.
12.	Перевірка випадкових відхилень.	Загальна кількість візитів при випадковому блуканні.	Відхилення від теоретично очікуваної кількості загальної кількості візитів при випадковому блуканні в заданий стан.
13.	Послідовний тест.	Міра узгодженості кількості всіх варіантів m-бітових шаблонів, які спостерігаються в ході виконання із тою кількістю, що очікується теоретично.	Нерівномірність розподілу m-бітових слів у послідовності.
14.	Перевірка стискання згідно алгоритму Лемпеля-Зіва.	Кількість різних слів у послідовності.	Велика ступінь стискання послідовності, що проходить тестування, у порівнянні із ступенем стискання, що теоретично очікується від випадкової послідовності.
15.	Перевірка шаблонів, що не перекриваються.	Міра узгодженості кількості неперіодичних шаблонів у послідовності, що проходить тест із теоретичним значенням.	Велика кількість заданих у послідовності неперіодичних шаблонів.
16.	Перевірка лінійної складності.	Міра узгодженості спостережуваної послідовності кількості подій, котрі полягають у появі фіксованої довжини еквівалентного ЛРР для заданого блока з теоретичним.	На недостатню складність тестованої послідовності вказує відхилення емпіричного розподілу довжин еквівалентних ЛРР послідовностей фіксованої довжини від теоретичного закону розподілу випадкової послідовності.

ДОДАТОК Б

РЕЗУЛЬТАТИ ТЕСТУВАННЯ ШИФРОГРАМ

ЗА ДОПОМОГОЮ ПАКЕТУ NIST STS

RESULTS FOR THE UNIFORMITY OF P-VALUES AND THE PROPORTION OF PASSING SEQUENCES

generator is < <Ris_4_8.bin>>

C1	C2	C3	C4	C5	C6	C7	C8	C9	C10	P-VALUE	PROPORTION	STATISTICAL TEST
6	11	6	11	12	9	13	9	11	12	0.798139	1.0000	Frequency
10	6	10	13	7	10	10	13	7	14	0.657933	0.9900	BlockFrequency
7	9	10	14	6	10	7	11	16	10	0.455937	1.0000	CumulativeSums
8	7	4	10	12	8	13	17	12	9	0.213309	1.0000	CumulativeSums
10	13	5	5	12	19	9	11	9	7	0.075719	0.9900	Runs
21	9	9	7	10	3	11	9	13	8	0.020548	0.9700	LongestRun
15	11	14	9	4	10	11	8	5	13	0.224821	0.9700	Rank
5	6	8	6	10	9	13	15	17	11	0.102526	1.0000	FFT
11	10	11	10	11	11	17	8	7	4	0.334538	0.9800	NonOverlappingTemplate
9	7	8	13	7	12	12	11	11	10	0.897763	1.0000	NonOverlappingTemplate
10	8	8	10	7	13	12	12	11	9	0.935716	0.9700	NonOverlappingTemplate
8	9	13	9	11	12	13	11	10	4	0.678686	0.9800	NonOverlappingTemplate
7	12	15	13	7	9	13	2	11	11	0.153763	0.9900	NonOverlappingTemplate
11	8	11	10	8	14	6	9	10	13	0.816537	0.9900	NonOverlappingTemplate
13	7	9	12	8	11	10	8	9	13	0.897763	0.9900	NonOverlappingTemplate
6	20	5	8	7	8	9	14	14	9	0.023545	1.0000	NonOverlappingTemplate
11	11	6	6	9	11	12	8	14	12	0.699313	1.0000	NonOverlappingTemplate
8	8	13	11	18	8	6	6	11	11	0.213309	1.0000	NonOverlappingTemplate
8	10	12	11	10	4	10	18	6	11	0.181557	0.9700	NonOverlappingTemplate
10	8	11	12	13	9	10	9	9	9	0.987896	1.0000	NonOverlappingTemplate
13	15	8	13	10	9	8	7	8	9	0.678686	1.0000	NonOverlappingTemplate
7	11	8	8	8	13	6	10	18	11	0.262249	1.0000	NonOverlappingTemplate
8	17	14	13	9	8	9	6	3	13	0.071177	1.0000	NonOverlappingTemplate
10	9	9	9	15	13	7	8	10	10	0.834308	1.0000	NonOverlappingTemplate
8	13	8	10	8	10	10	9	12	12	0.964295	0.9800	NonOverlappingTemplate
12	9	12	7	5	12	11	6	18	8	0.153763	0.9900	NonOverlappingTemplate
12	13	13	10	10	4	7	7	14	10	0.419021	0.9900	NonOverlappingTemplate
9	6	12	9	18	8	8	7	9	14	0.213309	1.0000	NonOverlappingTemplate
8	14	11	12	9	10	3	11	10	12	0.534146	0.9800	NonOverlappingTemplate
11	10	10	12	11	13	4	9	13	7	0.637119	0.9900	NonOverlappingTemplate
8	9	6	8	21	4	12	11	9	12	0.023545	0.9900	NonOverlappingTemplate
13	11	13	8	14	6	4	3	13	15	0.042808	1.0000	NonOverlappingTemplate
10	11	14	7	10	10	12	10	7	9	0.911413	0.9900	NonOverlappingTemplate
9	8	11	6	10	12	10	12	9	13	0.911413	1.0000	NonOverlappingTemplate
13	8	8	7	10	11	7	12	16	8	0.534146	0.9900	NonOverlappingTemplate
9	8	12	9	9	16	7	11	10	9	0.759756	0.9900	NonOverlappingTemplate
12	10	11	7	9	9	6	21	8	7	0.055361	0.9900	NonOverlappingTemplate
8	7	10	15	8	11	8	10	11	12	0.816537	1.0000	NonOverlappingTemplate
13	5	11	12	7	9	6	15	10	12	0.401199	1.0000	NonOverlappingTemplate
9	8	14	11	7	13	10	11	13	4	0.474986	0.9700	NonOverlappingTemplate
13	8	11	9	9	7	5	16	11	11	0.455937	0.9900	NonOverlappingTemplate
7	11	15	9	11	8	14	7	8	10	0.637119	1.0000	NonOverlappingTemplate
13	16	11	7	11	7	3	9	9	14	0.153763	0.9800	NonOverlappingTemplate
10	15	9	7	9	11	14	9	7	9	0.699313	1.0000	NonOverlappingTemplate
10	10	11	7	7	15	16	6	11	7	0.304126	1.0000	NonOverlappingTemplate
9	11	9	15	13	9	4	6	14	10	0.304126	0.9800	NonOverlappingTemplate
15	10	11	13	9	7	10	6	12	7	0.595549	0.9900	NonOverlappingTemplate
4	12	9	11	8	17	8	12	15	4	0.058984	1.0000	NonOverlappingTemplate
9	6	13	11	8	5	10	12	17	9	0.275709	1.0000	NonOverlappingTemplate
12	8	7	11	10	7	13	12	10	10	0.911413	0.9800	NonOverlappingTemplate
11	10	9	11	11	10	4	13	9	12	0.798139	0.9800	NonOverlappingTemplate
11	12	6	9	11	6	14	12	9	10	0.739918	0.9800	NonOverlappingTemplate
12	12	7	14	6	8	7	13	15	6	0.262249	0.9900	NonOverlappingTemplate
10	9	8	13	16	8	6	7	17	6	0.108791	0.9800	NonOverlappingTemplate
7	8	12	11	10	14	6	9	9	14	0.657933	0.9700	NonOverlappingTemplate
13	11	13	10	7	10	8	12	7	9	0.867692	0.9900	NonOverlappingTemplate
13	9	11	9	10	8	8	9	11	12	0.978072	0.9800	NonOverlappingTemplate
6	17	13	12	11	10	6	9	4	12	0.137282	0.9900	NonOverlappingTemplate
6	9	12	12	15	14	9	6	10	7	0.419021	0.9900	NonOverlappingTemplate
10	9	12	14	6	8	10	11	10	10	0.897763	1.0000	NonOverlappingTemplate
10	8	8	8	9	7	16	16	10	8	0.366918	0.9900	NonOverlappingTemplate
13	11	6	12	12	4	13	9	10	10	0.534146	0.9900	NonOverlappingTemplate

9	17	7	11	8	12	12	9	7	8	0.474986	0.9800	NonOverlappingTemplate
10	9	6	8	15	15	12	6	8	11	0.383827	1.0000	NonOverlappingTemplate
10	13	9	6	9	10	10	11	10	12	0.955835	0.9800	NonOverlappingTemplate
7	13	12	12	8	8	8	18	5	9	0.171867	0.9800	NonOverlappingTemplate
10	9	9	12	7	12	12	5	13	11	0.759756	0.9900	NonOverlappingTemplate
11	17	8	7	17	11	6	4	7	12	0.037566	1.0000	NonOverlappingTemplate
10	7	8	9	12	13	8	16	12	5	0.383827	0.9900	NonOverlappingTemplate
17	15	10	11	10	5	4	5	10	13	0.048716	0.9800	NonOverlappingTemplate
7	17	4	14	6	12	9	16	7	8	0.035174	1.0000	NonOverlappingTemplate
5	8	13	9	11	9	15	10	13	7	0.494392	1.0000	NonOverlappingTemplate
10	12	10	9	10	14	11	9	7	8	0.935716	0.9900	NonOverlappingTemplate
12	4	13	12	11	8	9	14	8	9	0.534146	0.9900	NonOverlappingTemplate
13	11	7	13	12	9	11	7	11	6	0.739918	0.9900	NonOverlappingTemplate
8	17	9	13	8	13	6	13	6	7	0.181557	1.0000	NonOverlappingTemplate
14	9	8	11	12	18	7	7	8	6	0.171867	0.9700	NonOverlappingTemplate
8	9	14	9	9	11	9	13	13	5	0.657933	0.9900	NonOverlappingTemplate
10	10	11	10	16	9	10	9	10	5	0.699313	0.9800	NonOverlappingTemplate
14	8	9	11	9	10	10	4	10	15	0.494392	0.9900	NonOverlappingTemplate
12	7	11	11	14	9	9	8	9	10	0.924076	0.9900	NonOverlappingTemplate
5	11	8	12	12	12	9	5	16	10	0.319084	0.9800	NonOverlappingTemplate
11	10	11	10	11	12	16	8	7	4	0.419021	0.9800	NonOverlappingTemplate
6	7	12	15	12	11	13	6	6	12	0.319084	1.0000	NonOverlappingTemplate
9	12	18	13	7	8	7	4	10	12	0.122325	0.9900	NonOverlappingTemplate
8	14	12	10	15	9	7	12	6	7	0.455937	0.9900	NonOverlappingTemplate
12	10	11	6	4	15	13	13	9	7	0.275709	1.0000	NonOverlappingTemplate
16	5	6	12	9	9	11	12	8	12	0.383827	0.9800	NonOverlappingTemplate
11	9	7	12	9	5	12	11	12	12	0.798139	0.9900	NonOverlappingTemplate
15	10	9	10	12	11	8	7	9	9	0.867692	1.0000	NonOverlappingTemplate
10	11	8	9	13	7	10	14	9	9	0.897763	0.9800	NonOverlappingTemplate
12	14	7	8	11	11	6	13	11	7	0.637119	0.9900	NonOverlappingTemplate
5	11	10	14	13	8	10	9	11	9	0.759756	0.9900	NonOverlappingTemplate
13	10	18	7	4	9	10	7	16	6	0.035174	0.9900	NonOverlappingTemplate
9	8	14	14	3	10	8	14	13	7	0.191687	0.9800	NonOverlappingTemplate
19	9	10	6	8	11	10	13	8	6	0.153763	1.0000	NonOverlappingTemplate
9	11	8	5	9	9	12	12	14	11	0.759756	1.0000	NonOverlappingTemplate
10	15	7	10	8	8	12	14	6	10	0.554420	0.9900	NonOverlappingTemplate
8	1	12	15	9	13	9	10	7	16	0.048716	1.0000	NonOverlappingTemplate
9	9	13	11	10	13	6	8	8	13	0.798139	0.9900	NonOverlappingTemplate
10	9	7	16	6	10	13	11	8	10	0.574903	1.0000	NonOverlappingTemplate
8	8	9	11	9	11	12	11	13	8	0.964295	1.0000	NonOverlappingTemplate
8	8	10	8	14	8	10	10	5	19	0.129620	0.9900	NonOverlappingTemplate
13	11	6	10	9	14	6	10	11	10	0.739918	0.9800	NonOverlappingTemplate
9	8	10	9	5	9	10	19	8	13	0.181557	0.9800	NonOverlappingTemplate
10	10	8	9	6	13	12	13	8	11	0.851383	1.0000	NonOverlappingTemplate
16	4	8	10	10	6	7	12	14	13	0.162606	0.9800	NonOverlappingTemplate
11	15	5	12	5	9	8	8	15	12	0.224821	0.9800	NonOverlappingTemplate
14	11	9	8	10	12	11	7	8	10	0.911413	0.9800	NonOverlappingTemplate
18	10	8	9	8	10	11	9	9	8	0.534146	0.9900	NonOverlappingTemplate
10	9	7	9	13	14	13	5	14	6	0.334538	1.0000	NonOverlappingTemplate
10	13	8	9	11	9	8	10	13	9	0.964295	1.0000	NonOverlappingTemplate
17	10	11	14	9	6	6	9	11	7	0.275709	0.9700	NonOverlappingTemplate
6	7	14	12	13	6	10	12	7	13	0.419021	1.0000	NonOverlappingTemplate
9	16	6	8	11	10	11	11	11	7	0.637119	0.9900	NonOverlappingTemplate
6	5	10	17	6	15	14	12	10	5	0.040108	1.0000	NonOverlappingTemplate
6	15	9	7	16	9	10	10	9	9	0.437274	0.9900	NonOverlappingTemplate
10	9	7	4	9	11	12	17	10	11	0.334538	0.9900	NonOverlappingTemplate
12	13	10	10	7	8	12	9	8	11	0.935716	0.9800	NonOverlappingTemplate
14	14	9	10	9	10	11	8	6	9	0.779188	0.9800	NonOverlappingTemplate
4	8	6	13	17	15	8	11	11	7	0.080519	1.0000	NonOverlappingTemplate
7	7	7	9	19	11	9	10	15	6	0.085587	0.9900	NonOverlappingTemplate
9	9	11	8	15	10	8	17	6	7	0.275709	0.9800	NonOverlappingTemplate
15	7	5	11	10	12	13	12	6	9	0.401199	0.9900	NonOverlappingTemplate
13	5	9	9	7	10	10	10	15	12	0.595549	0.9700	NonOverlappingTemplate
19	9	7	11	6	4	9	11	14	10	0.062821	0.9700	NonOverlappingTemplate
8	12	14	14	8	7	13	7	10	7	0.534146	0.9800	NonOverlappingTemplate
5	11	16	10	8	10	10	6	14	10	0.366918	1.0000	NonOverlappingTemplate
5	6	10	10	10	12	5	17	18	7	0.023545	0.9900	NonOverlappingTemplate
13	6	8	11	10	15	9	10	14	4	0.289667	0.9900	NonOverlappingTemplate
8	9	11	10	7	10	10	13	9	13	0.946308	0.9900	NonOverlappingTemplate

```
  7   8   9  11  11  14   8   5  12  15  0.437274   0.9900    NonOverlappingTemplate
 10   6  10  11   5  11   8  16   8  15  0.262249   0.9700    NonOverlappingTemplate
  8  14  11   8   8   9  14  10   8  10  0.834308   0.9900    NonOverlappingTemplate
  8   9  13  12  13   7   7   9  14   8  0.678686   1.0000    NonOverlappingTemplate
  9   6  11   7   8   9   6  12  15  17  0.181557   0.9900    NonOverlappingTemplate
  9  10  11   9  13  18  10   6   5   9  0.224821   0.9900    NonOverlappingTemplate
 11   5  13  12   9   9  11   9  10  11  0.883171   0.9900    NonOverlappingTemplate
  8   4  11   8   8  14  15  11   8  13  0.319084   1.0000    NonOverlappingTemplate
 10   9  10  10  12  12  11   5   9  12  0.911413   0.9800    NonOverlappingTemplate
 11   7  10   8   9   5  14  14  10  12  0.574903   1.0000    NonOverlappingTemplate
 11   9   7   5   9  16  15  11   5  12  0.171867   1.0000    NonOverlappingTemplate
  7  17   9   6  16   6   8   9   8  14  0.085587   0.9900    NonOverlappingTemplate
 13  12   5   9  11  10  10  12   9   9  0.867692   0.9800    NonOverlappingTemplate
  9   7  11   6  12  11  15  14   6   9  0.437274   0.9900    NonOverlappingTemplate
  6  13  11  10   7   9  10  12  13   9  0.834308   0.9900    NonOverlappingTemplate
  9  15  12   6   8  10  13   8  12   7  0.574903   1.0000    NonOverlappingTemplate
 13  12   9   7   8   9   8  15  10   9  0.759756   0.9800    NonOverlappingTemplate
 10  13   9  10   9   9  11  11   8  10  0.994250   0.9900    NonOverlappingTemplate
  7  10  17   9  13  11  11  11   5   6  0.262249   0.9900    NonOverlappingTemplate
 16   9   5  12   8   8  14  11   5  12  0.213309   0.9900    NonOverlappingTemplate
 11  12   8   9   9  10   7  11   6  17  0.474986   0.9800    NonOverlappingTemplate
 10   7   3  10  10  10  14  10  13  13  0.419021   0.9900    NonOverlappingTemplate
 13   8   6  16   7  13   4  11   9  13  0.162606   0.9700    NonOverlappingTemplate
 13  10   7  11   6  10   7  11  12  13  0.759756   0.9800    NonOverlappingTemplate
  5  11   8  12  12  12   8   6  16  10  0.366918   0.9800    NonOverlappingTemplate
 16   9   7   7  14  12   7   5  10  13  0.224821   0.9900    OverlappingTemplate
 11   8  13  14   5   8  11  11   7  12  0.595549   1.0000    Universal
  7  19  11   5   9   8  14   6  13   8  0.055361   0.9900    ApproximateEntropy
  4   7   7   6   7   3   3   8   9   7  0.689019   1.0000    RandomExcursions
 10   9   6   2   9   5   3   4   9   4  0.170294   1.0000    RandomExcursions
  4   9   5   6   4   3   4   6  12   8  0.222869   1.0000    RandomExcursions
  1   9   4  10   5   5   5   7   8   7  0.311542   1.0000    RandomExcursions
  2   3   8   9   7   9   4   9   6   4  0.287306   1.0000    RandomExcursions
  3   6  10   4   2   9   6   3   9   9  0.141256   1.0000    RandomExcursions
  4   5   8   5   2   4   5   9   6  13  0.095617   1.0000    RandomExcursions
  6   6   5   4   1   5   8   9  12   5  0.141256   1.0000    RandomExcursions
  3   3   7   7   8   5  10   7   4   7  0.551026   1.0000    RandomExcursionsVariant
  4   4   5   8   3   9   8   6   9   5  0.585209   1.0000    RandomExcursionsVariant
  5   4   9   2   6   3   8  11   8   5  0.204076   1.0000    RandomExcursionsVariant
  7   5   6   2   6   7   7   7   9   5  0.819544   1.0000    RandomExcursionsVariant
  7   6   5   7   4   9   5   6   2  10  0.517442   0.9672    RandomExcursionsVariant
  8   5   1   7   7   8   3   9   9   4  0.264458   0.9672    RandomExcursionsVariant
  6   4   5   3   7  12   5   3   8   8  0.242986   0.9836    RandomExcursionsVariant
  3   7   6   5   9   8   7   8   1   7  0.422034   1.0000    RandomExcursionsVariant
  5   5   5   7   8   4   9   4   7   7  0.875539   1.0000    RandomExcursionsVariant
  6   5   8  11   6   1   3  10   7   4  0.116519   1.0000    RandomExcursionsVariant
  6   9   6   3   3   5   8  10   4   7  0.452799   0.9836    RandomExcursionsVariant
  8   6   6   5   2   8   7   8   7   4  0.756476   0.9836    RandomExcursionsVariant
  5   4   9   9   8   4   7   6   8   1  0.337162   0.9836    RandomExcursionsVariant
  7   5   3   4  13   8   7   5   5   4  0.186566   0.9836    RandomExcursionsVariant
  7   6   4   3  11   9   3   4   6   8  0.287306   0.9836    RandomExcursionsVariant
  8   5   3   5   6   7   4   6   8   9  0.788728   0.9672    RandomExcursionsVariant
  2  11   2   8   7   4   3   9   7   8  0.095617   0.9672    RandomExcursionsVariant
  3   6  10   7   4   5   5   5   8   8  0.654467   0.9672    RandomExcursionsVariant
  8  10  10   6  13  11   7  11  11  13  0.834308   0.9900    Serial
  9  10  12  10  13   9  10   9   8  10  0.991468   0.9800    Serial
  9  14   7  12  11  11   5  13   6  12  0.474986   0.9900    LinearComplexity

- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
The minimum pass rate for each statistical test with the exception of the
random excursion (variant) test is approximately = 0.960150 for a
sample size = 100 binary sequences.

The minimum pass rate for the random excursion (variant) test
is approximately 0.951781 for a sample size = 61 binary sequences.

For further guidelines construct a probability table using the MAPLE program
provided in the addendum section of the documentation.
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
```

RESULTS FOR THE UNIFORMITY OF P-VALUES AND THE PROPORTION OF PASSING SEQUENCES

generator is <Ris_4_9.bin>

C1	C2	C3	C4	C5	C6	C7	C8	C9	C10	P-VALUE	PROPORTION	STATISTICAL TEST
10	10	12	7	11	7	10	15	9	9	0.834308	1.0000	Frequency
12	12	7	9	9	14	5	13	8	11	0.595549	1.0000	BlockFrequency
10	7	12	7	14	9	9	12	11	9	0.867692	0.9800	CumulativeSums
11	6	10	11	9	7	12	11	10	13	0.897763	1.0000	CumulativeSums
10	12	13	15	11	9	10	5	6	9	0.514124	0.9900	Runs
9	9	12	14	10	10	7	10	11	8	0.935716	1.0000	LongestRun
6	11	7	9	9	8	13	6	14	17	0.202268	1.0000	Rank
1	11	8	9	6	18	6	15	14	12	0.006661	1.0000	FFT
15	8	15	10	9	7	16	7	10	3	0.071177	0.9800	NonOverlappingTemplate
10	12	7	8	14	14	11	7	11	6	0.574903	1.0000	NonOverlappingTemplate
4	9	12	11	17	6	12	8	12	9	0.213309	1.0000	NonOverlappingTemplate
11	17	7	6	11	10	8	7	12	11	0.401199	0.9700	NonOverlappingTemplate
8	8	9	9	9	10	9	16	12	10	0.816537	0.9800	NonOverlappingTemplate
10	10	11	7	5	11	11	10	12	13	0.834308	0.9900	NonOverlappingTemplate
12	7	6	10	10	13	12	8	10	12	0.834308	0.9900	NonOverlappingTemplate
9	17	11	11	7	9	11	8	4	13	0.262249	0.9900	NonOverlappingTemplate
12	11	12	9	7	14	4	9	15	7	0.304126	0.9900	NonOverlappingTemplate
9	9	11	10	7	9	12	13	11	9	0.971699	1.0000	NonOverlappingTemplate
9	10	9	10	13	6	14	11	10	8	0.851383	0.9900	NonOverlappingTemplate
8	14	5	10	3	10	12	16	11	11	0.137282	1.0000	NonOverlappingTemplate
4	11	15	11	13	13	12	8	6	7	0.249284	0.9900	NonOverlappingTemplate
12	8	8	11	10	10	10	5	8	18	0.304126	0.9900	NonOverlappingTemplate
12	8	8	8	7	16	13	9	15	4	0.153763	0.9900	NonOverlappingTemplate
5	10	10	12	7	14	12	12	12	6	0.514124	0.9900	NonOverlappingTemplate
10	13	10	9	8	12	12	13	6	7	0.779188	0.9700	NonOverlappingTemplate
10	8	13	11	14	11	11	5	7	10	0.678686	0.9700	NonOverlappingTemplate
10	12	9	6	9	11	11	11	17	4	0.275709	1.0000	NonOverlappingTemplate
9	11	7	7	15	7	13	5	15	11	0.249284	1.0000	NonOverlappingTemplate
14	9	8	10	11	14	9	6	10	9	0.779188	1.0000	NonOverlappingTemplate
13	10	10	13	6	5	10	14	11	8	0.534146	0.9900	NonOverlappingTemplate
8	14	9	10	9	9	14	7	13	7	0.678686	1.0000	NonOverlappingTemplate
11	10	15	11	12	9	10	5	9	8	0.719747	0.9900	NonOverlappingTemplate
10	9	11	8	14	7	11	9	11	10	0.946308	0.9800	NonOverlappingTemplate
11	10	3	10	11	6	12	13	12	12	0.455937	0.9900	NonOverlappingTemplate
12	4	13	7	9	13	11	10	11	10	0.637119	1.0000	NonOverlappingTemplate
7	15	9	10	12	6	14	9	9	9	0.595549	0.9900	NonOverlappingTemplate
10	9	8	17	6	12	8	13	11	6	0.319084	0.9900	NonOverlappingTemplate
12	7	10	11	15	10	9	4	13	9	0.474986	0.9700	NonOverlappingTemplate
5	16	8	12	12	8	12	9	11	7	0.419021	0.9700	NonOverlappingTemplate
10	11	13	15	8	7	5	13	9	9	0.494392	0.9800	NonOverlappingTemplate
7	9	8	5	11	10	10	13	16	11	0.474986	0.9900	NonOverlappingTemplate
7	12	11	13	6	14	11	5	10	11	0.514124	0.9700	NonOverlappingTemplate
10	9	5	14	10	15	11	10	7	9	0.554420	0.9900	NonOverlappingTemplate
10	13	10	11	12	6	10	6	8	14	0.678686	0.9800	NonOverlappingTemplate
10	9	6	15	12	6	10	11	12	9	0.657933	1.0000	NonOverlappingTemplate
15	9	9	8	9	8	11	10	10	11	0.924076	1.0000	NonOverlappingTemplate
8	8	7	14	9	10	13	11	12	8	0.816537	0.9700	NonOverlappingTemplate
15	10	6	12	3	14	12	12	10	6	0.145326	0.9700	NonOverlappingTemplate
12	6	10	8	8	5	11	14	17	9	0.213309	0.9900	NonOverlappingTemplate
9	14	7	8	11	6	10	15	11	9	0.595549	0.9900	NonOverlappingTemplate
13	3	11	8	14	9	9	9	12	12	0.437274	0.9900	NonOverlappingTemplate
14	8	7	15	13	11	8	9	4	11	0.304126	1.0000	NonOverlappingTemplate
9	9	7	9	15	12	13	5	14	7	0.350485	0.9900	NonOverlappingTemplate
5	6	6	12	16	11	8	21	8	7	0.004981	1.0000	NonOverlappingTemplate
10	13	9	9	14	10	14	3	8	10	0.383827	0.9700	NonOverlappingTemplate
13	9	3	9	14	17	9	10	9	7	0.137282	0.9900	NonOverlappingTemplate
7	12	13	15	7	15	7	7	10	7	0.289667	1.0000	NonOverlappingTemplate
10	13	10	11	5	8	15	15	10	3	0.129620	1.0000	NonOverlappingTemplate
10	10	7	9	14	6	14	10	9	11	0.739918	0.9800	NonOverlappingTemplate
5	8	10	15	12	7	12	17	7	7	0.129620	1.0000	NonOverlappingTemplate
7	8	14	6	8	13	12	7	12	13	0.494392	1.0000	NonOverlappingTemplate
14	13	13	6	2	11	12	7	12	10	0.153763	1.0000	NonOverlappingTemplate

7	18	8	8	11	14	10	7	9	8	0.262249	0.9900	NonOverlappingTemplate
2	12	13	9	9	11	15	8	12	9	0.249284	0.9900	NonOverlappingTemplate
3	6	12	12	19	13	11	8	6	10	0.030806	1.0000	NonOverlappingTemplate
9	10	19	9	8	7	9	12	10	7	0.275709	0.9800	NonOverlappingTemplate
12	10	12	10	10	14	4	7	7	14	0.401199	0.9900	NonOverlappingTemplate
8	10	12	9	5	11	12	12	10	11	0.883171	0.9800	NonOverlappingTemplate
12	5	9	11	8	8	8	10	15	14	0.494392	0.9800	NonOverlappingTemplate
10	14	11	14	7	8	10	7	12	7	0.657933	1.0000	NonOverlappingTemplate
13	8	12	12	4	9	10	11	11	10	0.739918	0.9800	NonOverlappingTemplate
16	8	11	7	9	9	14	4	14	8	0.191687	0.9700	NonOverlappingTemplate
9	8	10	8	11	9	13	7	17	8	0.514124	0.9900	NonOverlappingTemplate
11	11	11	12	11	11	6	9	8	10	0.964295	0.9900	NonOverlappingTemplate
10	4	8	12	11	9	9	13	8	16	0.383827	0.9900	NonOverlappingTemplate
12	5	9	5	14	7	16	10	11	11	0.224821	0.9900	NonOverlappingTemplate
6	7	7	8	16	9	13	14	9	11	0.334538	1.0000	NonOverlappingTemplate
10	12	7	13	9	8	11	12	13	5	0.678686	0.9900	NonOverlappingTemplate
9	14	9	14	8	10	8	10	11	7	0.816537	1.0000	NonOverlappingTemplate
12	10	7	11	11	6	6	11	17	9	0.366918	0.9900	NonOverlappingTemplate
10	7	9	13	9	11	11	12	12	6	0.867692	1.0000	NonOverlappingTemplate
7	13	5	14	11	14	13	5	10	8	0.249284	1.0000	NonOverlappingTemplate
15	8	15	10	9	7	16	7	10	3	0.071177	0.9800	NonOverlappingTemplate
5	14	7	12	13	16	5	9	13	6	0.090936	0.9900	NonOverlappingTemplate
6	10	9	8	14	14	3	9	15	12	0.153763	0.9900	NonOverlappingTemplate
8	10	8	11	10	12	14	9	5	13	0.699313	0.9900	NonOverlappingTemplate
12	8	8	12	14	7	13	7	9	10	0.739918	0.9900	NonOverlappingTemplate
7	10	6	11	14	9	10	10	12	11	0.851383	1.0000	NonOverlappingTemplate
14	9	14	6	9	11	14	8	8	7	0.494392	1.0000	NonOverlappingTemplate
11	9	5	8	13	10	11	12	10	11	0.867692	1.0000	NonOverlappingTemplate
10	5	15	15	4	15	10	11	10	5	0.062821	1.0000	NonOverlappingTemplate
9	18	15	7	8	7	3	8	10	15	0.025193	0.9800	NonOverlappingTemplate
14	10	10	5	15	6	8	10	9	13	0.383827	0.9800	NonOverlappingTemplate
17	14	7	8	17	12	3	6	6	10	0.011791	0.9700	NonOverlappingTemplate
13	9	12	16	13	10	8	7	6	6	0.319084	0.9900	NonOverlappingTemplate
8	9	9	12	13	9	6	17	8	9	0.437274	0.9900	NonOverlappingTemplate
14	7	14	7	9	6	8	8	17	10	0.191687	0.9800	NonOverlappingTemplate
11	9	13	11	7	11	8	13	8	9	0.911413	1.0000	NonOverlappingTemplate
11	8	5	9	12	12	9	17	10	7	0.366918	1.0000	NonOverlappingTemplate
11	9	6	14	9	15	6	14	6	10	0.289667	0.9900	NonOverlappingTemplate
7	13	12	10	7	13	7	5	14	12	0.401199	1.0000	NonOverlappingTemplate
11	13	13	12	11	10	7	7	8	8	0.834308	0.9900	NonOverlappingTemplate
9	13	6	12	6	13	11	6	12	12	0.534146	0.9800	NonOverlappingTemplate
8	10	9	6	12	17	9	13	9	7	0.401199	0.9800	NonOverlappingTemplate
14	7	14	7	12	10	11	8	6	11	0.574903	0.9900	NonOverlappingTemplate
8	6	12	15	13	9	11	10	7	9	0.637119	1.0000	NonOverlappingTemplate
7	10	7	14	12	12	4	11	9	14	0.383827	1.0000	NonOverlappingTemplate
11	14	8	11	4	12	10	9	15	6	0.319084	0.9800	NonOverlappingTemplate
9	13	7	8	16	8	7	6	14	12	0.289667	0.9900	NonOverlappingTemplate
12	6	12	11	3	11	14	13	9	9	0.334538	0.9900	NonOverlappingTemplate
16	10	9	18	10	8	10	8	5	6	0.090936	1.0000	NonOverlappingTemplate
8	7	7	16	9	12	10	9	13	9	0.595549	0.9900	NonOverlappingTemplate
8	9	11	11	11	11	12	11	9	7	0.983453	0.9900	NonOverlappingTemplate
8	7	12	15	10	9	11	11	11	6	0.719747	0.9800	NonOverlappingTemplate
10	9	5	8	8	23	9	10	12	6	0.007694	0.9900	NonOverlappingTemplate
13	5	9	8	12	11	7	8	13	14	0.514124	0.9800	NonOverlappingTemplate
11	10	8	10	7	9	13	12	14	6	0.739918	0.9900	NonOverlappingTemplate
19	11	4	10	14	9	8	9	9	7	0.090936	0.9900	NonOverlappingTemplate
9	14	12	14	4	9	10	4	13	11	0.213309	0.9900	NonOverlappingTemplate
14	6	9	8	11	15	7	13	10	7	0.437274	0.9700	NonOverlappingTemplate
9	16	12	10	9	8	14	7	4	11	0.289667	0.9900	NonOverlappingTemplate
10	5	13	9	10	11	6	12	9	15	0.514124	1.0000	NonOverlappingTemplate
10	9	17	10	11	10	9	7	7	10	0.637119	1.0000	NonOverlappingTemplate
9	7	9	13	10	8	10	15	9	10	0.834308	0.9800	NonOverlappingTemplate
16	7	9	10	8	7	13	9	10	11	0.637119	0.9700	NonOverlappingTemplate
5	11	9	11	11	12	13	11	6	11	0.739918	0.9900	NonOverlappingTemplate
12	7	20	7	6	6	8	13	11	10	0.051942	0.9800	NonOverlappingTemplate
4	11	11	11	10	11	13	11	6	12	0.637119	1.0000	NonOverlappingTemplate
9	11	11	6	19	5	9	10	10	10	0.181557	0.9900	NonOverlappingTemplate
9	12	11	12	7	8	5	14	15	7	0.366918	0.9900	NonOverlappingTemplate
12	9	9	12	17	10	8	8	6	9	0.494392	0.9800	NonOverlappingTemplate

```
  9   6  12  13   9  12   6   9  10  14  0.657933   1.0000    NonOverlappingTemplate
 11   8  11   5  12  10  17   7   6  13  0.224821   0.9800    NonOverlappingTemplate
  9  12  13   8   8  10   8  12   8  12  0.924076   0.9900    NonOverlappingTemplate
  9  10  14   9  12   7  13   9   6  11  0.759756   1.0000    NonOverlappingTemplate
 14  14   5  10  13   4  11  13   6  10  0.171867   1.0000    NonOverlappingTemplate
 10   9   8  12  12  11   6  18   8   6  0.249284   0.9900    NonOverlappingTemplate
 11  12  10  12  13   6  11   7   5  13  0.554420   0.9900    NonOverlappingTemplate
 16  11   8   6   6  16   6   8  14   9  0.102526   1.0000    NonOverlappingTemplate
 10  15  11  10   7   9   7   9  11  11  0.851383   1.0000    NonOverlappingTemplate
 11  15   9   7  10   9  13  10  10   6  0.719747   0.9900    NonOverlappingTemplate
 10   9   9   6  10  12  16  13   6   9  0.494392   1.0000    NonOverlappingTemplate
  8   8   9  20   7  11   4   8  14  11  0.040108   1.0000    NonOverlappingTemplate
  5   8   9  14  12  15   7  13   9   8  0.366918   0.9800    NonOverlappingTemplate
 13   8   7  12  10  11   5  10  11  13  0.719747   1.0000    NonOverlappingTemplate
 12   7  14   7  12  11   6  12   8  11  0.657933   0.9900    NonOverlappingTemplate
  9  11  12  11  11   7  10   8   8  13  0.946308   1.0000    NonOverlappingTemplate
 10   9   6  11  10   9  15  13   8   9  0.759756   0.9900    NonOverlappingTemplate
  9   8  10  10  10   9  13  13   8  10  0.971699   1.0000    NonOverlappingTemplate
  7   9  12  10  11   5   9  16  10  11  0.554420   0.9700    NonOverlappingTemplate
 12   5  13   6  13  11  10   5  14  11  0.304126   0.9900    NonOverlappingTemplate
  6  13  10   6  10   7  13  11  12  12  0.657933   1.0000    NonOverlappingTemplate
 12   7  10  10   9  13   4  15  12   8  0.419021   1.0000    NonOverlappingTemplate
 14  10   9  14   6   9  14   8   7   9  0.534146   0.9900    NonOverlappingTemplate
  7   8  11   9  10   9  14  10  11  11  0.946308   0.9900    NonOverlappingTemplate
  7  13   5  14  11  14  13   5  10   8  0.249284   1.0000    NonOverlappingTemplate
 12  12   8  11   6  14  10   6  11  10  0.719747   1.0000    OverlappingTemplate
  8   6   9  12  13   8   7  10  14  13  0.616305   0.9700    Universal
 17  11   7   8   8   4  12  15  10   8  0.137282   0.9900    ApproximateEntropy
  4   9   4   6  16   2  10   4   5   4  0.001801   1.0000    RandomExcursions
  7   9   8   4   6   5   5   6  10   4  0.671779   0.9688    RandomExcursions
  8  11   8   9   5   4   4   3   8   4  0.253551   1.0000    RandomExcursions
 10   5   7   8   1  11   8   3   6   5  0.110952   0.9844    RandomExcursions
  8   4   8   7   4   6   5  10   5   7  0.739918   0.9844    RandomExcursions
  5  14   8   2   6   6   6   8   6   3  0.060239   1.0000    RandomExcursions
  7   7  11   4   5   5   5   7   8   5  0.671779   0.9844    RandomExcursions
  7   6   3   7   9   8   4   6   7   7  0.834308   1.0000    RandomExcursions
  4   6   5   6   5  12   6   4   8   8  0.437274   1.0000    RandomExcursionsVariant
  7   4   7   2   5  13   4   8   9   5  0.090936   1.0000    RandomExcursionsVariant
  5   8   3   4   8  13   1   8   8   6  0.043745   1.0000    RandomExcursionsVariant
  3  11   1   9   9   8   5   8   8   2  0.039244   1.0000    RandomExcursionsVariant
  2   8   7  10   9   7   4   3   8   6  0.299251   1.0000    RandomExcursionsVariant
  0   5  11  10   6   7   6   7   4   8  0.100508   1.0000    RandomExcursionsVariant
  2   4   6  10   7   7  11   4   6   7  0.253551   1.0000    RandomExcursionsVariant
  3   7   9   5   9   7   5   8   7   4  0.671779   0.9844    RandomExcursionsVariant
 10   4  12   9   2   6   6   8   3   4  0.060239   0.9844    RandomExcursionsVariant
  9   6   7   5   8   6   5   4   8   6  0.911413   0.9844    RandomExcursionsVariant
  6   7   4   9   6   4   8   6   5   9  0.804337   0.9844    RandomExcursionsVariant
  5   4   6   9   6   7   6   8   6   7  0.949602   0.9844    RandomExcursionsVariant
  3  10   3   7   9   8   5   5   6   8  0.437274   0.9844    RandomExcursionsVariant
  5   5   4  10   5   6   6   5   8  10  0.602458   0.9844    RandomExcursionsVariant
  5   3   6   7   5   7   7   6   6  12  0.500934   0.9844    RandomExcursionsVariant
  5   4   3   7   9   6  10   6   8   6  0.602458   0.9844    RandomExcursionsVariant
  4   3   7   4  13   6   7   5   6   9  0.162606   0.9844    RandomExcursionsVariant
  3   6   4   7   9   7   7   4   7  10  0.568055   0.9844    RandomExcursionsVariant
 11  13  14  12   9  10   7   8   4  12  0.494392   0.9800    Serial
  8  13  11  14   7   8   9  12   9   9  0.834308   0.9800    Serial
 10   7  11  15  12   9  13   8  10   5  0.554420   1.0000    LinearComplexity

- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
The minimum pass rate for each statistical test with the exception of the
random excursion (variant) test is approximately = 0.960150 for a
sample size = 100 binary sequences.

The minimum pass rate for the random excursion (variant) test
is approximately 0.952688 for a sample size = 64 binary sequences.

For further guidelines construct a probability table using the MAPLE program
provided in the addendum section of the documentation.
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
```

ДОДАТОК В

Список публікацій, в яких опубліковані основні наукові результати дисертації

1. Рудницький В. М., Лада Н. В., Кучук Г. А., Підласий Д. А. Архітектура СЕТ-операцій і технології потокового шифрування = Architecture of CET-operations and stream encryption technologies : монографія / Черкаси : видавець Пономаренко Р. В., 2024. 374 с. ISBN 978-966-2554-81-6. URL : https://dndivsovt.com/index.php/monograph/issue/view/22/22 (дата звернення: 13.09.2024).
2. Ларін В. В., Рудницький В. М., Підласий Д. А. Оцінка статистичних властивостей результатів шифрування на основі операцій, керованих інформацією. *Наукові праці Державного науково-дослідного інституту випробування і сертифікації озброєння та військової техніки*. 2024. Т. 22. № 4. С. 121–127. DOI : https://doi.org/10.37701/dndivsovt.22.2024.15 (дата звернення: 09.04.2025).
3. Підласий Д. А. Дослідження і синтез елементарних функцій операцій, керованих інформацією / *Технології розвитку безпілотних систем* : кол. монографія. Т. 2. Безекіпажні системи, розд. / [В. Г. Бабенко та ін. ; під ред. В. М. Рудницького]. Черкаси : видавець Третяков О. М., 2025. 207 с. С. 55–90. ISBN 978-617-8725-03-7. DOI : https://doi.org/10.5281/zenodo.19191122 (дата звернення: 28.03.2026).
4. Рудницький В. М., Ларін В. В., Мельник О. Г., Підласий Д. А. Дискретно-казуальне представлення моделей елементарних функцій і СЕТ-операцій. *Системи управління, навігації та зв'язку.* 2023. № 4. С. 96–101. DOI : https://doi.org/10.26906/SUNZ.2023.4.096 (дата звернення: 15.02.2024).
5. Рудницький В. М., Лада Н. В., Ларін В. В., Підласий Д. А. Дискретно-казуальне моделювання елементарних функцій операцій, керованих інформацією. *Системи управління, навігації та зв'язку.* 2024. С. 139–142. DOI : https://doi.org/10.26906/SUNZ.2024.4.139 (дата звернення: 11.02.2025).

6. Рудницький В. М. , Лада Н. В., Підласий Д. А., Мельник О. Г. Синтез дискретно-алгебраїчних моделей елементарних функцій операцій, керованих інформацією. Кібербезпека: освіта, наука, техніка. 2024. Т. 3, вип. 23. С. 6–16. DOI : https://doi.org/ 10.28925/2663-4023.2024.23.616 (дата звернення: 25.06.2025).
7. Рудницький, В. М., Тарасенко, Я. В., Лада, Н. В., Бабенко, В. Г., & Підласий, Д. А. (2025). АНАЛІЗ РЕЗУЛЬТАТІВ МОДЕЛЮВАННЯ СЕТ-ОПЕРАЦІЙ НА ОСНОВІ ЕЛЕМЕНТАРНИХ ФУНКЦІЙ ОПЕРАЦІЙ КЕРОВАНИХ ІНФОРМАЦІЄЮ. *Системи та технології*, *70*(2), 258-263. DOI: https://doi.org/10.32782/2521-6643-2025-2-70.29 (дата звернення: 11.01.2026).
8. V. Rudnytskyi, N. Lada, V. Larin, D. Holovniak, H. Haponenko, D. Pidlasyi and T. Stabetska. Discrete and casual modeling of CET-operations of data-controlled permutations. *Journal of Xidian University.* 2024. Vol. 18, iss. 6. P. 747–767. URL : https://drive.google.com/file/d/1iYOUKC7OuDlVXW81GDrhx09VkM9dQZz_/view (дата звернення: 08.02.2025).
9. V. Rudnytskyi, N. Lada, V. Larin, V. Tkachenko, T. Korotkyi, D. Pidlasyi and D. Tarasenko. Information system for modeling and research of pseudorandom sequences of CET-operations for post quantum stream encryption. *Journal of Xidian University.* 2024. Vol. 18, iss. 7. P. 1284–1298. DOI : https://doi.org/10.5281/Zenodo.13096683 (дата звернення: 09.02.2025).
10. V. Rudnytskyi1, V. Babenko, N. Lada, T. Stabetska, D. Pidlasyi, L. Parkhuts. Modeling of a cryptographic network based on application of CET-operations. *Workshop on Cyber Security and Data Protection II, CSDP-II.* Lviv, 2025. Vol. 4042. P. 64–79. URL : https://ceur-ws.org/Vol-4042/paper5.pdf (дата звернення: 15.02.2026).
11. V. Rudnytskyi, N. Lada, V. Babenko, H. Kuchuk, D. Pidlasyi, D. Kamak and Ye. Ivashchenko. Modeling of groups of dual-cycle non-commutative two-operand

CET-operations. *Journal of Xidian University.* 2024. Vol. 18, iss. 10. P. 916–958. DOI : https://doi.org/10.5281/Zenodo.13992956 (дата звернення: 11.02.2025).

12. V. Rudnytskyi, N. Lada, V. Larin, O. Melnyk, T. Stebetska, T. Korotkyi, D. Pidlasyi. Usage of non-commutative two-operand CET-operations in limited resources stream ciphers. *Journal of Xidian University*. 2024. Vol. 18, iss. 5. P. 1105–1120. DOI : https://doi.org/10.5281/Zenodo.11253625 (дата звернення: 03.06.2025).

Список публікацій, які засвідчують апробацію матеріалів дисертації:

1. Підласий Д. А. Мультиваріантне представлення CET-операцій на основі елементарних функцій операцій, керованих інформацією. *Сучасні напрями розвитку інформаційно-комунікаційних технологій та засобів управління* : *тези доповідей шістнадцятої міжнародної науково-технічної конференції (м. Баку – Харків – Жиліна, 29–30 квітня 2026 р.)* : зб. наукових праць. Т 3. 2026. С. 14. DOI : https://doi.org/10.32620/ICT.26.t3 (дата звернення: 05.05.2026).
2. Рудницький В. М., Ларін В. В. , Підласий Д. А. Дискретно-казуальне моделювання двохоперандних CET-операцій для потокового шифрування. *Новітні технології – для захисту повітряного простору : матеріали XXII міжнародної наукової конференції Харківського національного. університету Повітряних Сил імені Івана Кожедуба (м. Харків, 08–09 квітня 2026 р.)* : зб. наукових праць. 2026. С. 556. URL : https://hups.mil.gov.ua/wp-content/uploads/admission-university/naukovij_centr/XXI%D0%86_mizhnarodna_naukova_konferencia_KhNUPS_2026_V2.pdf (дата звернення: 15.05.2026).
3. Рудницький В. М., Безменов С. О., Підласий Д. А. Аналіз елементарних функцій операцій, керованих інформацією. *Безпілотна авіація у сучасній збройній боротьбі* : *матеріали науково-практичної конференції інженерно-авіаційного факультету Харківського національного.*

Університету Повітряних Сил імені Івана Кожедуба. (м. Харків, 7 грудня 2023 року.) : зб. наукових праць. 2023. С. 25. URL : https://www.hups.mil.gov.ua/assets/doc/science/stud-conf/bpla-hnups-konf.pdf (дата звернення: 16.04.2024).

ДОДАТОК Г

Документи про впровадження результатів дисертаційної роботи

Довідка

про впровадження результатів наукових досліджень
Підласого Дмитра Андрійовича

Результати дисертаційного дослідження Підласого Дмитра Андрійовича, а саме удосконалена система комп'ютерного потокового шифрування на основі випадкових підстановок операцій керованих інформацією при розробці макету захищеної системи дистанційного управління наземним самохідним роботизованим комплексом.

Впроваджена система потокового шифрування реалізована на рівні програмного модуля системи управління роботизованим комплексом "MOROZ-02L".

Директор ТОВ "МОРОЗ ТЕХ" Роман МОРОЗ