ЧЕРКАСЬКИЙ ДЕРЖАВНИЙ ТЕХНОЛОГІЧНИЙ УНІВЕРСИТЕТ
МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

Кваліфікаційна
наукова праця на
правах рукопису

БРЕУС Роксолана Василівна

УДК 004.056.55:004.312.2

ДИСЕРТАЦІЯ

ГЕНЕРАЦІЯ ПСЕВДОВИПАДКОВИХ ПОСЛІДОВНОСТЕЙ ОПЕРАЦІЙ СТРОГОГО СТІЙКОГО КРИПТОГРАФІЧНОГО КОДУВАННЯ НА ОСНОВІ ПЕРЕТВОРЕННЯ ДРУГОГО ОПЕРАНДА

05.13.05 – комп’ютерні системи і компоненти

Подається на здобуття наукового ступеня кандидата технічних наук

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

Р.В. БРЕУС

Науковий керівник Рудницький Володимир Миколайович, доктор технічних наук, професор

Черкаси - 2021

АНОТАЦІЯ

Бреус Р.В. Генерація псевдовипадкових послідовностей операцій строгого стійкого криптографічного кодування на основі перетворення другого операнда. – Кваліфікаційна наукова праця на правах рукопису.

Дисертація на здобуття наукового ступеня кандидата технічних наук (доктора філософії) за спеціальністю 05.13.05 «Комп'ютерні системи та компоненти». – Черкаський державний технологічний університет, Черкаси, 2021.

Дисертаційна робота присвячена підвищенню швидкості потокового шифрування за рахунок генерації псевдовипадкових послідовностей групи двохрозрядних двохоперандних операцій строгого стійкого криптографічного кодування на основі перетворення другого операнда.

У першому розділі приводиться огляд публікацій по синтезу операцій криптографічного кодування інформації. Визначені напрямки вдосконалення криптографічного кодування, сформульовані мета і на її основі – задачі дисертаційного дослідження. Другий розділ присвячений синтезу обернених ДДО ССКК на основі перетворення другого операнда, запропонована технологія дослідження взаємозв'язків між прямими та оберненими операціями криптоперетворення. Третій розділ присвячено розробці методу синтезу групи ДДО ССКК на основі перетворення другого операнда відомої операції. Взаємозв'язки між прямими і оберненими операціями дозволяють синтезувати обернені операції, а кожна обернена операція, в свою чергу, є прямою операцією для іншої оберненої операції, тобто шляхом перетворення другого операнда одноопераднною операцією можливо синтезувати іншу операцію. Четвертий розділ присвячено розробці методу генерації псевдовипадкових послідовностей ДДО ССКК на основі перетворення другого операнда, для цього узагальнено результати синтезу груп ДДО ССКК на основі першої операції.

Наукова новизна отриманих результатів:

- вперше розроблено метод синтезу обернених двохрозрядних двохоперандних операцій строгого стійкого криптографічного кодування на основі множини двохрозрядних двохоперандних операцій строгого стійкого криптографічного кодування, встановлених взаємозв'язків між прямими та оберненими операціями, шляхом перетворення другого операнда за рахунок реалізації побудованої моделі автомата синтезу другого операнда оберненої операції, що забезпечило можливість практичного застосування даних операцій;
- вперше розроблено метод синтезу групи двохрозрядних двохоперандних операцій строгого стійкого криптографічного кодування на основі використання відомої двохрозрядної двохоперандної операції строгого стійкого криптографічного кодування та перетвореннями другого операнда шляхом послідовного виконання над даною операцією групи двохрозрядних одноопераднних операцій, що забезпечило можливість збільшення варіативності криптопримітивів при практичному застосуванні даних операцій;
- вперше розроблено метод генерації псевдовипадкових послідовностей двохрозрядних двохоперандних операцій строгого стійкого криптографічного кодування на основі використання груп двохрозрядних двохоперандних операцій строгого стійкого криптографічного кодування і двохрозрядних одноопераднних операцій строгого стійкого криптографічного кодування, шляхом перетворень других операндів прямих та обернених двохоперандних операцій, що дозволило досягти підвищення швидкості потокового шифрування за рахунок генерації псевдовипадкових послідовностей прямих та обернених двохрозрядних двохоперандних операцій строгого стійкого криптографічного кодування.

Практичне значення отриманих результатів. Практична цінність роботи полягає в доведенні розроблених методів до дискретних моделей операцій та алгоритмів автоматичної генерації псевдовипадкових послідовностей операцій строгого стійкого кодування для систем потокового комп'ютерного шифрування.

Розширено варіативність криптографічних перетворень за рахунок збільшення кількості операцій з 12 до 24. Розроблений генератор

псевдовипадкових послідовностей двохрозрядних двохоперандних операцій строгого стійкого криптографічного кодування забезпечує синтез операцій на 15–20 % швидше порівняно з табличним методом синтезу при забезпеченні періоду послідовності $(24!)^2$. Отриманий результат забезпечив швидкість реалізації методу підвищення стійкості та надійності потокового шифрування при максимальній невизначеності результатів перетворення.

Реалізація. Дисертаційна робота виконувалася відповідно до плану НДР Черкаського державного технологічного університету. Одержані в ній теоретичні й практичні результати використані та впроваджені у таких закладах, установах, організаціях:

- Черкаський державний технологічний університет на кафедрі інформаційної безпеки та комп'ютерної інженерії – у матеріалах лекційних курсів «Комплексні системи захисту інформації», «Програмний захист інформації в інформаційно-комунікаційних системах». Акт впровадження від 10.06.2019;

- ТОВ «Нова пошта» – для підвищення захисту особистих даних працівників та клієнтів пошти, а також захисту оплати послуг шляхом використання методу синтезу обернених ДДО ССКК на основі перетворення другого операнда у вигляді реалізації моделі автомата побудови другого операнда оберненої операції. Акт впровадження від 15.12.2019;

- КНП «Черкаська міська консультативно-діагностична поліклініка» (філія №2) – для підвищення захисту персональних даних персоналу та пацієнтів за допомогою застосування методу синтезу групи ДДО ССКК на основі перетворення другого операнда відомої операції. Акт впровадження від 10.06.2020;

- ПАТ «Черкасиобленерго» – для підвищення захисту персональних даних, шляхом застосування методу генерації псевдовипадкових послідовностей ДДО ССКК на основі перетворення другого операнда, у працівників підприємства та клієнтів. Акт впровадження від 20.12.2019.

Ключові слова: комп'ютерна криптографія, операції криптографічного перетворення, потокові шифри, синтез операцій.

ABSTRACT

Breus R.V. Generation of pseudo-random sequences of operations of strict stable cryptographic coding based on the transformation of the second operand. – Qualifying scientific work on the rights of the manuscript.

Dissertation for the degree of Candidate of Technical Sciences (Doctor of Philosophy) in the specialty 05.13.05 "Computer Systems and Components". – Cherkasy State Technological University, Cherkasy, 2021.

The dissertation is devoted to increasing of the speed of streaming encryption at the expense of generating of pseudo - random sequences of a group of two-bit two-operand operations of a strict stable cryptographic coding (further TBTOO of SSCC) based on the transformation of the second operand.

The first section provides an overview of publications on the synthesis of operations of cryptographic coding of information. The directions of improvement of cryptographic coding are defined, the purpose and on its basis, the tasks of dissertation research are formulated. The second section is devoted to the synthesis of inverted TBTOO of SSCC based on the transformation of the second operand, the technology of studying the relationship between direct and inverse operations of cryptic transformation is proposed. The third section is devoted to the development of a method for the synthesis of the TBTOO of SSCC group based on the transformation of the second operand of a known operation. The relationship between direct and inverse operations allows the synthesis of inverse operations, and each inverse operation, in its turn, is a direct operation for another inverse operation, i.e. it is possible to synthesize another operation by converting the second operand with a single operand operation. The fourth section is devoted to the development of a method for generating pseudo-random sequences of TBTOO SSCC based on the transformation of the second operand, for this purpose, the results of synthesis of groups of TBTOO of SSCC based on the first operation are generalized.

Scientific novelty of the obtained results:

- for the first time the method of synthesis of inverse two-bit two-operand operations of strict stable cryptographic coding based on a set of two-bit two-operand operations of strict stable cryptographic coding is developed; the relationships between direct and inverse operations, by transforming the second operand are established; all previously mentioned measures provided the possibility of practical application of these operations;
- for the first time a method of synthesis of a group of two-bit two-operand operations of strict stable cryptographic coding on the basis of using the known two-bit two-operand operation of strict stable cryptographic coding and transformations of the second operand was developed. It was achieved by sequentially performing on this operation a group of two-bit single-operand operations, which provided the opportunity to increase the variability of crypto-primitives in the practical application of these operations;
- for the first time the method of generation of pseudo-random sequences of two-bit two-operand operations of strict stable cryptographic coding on the basis of use of groups of two-bit two-operand operations of strict stable cryptographic coding and two-bit one-operand operations of strict stable cryptographic coding was developed. It was done by transforming the second operands of direct and inverse two-operand operations, which allowed to increase the speed of streaming encryption by generating pseudo-random sequences of direct and inverse two-bit two-operand operations of strict stable cryptographic coding.

The practical significance of the results. The practical value of the work lies in bringing the developed methods to discrete models of operations and algorithms for automatic generation of pseudo-random sequences of operations of strict stable cryptographic coding for streaming computer encryption systems.

The variability of cryptographic transformations is expanded by increasing the number of operations from 12 to 24. The developed pseudo-random sequence generator of two-bit two-operand operations of strict stable cryptographic coding provides synthesis of operations 15-20% faster than the tabular method of synthesis when providing a sequence period $(24!)^2$. The obtained result provided

the speed of implementation of the method of increasing the stability and the reliability of streaming encryption with maximum uncertainty of the conversion results.

Realization. The dissertation was accomplished in accordance with the research plan of Cherkasy State Technological University. The theoretical and practical results obtained in it are used and implemented in the following institutions, establishments, organizations:

- Cherkasy State Technological University at the Department of Information Security and Computer Engineering – in the materials of lecture courses "Integrated Information Protection Systems", "Software Information Protection in Information and Communication Systems". Act of implementation dated June 10, 2019;

- Ltd. "Nova Poshta" - to increase the protection of personal data of employees and customers of the post office, as well as the protection of payment of services by using the method of synthesis of inverse TBTOO of SSCC based on the transformation of the second operand in the form of a model realization of the second operand. Act of implementation dated 15.12.2019;

- municipal enterprise "Cherkasy City Consultative and Diagnostic Polyclinic" (branch №2) - to increase the protection of personal data of the staff and the patients by applying the method of synthesis of the TBTOO of SSCC group based on the transformation of the second operand of the known operation. Act of implementation dated 10.06.2020;

- JSC "Cherkasyoblenergo" - to increase the protection of personal data, by applying the method of generating pseudo-random sequences of DDO of SSKK on the basis of the transformation of the second operand, employees and customers. Act of implementation dated 20.12.2019.

Key words: computer cryptography, cryptographic transformation operations, stream ciphers, operations synthesis.

Список публікацій здобувача:

1. Бреус Р. В. Синтез двохрозрядних двохоперандних операцій строгого стійкого криптографічного кодування шляхом перетворення другого операнда. *Системи управління, навігації та зв'язку*. Полтава: ПНТУ, 2019. Вип. 5 (57). С 29–32.

2. Рудницький В. М., Бреус Р. В., Лада Н. В. Генерація послідовностей операцій криптографічного перетворення. *Вісник Інженерної академії України.* Київ, 2019. Вип. 3. С.75–80.

3. Rudnitsky V., Berdibayev R., Breus R., Lada N., Pustovit M. Synthesis of reverse two-bit dual-operated strictly straight cryptographic coding on the basis of another operation. *Advanced Information Systems:* Quarterly scientific and technical journal. Kharkiv: National Technical University «Kharkiv Polytechnic Institute», 2019. Vol. 3, No. 4, pp. 109–114.

4. Lada N., Dzyuba V., Breus R., Lada S. Synthesis of sets of non-symmetric two-operand two-bit crypto operations within the permutation accuracy. *Technology audit and production reserves.* № 2/2(52), 2020, pp. 28–31.

5. Лада Н. В., Бреус Р. В., Лада С. В. Генерація моделей прямих і обернених двохрозрядних двохоперандних операцій строгого стійкого криптографічного кодування. *Science and Education a New Dimension Natural and Technical Science.* Budapest, 2020. V. 238, p. 27–30.

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

7. Бреус Р. В. Уніфікація опису операцій криптографічного перетворення. *Проблеми інформатизації: матеріали Четвертої міжнар. наук.-техн. конф.*: тези доп., (Черкаси – Баку – Бельсько-Бяла – Полтава, 3–4 листоп. 2016 р.). Черкаси: ЧДТУ, 2016. С. 9.

8. Бреус Р.В. Математичні моделі побудови операцій розширеного матричного криптографічного перетворення. *Проблеми інформатизації: матеріали П'ятої міжнар. наук.-техн. конф.*: тези доп., (Черкаси – Баку – Бельсько-Бяла – Полтава, 13-15 листоп. 2017 р.). Черкаси: ЧДТУ, 2017. С. 13.

9. Лада Н. В., Бреус Р. В., Рудницька Ю. В., Висоцький С. В. Аналіз групи двоопераднних симетричних криптовалютних операцій. *Проблеми інформатизації: матеріали Сьомої міжнар. наук.-техн. конф*.: тези доп., (Черкаси – Харків – Баку – Бельсько-Бяла, 13–15 листопада 2019 р.). Черкаси: ЧДТУ; Баку: ВА ЗС АР, Бельсько-Бяла: УТіГН, Харків: НТУ «ХПІ», 2019., Т.1, С. 85.

10. Jancarczyk D., Rudnytskyi V., Breus R., Pustovit M., Veselska O. and Ziubina R. Two-Operand Operations of Strict Stable Cryptographic Coding With Different Operands' Bits. *The 5-th IEEE International Symposium on Smart and Wireless Systems within the International Conferences on Intelligent Data Acquisition and Advanced Computing Systems*, 2020, Dortmund, Germany.

ЗМІСТ

ВСТУП

Актуальність теми. Науково-технічний прогрес відіграє важливу роль у сучасному суспільстві. Сучасна людина отримує в десятки разів більше інформації, ніж десятки років тому. Це пояснюється тим, що інформація стає доступною для будь-якої людини. У звязку з цим інформаційні ресурси стають уразливими, що, в свою чергу, призводить до збільшення комп'ютерних злочинів. Тому на даний час гостро постає питання захисту інформації.

Криптографічний захист інформації являється одним із найефективніших на сьогодні. Тому виникає необхідність вдосконалення існуючих та створення нових методів та засобів криптографічного захисту інформації, у зв'язку зі зростанням кіберзлочинів. Для досягнення такого результату необхідне покращення вже розроблених або створення нових алгоритмів криптоперетворення. Отже, дослідження та побудова нових операцій криптоперетворення на сьогоднішній день являється особливо актуальними.

У розвиток комп'ютерної криптографії значний внесок зробили такі вітчизняні та зарубіжні науковці, як І. Д. Горбенко, А. М. Олексійчук, Л. В. Ковальчук, К. Є. Шеннон, Брюс Шнайєр, Чарльз Г. Беннет, W. Diffie, Жиль Брассар, M. E. Hellman, U. M. Maurer, A. Shamir, N. Koblitz та ін.

Досить велика увага останнім часом приділяється криптографічному кодуванню, що являє собою один із напрямів комп'ютерної криптографії. Ще один напрям криптографії, який заслуговує на увагу – це побудова операцій з заданими властивостями. Досить цікавими дослідженнями можна назвати й ті, які направлені на побудову операцій криптоперетворення, що забезпечують максимальну невизначеність результатів шифрування. Проте залишилися ще не дослідженими процеси синтезу груп двохрозрядних двохоперандних операцій (ДДО) строгого стійкого криптографічного

кодування (ССКК), як такі, що можуть становити інтерес для підвищення швидкості потокового шифрування в рамках розроблення методів та інформаційних технологій розв’язання задач комп’ютерної криптографії та стеганографії.

Таким чином, можна стверджувати, що тема дисертаційного дослідження «Генерація псевдовипадкових послідовностей операцій строгого стійкого криптографічного кодування на основі перетворення другого операнда» є актуальною.

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

Дисертаційна робота виконана відповідно до Постанови Президії НАНУ від 30.01.19 №30 «Основні наукові напрями та найважливіші проблеми фундаментальних досліджень у галузі природничих, технічних і гуманітарних наук Національної академії наук України на 2019–2023 рр.», а саме – пп. 1.2.8.1 Розробка методів та інформаційних технологій розв’язання задач комп’ютерної криптографії та стеганографії. Результати дисертаційної роботи включені в НДР Черкаського державного технологічного університету: «Синтез операцій криптографічного перетворення з заданими характеристиками» (ДР № 0116U008714), «Розробка методів та засобів оцінки ефективності соціоінжинірінгу» (ДР № 0116U008715) у яких автор приймав участь як виконавець.

Мета і задачі дослідження. Основною метою дослідження є підвищення швидкості потокового шифрування за рахунок генерації псевдовипадкових послідовностей групи двохрозрядних двохоперандних операцій строгого стійкого криптографічного кодування на основі перетворення другого операнда.

Для досягнення поставленої мети сформульовано і вирішено такі задачі:

– розроблення методу синтезу обернених двохрозрядних двохоперандних операцій строгого стійкого криптографічного кодування на основі перетворення другого операнда;

– розроблення методу синтезу групи двохрозрядних двохоперандних операцій строгого криптографічного кодування на основі перетворення другого операнда відомої операції;

– розроблення методу генерації псевдовипадкових послідовностей двохрозрядних двохоперандних операцій строгого стійкого криптографічного кодування на основі перетворення другого операнда та його реалізація.

Об'єкт дослідження – процеси захисту інформації в кіберпросторі.

Предмет дослідження – метод генерації псевдовипадкових послідовностей прямих та обернених двохрозрядних двохоперандних операцій строгого стійкого криптографічного кодування на основі перетворення другого операнда та його реалізація

Методи дослідження. У процесі розробки методу синтезу обернених двохрозрядних двохоперандних операцій строгого стійкого криптографічного кодування на основі перетворення другого операнда використовувався математичний апарат криптографії, теорії інформації, теорії алгоритмів, дискретної математики. Для розробки методу синтезу групи двохрозрядних двохоперандних операцій строгого криптографічного кодування на основі перетворення другого операнда відомої операції – методи дискретної математики, теорія алгоритмів, криптографія, логіки. Для розробки методу генерації псевдовипадкових послідовностей двохрозрядних двохоперандних операцій строгого стійкого криптографічного кодування на основі перетворення другого операнда та можливості його реалізації використано методи теорії ймовірності, алгоритмів, інформації, криптографії із застосуванням методів дискретної математики.

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

1) вперше розроблено метод синтезу обернених двохрозрядних двохоперандних операцій строгого стійкого криптографічного кодування на основі перетворення другого операнда шляхом реалізації моделі автомата

побудови другого операнда оберненої операції, що забезпечило можливість практичного застосування даних операцій;

2) вперше розроблено метод синтезу групи двохрозрядних двохоперандних операцій строгого стійкого криптографічного кодування на основі перетворення другого операнда відомої операції шляхом виконання над ним двохрозрядної одноопераднної операції, що забезпечило можливість збільшення варіативності криптопримітивів при практичному застосуванні даних операцій;

3) вперше розроблено метод генерації псевдовипадкових послідовностей двохрозрядних двохоперандних операцій строгого стійкого криптографічного кодування на основі перетворення другого операнда, що дозволяє значно спростити процес дослідження та синтезу групи операцій строгого стійкого криптоперетворення та робить можливим використання його при вдосконаленні методу підвищення криптостійкості і надійності потокового шифрування.

Практичне значення отриманих результатів. Практична цінність роботи полягає в доведенні розроблених методів до дискретних моделей операцій та алгоритмів автоматичної генерації псевдовипадкових послідовностей операцій строгого стійкого кодування для систем потокового комп'ютерного шифрування.

Розширено варіативність криптографічних перетворень за рахунок збільшення кількості операцій з 12 до 24. Розроблений генератор псевдовипадкових послідовностей двохрозрядних двохоперандних операцій строгого стійкого криптографічного кодування забезпечує синтез операцій на 15-20% швидше порівняно з табличним методом синтезу при забезпеченні періоду послідовності $(24!)^2$. Отриманий результат забезпечив швидкість реалізації методу підвищення стійкості та надійності потокового шифрування при максимальній невизначеності результатів перетворення.

Реалізація. Дисертаційна робота виконувалася відповідно до планів НДР Черкаського державного технологічного університету. Одержані в ній

теоретичні й практичні результати використані та впроваджені у таких закладах:

– Черкаський державний технологічний університет на кафедрі інформаційної безпеки та комп'ютерної інженерії – у матеріалах лекційних курсів «Комплексні системи захисту інформації», «Програмний захист інформації в інформаційно-комунікаційних системах». Акт впровадження від 10.06.2019 р.

– «Нова пошта» – для підвищення захисту особистих даних праційників та клієнтів пошти, а також захисту оплати послуг шляхом використання методу синтезу обернених ДДО ССКК на основі перетворення другого операнда у вигляді реалізації моделі автомата побудови другого операнду оберненої операції. Акт впровадження від 15.12.2019 р.

– КНП «Черкаська міська консультативно-діагностична поліклініка» Філія №2 – для підвищення захисту персональних даних персоналу та пацієнтів за допомогою застосування методу синтезу групи ДДО ССКК на основі перетворення другого операнда відомої операції. Акт впровадження від 10.06.2020 р.

– ПАТ «Черкасиобленерго» – для підвищення захисту персональних даних, шляхом застосування методу генерації псевдовипадкових послідовностей ДДО ССКК на основі перетворення другого операнда, у працівників підприємства та клієнтів. Акт впровадження від 20.12.2019 р.

Особистий внесок здобувача. Всі нові результати дисертаційної роботи отримано автором самостійно. Результати, опубліковані в [1,7,8], отримані одноосібно. У наукових працях, опублікованих у співавторстві, з питань, що стосуються даного дослідження, автору належать: синтез операцій строгого стійкого кодування на основі перетворення другого операнда заданої операції [2, 10], встановлення взаємозв'язків між прямими і оберненими двохрозрядними двохоперандними операціями строгого стійкого криптографічного кодування [3], синтез строгого стійкого криптографічного

криптоперетворення [4, 6, 9], генерація операцій строгого стійкого кодування для прямого і оберненого криптографічного перетворення інформації [5].

Апробація результатів дисертації. Результати дисертаційної роботи доповідалися й обговорювалися на Четвертій міжнародній науково-технічній конференції «Проблеми інформатизації» (Черкаси – Баку – Бельсько-Бяла – Полтава, 2016), Пятій міжнародній науково-технічній конференції «Проблеми інформатизації» (Черкаси – Баку – Бельсько-Бяла – Полтава, 2017), Сьомій міжнародній науково-технічній конференції «Проблеми інформатизації» (Черкаси – Баку – Бельсько-Бяла – Полтава, 2019) The 5-th IEEE International Symposium on Smart and Wireless Systems within the International Conferences on Intelligent Data Acquisition and Advanced Computing Systems, 2020, Dortmund, Germany.

Публікації. Основні положення дисертації опубліковано у 10 друкованих працях, у тому числі: в 4 статтях у фахових виданнях України, 1 статті в закордонному виданні; колективній монографії, в матеріалах трьох міжнародних науково-технічних конференцій та в збірнику матеріалів міжнародного симпозіуму, проіндексованому в Scopus.

Структура і обсяг дисертації. Робота складається зі вступу, чотирьох розділів, висновків, списку використаних джерел, додатків. Загальний обсяг дисертації – 190 сторінок. Основний зміст викладений на 154 сторінках, у тому числі 12 таблиць, 12 рисунків. Список використаних джерел містить 127 найменувань. Робота містить 5 додатків.

РОЗДІЛ 1 СУЧАСНИЙ СТАН ТА ПЕРСПЕКТИВИ РОЗВИТКУ КОМП'ЮТЕРНОЇ КРИПТОГРАФІЇ

1.1 Проблеми комп'ютеризованого захисту інформації в Україні

На сьогоднішній день захист інформації перетворюється на одну з найактуальніших задач сучасного світу, унаслідок досить широкого розповсюдження в усі сфери людської діяльності, як, власне, різноманітних систем обробки інформації, а й безпосереднього розширення локальних та глобальних комп'ютерних мереж, за допомогою яких передається величезний обсяг інформації державного, військового, комерційного, приватного характеру, власники якої були б категорично проти ознайомлення з нею сторонніх осіб [11-13]. Проблема набула особливого загострення після прийняття урядом нашої держави Закону України «Про захист персональних даних» [14], головним призначенням якого є зобов'язання забезпечити обов'язковий захищений вигляд персональних даних працівників при їх зберіганні та передаванні [15].

Ще одним не менш важливим фактором загострення потреби в захисті інформації можна вважати широке впровадження різноманітних інформаційних технологій у майже всі сфери людської діяльності в Україні, починаючи від стрімкого зростання обігу пластикових карток, використання електронних паспортів та електронних медичних карт, впровадження шкільних щоденників, студентських квитків та залікових книжок тощо [16-18].

Зрештою, дедалі більше державних установ і приватних підприємств, як в Україні, так і за кордоном, переходять на електронний документообіг [19].

Однак, варто зазначити, що впровадження електронного документообігу також вимагає забезпечення юридичної чинності електронних цифрових підписів фізичних або юридичних осіб [20].

Таким чином, розповсюдження електронного документообігу та інших аналогічних технологій також потребує надійного високоефективного та загальнодоступного захисту інформації [21]. Отже, усі ці, та багато інших задач покликані розв’язувати різноманітні технології захисту інформації [22].

Зокрема, на сьогоднішній день досить розповсюдженими являються комп’ютерні злочини, адже вони пов’язані не лише з втручанням у безпосередню роботу комп’ютера, а й такі, в яких комп’ютер використовується як необхідний технічний засіб [23-24].

Серед найрозповсюдженіших причин комп'ютерних злочинів, вчинених на територій нашої держави, і, пов'язаних з ними, витоків (крадіжок) інформації, головними є такі [25]:

- по-перше, швидкий перехід від традиційної загальноприйнятої паперової технології зберігання та передавання необхідної конфіденційної інформації, до технології електронної за одночасного значного відставання технологій захисту інформації, що в електронному вигляді є зафіксованою на машинних носіях;

- по-друге, розширення доступу фізичних та юридичних осіб до інформаційних ресурсів, широке повсякденне використання локальних обчислювальних мереж, а також створення глобальних мереж;

- по-третє, постійне удосконалення програмних засобів, що викликає збільшення в них кількості уразливих місць і, як наслідок, зменшення їх надійності в розрізі інформаційної безпеки [26-29].

На сьогоднішній день ніхто не може вказати точну цифру загальних збитків, спричинених комп’ютерними злочинами, але світові експерти погоджуються, що відповідні суми спричинених збитків вимірюються мільярдами гривень, доларів та евро [30].

Серед основних причин збитків варто виокремити такі [31]:

- по-перше, співробітники організації позбавлені можливості виконувати свої професійні обов'язки через непрацездатність системи (мережі);

- по-друге, вартість викрадених і скомпрометованих даних;

- по-трете, витрати на відновлення роботи системи, що була уражена, на перевірку її цілісності, на безпосередню доробку уразливих місць, тощо [32-34].

Окрім вищезазначених наслідків, доцільно також врахувати й морально-психологічні, спричинені комп’ютерними злочинами, наслідки для власників та користувачів інформації й інформаційних систем [35].

Варто зазначити, також, щодо наслідків порушення безпеки, так званої «критичної» інфраструктури та відповідно «критичних» додатків у державному і військовому управлінні, управлінні національною безпекою, атомній енергетиці, медицині, ракетно-космічній галузі та у державній фінансовій сфері. Порушення інформаційної безпеки об’єктів сфери критичної інфраструктури України може призвести до надзвичайно тяжких наслідків як для безпеки і економіки держави, так і для навколишнього середовища, а також здоров'я і навіть для життя людей [36].

Отже, можемо резюмувати, що питання національної безпеки; економічні та юридичні питання, а також питання, що стосуються охорони державної, комерційної та, навіть, приватної таємниці – беззаперечно зумовлюють необхідність захисту інформації та інформаційної системи вцілому [36].

Варто зазначити, що Законом України «Про захист інформації в автоматизованих системах» визначено поняття «Захист інформації» як сукупність організаційно-технічних заходів і правових норм для запобігання заподіянню шкоди інтересам власника інформації чи автоматизованій системі та особам, які користуються інформацією [37].

Базовими принципами інформаційної безпеки прийнято вважати забезпечення цілісності інформації, забезпечення її конфіденційності і,

водночас, забезпечення її доступності для всіх авторизованих користувачів [38]. Таким чином, з цього погляду можна визначити наступні основні випадки порушення безпеки інформації, що підлягає захисту:

- несанкціонований доступ – доступ до конфіденційної інформації, що здійснюється з порушенням установлених в інформаційній системі правил розмежування доступу;

- витік інформації – результат дій порушника, унаслідок яких інформація стає відомою (доступною) суб'єктам, що не мають права доступу до неї;

- втрата інформації – дія, внаслідок якої інформація в інформаційній системі перестає існувати для фізичних або юридичних осіб, які мають право власності на неї в повному чи обмеженому обсязі;

- підробка інформації – навмисні дії, що призводять до змінення інформації, яка має оброблятися або зберігатися в інформаційній системі;

- блокування інформації – дії, наслідком яких є припинення доступу до інформації;

- порушення роботи інформаційної системи – дії або обставини, які призводять до спотворення процесу обробки інформації [38].

Розглянемо причини, за яких настають зазначені випадки більш детально [39].

По-перше, – це збої обладнання. До збоїв обладнання можна віднести перебої в електроживленні обладнання, несправності кабельної системи, несправності в роботі серверів, збої робочих станцій, збої роботи мережевих карт, дискових систем тощо [39].

По-друге, до причин настання випадків порушення безпеки інформації можна віднести некоректну роботу програмного забезпечення [40]. До такої некоректної роботи відносяться: повна втрата або часткове змінювання даних у разі помилок у діючому програмному забезпеченні, або, наприклад, втрата даних, спричинена зараженням системи комп'ютерними вірусами тощо [41].

По-третє, – це навмисні дії сторонніх осіб [42]. До таких дій відноситься несанкціоноване копіювання інформації, що підлягає захисту, її знищення, підробка (фальсифікація) або безпесереднє блокування, порушення роботи інформаційної системи, внаслідок якого був спричинений витік інформації [42].

Наступною причиною є помилки обслуговуючого персоналу та користувачів інформаційної системи [43]. До таких помилок належить випадкове знищення або ненавмисне змінення даних; некоректне (недбале) використання програмного та апаратного забезпечення, внаслідок якого відбувається порушення нормальної роботи захищеної інформаційної системи, виникнення вразливих місць інформаційної безпеки, повне або часткове знищення або змінення даних тощо [43].

Особливе місце серед помилок обслуговуючого персоналу та користувачів належить порушенням інтересів інших законних користувачів, а також помилкам, спричиненим неефективною організацією системи захисту інформації, наприклад, втрата конфіденційної інформації або інформації, що містить державну таємницю через неправильне зберігання архівних даних [44].

Останньою причиною за даною класифікацією є навмисні дії обслуговуючого персоналу та користувачів. До даного пункту належить усе зазначене у попередніх трьох пунктах, а також навмисне ознайомлення сторонніх осіб із конфіденційною інформацією організації [45].

Слід зазначити, що даний перелік не є виключним [46]. Порушенням безпеки можна також вважати і дії, за рахунок яких не відбувається безпосередня втрата або витік інформації. Порушення безпеки може бути спричинено діями, що передбачають пряме або непряме втручання до роботи системи [47].

В сучасних інформаційних джерелах вживаються також споріднені терміни, такі як: «безпека інформації» та «безпека інформаційних технологій» [48].

Надзвичайно важливим є розуміння того, що забезпечення безпеки інформаційних технологій повинно обов’язково являти собою комплексну проблему [48]. Відповідне комплексне вирішення даної проблеми повинно охоплювати правове регулювання використання ІТ, впровадження удосконалених технологій, їх розробки, застосування розвиненої системи сертифікації, а також безпосередне забезпечення відповідних організаційно-технічних умов експлуатації [49].

Розв'язання проблеми потребує значних витрат, тому першочерговим завданням є співставлення рівня необхідної інформаційної безпеки і «фінансів», що можуть бути виділені на її підтримку [50]. Витрати на захист інформації не повинні перевищувати її цінності. Для виконання даного правила необхідно визначити потенційні загрози, розрахувати імовірність їх настання, а також визначити та оцінити можливі наслідки порушення інформаційної безпеки. Після цього необхідно вибрати відповідні адекватні заходи та засоби забезпечення інформаційної безпеки і побудувати надійну високоефективну систему інформаційного захисту [51].

1.2 Сучасний стан захисту інформації в комп’ютерних системах і мережах

В провідних країнах світу, у тому числі США, КНР, Австралії та країнах-членах ЄС, розвиток гармонійного інформаційного суспільства визначено одним з головних пріоритетів державної політики [52].

Розглянемо фактори впливу на захист інформації в комп’ютерних системах і мережах за рахунок створення та впровадження політики держави у вищезазначеній сфері [53].

Державна інформаційна політика повинна бути обумовлена зростаючим значенням інформації в кожній сфері життєдіяльності особи, суспільства та держави [54].

При формуванні державної політики, зокрема нашої держави, необхідно враховувати прагнення України набути статусу асоційованого члена ЄС [54]. Також важливим є входження та формат перебування нашої країни в світовому інформаційному просторі. На даний формат впливає поява нових інформаційних загроз та зростання рівня традиційних загроз в інформаційній сфері [55].

Наступним фактором, що суттєво впливає на формування інформаційної політики є загострення комплексу проблем в інформаційній сфері, а також велика кількість неузгоджень та протиріч в нормативно-правовій базі регулювання інформаційної сфери України [55].

Особливо важливим є державний регулюючий вплив на існуючу та перспективну інформаційну сферу, за рахунок реалізації державної політики у сфері інформаційного суспільства [56].

Також важливою для захисту інформації в комп'ютерних системах і мережах є Концепція державної політики у сфері інформатизації та розвитку інформаційного суспільства. Дана Концепція визначена законодавчим актом, в якому позначені наступні компоненти: головна мета, основні завдання, шляхи ефективного розв'язання проблем, а також завдання та функції органів державної влади, механізми взаємодії даних органів між собою та суспільством [57].

Для забезпечення захисту інформації в комп'ютерних системах і мережах, а також з метою вирішення проблеми захисту національних інтересів України запропоновано створення Центрального органу виконавчої влади країни в сфері телекомунікації та інформатизації [57]. Як зазначається в [58], очолити цей Центральний орган має висококваліфікована в цій галузі, порядна та досвідчена людина-науковець.

Основним завданням вищезазначеної державної структури згідно [58] мають бути:

- всебічний прогресивний розвиток та захист галузі ІТ;

- впровадження заходів щодо підвищення інвестиційної привабливості даної структури;
- сприяння виходу нашої держави в світові лідери в ІТ галузі;
- всебічне стимулювання впровадження новітніх ІТ-технологій у вітчизняні виробництва;
- створення конкурентоспроможного національного інформаційного продукту, зокрема сучасних систем захисту інформаційних ресурсів в комп'ютерних системах і мережах [59].

Крім цього, вайжливішим завданням є забезпечення безпеки інформаційних ресурсів в комп'ютерних системах і мережах та інформаційно-телекомунікаційних системах вцілому, що функціонують в інтересах управління державою, і, разом з тим, забезпечують потреби оборони та безпеки держави, економічної, соціальної, кредитно-банківської та інших сфер, систему правління об'єктами критичної інфраструктури [60].

Для виконання даного завдання розробляються та впроваджуються національні стандарти. Крім того затверджуються технічні регламенти застосування інформаційних стандартів, а також технічні регламенти застосування інформаційно-комунікаційних технологій [61]. Дані документи повинні бути гармонізовані із відповідними стандартами держав-членів ЄС. Наприклад, Національні Стандарти України в сфері інформаційно-комунікаційних технологій вже узгоджені з вимогами міжнародної Конвенції про кіберзлочинність. Також необхідним є створення національної системи кібербезпеки на шляху розбудови сучасної, заможної України [62].

Захист інформації в комп'ютерних системах і мережах є невід'ємною складовою сучасного кіберпростору, який розширює свободу і можливості громадян, збагачує суспільство, створює глобальний світовий ринок ідей, досліджень та інновацій [63].

Стрімкий розвиток інформаційних технологій обумовлює появу нових загроз національній та міжнародній безпеці [64].

Зростає кількість та потужність кібератак, мотивованих інтересами окремих осіб, організацій та навіть держав [64]. З цього випливає необхідність вірного вибору використання методів, засобів і заходів ефективної протидії ним і правильного їх використання [65]. Кібербезпека в даному випадку визначається, як захист кібернетичних систем, які являються цілями для кібератак: системи керування, робототехніка, штучний інтелект, соціальні системи тощо [66]. Згідно з аналітичним терміном, кібербезпека охоплює широке значення засобів і концепцій, що пов'язані з забезпеченням інформаційної безпеки [67].

За стандартом ISO/IEC 27032 кібербезпека – стан захищеності інформації від кіберзагроз, тобто загроз доступності, повноти, цілісності, достовірності інформації, яка циркулює в об'єктах національної інформаційної інфраструктури [68].

Звернемось до міжнародного досвіду. Вже в 2010 році стало відомим шкідливе програмне забезпечення Stuxnet. Розповсюдження Stuxnet продемонструвало реальність загроз, які раніше вважалися лише уявними [69]. Це програмне забезпечення мало наступні важливі особливості: здатність атакувати локальні, не підключені до Інтернету мережі. Stuxnet був також призначений для атаки на обладнання промислового ядерного державного об'єкта [70]. Показовим є факт, що спеціалістами з кібербезпеки були виявилені зразки шкідливого програмного забезпечення, яке мало розвідувальні функції [70].

Наступними прикладами є найбільш відомі кібератаки з використанням DuQu, Flamer, Red October [71]. Було встановлено, що деякі з масштабних розвідувальних операцій у кіберпросторі проводились продовж досить тривалого часу, протягом майже десяти років. Цілями даних атак були США, країни Західної Європи, РФ, Казахстан, Білорусь, Україна [72].

Вищенаведений перелік шкідливих програм, які можуть становити загрозу національній кібербезпеці не є вичерпним. Даний перелік досить

стрімко поповнюється [73]. Варто зазначити, що також зростає кількість і частота кібератак, організаторами яких є організовані групи кіберзлочинців.

Дані групи кіберзловмисників досить часто є міжнародними. Для протистояння кібератакам – наслідкам діяльності таких організованих груп кіберзловмисників використовуються наступні засоби [74]:

- засоби антивірусного захисту,
- засоби криптографічного та стеганографічного захисту інформації;
- комплексні системи захисту інформації;
- високоефективні системи управління інформаційною безпекою;
- якісне навчання користувачів і підготовка фахівців тощо [74].

Розглянемо їх більш детально. Антивірусний захист полягає в виявленні та знешкодженні шкідливих програм, які було створено для порушення стабільності стану інформаційної безпеки у системі. Антивірусний захист є одним із ключових базових компонентів захисту сучасних інформаційно-телекомунікаційних систем [74].

Розробка та впровадження комплексних систем захисту інформації (КСЗІ) є наступним засобом забезпечення кібербезпеки. Особливо необхідним компонентом будь-якої інформаційної системи стає впровадження КСЗІ в комп’ютерних системах і мережах, в яких зберігається та обробляється інформація, що належить державі [75].

Розробка і впровадження КСЗІ передбачає декілька етапів: обстеження об’єкта, розробка моделі загроз, розробка моделі порушника, оцінка ризиків, розробка політики безпеки, державна експертиза КСЗІ на підтвердження відповідності [75]. Внесення будь-яких змін у системі вимагають повторного обстеження і обов’язкового внесення змін у модель загроз, переоцінки ризиків інформаційної безпеки, корегування політики безпеки тощо. Найбільш ефективним організаційним засобом забезпечення безпеки інформаційних об’єктів є впровадження системи управління інформаційною

безпекою (СУІБ). В основу системи управління інформаційною безпекою бажано покласти модель PDCA [76], компонентами якої є:

- етап планування (Plan), що включає в себе розроблення СУІБ, оцінювання ризиків і підбір заходів;
- етап дії (Do), що полягає в реалізації і впровадженні обраних заходів;
- етап перевірки (Check), що включає в себе оцінювання ефективності та продуктивності СУІБ. Check переважно виконують внутрішні аудитори;
- етап удосконалення (Act), що полягає в виконанні корегуючих дій [76].

Таким чином, кіберпростір є територією активного протистояння. На превеликий жаль, на сьогоднішній день в даному протистоянні спеціалісти з кібербезпеки поки що програють [77]. Сучасні інформаційні атаки в комп'ютерних системах і мережах використовують вразливості комп'ютерних систем і відповідно здійснюються за допомогою спеціально розробленого програмного забезпечення. В свою чергу, виявлення таких атак ускладнюється обмеженою кількістю спеціально визначених цілей. Здійснення атак на такі цілі не викликають збою роботи комп'ютерів, і тому, як наслідок, тривалий час не потрапляють у поле зору кіберзахисників та інших спеціалістів з антивірусних лабораторій [78]. На сьогоднішній день, для розробки дієвого механізму протидії кіберзагрозам, фахівція з інформаційної безпеки в Україні варто взяти за приклад існуючу дієву практику зарубіжних країн і міжнародної спільноти. Однак впровадження міжнародного досвіду на теренах нашої держави потребує обов'язкового приведення у відповідність до українських реалій [79].

1.3 Аналітичний огляд операції криптографічного перетворення інформації та постановка мети і задач дисертаційного дослідження

Застосування операцій криптографічного перетворення інформації в криптографічних алгоритмах за умови використання груп операцій криптографічного перетворення була висвітлена в [80-82]. Було повністю вивчено повну групу двохрозрядних одноопераднних операцій криптографічного кодування [83-86]. Зокрема, було побудовано пристрій криптографічного перетворення інформації. Саме цей пристрій і реалізував досліджену групу операцій на апаратному рівні [87].

Що стосується підвищення швидкості доступу до конфіденційної інформації, то для досягнення її використовувалось перекодування інформації [88-91]. Основа перекодування полягає у тому, що при переведенні закодованої одноопераднними операціями інформації, на основі однієї псевдовипадкової послідовності, не розкодовуючи її, перекодовують в закодовану на основі іншої псевдовипадкової послідовності.

Наступні дослідження, які проводились, обгрунтовували отримані результати [92-98], результатом яких стало можливим завершення дослідження одноопераднних операцій матричного криптоперетворення.

Разом з дослідженнями одноопераднних лінійних операцій матричного криптографічного перетворення, проводилось дослідження нелінійних одноопераднних операцій розширеного матричного криптографічного перетворення [99-101]. Щодо узагальнення результатів та побудови математичного апарату синтезу й аналізу нелінійних одноопераднних операцій розширеного матричного криптоперетворення, то на сьогоднішній день воно вже майже завершено [102-103].

Вплив надмірності на складність реалізації операцій криптографічного перетворення було досліджено у наступних працях [104-105].

Варто окремо виділити дослідження, які направлені на вивчення операцій криптоперетворення, реалізація яких керується як ключовою

послідовністю, так і інформацією, яка кодується [106]. Багато результатів було отримано в результаті даних робіт. Саме вони забезпечують можливість синтезу моделей одноопераднних операцій перестановок, керованих операцією [107-110]. Існують припущення, що шифрована інформація визначає правила виконання синтезу групи одноопераднних операцій [111-112].

У статті [113] показано, що реалізація одноопераднних операцій криптоперетворення значно важча, порівняно з двохопераднними операціями, зокрема, особлива складність виникає на програмному рівні. Саме тому подальші дослідження були направлені на створення синтезу та аналізу двохопераднних операцій криптографічного перетворення.

В праці [114-116] висвітлені результати розробки методів синтезу та аналізу деяких симетричних груп двохрозрядних операцій синтезованих на основі операцій додавання за модулем.

Методи синтезу та аналізу симетричних груп двохопераднних операцій, які були синтезовані за допомогою операцій додавання за модулем [117-119].

Результати досліджень, які були приведені у працях [120-121], показали можливість синтезу двохопераднних операцій криптографічного перетворення з заданою умовою досягнення максимальної невизначеності результатів шифрування.

Здатність операцій криптографічного додавання за модулем два з точністю до перестановки підвищувати якість потокового шифрування досліджена в [122]. Структурна схема потокового шифрування з використанням групи модифікованих операцій криптографічного додавання за модулем два з точністю до перестановки представлена на рис.1 [122].

Доведено, що дана схема потокового шифрування забезпечує підвищення стійкості та надійності криптографічного перетворення.

Застосування операцій строгого стійкого шифрування в наведеній на рис.1.1 схемі потокового шифрування, розширить варіативність алгоритму

перетворення інформації, крім того, забезпечить максимальну невизначеність кожного біта зашифрованої інформації [122].

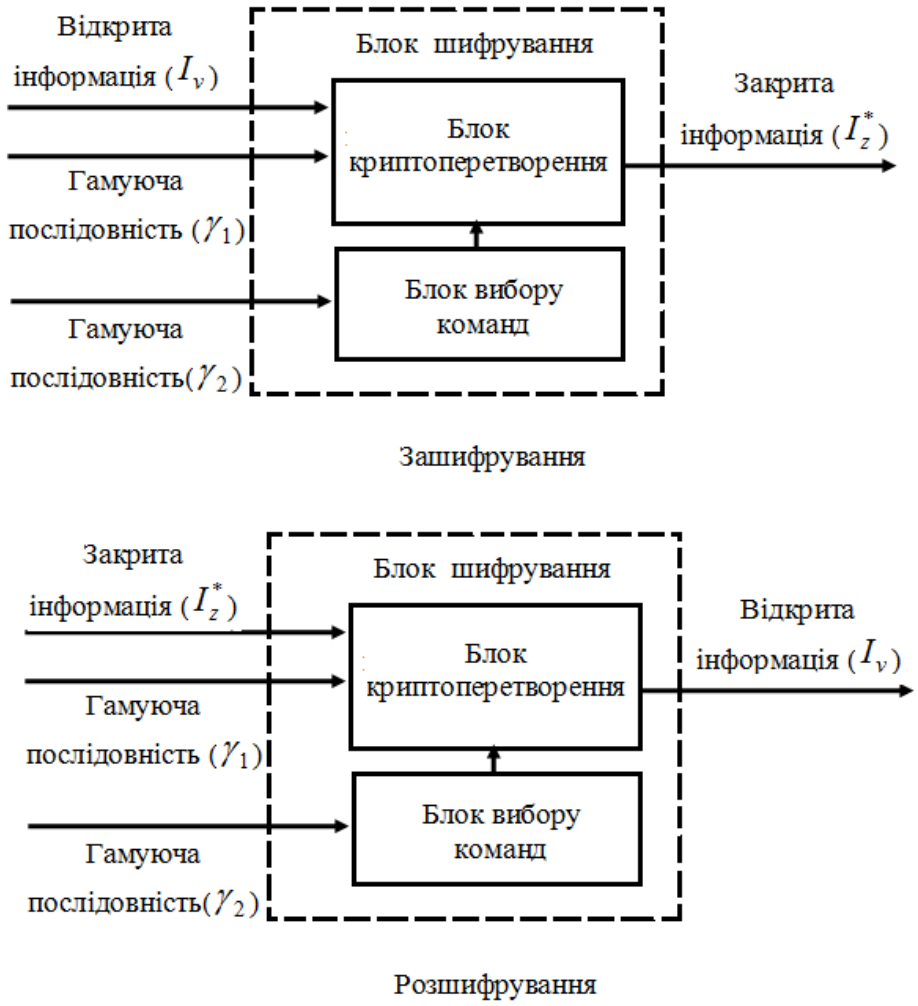


Рис. 1.1 Структурна схема потокового шифрування з використанням групи модифікованих операцій криптографічного додавання за модулем два з точністю до перестановки

Виходячи з наведених матеріалів, доцільно провести дослідження для створення можливості генерації операцій строгого стійкого кодування для вдосконалення функціонування блоку вибору команд.

Метою дисертаційного дослідження є підвищення швидкості потокового шифрування за рахунок генерації псевдовипадкових послідовностей групи ДДО ССКК на основі перетворення другого операнда.

Для досягнення поставленої мети сформульовано і вирішено такі задачі:

- провести синтез ДДО ССКК на основі перетворення другого операнда;

- провести синтез групи ДДО ССКК на основі перетворення другого операнда відомої операції;

- розробити метод генерації псевдовипадкових послідовностей ДДО ССКК на основі перетворення другого операнда та його реалізація.

Вирішення поставлених задач забезпечить підвищення швидкості потокового шифрування за рахунок генерації псевдовипадкових послідовностей групи ДДО ССКК на основі перетворення другого операнда.

Висновки з розділу 1

1. Розгрянуто основні проблеми компьютенної криптографії для захисту інформаційних ресурсів України в кіберпросторі.

2. Проведено аналітичний огляд найбільш поширених методів криптографічного захисту інформації щодо можливості їх використання для захисту інформації в глобальному кібернетичному просторі.

3. Встановлено, що одним з перспективних шляхів розвитку комп'ютерної криптографії, є впровадженя в перспективних комп'ютерних криптоалгоритмах операцій криптографічного кодування інформації. Визначені напрямки вдосконалення криптографічного кодування, сформульовані мета, і на її основі, задачі дисертаційного дослідження.

2 РОЗДІЛ
СИНТЕЗ ОБЕРНЕНИХ ДВОХРОЗРЯДНИХ ДВОХОПЕРАНДНИХ ОПЕРАЦІЙ СТРОГОГО СТІЙКОГО КРИПТОГРАФІЧНОГО КОДУВАННЯ НА ОСНОВІ ПЕРЕТВОРЕННЯ ДРУГОГО ОПЕРАНДА

2.1. Технологія дослідження взаємозв'язків між прямими і оберненими двохрозрядних двохоперандних операцій строгого стійкого криптографічного кодування

Безпека інформації являється одним із найбільш вагомих напрямів успішного розвитку суспільства у сьогоденні. У зв'язку зі зростанням кіберзлочинності, інформаційні ресурси потребують розробки нових та постійного вдосконалення вже існуючих засобів захисту [123]. Насамперед, це стосується криптографічного захисту інформації. Останніми напрямками в розвитку криптології є синтез нових операцій криптоперетворення [124].

Варто зауважити, що шляхи побудови нових операцій криптоперетворення для потокового та блокового шифрування залишаються недостатньо вивченими. Наприклад, досягнення максимальної невизначеності результатів шифрування може бути отримано за допомогою операцій криптоперетворення які відповідають критерію ССКК [125].

Класифікувати операції криптографічного перетворення можна наступним чином: одноопераднi, двоопераднi та багатоопераднi [126].

Група двохрозрядних двохоперандних операцій ССКК [10] включає в себе 24 операції криптоперетворення, які наведені в табл. 2.1 [3,127].

Таблиця 2.1

Група двохрозрядних двохоперандних операцій ССКК

№ п/п	Операції прямого криптоперетворення	Операції оберненого криптоперетворення
1	**2**	**3**
1	$O_1^k=\begin{bmatrix} x_1\cdot\bar{k}_1\oplus x_2\cdot k_1 \\ x_1\cdot k_1\oplus x_2\cdot\bar{k}_1 \end{bmatrix}\oplus\begin{bmatrix} k_2 \\ \bar{k}_2 \end{bmatrix}$	$O_1^d=\begin{bmatrix} x_1\cdot\bar{k}_1\oplus x_2\cdot k_1 \\ x_1\cdot k_1\oplus x_2\cdot\bar{k}_1 \end{bmatrix}\oplus\begin{bmatrix} k_1\oplus k_2 \\ \overline{k_1\oplus k_2} \end{bmatrix}$
2	$O_2^k=\begin{bmatrix} x_1\cdot\bar{k}_1\oplus x_2\cdot k_1 \\ x_1\cdot k_1\oplus x_2\cdot\bar{k}_1 \end{bmatrix}\oplus\begin{bmatrix} k_1\oplus k_2 \\ \overline{k_1\oplus k_2} \end{bmatrix}$	$O_2^d=\begin{bmatrix} x_1\cdot\bar{k}_1\oplus x_2\cdot k_1 \\ x_1\cdot k_1\oplus x_2\cdot\bar{k}_1 \end{bmatrix}\oplus\begin{bmatrix} k_2 \\ \bar{k}_2 \end{bmatrix}$
3	$O_3^k=\begin{bmatrix} x_1\cdot(\overline{k_1\oplus k_2})\oplus x_2\cdot(k_1\oplus k_2) \\ x_1\cdot(k_1\oplus k_2)\oplus x_2\cdot\overline{(k_1\oplus k_2)} \end{bmatrix}\oplus\begin{bmatrix} k_1 \\ \bar{k}_1 \end{bmatrix}$	$O_3^d=\begin{bmatrix} x_1\cdot(\overline{k_1\oplus k_2})\oplus x_2\cdot(k_1\oplus k_2) \\ x_1\cdot(k_1\oplus k_2)\oplus x_2\cdot\overline{(k_1\oplus k_2)} \end{bmatrix}\oplus\begin{bmatrix} k_2 \\ \bar{k}_2 \end{bmatrix}$
4	$O_4^k=\begin{bmatrix} x_1\cdot\bar{k}_2\oplus x_2\cdot k_2 \\ x_1\cdot k_2\oplus x_2\cdot\bar{k}_2 \end{bmatrix}\oplus\begin{bmatrix} k_1 \\ \bar{k}_1 \end{bmatrix}$	$O_4^d=\begin{bmatrix} x_1\cdot\bar{k}_2\oplus x_2\cdot k_2 \\ x_1\cdot k_2\oplus x_2\cdot\bar{k}_2 \end{bmatrix}\oplus\begin{bmatrix} k_1\oplus k_2 \\ \overline{k_1\oplus k_2} \end{bmatrix}$
5	$O_5^k=\begin{bmatrix} x_1\cdot\bar{k}_2\oplus x_2\cdot k_2 \\ x_1\cdot k_2\oplus x_2\cdot\bar{k}_2 \end{bmatrix}\oplus\begin{bmatrix} k_1\oplus k_2 \\ \overline{k_1\oplus k_2} \end{bmatrix}$	$O_5^d=\begin{bmatrix} x_1\cdot\bar{k}_2\oplus x_2\cdot k_2 \\ x_1\cdot k_2\oplus x_2\cdot\bar{k}_2 \end{bmatrix}\oplus\begin{bmatrix} k_1 \\ \bar{k}_1 \end{bmatrix}$
6	$O_6^k=\begin{bmatrix} x_1\cdot(\overline{k_1\oplus k_2})\oplus x_2\cdot(k_1\oplus k_2) \\ x_1\cdot(k_1\oplus k_2)\oplus x_2\cdot\overline{(k_1\oplus k_2)} \end{bmatrix}\oplus\begin{bmatrix} k_2 \\ \bar{k}_2 \end{bmatrix}$	$O_6^k=\begin{bmatrix} x_1\cdot(\overline{k_1\oplus k_2})\oplus x_2\cdot(k_1\oplus k_2) \\ x_1\cdot(k_1\oplus k_2)\oplus x_2\cdot\overline{(k_1\oplus k_2)} \end{bmatrix}\oplus\begin{bmatrix} k_1 \\ \bar{k}_1 \end{bmatrix}$
7	$O_7^k=\begin{bmatrix} x_1\cdot\bar{k}_1\oplus x_2\cdot k_1 \\ x_1\cdot k_1\oplus x_2\cdot\bar{k}_1 \end{bmatrix}\oplus\begin{bmatrix} \overline{k_1\oplus k_2} \\ k_1\oplus k_2 \end{bmatrix}$	$O_7^d=\begin{bmatrix} x_1\cdot\bar{k}_1\oplus x_2\cdot k_1 \\ x_1\cdot k_1\oplus x_2\cdot\bar{k}_1 \end{bmatrix}\oplus\begin{bmatrix} \bar{k}_2 \\ k_2 \end{bmatrix}$
8	$O_8^k=\begin{bmatrix} x_1\cdot\bar{k}_1\oplus x_2\cdot k_1 \\ x_1\cdot k_1\oplus x_2\cdot\bar{k}_1 \end{bmatrix}\oplus\begin{bmatrix} \bar{k}_2 \\ k_2 \end{bmatrix}$	$O_8^d=\begin{bmatrix} x_1\cdot\bar{k}_1\oplus x_2\cdot k_1 \\ x_1\cdot k_1\oplus x_2\cdot\bar{k}_1 \end{bmatrix}\oplus\begin{bmatrix} \overline{k_1\oplus k_2} \\ k_1\oplus k_2 \end{bmatrix}$
9	$O_9^k=\begin{bmatrix} x_1\cdot(\overline{k_1\oplus k_2})\oplus x_2\cdot(k_1\oplus k_2) \\ x_1\cdot(k_1\oplus k_2)\oplus x_2\cdot\overline{(k_1\oplus k_2)} \end{bmatrix}\oplus\begin{bmatrix} \bar{k}_2 \\ k_2 \end{bmatrix}$	$O_9^d=\begin{bmatrix} x_1\cdot(\overline{k_1\oplus k_2})\oplus x_2\cdot(k_1\oplus k_2) \\ x_1\cdot(k_1\oplus k_2)\oplus x_2\cdot\overline{(k_1\oplus k_2)} \end{bmatrix}\oplus\begin{bmatrix} \bar{k}_1 \\ k_1 \end{bmatrix}$
10	$O_{10}^k=\begin{bmatrix} x_1\cdot\bar{k}_2\oplus x_2\cdot k_2 \\ x_1\cdot k_2\oplus x_2\cdot\bar{k}_2 \end{bmatrix}\oplus\begin{bmatrix} \bar{k}_2 \\ k_2 \end{bmatrix}$	$O_{10}^d=\begin{bmatrix} x_1\cdot\bar{k}_2\oplus x_2\cdot k_2 \\ x_1\cdot k_2\oplus x_2\cdot\bar{k}_2 \end{bmatrix}\oplus\begin{bmatrix} \bar{k}_1 \\ k_1 \end{bmatrix}$
11	$O_{11}^k=\begin{bmatrix} x_1\cdot\bar{k}_2\oplus x_2\cdot k_2 \\ x_1\cdot k_2\oplus x_2\cdot\bar{k}_2 \end{bmatrix}\oplus\begin{bmatrix} \bar{k}_1 \\ k_1 \end{bmatrix}$	$O_{11}^d=\begin{bmatrix} x_1\cdot\bar{k}_2\oplus x_2\cdot k_2 \\ x_1\cdot k_2\oplus x_2\cdot\bar{k}_2 \end{bmatrix}\oplus\begin{bmatrix} \bar{k}_2 \\ k_2 \end{bmatrix}$

Продовження таблиці 2.1

1	2	3
12	$O_{12}^{k}=\begin{bmatrix} x_1\cdot(\overline{k_1\oplus k_2})\oplus x_2\cdot(k_1\oplus k_2) \\ x_1\cdot(k_1\oplus k_2)\oplus x_2\cdot(\overline{k_1\oplus k_2}) \end{bmatrix}\oplus\begin{bmatrix} \bar{k}_1 \\ k_1 \end{bmatrix}$	$O_{12}^{d}=\begin{bmatrix} x_1\cdot(\overline{k_1\oplus k_2})\oplus x_2\cdot(k_1\oplus k_2) \\ x_1\cdot(k_1\oplus k_2)\oplus x_2\cdot(\overline{k_1\oplus k_2}) \end{bmatrix}\oplus\begin{bmatrix} \bar{k}_2 \\ k_2 \end{bmatrix}$
13	$O_{13}^{k}=\begin{bmatrix} x_1\cdot(k_1\oplus k_2)\oplus x_2\cdot(\overline{k_1\oplus k_2}) \\ x_1\cdot(\overline{k_1\oplus k_2})\oplus x_2\cdot(k_1\oplus k_2) \end{bmatrix}\oplus\begin{bmatrix} k_2 \\ \bar{k}_2 \end{bmatrix}$	$O_{13}^{d}=\begin{bmatrix} x_1\cdot(k_1\oplus k_2)\oplus x_2\cdot(\overline{k_1\oplus k_2}) \\ x_1\cdot(\overline{k_1\oplus k_2})\oplus x_2\cdot(k_1\oplus k_2) \end{bmatrix}\oplus\begin{bmatrix} \bar{k}_1 \\ k_1 \end{bmatrix}$
14	$O_{14}^{k}=\begin{bmatrix} x_1\cdot k_2\oplus x_2\cdot\bar{k}_2 \\ x_1\cdot\bar{k}_2\oplus x_2\cdot k_2 \end{bmatrix}\oplus\begin{bmatrix} k_2 \\ \bar{k}_2 \end{bmatrix}$	$O_{14}^{d}=\begin{bmatrix} x_1\cdot k_2\oplus x_2\cdot\bar{k}_2 \\ x_1\cdot\bar{k}_2\oplus x_2\cdot k_2 \end{bmatrix}\oplus\begin{bmatrix} k_1 \\ \bar{k}_1 \end{bmatrix}$
15	$O_{15}^{k}=\begin{bmatrix} x_1\cdot k_2\oplus x_2\cdot\bar{k}_2 \\ x_1\cdot\bar{k}_2\oplus x_2\cdot k_2 \end{bmatrix}\oplus\begin{bmatrix} k_1 \\ \bar{k}_1 \end{bmatrix}$	$O_{15}^{d}=\begin{bmatrix} x_1\cdot k_2\oplus x_2\cdot\bar{k}_2 \\ x_1\cdot\bar{k}_2\oplus x_2\cdot k_2 \end{bmatrix}\oplus\begin{bmatrix} \overline{k_1\oplus k_2} \\ k_1\oplus k_2 \end{bmatrix}$
16	$O_{16}^{k}=\begin{bmatrix} x_1\cdot(k_1\oplus k_2)\oplus x_2\cdot(\overline{k_1\oplus k_2}) \\ x_1\cdot(\overline{k_1\oplus k_2})\oplus x_2\cdot(k_1\oplus k_2) \end{bmatrix}\oplus\begin{bmatrix} k_1 \\ \bar{k}_1 \end{bmatrix}$	$O_{16}^{d}=\begin{bmatrix} x_1\cdot(k_1\oplus k_2)\oplus x_2\cdot(\overline{k_1\oplus k_2}) \\ x_1\cdot(\overline{k_1\oplus k_2})\oplus x_2\cdot(k_1\oplus k_2) \end{bmatrix}\oplus\begin{bmatrix} \bar{k}_2 \\ k_2 \end{bmatrix}$
17	$O_{17}^{k}=\begin{bmatrix} x_1\cdot k_1\oplus x_2\cdot\bar{k}_1 \\ x_1\cdot\bar{k}_1\oplus x_2\cdot k_1 \end{bmatrix}\oplus\begin{bmatrix} k_1\oplus k_2 \\ \overline{k_1\oplus k_2} \end{bmatrix}$	$O_{17}^{d}=\begin{bmatrix} x_1\cdot k_1\oplus x_2\cdot\bar{k}_1 \\ x_1\cdot\bar{k}_1\oplus x_2\cdot k_1 \end{bmatrix}\oplus\begin{bmatrix} \bar{k}_2 \\ k_2 \end{bmatrix}$
18	$O_{18}^{k}=\begin{bmatrix} x_1\cdot k_1\oplus x_2\cdot\bar{k}_1 \\ x_1\cdot\bar{k}_1\oplus x_2\cdot k_1 \end{bmatrix}\oplus\begin{bmatrix} k_2 \\ \bar{k}_2 \end{bmatrix}$	$O_{18}^{d}=\begin{bmatrix} x_1\cdot k_1\oplus x_2\cdot\bar{k}_1 \\ x_1\cdot\bar{k}_1\oplus x_2\cdot k_1 \end{bmatrix}\oplus\begin{bmatrix} \overline{k_1\oplus k_2} \\ k_1\oplus k_2 \end{bmatrix}$
19	$O_{19}^{k}=\begin{bmatrix} x_1\cdot\bar{k}_2\oplus x_2\cdot k_2 \\ x_1\cdot k_2\oplus x_2\cdot\bar{k}_2 \end{bmatrix}\oplus\begin{bmatrix} k_1 \\ \bar{k}_1 \end{bmatrix}$	$O_{19}^{d}=\begin{bmatrix} x_1\cdot\bar{k}_2\oplus x_2\cdot k_2 \\ x_1\cdot k_2\oplus x_2\cdot\bar{k}_2 \end{bmatrix}\oplus\begin{bmatrix} k_2 \\ \bar{k}_2 \end{bmatrix}$
20	$O_{20}^{k}=\begin{bmatrix} x_1\cdot(k_1\oplus k_2)\oplus x_2\cdot(\overline{k_1\oplus k_2}) \\ x_1\cdot(\overline{k_1\oplus k_2})\oplus x_2\cdot(k_1\oplus k_2) \end{bmatrix}\oplus\begin{bmatrix} \bar{k}_1 \\ k_1 \end{bmatrix}$	$O_{20}^{d}=\begin{bmatrix} x_1\cdot(k_1\oplus k_2)\oplus x_2\cdot(\overline{k_1\oplus k_2}) \\ x_1\cdot(\overline{k_1\oplus k_2})\oplus x_2\cdot(k_1\oplus k_2) \end{bmatrix}\oplus\begin{bmatrix} k_2 \\ \bar{k}_2 \end{bmatrix}$
21	$O_{21}^{k}=\begin{bmatrix} x_1\cdot k_1\oplus x_2\cdot\bar{k}_1 \\ x_1\cdot\bar{k}_1\oplus x_2\cdot k_1 \end{bmatrix}\oplus\begin{bmatrix} \overline{k_1\oplus k_2} \\ k_1\oplus k_2 \end{bmatrix}$	$O_{21}^{d}=\begin{bmatrix} x_1\cdot k_1\oplus x_2\cdot\bar{k}_1 \\ x_1\cdot\bar{k}_1\oplus x_2\cdot k_1 \end{bmatrix}\oplus\begin{bmatrix} k_2 \\ \bar{k}_2 \end{bmatrix}$
22	$O_{22}^{k}=\begin{bmatrix} x_1\cdot k_1\oplus x_2\cdot\bar{k}_1 \\ x_1\cdot\bar{k}_1\oplus x_2\cdot k_1 \end{bmatrix}\oplus\begin{bmatrix} \bar{k}_2 \\ k_2 \end{bmatrix}$	$O_{22}^{d}=\begin{bmatrix} x_1\cdot k_1\oplus x_2\cdot\bar{k}_1 \\ x_1\cdot\bar{k}_1\oplus x_2\cdot k_1 \end{bmatrix}\oplus\begin{bmatrix} k_1\oplus k_2 \\ \overline{k_1\oplus k_2} \end{bmatrix}$
23	$O_{23}^{k}=\begin{bmatrix} x_1\cdot(k_1\oplus k_2)\oplus x_2\cdot(\overline{k_1\oplus k_2}) \\ x_1\cdot(\overline{k_1\oplus k_2})\oplus x_2\cdot(k_1\oplus k_2) \end{bmatrix}\oplus\begin{bmatrix} \bar{k}_2 \\ k_2 \end{bmatrix}$	$O_{23}^{d}=\begin{bmatrix} x_1\cdot(k_1\oplus k_2)\oplus x_2\cdot(\overline{k_1\oplus k_2}) \\ x_1\cdot(\overline{k_1\oplus k_2})\oplus x_2\cdot(k_1\oplus k_2) \end{bmatrix}\oplus\begin{bmatrix} k_1 \\ \bar{k}_1 \end{bmatrix}$
24	$O_{24}^{k}=\begin{bmatrix} x_1\cdot k_2\oplus x_2\cdot\bar{k}_2 \\ x_1\cdot\bar{k}_2\oplus x_2\cdot k_2 \end{bmatrix}\oplus\begin{bmatrix} \overline{k_1\oplus k_2} \\ k_1\oplus k_2 \end{bmatrix}$	$O_{24}^{d}=\begin{bmatrix} x_1\cdot k_2\oplus x_2\cdot\bar{k}_2 \\ x_1\cdot\bar{k}_2\oplus x_2\cdot k_2 \end{bmatrix}\oplus\begin{bmatrix} k_1 \\ \bar{k}_1 \end{bmatrix}$

Дані операції згруповані в табл. 2.1 таким чином, що кожній операції в першому стовпчику відповідає обернена їй операція з другого стовпчика і навпаки, операції з другого стовпчика відповідає обернена їй операція з першого стовпчика, тобто в кожному рядку представлені дві взаємообернені операції [3].

Проте основним недоліком даного підходу залишається необхідність зберігати в пам'яті всі прямі операції криптоперетворення, що може бути критичним при побудові систем малоресурсної криптографії. Для подолання даного протиріччя було б доцільно встановити взаємозв'язки між операціями, а також між прямими та оберненими операціями криптоперетворення.

2.2 Встановлення взаємозв'язків між прямими і оберненими операціями в групі двохрозрядних двохоперандних операцій строгого стійкого криптографічного кодування.

Для досягнення поставленої мети на даному етапі дослідження необхідно знайти взаємозв'язки між прямими та оберненими операціями криптоперетворення.

Нехай пряма операція буде O_1^k, тоді оберненою їй операцією буде O_2^k. Для знаходження взаємозв'язку, покажемо пряму та обернену операції криптоперетворення у розгорнутому представленні. Саме такий вигляд операцій показує взаємозв'язок між одноопераднними операціями криптоперетворення першого операнда, в залежності від значення другого операнда двохрозрядної двохоперандної операції криптографічного кодування.

Таким чином, наші операції мають наступний вигляд:

$$O_1^k = \begin{bmatrix} x_1 \cdot \bar{k}_1 \oplus x_2 \cdot k_1 \\ x_1 \cdot k_1 \oplus x_2 \cdot \bar{k}_1 \end{bmatrix} \oplus \begin{bmatrix} k_2 \\ \bar{k}_2 \end{bmatrix} = \begin{cases} \begin{bmatrix} x_1 \\ x_2 \oplus 1 \end{bmatrix}, \text{ якщо } k_1 = 0; k_2 = 0 \\ \begin{bmatrix} x_1 \oplus 1 \\ x_2 \end{bmatrix}, \text{якщо } k_1 = 0; k_2 = 1 \\ \begin{bmatrix} x_2 \\ x_1 \oplus 1 \end{bmatrix}, \text{ якщо } k_1 = 1; k_2 = 0 \\ \begin{bmatrix} x_2 \oplus 1 \\ x_1 \end{bmatrix}, \text{якщо } k_1 = 1; k_2 = 1 \end{cases} \quad (2.1)$$

$$O_2^k = \begin{bmatrix} x_1 \cdot \bar{k}_1 \oplus x_2 \cdot k_1 \\ x_1 \cdot k_1 \oplus x_2 \cdot \bar{k}_1 \end{bmatrix} \oplus \begin{bmatrix} k_1 \oplus k_2 \\ \overline{k_1 \oplus k_2} \end{bmatrix} = \begin{cases} \begin{bmatrix} x_1 \\ x_2 \oplus 1 \end{bmatrix}, \text{ якщо } k_1 = 0; k_2 = 0 \\ \begin{bmatrix} x_1 \oplus 1 \\ x_2 \end{bmatrix}, \text{якщо } k_1 = 0; k_2 = 1 \\ \begin{bmatrix} x_2 \oplus 1 \\ x_1 \end{bmatrix}, \text{ якщо } k_1 = 1; k_2 = 0 \\ \begin{bmatrix} x_2 \\ x_1 \oplus 1 \end{bmatrix}, \text{якщо } k_1 = 1; k_2 = 1 \end{cases} \quad (2.2)$$

Операції O_1^k та O_2^k відрізняються одна від одної порядком розміщення одноопераднної операції обробки першого операнда. Порядок розміщення одноопераднної операції обробки першого операнда визначається значенням другого операнда, тобто умовою виконання. Виходячи з цього для побудови оберненої операції достатньо в прямій операції змінити умови її виконання. Встановити взаємозв'язки між операціями можна на основі моделі перетворення значення другого операнда прямої операції в значення другого операнда оберненої операції.

Враховуючи це, встановимо взаємозв'язок між значеннями других операндів, на основі побудови дискретної моделі перетворення. Для цього використаємо значення другого операнда прямої операції як вхідні дані, а значення другого операнда оберненої операції, як результат реалізації моделі дискретного перетворення. Для мінімізації дискретного автомату, побудуємо таблицю істинності. Дані представлені в табл. 2.2 [3].

Таблиця 2.2

Таблиця істинтиності дискретного автомату перетворення O_1^k в O_2^k

Другий операнд прямої операції		Другий операнд оберненої операції	
k_1	k_2	k_1^*	k_2^*
0	0	0	0
0	1	0	1
1	0	1	1
1	1	1	0

Мінімізувавши дану таблицю істинності отримуємо дискретну модель автомата побудови другого операнду оберненої операції:

$$k_1^* = k_1,\ k_2^* = k_1 \oplus k_2 \qquad (2.3)$$

Дана модель дає можливість побудувати обернену операцію O_2^k, на основі прямої операції O_1^k.

По аналогії дослідимо взаємозв'язки між операціями O_3^k та O_6^k. Тобто, у даному випадку, за пряму операцію візьмемо O_3^k, тоді оберненою для неї операцією буде O_6^k. У розгорнутому представленні операції O_3^k та O_6^k будуть виглядати наступним чином:

$$O_3^k = \begin{bmatrix} x_1 \cdot (\overline{k_1 \oplus k_2}) \oplus x_2 \cdot (k_1 \oplus k_2) \\ x_1 \cdot (k_1 \oplus k_2) \oplus x_2 \cdot (\overline{k_1 \oplus k_2}) \end{bmatrix} \oplus \begin{bmatrix} k_1 \\ \bar{k}_1 \end{bmatrix} = \begin{cases} \begin{bmatrix} x_1 \\ x_2 \oplus 1 \end{bmatrix}, \text{ якщо } k_1 = 0; k_2 = 0 \\ \begin{bmatrix} x_2 \\ x_1 \oplus 1 \end{bmatrix}, \text{якщо } k_1 = 0; k_2 = 1 \\ \begin{bmatrix} x_2 \oplus 1 \\ x_1 \end{bmatrix}, \text{ якщо } k_1 = 1; k_2 = 0 \\ \begin{bmatrix} x_1 \oplus 1 \\ x_2 \end{bmatrix}, \text{якщо } k_1 = 1; k_2 = 1 \end{cases} \qquad (2.4)$$

$$O_6^{\kappa} = \begin{bmatrix} x_1 \cdot (\overline{k_1 \oplus k_2}) \oplus x_2 \cdot (k_1 \oplus k_2) \\ x_1 \cdot (k_1 \oplus k_2) \oplus x_2 \cdot (\overline{k_1 \oplus k_2}) \end{bmatrix} \oplus \begin{bmatrix} k_2 \\ \bar{k}_2 \end{bmatrix} = \begin{cases} \begin{bmatrix} x_1 \\ x_2 \oplus 1 \end{bmatrix}, \text{ якщо } k_1 = 0; k_2 = 0 \\ \begin{bmatrix} x_2 \oplus 1 \\ x_1 \end{bmatrix}, \text{якщо } k_1 = 0; k_2 = 1 \\ \begin{bmatrix} x_2 \\ x_1 \oplus 1 \end{bmatrix}, \text{ якщо } k_1 = 1; k_2 = 0 \\ \begin{bmatrix} x_1 \oplus 1 \\ x_2 \end{bmatrix}, \text{якщо } k_1 = 1; k_2 = 1 \end{cases} \quad (2.5)$$

де x – значення першого операнда, k – значення другого операнда.

Різницею між даними операціями є розташування одноопераднної операції обробки першого операнда, яке визначається значенням другого операнда, тобто його умовою виконання. Згідно вищевказаного, для побудови оберненої операції достатньо в прямій операції змінити умови її виконання. Тобто взаємозв'язки між операціями можна встановити на основі моделі перетворення значення другого операнда прямої операції в значення другого операнда оберненої операції.

Встановлюємо взаємозв'язок між значеннями других операндів на основі побудови дискретної моделі перетворення. За допомогою використання значення другого операнда прямої операції як вхідні дані, а значення другого операнда оберненої операції як результат реалізації моделі дискретного перетворення можна побудувати таблицю істинності дискретної моделі автомата для O_3^k і O_6^k (табл. 2.3) [3]:

Таблиця 2.3

Таблиця істинності дискретного автомату перетворення O_3^k та O_6^k

Другий операнд прямої операції		**Другий операнд оберненої операції**	
k_1	k_2	k_1^*	k_2^*
0	0	0	0
0	1	1	0
1	0	0	1
1	1	1	1

Якщо мінімізувати дану таблицю істинності, отримуємо дискретну модель автомата побудови другого операнда оберненої операції:

$$k_1^* = k_2\ ,\ k_2^* = k_1 \qquad (2.6)$$

Дана модель автомата дає можливість на основі прямої операції O_3^k побудувати обернену до неї операцію O_6^k (2.6).

Згідно вже сказаного раніше, дослідимо взаємозв'язки між операціями O_4^k та O_5^k. Прямою операцією, в даному випадку, виступає O_4^k, а оберненою до неї операцією буде O_5^k. У розгорнутому представленні операції O_4^k і O_5^k мають наступний вигляд: (2.7-2.8)

$$O_4^k = \begin{bmatrix} x_1 \cdot \bar{k}_2 \oplus x_2 \cdot k_2 \\ x_1 \cdot k_2 \oplus x_2 \cdot \bar{k}_2 \end{bmatrix} \oplus \begin{bmatrix} k_1 \\ \bar{k}_1 \end{bmatrix} = \begin{cases} \begin{bmatrix} x_1 \\ x_2 \oplus 1 \end{bmatrix}, \text{ якщо } k_1 = 0;\ k_2 = 0 \\ \begin{bmatrix} x_2 \\ x_1 \oplus 1 \end{bmatrix}, \text{якщо } k_1 = 0;\ k_2 = 1 \\ \begin{bmatrix} x_1 \oplus 1 \\ x_2 \end{bmatrix}, \text{ якщо } k_1 = 1;\ k_2 = 0 \\ \begin{bmatrix} x_2 \oplus 1 \\ x_1 \end{bmatrix}, \text{якщо } k_1 = 1;\ k_2 = 1 \end{cases} \qquad (2.7)$$

$$O_5^k = \begin{bmatrix} x_1 \cdot \bar{k}_2 \oplus x_2 \cdot k_2 \\ x_1 \cdot k_2 \oplus x_2 \cdot \bar{k}_2 \end{bmatrix} \oplus \begin{bmatrix} k_1 \oplus k_2 \\ \overline{k_1 \oplus k_2} \end{bmatrix} = \begin{cases} \begin{bmatrix} x_1 \\ x_2 \oplus 1 \end{bmatrix}, \text{ якщо } k_1 = 0;\ k_2 = 0 \\ \begin{bmatrix} x_2 \oplus 1 \\ x_1 \end{bmatrix}, \text{якщо } k_1 = 0;\ k_2 = 1 \\ \begin{bmatrix} x_1 \oplus 1 \\ x_2 \end{bmatrix}, \text{ якщо } k_1 = 1;\ k_2 = 0 \\ \begin{bmatrix} x_2 \\ x_1 \oplus 1 \end{bmatrix}, \text{якщо } k_1 = 1;\ k_2 = 1 \end{cases} \qquad (2.8)$$

де x – значення першого операнда, k – значення другого операнда.

Аналогічно попереднім операціям, дослідимо взаємозв'язки між операціями O_4^k та O_5^k та побудуємо таблицю істинності дискретної моделі автомата для O_4^k та O_5^k (табл. 2.4):

Дискретна модель дає можливість побудувати обернену операцію O_5^k на основі прямої операції O_4^k .

На основі даного твердження було знайдено взаємозв'язки між всіма двохрозрядними двохоперандними операціями групи операцій ССКК, що досліджувалась [3].

$$k_1^* = \overline{k_1 \oplus k_2}\ ,\ k_2^* = k_2 \qquad (2.9)$$

Таблиця 2.4

Таблиця істинності дискретного автомату перетворення O_4^k та O_5^k

Другий операнд прямої операції		Другий операнд оберненої операції	
k_1	k_2	k_1^*	k_2^*
0	0	1	0
0	1	0	1
1	0	0	0
1	1	1	1

За результатами дослідження визначені та формалізовані взаємозв'язки між прямими і оберненими операціями криптографічного перетворення. Наведені приклади показують коректність запропонованого підходу для проведення досліджень. Аналогічно до наведених прикладів було встановлено всі взаємозв'язки в групі двохрозрядних двохоперандних операцій ССКК.

2.3 Синтез обернених двохрозрядних двохоперандних операцій строгого стійкого криптографічного кодування на основі встановлених взаємозв'язків

Формалізовані взаємозв'язки між прямими і оберненими операціями дозволяють побудувати метод синтезу обернених двохрозрядних двохоперандних операцій ССКК на основі перетворення другого операнда.

Обернена операція ССКК, як і пряма операція, просто реалізуються як на апаратному, так і програмному рівнях, адже, синтез оберненої операції з урахуванням перспективи, як в прямому, так і в оберненому каналах шифрування однакових гамуючих послідовностей операцій було доведено [8,156].

Оскільки в результаті синтезу прямої та оберненої операцій виявлено, що має місце повторення операцій, то існує потреба використати перетворення другого операнда для покращення якостей криптографічного кодування. Отримані взаємозв'язки створили теоретичне підґрунтя для побудови методу синтезу обернених двохрозрядних двохоперандних операцій ССКК, на основі перетворення другого операнда [4,6].

Для досягнення результату, необхідно формалізувати та довести коректність застосування виявлених взаємозв'язків для побудови обернених двохрозрядних двохоперандних операцій ССКК, шляхом перетворення другого операнда [3,8].

Візьмемо операцію $O_1^k = \begin{bmatrix} x_1 \cdot \bar{k}_1 \oplus x_2 \cdot k_1 \\ x_1 \cdot k_1 \oplus x_2 \cdot \bar{k}_1 \end{bmatrix} \oplus \begin{bmatrix} k_2 \\ \bar{k}_2 \end{bmatrix}$ за операцію кодування, а $O_1^d = \begin{bmatrix} x_1 \cdot \bar{k}_1 \oplus x_2 \cdot k_1 \\ x_1 \cdot k_1 \oplus x_2 \cdot \bar{k}_1 \end{bmatrix} \oplus \begin{bmatrix} k_1 \oplus k_2 \\ \overline{k_1 \oplus k_2} \end{bmatrix}$ – за операцію декодування, тоді O_1^k можна застосувати в якості O_1^d, за умови $k_1^* = k_1$, $k_2^* = k_1 \oplus k_2$.

Оскільки дані операції задані моделями:

$$O_1^k = \begin{bmatrix} x_1 \cdot \bar{k}_1 \oplus x_2 \cdot k_1 \\ x_1 \cdot k_1 \oplus x_2 \cdot \bar{k}_1 \end{bmatrix} \oplus \begin{bmatrix} k_2 \\ \bar{k}_2 \end{bmatrix} = \begin{cases} \begin{bmatrix} x_1 \\ x_2 \oplus 1 \end{bmatrix}, \text{ якщо } k_1 = 0; k_2 = 0 \\ \begin{bmatrix} x_1 \oplus 1 \\ x_2 \end{bmatrix}, \text{якщо } k_1 = 0; k_2 = 1 \\ \begin{bmatrix} x_2 \\ x_1 \oplus 1 \end{bmatrix}, \text{ якщо } k_1 = 1; k_2 = 0 \\ \begin{bmatrix} x_2 \oplus 1 \\ x_1 \end{bmatrix}, \text{якщо } k_1 = 1; k_2 = 1 \end{cases} \quad (2.10)$$

$$O_1^d = \begin{bmatrix} x_1 \cdot \bar{k}_1 \oplus x_2 \cdot k_1 \\ x_1 \cdot k_1 \oplus x_2 \cdot \bar{k}_1 \end{bmatrix} \oplus \begin{bmatrix} k_1 \oplus k_2 \\ \overline{k_1 \oplus k_2} \end{bmatrix} = \begin{cases} \begin{bmatrix} x_1 \\ x_2 \oplus 1 \end{bmatrix}, \text{ якщо } k_1 = 0; k_2 = 0 \\ \begin{bmatrix} x_1 \oplus 1 \\ x_2 \end{bmatrix}, \text{якщо } k_1 = 0; k_2 = 1 \\ \begin{bmatrix} x_2 \oplus 1 \\ x_1 \end{bmatrix}, \text{ якщо } k_1 = 1; k_2 = 0 \\ \begin{bmatrix} x_2 \\ x_1 \oplus 1 \end{bmatrix}, \text{якщо } k_1 = 1; k_2 = 1 \end{cases} \quad (2.11)$$

Таким чином, використавши дану умову для другого операнда, отримуємо наступне перетворення:

$$O_1^{k^*} = \begin{cases} \begin{bmatrix} x_1 \\ x_2 \oplus 1 \end{bmatrix}, \text{ якщо } k_1^* = 0; k_2^* = 0 \\ \begin{bmatrix} x_1 \oplus 1 \\ x_2 \end{bmatrix}, \text{якщо } k_1^* = 0; k_2^* = 1 \\ \begin{bmatrix} x_2 \\ x_1 \oplus 1 \end{bmatrix}, \text{ якщо } k_1^* = 1; k_2^* = 0 \\ \begin{bmatrix} x_2 \oplus 1 \\ x_1 \end{bmatrix}, \text{якщо } k_1^* = 1; k_2^* = 1 \end{cases} = \begin{cases} \begin{bmatrix} x_1 \\ x_2 \oplus 1 \end{bmatrix}, \text{ якщо } k_1 = 0; k_2 = 0 \\ \begin{bmatrix} x_1 \oplus 1 \\ x_2 \end{bmatrix}, \text{якщо } k_1 = 0; k_2 = 1 \\ \begin{bmatrix} x_2 \\ x_1 \oplus 1 \end{bmatrix}, \text{ якщо } k_1 = 1; k_2 = 1 \\ \begin{bmatrix} x_2 \oplus 1 \\ x_1 \end{bmatrix}, \text{якщо } k_1 = 1; k_2 = 0 \end{cases} = \begin{cases} \begin{bmatrix} x_1 \\ x_2 \oplus 1 \end{bmatrix}, \text{ якщо } k_1 = 0; k_2 = 0 \\ \begin{bmatrix} x_1 \oplus 1 \\ x_2 \end{bmatrix}, \text{якщо } k_1 = 0; k_2 = 1 \\ \begin{bmatrix} x_2 \oplus 1 \\ x_1 \end{bmatrix}, \text{ якщо } k_1 = 1; k_2 = 0 \\ \begin{bmatrix} x_2 \\ x_1 \oplus 1 \end{bmatrix}, \text{якщо } k_1 = 1; k_2 = 1 \end{cases} = O_1^d \quad (2.12)$$

Що й потрібно було довести.

Розглянемо наступну пару операцій: $O_2^k = \begin{bmatrix} x_1 \cdot \bar{k}_1 \oplus x_2 \cdot k_1 \\ x_1 \cdot k_1 \oplus x_2 \cdot \bar{k}_1 \end{bmatrix} \oplus \begin{bmatrix} k_1 \oplus k_2 \\ \overline{k_1 \oplus k_2} \end{bmatrix}$ – операція кодування, а $O_2^d = \begin{bmatrix} x_1 \cdot \bar{k}_1 \oplus x_2 \cdot k_1 \\ x_1 \cdot k_1 \oplus x_2 \cdot \bar{k}_1 \end{bmatrix} \oplus \begin{bmatrix} k_2 \\ \bar{k}_2 \end{bmatrix}$ – операція декодування, тоді O_2^k можна застосувати в якості O_2^d, за наступної умови $k_1^* = k_1$, $k_2^* = k_1 \oplus k_2$.

Так як вигляд операцій в розгорнутому вигляді матиме наступне представлення:

$$O_2^k=\begin{bmatrix} x_1\cdot\bar{k}_1\oplus x_2\cdot k_1 \\ x_1\cdot k_1\oplus x_2\cdot\bar{k}_1 \end{bmatrix}\oplus\begin{bmatrix} k_1\oplus k_2 \\ \overline{k_1\oplus k_2} \end{bmatrix}=\begin{cases} \begin{bmatrix} x_1 \\ x_2\oplus 1 \end{bmatrix}, \text{ якщо } k_1=0;\ k_2=0 \\ \begin{bmatrix} x_1\oplus 1 \\ x_2 \end{bmatrix}, \text{якщо } k_1=0;\ k_2=1 \\ \begin{bmatrix} x_2\oplus 1 \\ x_1 \end{bmatrix}, \text{ якщо } k_1=1;\ k_2=0 \\ \begin{bmatrix} x_2 \\ x_1\oplus 1 \end{bmatrix}, \text{якщо } k_1=1;\ k_2=1 \end{cases} \quad (2.13)$$

$$O_2^d=\begin{bmatrix} x_1\cdot\bar{k}_1\oplus x_2\cdot k_1 \\ x_1\cdot k_1\oplus x_2\cdot\bar{k}_1 \end{bmatrix}\oplus\begin{bmatrix} k_2 \\ \bar{k}_2 \end{bmatrix}=\begin{cases} \begin{bmatrix} x_1 \\ x_2\oplus 1 \end{bmatrix}, \text{ якщо } k_1=0;\ k_2=0 \\ \begin{bmatrix} x_1\oplus 1 \\ x_2 \end{bmatrix}, \text{якщо } k_1=0;\ k_2=1 \\ \begin{bmatrix} x_2 \\ x_1\oplus 1 \end{bmatrix}, \text{ якщо } k_1=1;\ k_2=0 \\ \begin{bmatrix} x_2\oplus 1 \\ x_1 \end{bmatrix}, \text{якщо } k_1=1;\ k_2=1 \end{cases} \quad (2.14)$$

отримуємо наступне перетворення:

$$O_2^{k*}=\begin{cases} \begin{bmatrix} x_1 \\ x_2\oplus 1 \end{bmatrix}, \text{ якщо } k_1^*=0;\ k_2^*=0 \\ \begin{bmatrix} x_1\oplus 1 \\ x_2 \end{bmatrix}, \text{якщо } k_1^*=0;\ k_2^*=1 \\ \begin{bmatrix} x_2\oplus 1 \\ x_1 \end{bmatrix}, \text{ якщо } k_1^*=1;\ k_2^*=0 \\ \begin{bmatrix} x_2 \\ x_1\oplus 1 \end{bmatrix}, \text{якщо } k_1^*=1;\ k_2^*=1 \end{cases}=\begin{cases} \begin{bmatrix} x_1 \\ x_2\oplus 1 \end{bmatrix}, \text{ якщо } k_1=0;\ k_2=0 \\ \begin{bmatrix} x_1\oplus 1 \\ x_2 \end{bmatrix}, \text{якщо } k_1=0;\ k_2=1 \\ \begin{bmatrix} x_2\oplus 1 \\ x_1 \end{bmatrix}, \text{ якщо } k_1=1;\ k_2=1 \\ \begin{bmatrix} x_2 \\ x_1\oplus 1 \end{bmatrix}, \text{якщо } k_1=1;\ k_2=0 \end{cases}=\begin{cases} \begin{bmatrix} x_1 \\ x_2\oplus 1 \end{bmatrix}, \text{ якщо } k_1=0;\ k_2=0 \\ \begin{bmatrix} x_1\oplus 1 \\ x_2 \end{bmatrix}, \text{якщо } k_1=0;\ k_2=1 \\ \begin{bmatrix} x_2 \\ x_1\oplus 1 \end{bmatrix}, \text{ якщо } k_1=1;\ k_2=0 \\ \begin{bmatrix} x_2\oplus 1 \\ x_1 \end{bmatrix}, \text{якщо } k_1=1;\ k_2=1 \end{cases}=O_2^d \quad (2.15)$$

Що доводить коректність застосування виявлених умов перетворення.

Наступна комбінація операцій: $O_3^k=\begin{bmatrix} x_1\cdot\overline{(k_1\oplus k_2)}\oplus x_2\cdot(k_1\oplus k_2) \\ x_1\cdot(k_1\oplus k_2)\oplus x_2\cdot\overline{(k_1\oplus k_2)} \end{bmatrix}\oplus\begin{bmatrix} k_1 \\ \bar{k}_1 \end{bmatrix}$ – операція кодування, а $O_3^d=\begin{bmatrix} x_1\cdot\overline{(k_1\oplus k_2)}\oplus x_2\cdot(k_1\oplus k_2) \\ x_1\cdot(k_1\oplus k_2)\oplus x_2\cdot\overline{(k_1\oplus k_2)} \end{bmatrix}\oplus\begin{bmatrix} k_2 \\ \bar{k}_2 \end{bmatrix}$ – операція декодування. Згідно попереднього прикладу можна стверджувати, що O_3^k застосовується в якості O_3^d, за умови $k_1^*=k_2$, $k_2^*=k_1$.

Так як дані операції можна представити моделями:

$$O_3^k = \begin{bmatrix} x_1 \cdot (\overline{k_1 \oplus k_2}) \oplus x_2 \cdot (k_1 \oplus k_2) \\ x_1 \cdot (k_1 \oplus k_2) \oplus x_2 \cdot (\overline{k_1 \oplus k_2}) \end{bmatrix} \oplus \begin{bmatrix} k_1 \\ \bar{k}_1 \end{bmatrix} = \begin{cases} \begin{bmatrix} x_1 \\ x_2 \oplus 1 \end{bmatrix}, \text{ якщо } k_1 = 0; k_2 = 0 \\ \begin{bmatrix} x_2 \\ x_1 \oplus 1 \end{bmatrix}, \text{якщо } k_1 = 0; k_2 = 1 \\ \begin{bmatrix} x_2 \oplus 1 \\ x_1 \end{bmatrix}, \text{ якщо } k_1 = 1; k_2 = 0 \\ \begin{bmatrix} x_1 \oplus 1 \\ x_2 \end{bmatrix}, \text{якщо } k_1 = 1; k_2 = 1 \end{cases} \quad (2.16)$$

$$O_3^d = \begin{bmatrix} x_1 \cdot (\overline{k_1 \oplus k_2}) \oplus x_2 \cdot (k_1 \oplus k_2) \\ x_1 \cdot (k_1 \oplus k_2) \oplus x_2 \cdot (\overline{k_1 \oplus k_2}) \end{bmatrix} \oplus \begin{bmatrix} k_2 \\ \bar{k}_2 \end{bmatrix} = \begin{cases} \begin{bmatrix} x_1 \\ x_2 \oplus 1 \end{bmatrix}, \text{ якщо } k_1 = 0; k_2 = 0 \\ \begin{bmatrix} x_2 \oplus 1 \\ x_1 \end{bmatrix}, \text{якщо } k_1 = 0; k_2 = 1 \\ \begin{bmatrix} x_2 \\ x_1 \oplus 1 \end{bmatrix}, \text{ якщо } k_1 = 1; k_2 = 0 \\ \begin{bmatrix} x_1 \oplus 1 \\ x_2 \end{bmatrix}, \text{якщо } k_1 = 1; k_2 = 1 \end{cases} \quad (2.17)$$

Отримуємо перетворення у вигляді:

$$O_3^{k*} = \begin{cases} \begin{bmatrix} x_1 \\ x_2 \oplus 1 \end{bmatrix}, \text{ якщо } k_1^* = 0; k_2^* = 0 \\ \begin{bmatrix} x_2 \\ x_1 \oplus 1 \end{bmatrix}, \text{якщо } k_1^* = 0; k_2^* = 1 \\ \begin{bmatrix} x_2 \oplus 1 \\ x_1 \end{bmatrix}, \text{ якщо } k_1^* = 1; k_2^* = 0 \\ \begin{bmatrix} x_1 \oplus 1 \\ x_2 \end{bmatrix}, \text{якщо } k_1^* = 1; k_2^* = 1 \end{cases} = \begin{cases} \begin{bmatrix} x_1 \\ x_2 \oplus 1 \end{bmatrix}, \text{ якщо } k_1 = 0; k_2 = 0 \\ \begin{bmatrix} x_2 \\ x_1 \oplus 1 \end{bmatrix}, \text{якщо } k_1 = 1; k_2 = 0 \\ \begin{bmatrix} x_2 \oplus 1 \\ x_1 \end{bmatrix}, \text{ якщо } k_1 = 0; k_2 = 1 \\ \begin{bmatrix} x_1 \oplus 1 \\ x_2 \end{bmatrix}, \text{якщо } k_1 = 1; k_2 = 1 \end{cases} = \begin{cases} \begin{bmatrix} x_1 \\ x_2 \oplus 1 \end{bmatrix}, \text{ якщо } k_1 = 0; k_2 = 0 \\ \begin{bmatrix} x_1 \\ x_2 \oplus 1 \end{bmatrix}, \text{якщо } k_1 = 0; k_2 = 1 \\ \begin{bmatrix} x_2 \\ x_1 \oplus 1 \end{bmatrix}, \text{ якщо } k_1 = 1; k_2 = 0 \\ \begin{bmatrix} x_2 \oplus 1 \\ x_1 \end{bmatrix}, \text{якщо } k_1 = 1; k_2 = 1 \end{cases} = O_3^d \quad (2.18)$$

Що й необхідно було довести.

Якщо $O_4^k = \begin{bmatrix} x_1 \cdot \bar{k}_2 \oplus x_2 \cdot k_2 \\ x_1 \cdot k_2 \oplus x_2 \cdot \bar{k}_2 \end{bmatrix} \oplus \begin{bmatrix} k_1 \\ \bar{k}_1 \end{bmatrix}$ операція кодування, а $O_4^d = \begin{bmatrix} x_1 \cdot \bar{k}_2 \oplus x_2 \cdot k_2 \\ x_1 \cdot k_2 \oplus x_2 \cdot \bar{k}_2 \end{bmatrix} \oplus \begin{bmatrix} k_1 \oplus k_2 \\ \overline{k_1 \oplus k_2} \end{bmatrix}$ операція декодування, тоді O_4^k можна застосувати в якості O_4^d, за умови $k_1^* = k_1 \oplus k_2$, $k_2^* = k_2$.

Так як дані операції можна представити наступними моделями:

$$O_4^k = \begin{bmatrix} x_1 \cdot \bar{k}_2 \oplus x_2 \cdot k_2 \\ x_1 \cdot k_2 \oplus x_2 \cdot \bar{k}_2 \end{bmatrix} \oplus \begin{bmatrix} k_1 \\ \bar{k}_1 \end{bmatrix} = \begin{cases} \begin{bmatrix} x_1 \\ x_2 \oplus 1 \end{bmatrix}, \text{ якщо } k_1 = 0; k_2 = 0 \\ \begin{bmatrix} x_2 \\ x_1 \oplus 1 \end{bmatrix}, \text{якщо } k_1 = 0; k_2 = 1 \\ \begin{bmatrix} x_1 \oplus 1 \\ x_2 \end{bmatrix}, \text{ якщо } k_1 = 1; k_2 = 0 \\ \begin{bmatrix} x_2 \oplus 1 \\ x_1 \end{bmatrix}, \text{якщо } k_1 = 1; k_2 = 1 \end{cases} \quad (2.19)$$

$$O_4^d = \begin{bmatrix} x_1 \cdot \bar{k}_2 \oplus x_2 \cdot k_2 \\ x_1 \cdot k_2 \oplus x_2 \cdot \bar{k}_2 \end{bmatrix} \oplus \begin{bmatrix} k_1 \oplus k_2 \\ \overline{k_1 \oplus k_2} \end{bmatrix} = \begin{cases} \begin{bmatrix} x_1 \\ x_2 \oplus 1 \end{bmatrix}, \text{ якщо } k_1 = 0; k_2 = 0 \\ \begin{bmatrix} x_2 \oplus 1 \\ x_1 \end{bmatrix}, \text{якщо } k_1 = 0; k_2 = 1 \\ \begin{bmatrix} x_1 \oplus 1 \\ x_2 \end{bmatrix}, \text{ якщо } k_1 = 1; k_2 = 0 \\ \begin{bmatrix} x_2 \\ x_1 \oplus 1 \end{bmatrix}, \text{якщо } k_1 = 1; k_2 = 1 \end{cases} \quad (2.20)$$

отримуємо наступне перетворення:

$$O_4^{k*} = \begin{cases} \begin{bmatrix} x_1 \\ x_2 \oplus 1 \end{bmatrix}, \text{ якщо } k_1 = 0; k_2 = 0 \\ \begin{bmatrix} x_2 \\ x_1 \oplus 1 \end{bmatrix}, \text{якщо } k_1 = 0; k_2 = 1 \\ \begin{bmatrix} x_1 \oplus 1 \\ x_2 \end{bmatrix}, \text{ якщо } k_1 = 1; k_2 = 0 \\ \begin{bmatrix} x_2 \oplus 1 \\ x_1 \end{bmatrix}, \text{якщо } k_1 = 1; k_2 = 1 \end{cases} = \begin{cases} \begin{bmatrix} x_1 \\ x_2 \oplus 1 \end{bmatrix}, \text{ якщо } k_1 = 0; k_2 = 0 \\ \begin{bmatrix} x_2 \\ x_1 \oplus 1 \end{bmatrix}, \text{ якщо } k_1 = 1; k_2 = 1 \\ \begin{bmatrix} x_2 \oplus 1 \\ x_1 \end{bmatrix}, \text{якщо } k_1 = 1; k_2 = 0 \\ \begin{bmatrix} x_1 \oplus 1 \\ x_2 \end{bmatrix}, \text{якщо } k_1 = 0; k_2 = 1 \end{cases} = \begin{cases} \begin{bmatrix} x_1 \\ x_2 \oplus 1 \end{bmatrix}, \text{ якщо } k_1 = 0; k_2 = 0 \\ \begin{bmatrix} x_2 \oplus 1 \\ x_1 \end{bmatrix}, \text{якщо } k_1 = 0; k_2 = 1 \\ \begin{bmatrix} x_1 \oplus 1 \\ x_2 \end{bmatrix}, \text{якщо } k_1 = 1; k_2 = 0 \\ \begin{bmatrix} x_2 \\ x_1 \oplus 1 \end{bmatrix}, \text{якщо } k_1 = 1; k_2 = 1 \end{cases} = O_4^d \quad (2.21)$$

Це доводить, що застосування виявлених взаємозв'язків є коректним.

Візьмемо наступну пару операцій, де $O_5^k = \begin{bmatrix} x_1 \cdot \bar{k}_2 \oplus x_2 \cdot k_2 \\ x_1 \cdot k_2 \oplus x_2 \cdot \bar{k}_2 \end{bmatrix} \oplus \begin{bmatrix} k_1 \oplus k_2 \\ \overline{k_1 \oplus k_2} \end{bmatrix}$ – операція кодування, а $O_5^d = \begin{bmatrix} x_1 \cdot \bar{k}_2 \oplus x_2 \cdot k_2 \\ x_1 \cdot k_2 \oplus x_2 \cdot \bar{k}_2 \end{bmatrix} \oplus \begin{bmatrix} k_1 \\ \bar{k}_1 \end{bmatrix}$ – операція декодування, тоді O_5^k можна застосувати в якості O_5^d, за умови, $k_1^* = k_1 \oplus k_2$ $k_2^* = k_2$.

Так як:

$$O_5^k = \begin{bmatrix} x_1 \cdot \bar{k}_2 \oplus x_2 \cdot k_2 \\ x_1 \cdot k_2 \oplus x_2 \cdot \bar{k}_2 \end{bmatrix} \oplus \begin{bmatrix} k_1 \oplus k_2 \\ \overline{k_1 \oplus k_2} \end{bmatrix} = \begin{cases} \begin{bmatrix} x_1 \\ x_2 \oplus 1 \end{bmatrix}, \text{ якщо } k_1 = 0; k_2 = 0 \\ \begin{bmatrix} x_2 \oplus 1 \\ x_1 \end{bmatrix}, \text{якщо } k_1 = 0; k_2 = 1 \\ \begin{bmatrix} x_1 \oplus 1 \\ x_2 \end{bmatrix}, \text{ якщо } k_1 = 1; k_2 = 0 \\ \begin{bmatrix} x_2 \\ x_1 \oplus 1 \end{bmatrix}, \text{якщо } k_1 = 1; k_2 = 1 \end{cases} \quad (2.22)$$

$$O_5^d = \begin{bmatrix} x_1 \cdot \bar{k}_2 \oplus x_2 \cdot k_2 \\ x_1 \cdot k_2 \oplus x_2 \cdot \bar{k}_2 \end{bmatrix} \oplus \begin{bmatrix} k_1 \\ \bar{k}_1 \end{bmatrix} = \begin{cases} \begin{bmatrix} x_1 \\ x_2 \oplus 1 \end{bmatrix}, \text{ якщо } k_1 = 0; k_2 = 0 \\ \begin{bmatrix} x_2 \\ x_1 \oplus 1 \end{bmatrix}, \text{якщо } k_1 = 0; k_2 = 1 \\ \begin{bmatrix} x_1 \oplus 1 \\ x_2 \end{bmatrix}, \text{ якщо } k_1 = 1; k_2 = 0 \\ \begin{bmatrix} x_2 \oplus 1 \\ x_1 \end{bmatrix}, \text{якщо } k_1 = 1; k_2 = 1 \end{cases} \quad (2.23)$$

отримуємо наступне:

$$O_5^{k*} = \begin{cases} \begin{bmatrix} x_1 \\ x_2 \oplus 1 \end{bmatrix}, \text{ якщо } k_1 = 0; k_2 = 0 \\ \begin{bmatrix} x_2 \oplus 1 \\ x_1 \end{bmatrix}, \text{якщо } k_1 = 0; k_2 = 1 \\ \begin{bmatrix} x_1 \oplus 1 \\ x_2 \end{bmatrix}, \text{ якщо } k_1 = 1; k_2 = 0 \\ \begin{bmatrix} x_2 \\ x_1 \oplus 1 \end{bmatrix}, \text{якщо } k_1 = 1; k_2 = 1 \end{cases} = \begin{cases} \begin{bmatrix} x_1 \\ x_2 \oplus 1 \end{bmatrix}, \text{ якщо } k_1 = 0; k_2 = 0 \\ \begin{bmatrix} x_2 \\ x_1 \oplus 1 \end{bmatrix}, \text{якщо } k_1 = 1; k_2 = 1 \\ \begin{bmatrix} x_1 \oplus 1 \\ x_2 \end{bmatrix}, \text{ якщо } k_1 = 1; k_2 = 0 \\ \begin{bmatrix} x_2 \oplus 1 \\ x_1 \end{bmatrix}, \text{якщо } k_1 = 0; k_2 = 1 \end{cases} = \begin{cases} \begin{bmatrix} x_1 \\ x_2 \oplus 1 \end{bmatrix}, \text{ якщо } k_1 = 0; k_2 = 0 \\ \begin{bmatrix} x_2 \\ x_1 \oplus 1 \end{bmatrix}, \text{якщо } k_1 = 0; k_2 = 1 \\ \begin{bmatrix} x_1 \oplus 1 \\ x_2 \end{bmatrix}, \text{ якщо } k_1 = 1; k_2 = 0 \\ \begin{bmatrix} x_2 \oplus 1 \\ x_1 \end{bmatrix}, \text{якщо } k_1 = 1; k_2 = 1 \end{cases} = O_5^d \quad (2.24)$$

Що й потрібно було довести.

Якщо $O_6^k = \begin{bmatrix} x_1 \cdot (\overline{k_1 \oplus k_2}) \oplus x_2 \cdot (k_1 \oplus k_2) \\ x_1 \cdot (k_1 \oplus k_2) \oplus x_2 \cdot (\overline{k_1 \oplus k_2}) \end{bmatrix} \oplus \begin{bmatrix} k_2 \\ \bar{k}_2 \end{bmatrix}$ операція кодування, а $O_6^d = \begin{bmatrix} x_1 \cdot (\overline{k_1 \oplus k_2}) \oplus x_2 \cdot (k_1 \oplus k_2) \\ x_1 \cdot (k_1 \oplus k_2) \oplus x_2 \cdot (\overline{k_1 \oplus k_2}) \end{bmatrix} \oplus \begin{bmatrix} k_1 \\ \bar{k}_1 \end{bmatrix}$ операція декодування, тоді O_6^k можна застосувати в якості O_6^d, за умови $k_1^* = k_2$, $k_2^* = k_1$.

Так як модельне представлення операцій виглядає наступним чином:

$$O_6^k = \begin{bmatrix} x_1 \cdot (\overline{k_1 \oplus k_2}) \oplus x_2 \cdot (k_1 \oplus k_2) \\ x_1 \cdot (k_1 \oplus k_2) \oplus x_2 \cdot (\overline{k_1 \oplus k_2}) \end{bmatrix} \oplus \begin{bmatrix} k_2 \\ \bar{k}_2 \end{bmatrix} = \begin{cases} \begin{bmatrix} x_1 \\ x_2 \oplus 1 \end{bmatrix}, \text{ якщо } k_1 = 0; k_2 = 0 \\ \begin{bmatrix} x_2 \oplus 1 \\ x_1 \end{bmatrix}, \text{якщо } k_1 = 0; k_2 = 1 \\ \begin{bmatrix} x_2 \\ x_1 \oplus 1 \end{bmatrix}, \text{ якщо } k_1 = 1; k_2 = 0 \\ \begin{bmatrix} x_1 \oplus 1 \\ x_2 \end{bmatrix}, \text{якщо } k_1 = 1; k_2 = 1 \end{cases} \quad (2.25)$$

$$O_6^d = \begin{bmatrix} x_1 \cdot (\overline{k_1 \oplus k_2}) \oplus x_2 \cdot (k_1 \oplus k_2) \\ x_1 \cdot (k_1 \oplus k_2) \oplus x_2 \cdot (\overline{k_1 \oplus k_2}) \end{bmatrix} \oplus \begin{bmatrix} k_1 \\ \bar{k}_1 \end{bmatrix} = \begin{cases} \begin{bmatrix} x_1 \\ x_2 \oplus 1 \end{bmatrix}, \text{ якщо } k_1 = 0; k_2 = 0 \\ \begin{bmatrix} x_2 \\ x_1 \oplus 1 \end{bmatrix}, \text{якщо } k_1 = 0; k_2 = 1 \\ \begin{bmatrix} x_2 \oplus 1 \\ x_1 \end{bmatrix}, \text{ якщо } k_1 = 1; k_2 = 0 \\ \begin{bmatrix} x_1 \oplus 1 \\ x_2 \end{bmatrix}, \text{якщо } k_1 = 1; k_2 = 1 \end{cases} \quad (2.26)$$

отримуємо:

$$O_6^{k*} = \begin{cases} \begin{bmatrix} x_1 \\ x_2 \oplus 1 \end{bmatrix}, \text{ якщо } k_1 = 0; k_2 = 0 \\ \begin{bmatrix} x_2 \oplus 1 \\ x_1 \end{bmatrix}, \text{якщо } k_1 = 0; k_2 = 1 \\ \begin{bmatrix} x_2 \\ x_1 \oplus 1 \end{bmatrix}, \text{ якщо } k_1 = 1; k_2 = 0 \\ \begin{bmatrix} x_1 \oplus 1 \\ x_2 \end{bmatrix}, \text{якщо } k_1 = 1; k_2 = 1 \end{cases} = \begin{cases} \begin{bmatrix} x_1 \\ x_2 \oplus 1 \end{bmatrix}, \text{ якщо } k_1 = 0; k_2 = 0 \\ \begin{bmatrix} x_2 \\ x_1 \oplus 1 \end{bmatrix}, \text{ якщо } k_1 = 1; k_2 = 0 \\ \begin{bmatrix} x_2 \oplus 1 \\ x_1 \end{bmatrix}, \text{якщо } k_1 = 0; k_2 = 1 \\ \begin{bmatrix} x_1 \oplus 1 \\ x_2 \end{bmatrix}, \text{якщо } k_1 = 1; k_2 = 1 \end{cases} = \begin{cases} \begin{bmatrix} x_1 \\ x_2 \oplus 1 \end{bmatrix}, \text{ якщо } k_1 = 0; k_2 = 0 \\ \begin{bmatrix} x_2 \\ x_1 \oplus 1 \end{bmatrix}, \text{якщо } k_1 = 0; k_2 = 1 \\ \begin{bmatrix} x_2 \oplus 1 \\ x_1 \end{bmatrix}, \text{якщо } k_1 = 1; k_2 = 0 \\ \begin{bmatrix} x_1 \oplus 1 \\ x_2 \end{bmatrix}, \text{якщо } k_1 = 1; k_2 = 1 \end{cases} = O_6^d \quad (2.27)$$

Саме це й необхідно було довести.

У разі, якщо $O_7^k = \begin{bmatrix} x_1 \cdot \bar{k}_1 \oplus x_2 \cdot k_1 \\ x_1 \cdot k_1 \oplus x_2 \cdot \bar{k}_1 \end{bmatrix} \oplus \begin{bmatrix} \overline{k_1 \oplus k_2} \\ k_1 \oplus k_2 \end{bmatrix}$ – це операція кодування, а $O_7^d = \begin{bmatrix} x_1 \cdot \bar{k}_1 \oplus x_2 \cdot k_1 \\ x_1 \cdot k_1 \oplus x_2 \cdot \bar{k}_1 \end{bmatrix} \oplus \begin{bmatrix} \bar{k}_2 \\ k_2 \end{bmatrix}$ – операція декодування, тоді O_7^k можна застосувати у якості O_7^d, за умови $k_1^* = k_1$, $k_2^* = k_1 \oplus k_2$.

Так як:

$$O_7^k = \begin{bmatrix} x_1 \cdot \bar{k}_1 \oplus x_2 \cdot k_1 \\ x_1 \cdot k_1 \oplus x_2 \cdot \bar{k}_1 \end{bmatrix} \oplus \begin{bmatrix} \overline{k_1 \oplus k_2} \\ k_1 \oplus k_2 \end{bmatrix} = \begin{cases} \begin{bmatrix} x_1 \oplus 1 \\ x_2 \end{bmatrix}, \text{ якщо } k_1 = 0; k_2 = 0 \\ \begin{bmatrix} x_1 \\ x_2 \oplus 1 \end{bmatrix}, \text{якщо } k_1 = 0; k_2 = 1 \\ \begin{bmatrix} x_2 \\ x_1 \oplus 1 \end{bmatrix}, \text{ якщо } k_1 = 1; k_2 = 0 \\ \begin{bmatrix} x_2 \oplus 1 \\ x_1 \end{bmatrix}, \text{якщо } k_1 = 1; k_2 = 1 \end{cases} \quad (2.28)$$

$$O_7^d = \begin{bmatrix} x_1 \cdot \bar{k}_1 \oplus x_2 \cdot k_1 \\ x_1 \cdot k_1 \oplus x_2 \cdot \bar{k}_1 \end{bmatrix} \oplus \begin{bmatrix} \bar{k}_2 \\ k_2 \end{bmatrix} = \begin{cases} \begin{bmatrix} x_1 \oplus 1 \\ x_2 \end{bmatrix}, \text{ якщо } k_1 = 0; k_2 = 0 \\ \begin{bmatrix} x_1 \\ x_2 \oplus 1 \end{bmatrix}, \text{якщо } k_1 = 0; k_2 = 1 \\ \begin{bmatrix} x_2 \oplus 1 \\ x_1 \end{bmatrix}, \text{ якщо } k_1 = 1; k_2 = 0 \\ \begin{bmatrix} x_2 \\ x_1 \oplus 1 \end{bmatrix}, \text{якщо } k_1 = 1; k_2 = 1 \end{cases} \quad (2.29)$$

отримуємо:

$$O_7^{k*} = \begin{cases} \begin{bmatrix} x_1 \oplus 1 \\ x_2 \end{bmatrix}, \text{ якщо } k_1 = 0; k_2 = 0 \\ \begin{bmatrix} x_1 \\ x_2 \oplus 1 \end{bmatrix}, \text{якщо } k_1 = 0; k_2 = 1 \\ \begin{bmatrix} x_2 \\ x_1 \oplus 1 \end{bmatrix}, \text{ якщо } k_1 = 1; k_2 = 0 \\ \begin{bmatrix} x_2 \oplus 1 \\ x_1 \end{bmatrix}, \text{якщо } k_1 = 1; k_2 = 1 \end{cases} = \begin{cases} \begin{bmatrix} x_1 \oplus 1 \\ x_2 \end{bmatrix}, \text{ якщо } k_1 = 0; k_2 = 0 \\ \begin{bmatrix} x_1 \\ x_2 \oplus 1 \end{bmatrix}, \text{якщо } k_1 = 0; k_2 = 1 \\ \begin{bmatrix} x_2 \\ x_1 \oplus 1 \end{bmatrix}, \text{ якщо } k_1 = 1; k_2 = 0 \\ \begin{bmatrix} x_2 \oplus 1 \\ x_1 \end{bmatrix}, \text{якщо } k_1 = 1; k_2 = 1 \end{cases} = \begin{cases} \begin{bmatrix} x_1 \oplus 1 \\ x_2 \end{bmatrix}, \text{ якщо } k_1 = 0; k_2 = 0 \\ \begin{bmatrix} x_1 \\ x_2 \oplus 1 \end{bmatrix}, \text{якщо } k_1 = 0; k_2 = 1 \\ \begin{bmatrix} x_2 \oplus 1 \\ x_1 \end{bmatrix}, \text{ якщо } k_1 = 1; k_2 = 0 \\ \begin{bmatrix} x_2 \\ x_1 \oplus 1 \end{bmatrix}, \text{якщо } k_1 = 1; k_2 = 1 \end{cases} = O_7^d \quad (2.30)$$

Це й потрібно було довести.

Якщо використати $O_8^k = \begin{bmatrix} x_1 \cdot \bar{k}_1 \oplus x_2 \cdot k_1 \\ x_1 \cdot k_1 \oplus x_2 \cdot \bar{k}_1 \end{bmatrix} \oplus \begin{bmatrix} \bar{k}_2 \\ k_2 \end{bmatrix}$, як операцію кодування, а $O_8^d = \begin{bmatrix} x_1 \cdot \bar{k}_1 \oplus x_2 \cdot k_1 \\ x_1 \cdot k_1 \oplus x_2 \cdot \bar{k}_1 \end{bmatrix} \oplus \begin{bmatrix} \overline{k_1 \oplus k_2} \\ k_1 \oplus k_2 \end{bmatrix}$ операцію декодування, тоді O_8^k можна застосувати в якості O_8^d, за умови $k_1^* = k_1$, $k_2^* = k_1 \oplus k_2$.

Розгорнутий вигляд операцій матиме наступний вигляд:

$$O_8^k = \begin{bmatrix} x_1 \cdot \bar{k}_1 \oplus x_2 \cdot k_1 \\ x_1 \cdot k_1 \oplus x_2 \cdot \bar{k}_1 \end{bmatrix} \oplus \begin{bmatrix} \bar{k}_2 \\ k_2 \end{bmatrix} = \begin{cases} \begin{bmatrix} x_1 \oplus 1 \\ x_2 \end{bmatrix}, \text{ якщо } k_1 = 0; k_2 = 0 \\ \begin{bmatrix} x_1 \\ x_2 \oplus 1 \end{bmatrix}, \text{якщо } k_1 = 0; k_2 = 1 \\ \begin{bmatrix} x_2 \oplus 1 \\ x_1 \end{bmatrix}, \text{ якщо } k_1 = 1; k_2 = 0 \\ \begin{bmatrix} x_2 \\ x_1 \oplus 1 \end{bmatrix}, \text{якщо } k_1 = 1; k_2 = 1 \end{cases} \quad (2.31)$$

$$O_8^d = \begin{bmatrix} x_1 \cdot \bar{k}_1 \oplus x_2 \cdot k_1 \\ x_1 \cdot k_1 \oplus x_2 \cdot \bar{k}_1 \end{bmatrix} \oplus \begin{bmatrix} \overline{k_1 \oplus k_2} \\ k_1 \oplus k_2 \end{bmatrix} = \begin{cases} \begin{bmatrix} x_1 \oplus 1 \\ x_2 \end{bmatrix}, \text{ якщо } k_1 = 0; k_2 = 0 \\ \begin{bmatrix} x_1 \\ x_2 \oplus 1 \end{bmatrix}, \text{якщо } k_1 = 0; k_2 = 1 \\ \begin{bmatrix} x_2 \\ x_1 \oplus 1 \end{bmatrix}, \text{ якщо } k_1 = 1; k_2 = 0 \\ \begin{bmatrix} x_2 \oplus 1 \\ x_1 \end{bmatrix}, \text{якщо } k_1 = 1; k_2 = 1 \end{cases} \quad (2.32)$$

При цьому перетворення матиме такий вигляд:

$$O_8^{k*} = \begin{cases} \begin{bmatrix} x_1 \oplus 1 \\ x_2 \end{bmatrix}, \text{ якщо } k_1 = 0; k_2 = 0 \\ \begin{bmatrix} x_1 \\ x_2 \oplus 1 \end{bmatrix}, \text{якщо } k_1 = 0; k_2 = 1 \\ \begin{bmatrix} x_2 \oplus 1 \\ x_1 \end{bmatrix}, \text{ якщо } k_1 = 1; k_2 = 0 \\ \begin{bmatrix} x_2 \\ x_1 \oplus 1 \end{bmatrix}, \text{якщо } k_1 = 1; k_2 = 1 \end{cases} = \begin{cases} \begin{bmatrix} x_1 \oplus 1 \\ x_2 \end{bmatrix}, \text{ якщо } k_1 = 0; k_2 = 0 \\ \begin{bmatrix} x_1 \\ x_2 \oplus 1 \end{bmatrix}, \text{якщо } k_1 = 0; k_2 = 1 \\ \begin{bmatrix} x_2 \\ x_1 \oplus 1 \end{bmatrix}, \text{ якщо } k_1 = 1; k_2 = 1 \\ \begin{bmatrix} x_2 \oplus 1 \\ x_1 \end{bmatrix}, \text{якщо } k_1 = 1; k_2 = 0 \end{cases} = \begin{cases} \begin{bmatrix} x_1 \oplus 1 \\ x_2 \end{bmatrix}, \text{ якщо } k_1 = 0; k_2 = 0 \\ \begin{bmatrix} x_1 \\ x_2 \oplus 1 \end{bmatrix}, \text{якщо } k_1 = 0; k_2 = 1 \\ \begin{bmatrix} x_2 \\ x_1 \oplus 1 \end{bmatrix}, \text{ якщо } k_1 = 1; k_2 = 0 \\ \begin{bmatrix} x_2 \oplus 1 \\ x_1 \end{bmatrix}, \text{якщо } k_1 = 1; k_2 = 1 \end{cases} = O_8^d \quad (2.33)$$

Що і потрібно було довести.

Якщо $O_9^k = \begin{bmatrix} x_1 \cdot (\overline{k_1 \oplus k_2}) \oplus x_2 \cdot (k_1 \oplus k_2) \\ x_1 \cdot (k_1 \oplus k_2) \oplus x_2 \cdot (\overline{k_1 \oplus k_2}) \end{bmatrix} \oplus \begin{bmatrix} \bar{k}_2 \\ k_2 \end{bmatrix}$ – операція кодування, а $O_9^d = \begin{bmatrix} x_1 \cdot (\overline{k_1 \oplus k_2}) \oplus x_2 \cdot (k_1 \oplus k_2) \\ x_1 \cdot (k_1 \oplus k_2) \oplus x_2 \cdot (\overline{k_1 \oplus k_2}) \end{bmatrix} \oplus \begin{bmatrix} \bar{k}_1 \\ k_1 \end{bmatrix}$ – операція декодування, тоді O_9^k можна застосувати в якості O_9^d, за умови, $k_1^* = k_2$, $k_2^* = k_1$.

Так як модельне представлення даних операцій виглядає наступним чином:

$$O_9^k = \begin{bmatrix} x_1 \cdot (\overline{k_1 \oplus k_2}) \oplus x_2 \cdot (k_1 \oplus k_2) \\ x_1 \cdot (k_1 \oplus k_2) \oplus x_2 \cdot (\overline{k_1 \oplus k_2}) \end{bmatrix} \oplus \begin{bmatrix} \bar{k}_2 \\ k_2 \end{bmatrix} = \begin{cases} \begin{bmatrix} x_1 \oplus 1 \\ x_2 \end{bmatrix}, \text{ якщо } k_1 = 0; k_2 = 0 \\ \begin{bmatrix} x_2 \\ x_1 \oplus 1 \end{bmatrix}, \text{якщо } k_1 = 0; k_2 = 1 \\ \begin{bmatrix} x_2 \oplus 1 \\ x_1 \end{bmatrix}, \text{ якщо } k_1 = 1; k_2 = 0 \\ \begin{bmatrix} x_1 \\ x_2 \oplus 1 \end{bmatrix}, \text{якщо } k_1 = 1; k_2 = 1 \end{cases} \quad (2.34)$$

$$O_9^d = \begin{bmatrix} x_1 \cdot (\overline{k_1 \oplus k_2}) \oplus x_2 \cdot (k_1 \oplus k_2) \\ x_1 \cdot (k_1 \oplus k_2) \oplus x_2 \cdot (\overline{k_1 \oplus k_2}) \end{bmatrix} \oplus \begin{bmatrix} \bar{k}_1 \\ k_1 \end{bmatrix} = \begin{cases} \begin{bmatrix} x_1 \oplus 1 \\ x_2 \end{bmatrix}, \text{ якщо } k_1 = 0; k_2 = 0 \\ \begin{bmatrix} x_2 \oplus 1 \\ x_1 \end{bmatrix}, \text{якщо } k_1 = 0; k_2 = 1 \\ \begin{bmatrix} x_2 \\ x_1 \oplus 1 \end{bmatrix}, \text{ якщо } k_1 = 1; k_2 = 0 \\ \begin{bmatrix} x_1 \\ x_2 \oplus 1 \end{bmatrix}, \text{якщо } k_1 = 1; k_2 = 1 \end{cases} \quad (2.35)$$

отримуємо:

$$O_9^{k*} = \begin{cases} \begin{bmatrix} x_1 \oplus 1 \\ x_2 \end{bmatrix}, \text{ якщо } k_1 = 0; k_2 = 0 \\ \begin{bmatrix} x_2 \\ x_1 \oplus 1 \end{bmatrix}, \text{якщо } k_1 = 0; k_2 = 1 \\ \begin{bmatrix} x_2 \oplus 1 \\ x_1 \end{bmatrix}, \text{ якщо } k_1 = 1; k_2 = 0 \\ \begin{bmatrix} x_1 \\ x_2 \oplus 1 \end{bmatrix}, \text{якщо } k_1 = 1; k_2 = 1 \end{cases} = \begin{cases} \begin{bmatrix} x_1 \\ x_2 \oplus 1 \end{bmatrix}, \text{ якщо } k_1 = 0; k_2 = 0 \\ \begin{bmatrix} x_2 \oplus 1 \\ x_1 \end{bmatrix}, \text{ якщо } k_1 = 1; k_2 = 0 \\ \begin{bmatrix} x_2 \\ x_1 \oplus 1 \end{bmatrix}, \text{якщо } k_1 = 0; k_2 = 1 \\ \begin{bmatrix} x_1 \\ x_2 \oplus 1 \end{bmatrix}, \text{якщо } k_1 = 1; k_2 = 1 \end{cases} = \begin{cases} \begin{bmatrix} x_1 \oplus 1 \\ x_2 \end{bmatrix}, \text{ якщо } k_1 = 0; k_2 = 0 \\ \begin{bmatrix} x_2 \oplus 1 \\ x_1 \end{bmatrix}, \text{якщо } k_1 = 0; k_2 = 1 \\ \begin{bmatrix} x_2 \\ x_1 \oplus 1 \end{bmatrix}, \text{якщо } k_1 = 1; k_2 = 0 \\ \begin{bmatrix} x_1 \\ x_2 \oplus 1 \end{bmatrix}, \text{якщо } k_1 = 1; k_2 = 1 \end{cases} = O_9^d \quad (2.36)$$

Отже, наше твердження вірне.

Якщо $O_{10}^k = \begin{bmatrix} x_1 \cdot \bar{k}_2 \oplus x_2 \cdot k_2 \\ x_1 \cdot k_2 \oplus x_2 \cdot \bar{k}_2 \end{bmatrix} \oplus \begin{bmatrix} \bar{k}_2 \\ k_2 \end{bmatrix}$ – операція кодування, а $O_{10}^d = \begin{bmatrix} x_1 \cdot \bar{k}_2 \oplus x_2 \cdot k_2 \\ x_1 \cdot k_2 \oplus x_2 \cdot \bar{k}_2 \end{bmatrix} \oplus \begin{bmatrix} \bar{k}_1 \\ k_1 \end{bmatrix}$ – операція декодування, тоді O_{10}^k можна застосувати в якості O_{10}^d, за умови $k_1^* = k_1 \oplus k_2$, $k_2^* = k_2$.

Так як:

$$O_{10}^{k}=\begin{bmatrix} x_1\cdot\bar{k}_2\oplus x_2\cdot k_2 \\ x_1\cdot k_2\oplus x_2\cdot\bar{k}_2 \end{bmatrix}\oplus\begin{bmatrix}\bar{k}_2\\ k_2\end{bmatrix}=\begin{cases}\begin{bmatrix} x_1\oplus 1\\ x_2\end{bmatrix}, \text{ якщо } k_1=0;\ k_2=0\\ \begin{bmatrix} x_2\\ x_1\oplus 1\end{bmatrix}, \text{якщо } k_1=0;\ k_2=1\\ \begin{bmatrix} x_1\\ x_2\oplus 1\end{bmatrix}, \text{ якщо } k_1=1;\ k_2=0\\ \begin{bmatrix} x_2\oplus 1\\ x_1\end{bmatrix}, \text{якщо } k_1=1;\ k_2=1\end{cases} \quad (2.37)$$

$$O_{10}^{d}=\begin{bmatrix} x_1\cdot\bar{k}_2\oplus x_2\cdot k_2 \\ x_1\cdot k_2\oplus x_2\cdot\bar{k}_2 \end{bmatrix}\oplus\begin{bmatrix}\bar{k}_1\\ k_1\end{bmatrix}=\begin{cases}\begin{bmatrix} x_1\oplus 1\\ x_2\end{bmatrix}, \text{ якщо } k_1=0;\ k_2=0\\ \begin{bmatrix} x_2\oplus 1\\ x_1\end{bmatrix}, \text{якщо } k_1=0;\ k_2=1\\ \begin{bmatrix} x_1\\ x_2\oplus 1\end{bmatrix}, \text{ якщо } k_1=1;\ k_2=0\\ \begin{bmatrix} x_2\\ x_1\oplus 1\end{bmatrix}, \text{якщо } k_1=1;\ k_2=1\end{cases} \quad (2.38)$$

отримуємо наступне перетворення:

$$O_{10}^{k*}=\begin{cases}\begin{bmatrix} x_1\oplus 1\\ x_2\end{bmatrix}, \text{ якщо } k_1=0;\ k_2=0\\ \begin{bmatrix} x_2\\ x_1\oplus 1\end{bmatrix}, \text{якщо } k_1=0;\ k_2=1\\ \begin{bmatrix} x_1\\ x_2\oplus 1\end{bmatrix}, \text{ якщо } k_1=1;\ k_2=0\\ \begin{bmatrix} x_2\oplus 1\\ x_1\end{bmatrix}, \text{якщо } k_1=1;\ k_2=1\end{cases}=\begin{cases}\begin{bmatrix} x_1\oplus 1\\ x_2\end{bmatrix}, \text{ якщо } k_1=0;\ k_2=0\\ \begin{bmatrix} x_2\oplus 1\\ x_1\end{bmatrix}, \text{якщо } k_1=1;\ k_2=1\\ \begin{bmatrix} x_1\\ x_2\oplus 1\end{bmatrix}, \text{ якщо } k_1=1;\ k_2=0\\ \begin{bmatrix} x_2\\ x_1\oplus 1\end{bmatrix}, \text{якщо } k_1=0;\ k_2=1\end{cases}=\begin{cases}\begin{bmatrix} x_1\oplus 1\\ x_2\end{bmatrix}, \text{ якщо } k_1=0;\ k_2=0\\ \begin{bmatrix} x_2\oplus 1\\ x_1\end{bmatrix}, \text{якщо } k_1=0;\ k_2=1\\ \begin{bmatrix} x_1\\ x_2\oplus 1\end{bmatrix}, \text{ якщо } k_1=1;\ k_2=0\\ \begin{bmatrix} x_2\\ x_1\oplus 1\end{bmatrix}, \text{якщо } k_1=1;\ k_2=1\end{cases}=O_{10}^{d} \quad (2.39)$$

Тобто наше твердження вірне.

Якщо $O_{11}^{k}=\begin{bmatrix} x_1\cdot\bar{k}_2\oplus x_2\cdot k_2 \\ x_1\cdot k_2\oplus x_2\cdot\bar{k}_2 \end{bmatrix}\oplus\begin{bmatrix}\bar{k}_1\\ k_1\end{bmatrix}$ – операція кодування, а $O_{11}^{d}=\begin{bmatrix} x_1\cdot\bar{k}_2\oplus x_2\cdot k_2 \\ x_1\cdot k_2\oplus x_2\cdot\bar{k}_2 \end{bmatrix}\oplus\begin{bmatrix}\bar{k}_2\\ k_2\end{bmatrix}$ – операція декодування, тоді O_{11}^{k} можна застосувати в якості O_{11}^{d}, за умови $k_1^{*}=k_1\oplus k_2$, $k_2^{*}=k_2$.

Так як:

$$O_{11}^{k}=\begin{bmatrix} x_1\cdot\bar{k}_2\oplus x_2\cdot k_2 \\ x_1\cdot k_2\oplus x_2\cdot\bar{k}_2 \end{bmatrix}\oplus\begin{bmatrix}\bar{k}_1\\ k_1\end{bmatrix}=\begin{cases}\begin{bmatrix}x_1\oplus 1\\ x_2\end{bmatrix}, \text{ якщо } k_1=0;\ k_2=0\\ \begin{bmatrix}x_2\oplus 1\\ x_1\end{bmatrix}, \text{якщо } k_1=0;\ k_2=1\\ \begin{bmatrix}x_1\\ x_2\oplus 1\end{bmatrix}, \text{ якщо } k_1=1;\ k_2=0\\ \begin{bmatrix}x_2\\ x_1\oplus 1\end{bmatrix}, \text{якщо } k_1=1;\ k_2=1\end{cases} \quad (2.40)$$

$$O_{11}^{d}=\begin{bmatrix} x_1\cdot\bar{k}_2\oplus x_2\cdot k_2 \\ x_1\cdot k_2\oplus x_2\cdot\bar{k}_2 \end{bmatrix}\oplus\begin{bmatrix}\bar{k}_2\\ k_2\end{bmatrix}=\begin{cases}\begin{bmatrix}x_1\oplus 1\\ x_2\end{bmatrix}, \text{ якщо } k_1=0;\ k_2=0\\ \begin{bmatrix}x_2\\ x_1\oplus 1\end{bmatrix}, \text{якщо } k_1=0;\ k_2=1\\ \begin{bmatrix}x_1\\ x_2\oplus 1\end{bmatrix}, \text{ якщо } k_1=1;\ k_2=0\\ \begin{bmatrix}x_2\oplus 1\\ x_1\end{bmatrix}, \text{якщо } k_1=1;\ k_2=1\end{cases} \quad (2.41)$$

отримуємо:

$$O_{11}^{k*}=\begin{cases}\begin{bmatrix}x_1\oplus 1\\ x_2\end{bmatrix}, \text{ якщо } k_1=0;\ k_2=0\\ \begin{bmatrix}x_2\oplus 1\\ x_1\end{bmatrix}, \text{якщо } k_1=0;\ k_2=1\\ \begin{bmatrix}x_1\\ x_2\oplus 1\end{bmatrix}, \text{ якщо } k_1=1;\ k_2=0\\ \begin{bmatrix}x_2\\ x_1\oplus 1\end{bmatrix}, \text{якщо } k_1=1;\ k_2=1\end{cases}=\begin{cases}\begin{bmatrix}x_1\oplus 1\\ x_2\end{bmatrix}, \text{ якщо } k_1=0;\ k_2=0\\ \begin{bmatrix}x_2\\ x_1\oplus 1\end{bmatrix}, \text{якщо } k_1=1;\ k_2=1\\ \begin{bmatrix}x_1\\ x_2\oplus 1\end{bmatrix}, \text{ якщо } k_1=1;\ k_2=0\\ \begin{bmatrix}x_2\oplus 1\\ x_1\end{bmatrix}, \text{якщо } k_1=0;\ k_2=1\end{cases}=\begin{cases}\begin{bmatrix}x_1\oplus 1\\ x_2\end{bmatrix}, \text{ якщо } k_1=0;\ k_2=0\\ \begin{bmatrix}x_2\\ x_1\oplus 1\end{bmatrix}, \text{якщо } k_1=0;\ k_2=1\\ \begin{bmatrix}x_1\\ x_2\oplus 1\end{bmatrix}, \text{ якщо } k_1=1;\ k_2=0\\ \begin{bmatrix}x_2\oplus 1\\ x_1\end{bmatrix}, \text{якщо } k_1=1;\ k_2=1\end{cases}=O_{11}^{d} \quad (2.42)$$

Що і потрібно було довести.

Якщо $O_{12}^{k}=\begin{bmatrix} x_1\cdot(\overline{k_1\oplus k_2})\oplus x_2\cdot(k_1\oplus k_2) \\ x_1\cdot(k_1\oplus k_2)\oplus x_2\cdot(\overline{k_1\oplus k_2}) \end{bmatrix}\oplus\begin{bmatrix}\bar{k}_1\\ k_1\end{bmatrix}$ – операція кодування, а $O_{12}^{d}=\begin{bmatrix} x_1\cdot(\overline{k_1\oplus k_2})\oplus x_2\cdot(k_1\oplus k_2) \\ x_1\cdot(k_1\oplus k_2)\oplus x_2\cdot(\overline{k_1\oplus k_2}) \end{bmatrix}\oplus\begin{bmatrix}\bar{k}_2\\ k_2\end{bmatrix}$ – операція декодування, тоді O_{12}^{k} можна застосувати в якості O_{12}^{d}, за умови $k_1^*=k_2$, $k_2^*=k_1$.

Так як розгорнутий вигляд операцій має наступний вигляд:

$$O_{12}^{k}=\begin{bmatrix} x_1\cdot(\overline{k_1\oplus k_2})\oplus x_2\cdot(k_1\oplus k_2) \\ x_1\cdot(k_1\oplus k_2)\oplus x_2\cdot(\overline{k_1\oplus k_2}) \end{bmatrix}\oplus\begin{bmatrix}\bar{k}_1\\ k_1\end{bmatrix}=\begin{cases}\begin{bmatrix}x_1\oplus 1\\ x_2\end{bmatrix}, \text{ якщо } k_1=0;\ k_2=0\\ \begin{bmatrix}x_2\oplus 1\\ x_1\end{bmatrix}, \text{якщо } k_1=0;\ k_2=1\\ \begin{bmatrix}x_2\\ x_1\oplus 1\end{bmatrix}, \text{якщо } k_1=1;\ k_2=0\\ \begin{bmatrix}x_1\\ x_2\oplus 1\end{bmatrix}, \text{якщо } k_1=1;\ k_2=1\end{cases} \quad (2.43)$$

$$O_{12}^{d}=\begin{bmatrix} x_1\cdot(\overline{k_1\oplus k_2})\oplus x_2\cdot(k_1\oplus k_2) \\ x_1\cdot(k_1\oplus k_2)\oplus x_2\cdot(\overline{k_1\oplus k_2}) \end{bmatrix}\oplus\begin{bmatrix}\bar{k}_2\\ k_2\end{bmatrix}=\begin{cases}\begin{bmatrix}x_1\oplus 1\\ x_2\end{bmatrix}, \text{ якщо } k_1=0;\ k_2=0\\ \begin{bmatrix}x_2\\ x_1\oplus 1\end{bmatrix}, \text{якщо } k_1=0;\ k_2=1\\ \begin{bmatrix}x_2\oplus 1\\ x_1\end{bmatrix}, \text{якщо } k_1=1;\ k_2=0\\ \begin{bmatrix}x_1\\ x_2\oplus 1\end{bmatrix}, \text{якщо } k_1=1;\ k_2=1\end{cases} \quad (2.44)$$

отримуємо перетворення такого вигляду:

$$O_{12}^{k*}=\begin{cases}\begin{bmatrix}x_1\oplus 1\\ x_2\end{bmatrix}, \text{ якщо } k_1=0;\ k_2=0\\ \begin{bmatrix}x_2\oplus 1\\ x_1\end{bmatrix}, \text{якщо } k_1=0;\ k_2=1\\ \begin{bmatrix}x_2\\ x_1\oplus 1\end{bmatrix}, \text{якщо } k_1=1;\ k_2=0\\ \begin{bmatrix}x_1\\ x_2\oplus 1\end{bmatrix}, \text{якщо } k_1=1;\ k_2=1\end{cases}=\begin{cases}\begin{bmatrix}x_1\\ x_2\oplus 1\end{bmatrix}, \text{ якщо } k_1=0;\ k_2=0\\ \begin{bmatrix}x_2\\ x_1\oplus 1\end{bmatrix}, \text{якщо } k_1=1;\ k_2=0\\ \begin{bmatrix}x_2\oplus 1\\ x_1\end{bmatrix}, \text{якщо } k_1=0;\ k_2=1\\ \begin{bmatrix}x_1\\ x_2\oplus 1\end{bmatrix}, \text{якщо } k_1=1;\ k_2=1\end{cases}=\begin{cases}\begin{bmatrix}x_1\oplus 1\\ x_2\end{bmatrix}, \text{ якщо } k_1=0;\ k_2=0\\ \begin{bmatrix}x_2\\ x_1\oplus 1\end{bmatrix}, \text{якщо } k_1=0;\ k_2=1\\ \begin{bmatrix}x_2\oplus 1\\ x_1\end{bmatrix}, \text{якщо } k_1=1;\ k_2=0\\ \begin{bmatrix}x_1\\ x_2\oplus 1\end{bmatrix}, \text{якщо } k_1=1;\ k_2=1\end{cases}=O_{12}^{d} \quad (2.45)$$

Отже, наше твердження вірне.

Якщо $O_{13}^{k}=\begin{bmatrix} x_1\cdot(k_1\oplus k_2)\oplus x_2\cdot(\overline{k_1\oplus k_2}) \\ x_1\cdot(\overline{k_1\oplus k_2})\oplus x_2\cdot(k_1\oplus k_2) \end{bmatrix}\oplus\begin{bmatrix}k_2\\ \bar{k}_2\end{bmatrix}$ – операція кодування, а $O_{13}^{d}=\begin{bmatrix} x_1\cdot(k_1\oplus k_2)\oplus x_2\cdot(\overline{k_1\oplus k_2}) \\ x_1\cdot(\overline{k_1\oplus k_2})\oplus x_2\cdot(k_1\oplus k_2) \end{bmatrix}\oplus\begin{bmatrix}\bar{k}_1\\ k_1\end{bmatrix}$ – операція декодування, тоді O_{13}^{k} можна застосувати в якості O_{13}^{d}, за умови $k_1^{*}=\bar{k}_2$, $k_2^{*}=\bar{k}_1$.

Так як:

$$O_{13}^{k}=\begin{bmatrix} x_1\cdot(k_1\oplus k_2)\oplus x_2\cdot(\overline{k_1\oplus k_2}) \\ x_1\cdot(\overline{k_1\oplus k_2})\oplus x_2\cdot(k_1\oplus k_2) \end{bmatrix}\oplus\begin{bmatrix} k_2 \\ \bar{k}_2 \end{bmatrix}=\begin{cases} \begin{bmatrix} x_2 \\ x_1\oplus 1 \end{bmatrix}, \text{ якщо } k_1=0;\ k_2=0 \\ \begin{bmatrix} x_1\oplus 1 \\ x_2 \end{bmatrix}, \text{якщо } k_1=0;\ k_2=1 \\ \begin{bmatrix} x_1 \\ x_2\oplus 1 \end{bmatrix}, \text{ якщо } k_1=1;\ k_2=0 \\ \begin{bmatrix} x_2\oplus 1 \\ x_1 \end{bmatrix}, \text{якщо } k_1=1;\ k_2=1 \end{cases} \quad (2.46)$$

$$O_{13}^{d}=\begin{bmatrix} x_1\cdot(k_1\oplus k_2)\oplus x_2\cdot(\overline{k_1\oplus k_2}) \\ x_1\cdot(\overline{k_1\oplus k_2})\oplus x_2\cdot(k_1\oplus k_2) \end{bmatrix}\oplus\begin{bmatrix} \bar{k}_1 \\ k_1 \end{bmatrix}=\begin{cases} \begin{bmatrix} x_2\oplus 1 \\ x_1 \end{bmatrix}, \text{ якщо } k_1=0;\ k_2=0 \\ \begin{bmatrix} x_1\oplus 1 \\ x_2 \end{bmatrix}, \text{якщо } k_1=0;\ k_2=1 \\ \begin{bmatrix} x_1 \\ x_2\oplus 1 \end{bmatrix}, \text{ якщо } k_1=1;\ k_2=0 \\ \begin{bmatrix} x_2 \\ x_1\oplus 1 \end{bmatrix}, \text{якщо } k_1=1;\ k_2=1 \end{cases} \quad (2.47)$$

отримуємо наступне перетворення:

$$O_{13}^{k*}=\begin{cases} \begin{bmatrix} x_2 \\ x_1\oplus 1 \end{bmatrix}, \text{ якщо } k_1=0;\ k_2=0 \\ \begin{bmatrix} x_1\oplus 1 \\ x_2 \end{bmatrix}, \text{якщо } k_1=0;\ k_2=1 \\ \begin{bmatrix} x_1 \\ x_2\oplus 1 \end{bmatrix}, \text{ якщо } k_1=1;\ k_2=0 \\ \begin{bmatrix} x_2\oplus 1 \\ x_1 \end{bmatrix}, \text{якщо } k_1=1;\ k_2=1 \end{cases}=\begin{cases} \begin{bmatrix} x_2\oplus 1 \\ x_1 \end{bmatrix}, \text{якщо } k_1=1;\ k_2=1 \\ \begin{bmatrix} x_1 \\ x_2\oplus 1 \end{bmatrix}, \text{ якщо } k_1=1;\ k_2=0 \\ \begin{bmatrix} x_1\oplus 1 \\ x_2 \end{bmatrix}, \text{якщо } k_1=0;\ k_2=1 \\ \begin{bmatrix} x_2 \\ x_1\oplus 1 \end{bmatrix}, \text{ якщо } k_1=0;\ k_2=0 \end{cases}=\begin{cases} \begin{bmatrix} x_2\oplus 1 \\ x_1 \end{bmatrix}, \text{ якщо } k_1=0;\ k_2=0 \\ \begin{bmatrix} x_1\oplus 1 \\ x_2 \end{bmatrix}, \text{якщо } k_1=0;\ k_2=1 \\ \begin{bmatrix} x_1 \\ x_2\oplus 1 \end{bmatrix}, \text{ якщо } k_1=1;\ k_2=0 \\ \begin{bmatrix} x_2 \\ x_1\oplus 1 \end{bmatrix}, \text{якщо } k_1=1;\ k_2=1 \end{cases}=O_{13}^{d} \quad (2.48)$$

Що і потрібно було довести.

Якщо $O_{14}^{k}=\begin{bmatrix} x_1\cdot k_2\oplus x_2\cdot\bar{k}_2 \\ x_1\cdot\bar{k}_2\oplus x_2\cdot k_2 \end{bmatrix}\oplus\begin{bmatrix} k_2 \\ \bar{k}_2 \end{bmatrix}$ – операція кодування, а $O_{14}^{d}=\begin{bmatrix} x_1\cdot k_2\oplus x_2\cdot\bar{k}_2 \\ x_1\cdot\bar{k}_2\oplus x_2\cdot k_2 \end{bmatrix}\oplus\begin{bmatrix} k_1 \\ \bar{k}_1 \end{bmatrix}$ – операція декодування, тоді O_{14}^{k} можна застосувати в якості O_{14}^{d}, за умови $k_1^{*}=\overline{k_1\oplus k_2}$, $k_2^{*}=k_2$.

Так як:

$$O_{14}^{k}=\begin{bmatrix} x_1\cdot k_2\oplus x_2\cdot\bar{k}_2 \\ x_1\cdot\bar{k}_2\oplus x_2\cdot k_2 \end{bmatrix}\oplus\begin{bmatrix} k_2 \\ \bar{k}_2 \end{bmatrix}=\begin{cases} \begin{bmatrix} x_2 \\ x_1\oplus 1 \end{bmatrix}, якщо\ k_1=0;\ k_2=0 \\ \begin{bmatrix} x_1\oplus 1 \\ x_2 \end{bmatrix}, якщо\ k_1=0;\ k_2=1 \\ \begin{bmatrix} x_2\oplus 1 \\ x_1 \end{bmatrix}, якщо\ k_1=1;\ k_2=0 \\ \begin{bmatrix} x_1 \\ x_2\oplus 1 \end{bmatrix}, якщо\ k_1=1;\ k_2=1 \end{cases} \quad (2.49)$$

$$O_{14}^{d}=\begin{bmatrix} x_1\cdot k_2\oplus x_2\cdot\bar{k}_2 \\ x_1\cdot\bar{k}_2\oplus x_2\cdot k_2 \end{bmatrix}\oplus\begin{bmatrix} k_1 \\ \bar{k}_1 \end{bmatrix}=\begin{cases} \begin{bmatrix} x_2\oplus 1 \\ x_1 \end{bmatrix}, якщо\ k_1=0;\ k_2=0 \\ \begin{bmatrix} x_1\oplus 1 \\ x_2 \end{bmatrix}, якщо\ k_1=0;\ k_2=1 \\ \begin{bmatrix} x_2 \\ x_1\oplus 1 \end{bmatrix}, якщо\ k_1=1;\ k_2=0 \\ \begin{bmatrix} x_1 \\ x_2\oplus 1 \end{bmatrix}, якщо\ k_1=1;\ k_2=1 \end{cases} \quad (2.50)$$

отримуємо:

$$O_{14}^{k*}=\begin{cases} \begin{bmatrix} x_2 \\ x_1\oplus 1 \end{bmatrix}, якщо\ k_1=0;\ k_2=0 \\ \begin{bmatrix} x_1\oplus 1 \\ x_2 \end{bmatrix}, якщо\ k_1=0;\ k_2=1 \\ \begin{bmatrix} x_2\oplus 1 \\ x_1 \end{bmatrix}, якщо\ k_1=1;\ k_2=0 \\ \begin{bmatrix} x_1 \\ x_2\oplus 1 \end{bmatrix}, якщо\ k_1=1;\ k_2=1 \end{cases}=\begin{cases} \begin{bmatrix} x_2\oplus 1 \\ x_1 \end{bmatrix}, якщо\ k_1=1;\ k_2=0 \\ \begin{bmatrix} x_1\oplus 1 \\ x_2 \end{bmatrix}, якщо\ k_1=0;\ k_2=1 \\ \begin{bmatrix} x_2 \\ x_1\oplus 1 \end{bmatrix}, якщо\ k_1=0;\ k_2=0 \\ \begin{bmatrix} x_1 \\ x_2\oplus 1 \end{bmatrix}, якщо\ k_1=1;\ k_2=1 \end{cases}=\begin{cases} \begin{bmatrix} x_2\oplus 1 \\ x_1 \end{bmatrix}, якщо\ k_1=0;\ k_2=0 \\ \begin{bmatrix} x_1\oplus 1 \\ x_2 \end{bmatrix}, якщо\ k_1=0;\ k_2=1 \\ \begin{bmatrix} x_2 \\ x_1\oplus 1 \end{bmatrix}, якщо\ k_1=1;\ k_2=0 \\ \begin{bmatrix} x_1 \\ x_2\oplus 1 \end{bmatrix}, якщо\ k_1=1;\ k_2=1 \end{cases}=O_{14}^{d} \quad (2.51)$$

Що й доведено.

У випадку, коли $O_{15}^{k}=\begin{bmatrix} x_1\cdot k_2\oplus x_2\cdot\bar{k}_2 \\ x_1\cdot\bar{k}_2\oplus x_2\cdot k_2 \end{bmatrix}\oplus\begin{bmatrix} k_1 \\ \bar{k}_1 \end{bmatrix}$ – операція кодування, а $O_{15}^{d}=\begin{bmatrix} x_1\cdot k_2\oplus x_2\cdot\bar{k}_2 \\ x_1\cdot\bar{k}_2\oplus x_2\cdot k_2 \end{bmatrix}\oplus\begin{bmatrix} \overline{k_1\oplus k_2} \\ k_1\oplus k_2 \end{bmatrix}$ – операція декодування, тоді O_{15}^{k} можна застосувати в якості O_{15}^{d}, за умови $k_1^{*}=\overline{k_1\oplus k_2}$, $k_2^{*}=k_2$.

Так як модельне представлення даних операцій наступне:

$$O_{15}^{k}=\begin{bmatrix} x_1\cdot k_2\oplus x_2\cdot\bar{k}_2 \\ x_1\cdot\bar{k}_2\oplus x_2\cdot k_2 \end{bmatrix}\oplus\begin{bmatrix} k_1 \\ \bar{k}_1 \end{bmatrix}=\begin{cases} \begin{bmatrix} x_2 \\ x_1\oplus 1 \end{bmatrix}, якщо\ k_1=0;\ k_2=0 \\ \begin{bmatrix} x_1 \\ x_2\oplus 1 \end{bmatrix}, якщо\ k_1=0;\ k_2=1 \\ \begin{bmatrix} x_2\oplus 1 \\ x_1 \end{bmatrix}, якщо\ k_1=1;\ k_2=0 \\ \begin{bmatrix} x_1\oplus 1 \\ x_2 \end{bmatrix}, якщо\ k_1=1;\ k_2=1 \end{cases} \quad (2.52)$$

$$O_{15}^{d}=\begin{bmatrix} x_1\cdot k_2\oplus x_2\cdot\bar{k}_2 \\ x_1\cdot\bar{k}_2\oplus x_2\cdot k_2 \end{bmatrix}\oplus\begin{bmatrix} \overline{k_1\oplus k_2} \\ k_1\oplus k_2 \end{bmatrix}=\begin{cases} \begin{bmatrix} x_2\oplus 1 \\ x_1 \end{bmatrix}, якщо\ k_1=0;\ k_2=0 \\ \begin{bmatrix} x_1 \\ x_2\oplus 1 \end{bmatrix}, якщо\ k_1=0;\ k_2=1 \\ \begin{bmatrix} x_2 \\ x_1\oplus 1 \end{bmatrix}, якщо\ k_1=1;\ k_2=0 \\ \begin{bmatrix} x_1\oplus 1 \\ x_2 \end{bmatrix}, якщо\ k_1=1;\ k_2=1 \end{cases} \quad (2.53)$$

отримуємо наступне перетворення:

$$O_{15}^{k*}=\begin{cases} \begin{bmatrix} x_2 \\ x_1\oplus 1 \end{bmatrix}, якщо\ k_1=0;\ k_2=0 \\ \begin{bmatrix} x_1 \\ x_2\oplus 1 \end{bmatrix}, якщо\ k_1=0;\ k_2=1 \\ \begin{bmatrix} x_2\oplus 1 \\ x_1 \end{bmatrix}, якщо\ k_1=1;\ k_2=0 \\ \begin{bmatrix} x_1\oplus 1 \\ x_2 \end{bmatrix}, якщо\ k_1=1;\ k_2=1 \end{cases}=\begin{cases} \begin{bmatrix} x_2\oplus 1 \\ x_1 \end{bmatrix}, якщо\ k_1=1;\ k_2=0 \\ \begin{bmatrix} x_1 \\ x_2\oplus 1 \end{bmatrix}, якщо\ k_1=0;\ k_2=1 \\ \begin{bmatrix} x_2 \\ x_1\oplus 1 \end{bmatrix}, якщо\ k_1=0;\ k_2=0 \\ \begin{bmatrix} x_1\oplus 1 \\ x_2 \end{bmatrix}, якщо\ k_1=1;\ k_2=1 \end{cases}=\begin{cases} \begin{bmatrix} x_2\oplus 1 \\ x_1 \end{bmatrix}, якщо\ k_1=0;\ k_2=0 \\ \begin{bmatrix} x_1 \\ x_2\oplus 1 \end{bmatrix}, якщо\ k_1=0;\ k_2=1 \\ \begin{bmatrix} x_2 \\ x_1\oplus 1 \end{bmatrix}, якщо\ k_1=1;\ k_2=0 \\ \begin{bmatrix} x_1\oplus 1 \\ x_2 \end{bmatrix}, якщо\ k_1=1;\ k_2=1 \end{cases}=O_{15}^{d} \quad (2.54)$$

Це доводить, що застосування виявлених взаємозв'язків є коректним.

Якщо $O_{16}^{k}=\begin{bmatrix} x_1\cdot(k_1\oplus k_2)\oplus x_2\cdot(\overline{k_1\oplus k_2}) \\ x_1\cdot(\overline{k_1\oplus k_2})\oplus x_2\cdot(k_1\oplus k_2) \end{bmatrix}\oplus\begin{bmatrix} k_1 \\ \bar{k}_1 \end{bmatrix}$ – операція кодування, а

$O_{16}^{d}=\begin{bmatrix} x_1\cdot(k_1\oplus k_2)\oplus x_2\cdot(\overline{k_1\oplus k_2}) \\ x_1\cdot(\overline{k_1\oplus k_2})\oplus x_2\cdot(k_1\oplus k_2) \end{bmatrix}\oplus\begin{bmatrix} \bar{k}_2 \\ k_2 \end{bmatrix}$ – операція декодування, тоді O_{16}^{k} можна застосувати в якості O_{16}^{d}, за умови $k_1^*=\bar{k}_2$, $k_2^*=\bar{k}_1$.

Так як модельне представлення даних операцій має наступний вигляд:

$$O_{16}^{k}=\begin{bmatrix} x_1\cdot(k_1\oplus k_2)\oplus x_2\cdot(\overline{k_1\oplus k_2}) \\ x_1\cdot(\overline{k_1\oplus k_2})\oplus x_2\cdot(k_1\oplus k_2) \end{bmatrix}\oplus\begin{bmatrix} k_1 \\ \bar{k}_1 \end{bmatrix}=\begin{cases} \begin{bmatrix} x_2 \\ x_1\oplus 1 \end{bmatrix}, \textit{якщо } k_1=0;\ k_2=0 \\ \begin{bmatrix} x_1 \\ x_2\oplus 1 \end{bmatrix}, \textit{якщо } k_1=0;\ k_2=1 \\ \begin{bmatrix} x_1\oplus 1 \\ x_2 \end{bmatrix}, \textit{якщо } k_1=1;\ k_2=0 \\ \begin{bmatrix} x_2\oplus 1 \\ x_1 \end{bmatrix}, \textit{якщо } k_1=1;\ k_2=1 \end{cases} \quad (2.55)$$

$$O_{16}^{d}=\begin{bmatrix} x_1\cdot(k_1\oplus k_2)\oplus x_2\cdot(\overline{k_1\oplus k_2}) \\ x_1\cdot(\overline{k_1\oplus k_2})\oplus x_2\cdot(k_1\oplus k_2) \end{bmatrix}\oplus\begin{bmatrix} \bar{k}_2 \\ k_2 \end{bmatrix}=\begin{cases} \begin{bmatrix} x_2\oplus 1 \\ x_1 \end{bmatrix}, \textit{якщо } k_1=0;\ k_2=0 \\ \begin{bmatrix} x_1 \\ x_2\oplus 1 \end{bmatrix}, \textit{якщо } k_1=0;\ k_2=1 \\ \begin{bmatrix} x_1\oplus 1 \\ x_2 \end{bmatrix}, \textit{якщо } k_1=1;\ k_2=0 \\ \begin{bmatrix} x_2 \\ x_1\oplus 1 \end{bmatrix}, \textit{якщо } k_1=1;\ k_2=1 \end{cases} \quad (2.56)$$

отримуємо:

$$O_{16}^{k*}=\begin{cases} \begin{bmatrix} x_2 \\ x_1\oplus 1 \end{bmatrix}, \textit{ якщо } k_1=0;\ k_2=0 \\ \begin{bmatrix} x_1 \\ x_2\oplus 1 \end{bmatrix}, \textit{якщо } k_1=0;\ k_2=1 \\ \begin{bmatrix} x_1\oplus 1 \\ x_2 \end{bmatrix}, \textit{ якщо } k_1=1;\ k_2=0 \\ \begin{bmatrix} x_2\oplus 1 \\ x_1 \end{bmatrix}, \textit{якщо } k_1=1;\ k_2=1 \end{cases}=\begin{cases} \begin{bmatrix} x_2\oplus 1 \\ x_1 \end{bmatrix}, \textit{якщо } k_1=1;\ k_2=1 \\ \begin{bmatrix} x_1 \\ x_2\oplus 1 \end{bmatrix}, \textit{якщо } k_1=0;\ k_2=1 \\ \begin{bmatrix} x_1\oplus 1 \\ x_2 \end{bmatrix}, \textit{ якщо } k_1=1;\ k_2=0 \\ \begin{bmatrix} x_2 \\ x_1\oplus 1 \end{bmatrix}, \textit{ якщо } k_1=0;\ k_2=0 \end{cases}=\begin{cases} \begin{bmatrix} x_2\oplus 1 \\ x_1 \end{bmatrix}, \textit{ якщо } k_1=0;\ k_2=0 \\ \begin{bmatrix} x_1 \\ x_2\oplus 1 \end{bmatrix}, \textit{якщо } k_1=0;\ k_2=1 \\ \begin{bmatrix} x_1\oplus 1 \\ x_2 \end{bmatrix}, \textit{ якщо } k_1=1;\ k_2=0 \\ \begin{bmatrix} x_2 \\ x_1\oplus 1 \end{bmatrix}, \textit{якщо } k_1=1;\ k_2=1 \end{cases}=O_{16}^{d} \quad (2.57)$$

Що й доводить наше твердження.

Візьмемо наступну пару операцій: нехай $O_{17}^{k}=\begin{bmatrix} x_1\cdot k_1\oplus x_2\cdot\bar{k}_1 \\ x_1\cdot\bar{k}_1\oplus x_2\cdot k_1 \end{bmatrix}\oplus\begin{bmatrix} k_1\oplus k_2 \\ \overline{k_1\oplus k_2} \end{bmatrix}$ – операція кодування, а $O_{17}^{d}=\begin{bmatrix} x_1\cdot k_1\oplus x_2\cdot\bar{k}_1 \\ x_1\cdot\bar{k}_1\oplus x_2\cdot k_1 \end{bmatrix}\oplus\begin{bmatrix} \bar{k}_2 \\ k_2 \end{bmatrix}$ – операція декодування. Тоді застосуємо O_{17}^{k} в якості O_{17}^{d}, за умови $k_1^*=k_1$, $k_2^*=\overline{k_1\oplus k_2}$.

Так як:

$$O_{17}^{k}=\begin{bmatrix} x_1\cdot k_1\oplus x_2\cdot\bar{k}_1 \\ x_1\cdot\bar{k}_1\oplus x_2\cdot k_1 \end{bmatrix}\oplus\begin{bmatrix} k_1\oplus k_2 \\ \overline{k_1\oplus k_2} \end{bmatrix}=\begin{cases} \begin{bmatrix} x_2 \\ x_1\oplus 1 \end{bmatrix}, якщо\ k_1=0;\ k_2=0 \\ \begin{bmatrix} x_2\oplus 1 \\ x_1 \end{bmatrix}, якщо\ k_1=0;\ k_2=1 \\ \begin{bmatrix} x_1\oplus 1 \\ x_2 \end{bmatrix}, якщо\ k_1=1;\ k_2=0 \\ \begin{bmatrix} x_1 \\ x_2\oplus 1 \end{bmatrix}, якщо\ k_1=1;\ k_2=1 \end{cases} \quad (2.58)$$

$$O_{17}^{d}=\begin{bmatrix} x_1\cdot k_1\oplus x_2\cdot\bar{k}_1 \\ x_1\cdot\bar{k}_1\oplus x_2\cdot k_1 \end{bmatrix}\oplus\begin{bmatrix} \bar{k}_2 \\ k_2 \end{bmatrix}=\begin{cases} \begin{bmatrix} x_2\oplus 1 \\ x_1 \end{bmatrix}, якщо\ k_1=0;\ k_2=0 \\ \begin{bmatrix} x_2 \\ x_1\oplus 1 \end{bmatrix}, якщо\ k_1=0;\ k_2=1 \\ \begin{bmatrix} x_1\oplus 1 \\ x_2 \end{bmatrix}, якщо\ k_1=1;\ k_2=0 \\ \begin{bmatrix} x_1 \\ x_2\oplus 1 \end{bmatrix}, якщо\ k_1=1;\ k_2=1 \end{cases} \quad (2.59)$$

в результаті отримуємо наступне перетворення:

$$O_{17}^{k*}=\begin{cases} \begin{bmatrix} x_2 \\ x_1\oplus 1 \end{bmatrix}, якщо\ k_1=0;\ k_2=0 \\ \begin{bmatrix} x_2\oplus 1 \\ x_1 \end{bmatrix}, якщо\ k_1=0;\ k_2=1 \\ \begin{bmatrix} x_1\oplus 1 \\ x_2 \end{bmatrix}, якщо\ k_1=1;\ k_2=0 \\ \begin{bmatrix} x_1 \\ x_2\oplus 1 \end{bmatrix}, якщо\ k_1=1;\ k_2=1 \end{cases}=\begin{cases} \begin{bmatrix} x_2\oplus 1 \\ x_1 \end{bmatrix}, якщо\ k_1=0;\ k_2=1 \\ \begin{bmatrix} x_2 \\ x_1\oplus 1 \end{bmatrix}, якщо\ k_1=0;\ k_2=0 \\ \begin{bmatrix} x_1\oplus 1 \\ x_2 \end{bmatrix}, якщо\ k_1=1;\ k_2=0 \\ \begin{bmatrix} x_1 \\ x_2\oplus 1 \end{bmatrix}, якщо\ k_1=1;\ k_2=1 \end{cases}=\begin{cases} \begin{bmatrix} x_2\oplus 1 \\ x_1 \end{bmatrix}, якщо\ k_1=0;\ k_2=0 \\ \begin{bmatrix} x_2 \\ x_1\oplus 1 \end{bmatrix}, якщо\ k_1=0;\ k_2=1 \\ \begin{bmatrix} x_1\oplus 1 \\ x_2 \end{bmatrix}, якщо\ k_1=1;\ k_2=0 \\ \begin{bmatrix} x_1 \\ x_2\oplus 1 \end{bmatrix}, якщо\ k_1=1;\ k_2=1 \end{cases}=O_{17}^{d} \quad (2.60)$$

Що доводить коректність застосування визначених взаємозв'язків.

Якщо $O_{18}^{k}=\begin{bmatrix} x_1\cdot k_1\oplus x_2\cdot\bar{k}_1 \\ x_1\cdot\bar{k}_1\oplus x_2\cdot k_1 \end{bmatrix}\oplus\begin{bmatrix} k_2 \\ \bar{k}_2 \end{bmatrix}$ – операція кодування, а $O_{18}^{d}=\begin{bmatrix} x_1\cdot k_1\oplus x_2\cdot\bar{k}_1 \\ x_1\cdot\bar{k}_1\oplus x_2\cdot k_1 \end{bmatrix}\oplus\begin{bmatrix} \overline{k_1\oplus k_2} \\ k_1\oplus k_2 \end{bmatrix}$ – операція декодування, тоді O_{18}^{k} можна застосувати в якості, O_{18}^{d} за умови $k_1^*=k_1$, $k_2^*=\overline{k_1\oplus k_2}$.

Так як:

$$O_{18}^{k}=\begin{bmatrix} x_1\cdot k_1\oplus x_2\cdot\bar{k}_1 \\ x_1\cdot\bar{k}_1\oplus x_2\cdot k_1 \end{bmatrix}\oplus\begin{bmatrix} k_2 \\ \bar{k}_2 \end{bmatrix}=\begin{cases} \begin{bmatrix} x_2 \\ x_1\oplus 1 \end{bmatrix}, \text{ якщо } k_1=0;\ k_2=0 \\ \begin{bmatrix} x_2\oplus 1 \\ x_1 \end{bmatrix}, \text{якщо } k_1=0;\ k_2=1 \\ \begin{bmatrix} x_1 \\ x_2\oplus 1 \end{bmatrix}, \text{ якщо } k_1=1;\ k_2=0 \\ \begin{bmatrix} x_1\oplus 1 \\ x_2 \end{bmatrix}, \text{якщо } k_1=1;\ k_2=1 \end{cases} \quad (2.61)$$

$$O_{18}^{d}=\begin{bmatrix} x_1\cdot k_1\oplus x_2\cdot\bar{k}_1 \\ x_1\cdot\bar{k}_1\oplus x_2\cdot k_1 \end{bmatrix}\oplus\begin{bmatrix} \overline{k_1\oplus k_2} \\ k_1\oplus k_2 \end{bmatrix}=\begin{cases} \begin{bmatrix} x_2\oplus 1 \\ x_1 \end{bmatrix}, \text{ якщо } k_1=0;\ k_2=0 \\ \begin{bmatrix} x_2 \\ x_1\oplus 1 \end{bmatrix}, \text{якщо } k_1=0;\ k_2=1 \\ \begin{bmatrix} x_1 \\ x_2\oplus 1 \end{bmatrix}, \text{ якщо } k_1=1;\ k_2=0 \\ \begin{bmatrix} x_1\oplus 1 \\ x_2 \end{bmatrix}, \text{якщо } k_1=1;\ k_2=1 \end{cases} \quad (2.62)$$

отримуємо:

$$O_{18}^{k*}=\begin{cases} \begin{bmatrix} x_2 \\ x_1\oplus 1 \end{bmatrix}, \text{якщо } k_1=0;\ k_2=0 \\ \begin{bmatrix} x_2\oplus 1 \\ x_1 \end{bmatrix}, \text{якщо } k_1=0;\ k_2=1 \\ \begin{bmatrix} x_1 \\ x_2\oplus 1 \end{bmatrix}, \text{якщо } k_1=1;\ k_2=0 \\ \begin{bmatrix} x_1\oplus 1 \\ x_2 \end{bmatrix}, \text{якщо } k_1=1;\ k_2=1 \end{cases}=\begin{cases} \begin{bmatrix} x_2\oplus 1 \\ x_1 \end{bmatrix}, \text{якщо } k_1=0;\ k_2=1 \\ \begin{bmatrix} x_2 \\ x_1\oplus 1 \end{bmatrix}, \text{якщо } k_1=0;\ k_2=0 \\ \begin{bmatrix} x_1 \\ x_2\oplus 1 \end{bmatrix}, \text{якщо } k_1=1;\ k_2=0 \\ \begin{bmatrix} x_1\oplus 1 \\ x_2 \end{bmatrix}, \text{якщо } k_1=1;\ k_2=1 \end{cases}=\begin{cases} \begin{bmatrix} x_2\oplus 1 \\ x_1 \end{bmatrix}, \text{якщо } k_1=0;\ k_2=0 \\ \begin{bmatrix} x_2 \\ x_1\oplus 1 \end{bmatrix}, \text{якщо } k_1=0;\ k_2=1 \\ \begin{bmatrix} x_1 \\ x_2\oplus 1 \end{bmatrix}, \text{якщо } k_1=1;\ k_2=0 \\ \begin{bmatrix} x_1\oplus 1 \\ x_2 \end{bmatrix}, \text{якщо } k_1=1;\ k_2=1 \end{cases}=O_{18}^{d} \quad (2.63)$$

Що і потрібно було довести.

Якщо $O_{19}^{k}=\begin{bmatrix} x_1\cdot\bar{k}_2\oplus x_2\cdot k_2 \\ x_1\cdot k_2\oplus x_2\cdot\bar{k}_2 \end{bmatrix}\oplus\begin{bmatrix} k_1 \\ \bar{k}_1 \end{bmatrix}$ – операція кодування, а $O_{19}^{d}=\begin{bmatrix} x_1\cdot\bar{k}_2\oplus x_2\cdot k_2 \\ x_1\cdot k_2\oplus x_2\cdot\bar{k}_2 \end{bmatrix}\oplus\begin{bmatrix} k_2 \\ \bar{k}_2 \end{bmatrix}$ – операція декодування, тоді O_{19}^{k} можна застосувати в якості O_{19}^{d}, за умови $k_1^{*}=\overline{k_1\oplus k_2}$, $k_2^{*}=k_2$.

Так як:

$$O_{19}^{k}=\begin{bmatrix} x_1\cdot\bar{k}_2\oplus x_2\cdot k_2 \\ x_1\cdot k_2\oplus x_2\cdot\bar{k}_2 \end{bmatrix}\oplus\begin{bmatrix} k_1 \\ \bar{k}_1 \end{bmatrix}=\begin{cases} \begin{bmatrix} x_2\oplus 1 \\ x_1 \end{bmatrix}, \text{ якщо } k_1=0;\ k_2=0 \\ \begin{bmatrix} x_1\oplus 1 \\ x_2 \end{bmatrix}, \text{якщо } k_1=0;\ k_2=1 \\ \begin{bmatrix} x_2 \\ x_1\oplus 1 \end{bmatrix}, \text{ якщо } k_1=1;\ k_2=0 \\ \begin{bmatrix} x_1 \\ x_2\oplus 1 \end{bmatrix}, \text{якщо } k_1=1;\ k_2=1 \end{cases} \quad (2.64)$$

$$O_{19}^{d}=\begin{bmatrix} x_1\cdot\bar{k}_2\oplus x_2\cdot k_2 \\ x_1\cdot k_2\oplus x_2\cdot\bar{k}_2 \end{bmatrix}\oplus\begin{bmatrix} k_2 \\ \bar{k}_2 \end{bmatrix}=\begin{cases} \begin{bmatrix} x_2 \\ x_1\oplus 1 \end{bmatrix}, \text{ якщо } k_1=0;\ k_2=0 \\ \begin{bmatrix} x_1\oplus 1 \\ x_2 \end{bmatrix}, \text{якщо } k_1=0;\ k_2=1 \\ \begin{bmatrix} x_2\oplus 1 \\ x_1 \end{bmatrix}, \text{ якщо } k_1=1;\ k_2=0 \\ \begin{bmatrix} x_1 \\ x_2\oplus 1 \end{bmatrix}, \text{якщо } k_1=1;\ k_2=1 \end{cases} \quad (2.65)$$

отримуємо наступне перетворення:

$$O_{19}^{k*}=\begin{cases} \begin{bmatrix} x_2\oplus 1 \\ x_1 \end{bmatrix}, \text{якщо } k_1=0;\ k_2=0 \\ \begin{bmatrix} x_1\oplus 1 \\ x_2 \end{bmatrix}, \text{якщо } k_1=0;\ k_2=1 \\ \begin{bmatrix} x_2 \\ x_1\oplus 1 \end{bmatrix}, \text{якщо } k_1=1;\ k_2=0 \\ \begin{bmatrix} x_1 \\ x_2\oplus 1 \end{bmatrix}, \text{якщо } k_1=1;\ k_2=1 \end{cases}=\begin{cases} \begin{bmatrix} x_2 \\ x_1\oplus 1 \end{bmatrix}, \text{якщо } k_1=1;\ k_2=0 \\ \begin{bmatrix} x_1\oplus 1 \\ x_2 \end{bmatrix}, \text{якщо } k_1=0;\ k_2=1 \\ \begin{bmatrix} x_2\oplus 1 \\ x_1 \end{bmatrix}, \text{якщо } k_1=0;\ k_2=0 \\ \begin{bmatrix} x_1 \\ x_2\oplus 1 \end{bmatrix}, \text{якщо } k_1=1;\ k_2=1 \end{cases}=\begin{cases} \begin{bmatrix} x_2 \\ x_1\oplus 1 \end{bmatrix}, \text{якщо } k_1=0;\ k_2=0 \\ \begin{bmatrix} x_1\oplus 1 \\ x_2 \end{bmatrix}, \text{якщо } k_1=0;\ k_2=1 \\ \begin{bmatrix} x_2\oplus 1 \\ x_1 \end{bmatrix}, \text{якщо } k_1=1;\ k_2=0 \\ \begin{bmatrix} x_1 \\ x_2\oplus 1 \end{bmatrix}, \text{якщо } k_1=1;\ k_2=1 \end{cases}=O_{19}^{d} \quad (2.66)$$

Що й доводить правильність застосування умови перетворення.

Якщо $O_{20}^{k}=\begin{bmatrix} x_1\cdot(k_1\oplus k_2)\oplus x_2\cdot\overline{(k_1\oplus k_2)} \\ x_1\cdot\overline{(k_1\oplus k_2)}\oplus x_2\cdot(k_1\oplus k_2) \end{bmatrix}\oplus\begin{bmatrix} \bar{k}_1 \\ k_1 \end{bmatrix}$ – операція кодування, а

$O_{20}^{d}=\begin{bmatrix} x_1\cdot(k_1\oplus k_2)\oplus x_2\cdot\overline{(k_1\oplus k_2)} \\ x_1\cdot\overline{(k_1\oplus k_2)}\oplus x_2\cdot(k_1\oplus k_2) \end{bmatrix}\oplus\begin{bmatrix} k_2 \\ \bar{k}_2 \end{bmatrix}$ – операція декодування, тоді O_{20}^{k} можна застосувати в якості O_{20}^{d}, за умови $k_1^*=\bar{k}_2$, $k_2^*=\bar{k}_1$.

Так як:

$$O_{20}^{k}=\begin{bmatrix} x_1\cdot(k_1\oplus k_2)\oplus x_2\cdot\overline{(k_1\oplus k_2)} \\ x_1\cdot\overline{(k_1\oplus k_2)}\oplus x_2\cdot(k_1\oplus k_2) \end{bmatrix}\oplus\begin{bmatrix}\bar{k}_1\\ k_1\end{bmatrix}=\begin{cases}\begin{bmatrix}x_2\oplus 1\\ x_1\end{bmatrix}, \text{ якщо } k_1=0;\ k_2=0\\ \begin{bmatrix}x_1\oplus 1\\ x_2\end{bmatrix}, \text{якщо } k_1=0;\ k_2=1\\ \begin{bmatrix}x_1\\ x_2\oplus 1\end{bmatrix}, \text{ якщо } k_1=1;\ k_2=0\\ \begin{bmatrix}x_2\\ x_1\oplus 1\end{bmatrix}, \text{якщо } k_1=1;\ k_2=1\end{cases} \quad (2.67)$$

$$O_{20}^{d}=\begin{bmatrix} x_1\cdot\bar{k}_1\oplus x_2\cdot k_1 \\ x_1\cdot k_1\oplus x_2\cdot\bar{k}_1 \end{bmatrix}\oplus\begin{bmatrix}k_1\oplus k_2\\ \overline{k_1\oplus k_2}\end{bmatrix}=\begin{cases}\begin{bmatrix}x_2\\ x_1\oplus 1\end{bmatrix}, \text{ якщо } k_1=0;\ k_2=0\\ \begin{bmatrix}x_1\oplus 1\\ x_2\end{bmatrix}, \text{якщо } k_1=0;\ k_2=1\\ \begin{bmatrix}x_1\\ x_2\oplus 1\end{bmatrix}, \text{ якщо } k_1=1;\ k_2=0\\ \begin{bmatrix}x_2\oplus 1\\ x_1\end{bmatrix}, \text{якщо } k_1=1;\ k_2=1\end{cases} \quad (2.68)$$

отримуємо наступне перетворення:

$$O_{20}^{k*}=\begin{cases}\begin{bmatrix}x_2\oplus 1\\ x_1\end{bmatrix}, \text{якщо } k_1=0;\ k_2=0\\ \begin{bmatrix}x_1\oplus 1\\ x_2\end{bmatrix}, \text{якщо } k_1=0;\ k_2=1\\ \begin{bmatrix}x_1\\ x_2\oplus 1\end{bmatrix}, \text{якщо } k_1=1;\ k_2=0\\ \begin{bmatrix}x_2\\ x_1\oplus 1\end{bmatrix}, \text{якщо } k_1=1;\ k_2=1\end{cases}=\begin{cases}\begin{bmatrix}x_2\oplus 1\\ x_1\end{bmatrix}, \text{якщо } k_1=0;\ k_2=0\\ \begin{bmatrix}x_1\\ x_2\oplus 1\end{bmatrix}, \text{якщо } k_1=1;\ k_2=0\\ \begin{bmatrix}x_1\oplus 1\\ x_2\end{bmatrix}, \text{якщо } k_1=0;\ k_2=1\\ \begin{bmatrix}x_2\\ x_1\oplus 1\end{bmatrix}, \text{якщо } k_1=1;\ k_2=1\end{cases}=\begin{cases}\begin{bmatrix}x_2\\ x_1\oplus 1\end{bmatrix}, \text{якщо } k_1=0;\ k_2=0\\ \begin{bmatrix}x_1\oplus 1\\ x_2\end{bmatrix}, \text{якщо } k_1=0;\ k_2=1\\ \begin{bmatrix}x_1\\ x_2\oplus 1\end{bmatrix}, \text{якщо } k_1=1;\ k_2=0\\ \begin{bmatrix}x_2\oplus 1\\ x_1\end{bmatrix}, \text{якщо } k_1=1;\ k_2=1\end{cases}=O_{20}^{d} \quad (2.69)$$

Що і потрібно було довести.

Якщо $O_{21}^{k}=\begin{bmatrix} x_1\cdot k_1\oplus x_2\cdot\bar{k}_1 \\ x_1\cdot\bar{k}_1\oplus x_2\cdot k_1 \end{bmatrix}\oplus\begin{bmatrix}\overline{k_1\oplus k_2}\\ k_1\oplus k_2\end{bmatrix}$ – операція кодування, а $O_{21}^{d}=\begin{bmatrix} x_1\cdot k_1\oplus x_2\cdot\bar{k}_1 \\ x_1\cdot\bar{k}_1\oplus x_2\cdot k_1 \end{bmatrix}\oplus\begin{bmatrix}k_2\\ \bar{k}_2\end{bmatrix}$ – операція декодування, тоді O_{21}^{k} можна застосувати в якості O_{21}^{d}, за умови $k_1^{*}=k_1,\ k_2^{*}=\overline{k_1\oplus k_2}$.

Так як:

$$O_{21}^{k}=\begin{bmatrix} x_1\cdot k_1\oplus x_2\cdot\bar{k}_1 \\ x_1\cdot\bar{k}_1\oplus x_2\cdot k_1 \end{bmatrix}\oplus\begin{bmatrix} \overline{k_1\oplus k_2} \\ k_1\oplus k_2 \end{bmatrix}=\begin{cases} \begin{bmatrix} x_2\oplus 1 \\ x_1 \end{bmatrix}, \text{ якщо } k_1=0;\ k_2=0 \\ \begin{bmatrix} x_2 \\ x_1\oplus 1 \end{bmatrix}, \text{якщо } k_1=0;\ k_2=1 \\ \begin{bmatrix} x_1 \\ x_2\oplus 1 \end{bmatrix}, \text{ якщо } k_1=1;\ k_2=0 \\ \begin{bmatrix} x_1\oplus 1 \\ x_2 \end{bmatrix}, \text{якщо } k_1=1;\ k_2=1 \end{cases} \quad (2.70)$$

$$O_{21}^{d}=\begin{bmatrix} x_1\cdot k_1\oplus x_2\cdot\bar{k}_1 \\ x_1\cdot\bar{k}_1\oplus x_2\cdot k_1 \end{bmatrix}\oplus\begin{bmatrix} k_2 \\ \bar{k}_2 \end{bmatrix}=\begin{cases} \begin{bmatrix} x_2 \\ x_1\oplus 1 \end{bmatrix}, \text{ якщо } k_1=0;\ k_2=0 \\ \begin{bmatrix} x_2\oplus 1 \\ x_1 \end{bmatrix}, \text{якщо } k_1=0;\ k_2=1 \\ \begin{bmatrix} x_1 \\ x_2\oplus 1 \end{bmatrix}, \text{ якщо } k_1=1;\ k_2=0 \\ \begin{bmatrix} x_1\oplus 1 \\ x_2 \end{bmatrix}, \text{якщо } k_1=1;\ k_2=1 \end{cases} \quad (2.71)$$

отримуємо наступне перетворення:

$$O_{21}^{k*}=\begin{cases} \begin{bmatrix} x_2\oplus 1 \\ x_1 \end{bmatrix}, \text{якщо } k_1=0;\ k_2=0 \\ \begin{bmatrix} x_2 \\ x_1\oplus 1 \end{bmatrix}, \text{якщо } k_1=0;\ k_2=1 \\ \begin{bmatrix} x_1 \\ x_2\oplus 1 \end{bmatrix}, \text{якщо } k_1=1;\ k_2=0 \\ \begin{bmatrix} x_1\oplus 1 \\ x_2 \end{bmatrix}, \text{якщо } k_1=1;\ k_2=1 \end{cases}=\begin{cases} \begin{bmatrix} x_2 \\ x_1\oplus 1 \end{bmatrix}, \text{якщо } k_1=0;\ k_2=1 \\ \begin{bmatrix} x_2\oplus 1 \\ x_1 \end{bmatrix}, \text{якщо } k_1=0;\ k_2=0 \\ \begin{bmatrix} x_1 \\ x_2\oplus 1 \end{bmatrix}, \text{якщо } k_1=1;\ k_2=0 \\ \begin{bmatrix} x_1\oplus 1 \\ x_2 \end{bmatrix}, \text{якщо } k_1=1;\ k_2=1 \end{cases}=\begin{cases} \begin{bmatrix} x_2 \\ x_1\oplus 1 \end{bmatrix}, \text{якщо } k_1=0;\ k_2=0 \\ \begin{bmatrix} x_2\oplus 1 \\ x_1 \end{bmatrix}, \text{якщо } k_1=0;\ k_2=1 \\ \begin{bmatrix} x_1 \\ x_2\oplus 1 \end{bmatrix}, \text{якщо } k_1=1;\ k_2=0 \\ \begin{bmatrix} x_1\oplus 1 \\ x_2 \end{bmatrix}, \text{якщо } k_1=1;\ k_2=1 \end{cases}=O_{21}^{d} \quad (2.72)$$

Що і потрібно було довести.

Якщо $O_{22}^{k}=\begin{bmatrix} x_1\cdot k_1\oplus x_2\cdot\bar{k}_1 \\ x_1\cdot\bar{k}_1\oplus x_2\cdot k_1 \end{bmatrix}\oplus\begin{bmatrix} \bar{k}_2 \\ k_2 \end{bmatrix}$ – операція кодування, а $O_{22}^{d}=\begin{bmatrix} x_1\cdot k_1\oplus x_2\cdot\bar{k}_1 \\ x_1\cdot\bar{k}_1\oplus x_2\cdot k_1 \end{bmatrix}\oplus\begin{bmatrix} k_1\oplus k_2 \\ \overline{k_1\oplus k_2} \end{bmatrix}$ – операція декодування, тоді O_{22}^{k} можна застосувати в якості O_{22}^{d}, за умови $k_1^{*}=k_1$, $k_2^{*}=\overline{k_1\oplus k_2}$.

Так як:

$$O_{22}^{k}=\begin{bmatrix} x_1\cdot k_1\oplus x_2\cdot\bar{k}_1 \\ x_1\cdot\bar{k}_1\oplus x_2\cdot k_1 \end{bmatrix}\oplus\begin{bmatrix}\bar{k}_2\\ k_2\end{bmatrix}=\begin{cases}\begin{bmatrix}x_2\oplus 1\\ x_1\end{bmatrix}, якщо\ k_1=0;\ k_2=0\\ \begin{bmatrix}x_2\\ x_1\oplus 1\end{bmatrix}, якщо\ k_1=0;\ k_2=1\\ \begin{bmatrix}x_1\oplus 1\\ x_2\end{bmatrix}, якщо\ k_1=1;\ k_2=0\\ \begin{bmatrix}x_1\\ x_2\oplus 1\end{bmatrix}, якщо\ k_1=1;\ k_2=1\end{cases} \quad (2.73)$$

$$O_{22}^{d}=\begin{bmatrix} x_1\cdot k_1\oplus x_2\cdot\bar{k}_1 \\ x_1\cdot\bar{k}_1\oplus x_2\cdot k_1 \end{bmatrix}\oplus\begin{bmatrix}k_1\oplus k_2\\ \overline{k_1\oplus k_2}\end{bmatrix}=\begin{cases}\begin{bmatrix}x_2\\ x_1\oplus 1\end{bmatrix}, якщо\ k_1=0;\ k_2=0\\ \begin{bmatrix}x_2\oplus 1\\ x_1\end{bmatrix}, якщо\ k_1=0;\ k_2=1\\ \begin{bmatrix}x_1\oplus 1\\ x_2\end{bmatrix}, якщо\ k_1=1;\ k_2=0\\ \begin{bmatrix}x_1\\ x_2\oplus 1\end{bmatrix}, якщо\ k_1=1;\ k_2=1\end{cases} \quad (2.74)$$

отримуємо такий результат перетворення:

$$O_{22}^{k*}=\begin{cases}\begin{bmatrix}x_2\oplus 1\\ x_1\end{bmatrix}, якщо\ k_1=0;\ k_2=0\\ \begin{bmatrix}x_2\\ x_1\oplus 1\end{bmatrix}, якщо\ k_1=0;\ k_2=1\\ \begin{bmatrix}x_1\oplus 1\\ x_2\end{bmatrix}, якщо\ k_1=1;\ k_2=0\\ \begin{bmatrix}x_1\\ x_2\oplus 1\end{bmatrix}, якщо\ k_1=1;\ k_2=1\end{cases}=\begin{cases}\begin{bmatrix}x_2\\ x_1\oplus 1\end{bmatrix}, якщо\ k_1=0;\ k_2=1\\ \begin{bmatrix}x_2\oplus 1\\ x_1\end{bmatrix}, якщо\ k_1=0;\ k_2=0\\ \begin{bmatrix}x_1\oplus 1\\ x_2\end{bmatrix}, якщо\ k_1=1;\ k_2=0\\ \begin{bmatrix}x_1\\ x_2\oplus 1\end{bmatrix}, якщо\ k_1=1;\ k_2=1\end{cases}=\begin{cases}\begin{bmatrix}x_2\\ x_1\oplus 1\end{bmatrix}, якщо\ k_1=0;\ k_2=0\\ \begin{bmatrix}x_2\oplus 1\\ x_1\end{bmatrix}, якщо\ k_1=0;\ k_2=1\\ \begin{bmatrix}x_1\oplus 1\\ x_2\end{bmatrix}, якщо\ k_1=1;\ k_2=0\\ \begin{bmatrix}x_1\\ x_2\oplus 1\end{bmatrix}, якщо\ k_1=1;\ k_2=1\end{cases}=O_{22}^{d} \quad (2.75)$$

Що і доводить вірність нашого твердження.

Якщо $O_{23}^{k}=\begin{bmatrix} x_1\cdot(k_1\oplus k_2)\oplus x_2\cdot\overline{(k_1\oplus k_2)} \\ x_1\cdot\overline{(k_1\oplus k_2)}\oplus x_2\cdot(k_1\oplus k_2) \end{bmatrix}\oplus\begin{bmatrix}\bar{k}_2\\ k_2\end{bmatrix}$ – операція кодування, а

$O_{23}^{d}=\begin{bmatrix} x_1\cdot(k_1\oplus k_2)\oplus x_2\cdot\overline{(k_1\oplus k_2)} \\ x_1\cdot\overline{(k_1\oplus k_2)}\oplus x_2\cdot(k_1\oplus k_2) \end{bmatrix}\oplus\begin{bmatrix}k_1\\ \bar{k}_1\end{bmatrix}$ – операція декодування, тоді O_{23}^{k} можна

застосувати в якості O_{23}^{d}, за умови $k_1^*=\bar{k}_2$, $k_2^*=\bar{k}_1$.

Так як розгорнутий вигдяд операцій наступний:

$$O_{23}^{k}=\begin{bmatrix} x_1\cdot(k_1\oplus k_2)\oplus x_2\cdot(\overline{k_1\oplus k_2}) \\ x_1\cdot(\overline{k_1\oplus k_2})\oplus x_2\cdot(k_1\oplus k_2) \end{bmatrix}\oplus\begin{bmatrix} \bar{k}_2 \\ k_2 \end{bmatrix}=\begin{cases} \begin{bmatrix} x_2\oplus 1 \\ x_1 \end{bmatrix}, \text{ якщо } k_1=0;\ k_2=0 \\ \begin{bmatrix} x_1 \\ x_2\oplus 1 \end{bmatrix}, \text{якщо } k_1=0;\ k_2=1 \\ \begin{bmatrix} x_1\oplus 1 \\ x_2 \end{bmatrix}, \text{ якщо } k_1=1;\ k_2=0 \\ \begin{bmatrix} x_2 \\ x_1\oplus 1 \end{bmatrix}, \text{якщо } k_1=1;\ k_2=1 \end{cases} \quad (2.76)$$

$$O_{23}^{d}=\begin{bmatrix} x_1\cdot(k_1\oplus k_2)\oplus x_2\cdot(\overline{k_1\oplus k_2}) \\ x_1\cdot(\overline{k_1\oplus k_2})\oplus x_2\cdot(k_1\oplus k_2) \end{bmatrix}\oplus\begin{bmatrix} k_1 \\ \bar{k}_1 \end{bmatrix}=\begin{cases} \begin{bmatrix} x_2 \\ x_1\oplus 1 \end{bmatrix}, \text{ якщо } k_1=0;\ k_2=0 \\ \begin{bmatrix} x_1 \\ x_2\oplus 1 \end{bmatrix}, \text{якщо } k_1=0;\ k_2=1 \\ \begin{bmatrix} x_1\oplus 1 \\ x_2 \end{bmatrix}, \text{ якщо } k_1=1;\ k_2=0 \\ \begin{bmatrix} x_2\oplus 1 \\ x_1 \end{bmatrix}, \text{якщо } k_1=1;\ k_2=1 \end{cases} \quad (2.74)$$

згідно цього отримуємо перетворення:

$$O_{23}^{k*}=\begin{cases} \begin{bmatrix} x_2\oplus 1 \\ x_1 \end{bmatrix}, \text{ якщо } k_1=0;\ k_2=0 \\ \begin{bmatrix} x_1 \\ x_2\oplus 1 \end{bmatrix}, \text{якщо } k_1=0;\ k_2=1 \\ \begin{bmatrix} x_1\oplus 1 \\ x_2 \end{bmatrix}, \text{ якщо } k_1=1;\ k_2=0 \\ \begin{bmatrix} x_2 \\ x_1\oplus 1 \end{bmatrix}, \text{якщо } k_1=1;\ k_2=1 \end{cases}=\begin{cases} \begin{bmatrix} x_2 \\ x_1\oplus 1 \end{bmatrix}, \text{якщо } k_1=1;\ k_2=1 \\ \begin{bmatrix} x_1 \\ x_2\oplus 1 \end{bmatrix}, \text{якщо } k_1=0;\ k_2=1 \\ \begin{bmatrix} x_1\oplus 1 \\ x_2 \end{bmatrix}, \text{якщо } k_1=1;\ k_2=0 \\ \begin{bmatrix} x_2\oplus 1 \\ x_1 \end{bmatrix}, \text{ якщо } k_1=0;\ k_2=0 \end{cases}=\begin{cases} \begin{bmatrix} x_2 \\ x_1\oplus 1 \end{bmatrix}, \text{ якщо } k_1=0;\ k_2=0 \\ \begin{bmatrix} x_1 \\ x_2\oplus 1 \end{bmatrix}, \text{якщо } k_1=0;\ k_2=1 \\ \begin{bmatrix} x_1\oplus 1 \\ x_2 \end{bmatrix}, \text{якщо } k_1=1;\ k_2=0 \\ \begin{bmatrix} x_2\oplus 1 \\ x_1 \end{bmatrix}, \text{якщо } k_1=1;\ k_2=1 \end{cases}=O_{23}^{d} \quad (2.75)$$

Що і необхідно було довести.

Якщо $O_{24}^{k}=\begin{bmatrix} x_1\cdot k_2\oplus x_2\cdot\bar{k}_2 \\ x_1\cdot\bar{k}_2\oplus x_2\cdot k_2 \end{bmatrix}\oplus\begin{bmatrix} \overline{k_1\oplus k_2} \\ k_1\oplus k_2 \end{bmatrix}$ – операція кодування, а $O_{24}^{d}=\begin{bmatrix} x_1\cdot k_2\oplus x_2\cdot\bar{k}_2 \\ x_1\cdot\bar{k}_2\oplus x_2\cdot k_2 \end{bmatrix}\oplus\begin{bmatrix} k_1 \\ \bar{k}_1 \end{bmatrix}$ – операція декодування, тоді O_{24}^{k} можна застосувати в якості O_{24}^{d}, за умови $k_1^*=\overline{k_1\oplus k_2}$, $k_2^*=k_2$.

Так як:

$$O_{24}^{k}=\begin{bmatrix} x_1\cdot k_2 \oplus x_2\cdot \bar{k}_2 \\ x_1\cdot \bar{k}_2 \oplus x_2\cdot k_2 \end{bmatrix} \oplus \begin{bmatrix} \overline{k_1 \oplus k_2} \\ k_1 \oplus k_2 \end{bmatrix} = \begin{cases} \begin{bmatrix} x_2 \oplus 1 \\ x_1 \end{bmatrix}, \text{ якщо } k_1=0;\ k_2=0 \\ \begin{bmatrix} x_1 \\ x_2 \oplus 1 \end{bmatrix}, \text{якщо } k_1=0;\ k_2=1 \\ \begin{bmatrix} x_2 \\ x_1 \oplus 1 \end{bmatrix}, \text{ якщо } k_1=1;\ k_2=0 \\ \begin{bmatrix} x_1 \oplus 1 \\ x_2 \end{bmatrix}, \text{якщо } k_1=1;\ k_2=1 \end{cases} \quad (2.76)$$

$$O_{24}^{d}=\begin{bmatrix} x_1\cdot k_2 \oplus x_2\cdot \bar{k}_2 \\ x_1\cdot \bar{k}_2 \oplus x_2\cdot k_2 \end{bmatrix} \oplus \begin{bmatrix} k_1 \\ \bar{k}_1 \end{bmatrix} = \begin{cases} \begin{bmatrix} x_2 \\ x_1 \oplus 1 \end{bmatrix}, \text{ якщо } k_1=0;\ k_2=0 \\ \begin{bmatrix} x_1 \\ x_2 \oplus 1 \end{bmatrix}, \text{якщо } k_1=0;\ k_2=1 \\ \begin{bmatrix} x_2 \oplus 1 \\ x_1 \end{bmatrix}, \text{ якщо } k_1=1;\ k_2=0 \\ \begin{bmatrix} x_1 \oplus 1 \\ x_2 \end{bmatrix}, \text{якщо } k_1=1;\ k_2=1 \end{cases} \quad (2.77)$$

отримуємо наступний результат перетворення:

$$O_{24}^{k*}=\begin{cases} \begin{bmatrix} x_2 \oplus 1 \\ x_1 \end{bmatrix}, \text{ якщо } k_1=0;\ k_2=0 \\ \begin{bmatrix} x_1 \\ x_2 \oplus 1 \end{bmatrix}, \text{якщо } k_1=0;\ k_2=1 \\ \begin{bmatrix} x_2 \\ x_1 \oplus 1 \end{bmatrix}, \text{ якщо } k_1=1;\ k_2=0 \\ \begin{bmatrix} x_1 \oplus 1 \\ x_2 \end{bmatrix}, \text{якщо } k_1=1;\ k_2=1 \end{cases} = \begin{cases} \begin{bmatrix} x_2 \\ x_1 \oplus 1 \end{bmatrix}, \text{ якщо } k_1=1;\ k_2=0 \\ \begin{bmatrix} x_1 \\ x_2 \oplus 1 \end{bmatrix}, \text{якщо } k_1=0;\ k_2=1 \\ \begin{bmatrix} x_2 \oplus 1 \\ x_1 \end{bmatrix}, \text{ якщо } k_1=0;\ k_2=0 \\ \begin{bmatrix} x_1 \oplus 1 \\ x_2 \end{bmatrix}, \text{якщо } k_1=1;\ k_2=1 \end{cases} = \begin{cases} \begin{bmatrix} x_2 \\ x_1 \oplus 1 \end{bmatrix}, \text{ якщо } k_1=0;\ k_2=0 \\ \begin{bmatrix} x_1 \\ x_2 \oplus 1 \end{bmatrix}, \text{якщо } k_1=0;\ k_2=1 \\ \begin{bmatrix} x_2 \oplus 1 \\ x_1 \end{bmatrix}, \text{ якщо } k_1=1;\ k_2=0 \\ \begin{bmatrix} x_1 \oplus 1 \\ x_2 \end{bmatrix}, \text{якщо } k_1=1;\ k_2=1 \end{cases} = O_{24}^{d} \quad (2.78)$$

Саме це й потрібно було довести.

Таким чином, в результаті було побудовано обернені операції для всієї групи двохрозрядних двохоперандних операцій ССКК.

2.4 Узагальнення результатів дслідження взаємозв'язків між прямими і оберненими двохрозрядних двохоперандних операцій строгого стійкого криптографічного кодування на основі перетворення другого операнда

Результати даного дослідження наведені в табл.2.5. В даній таблиці виділено визначені підгрупи операцій які мають однакові взаємозв'язки, що, в свою чергу, забезпечує спрощення алгоритмів криптографічного захисту інформації [3].

Таблиця 2.5

Результати синтезу операцій на основі встановлених взаємозв'язків

№ п/п	Пряма операція криптоперетворення	Обернена операція криптоперетворення	Модель автомата побудови другого операнду оберненої операції
1	2	3	4
1	$O_1^k=\begin{bmatrix} x_1\cdot\bar{k}_1\oplus x_2\cdot k_1 \\ x_1\cdot k_1\oplus x_2\cdot\bar{k}_1\end{bmatrix}\oplus\begin{bmatrix} k_2 \\ \bar{k}_2\end{bmatrix}$	$O_1^d=\begin{bmatrix} x_1\cdot\bar{k}_1\oplus x_2\cdot k_1 \\ x_1\cdot k_1\oplus x_2\cdot\bar{k}_1\end{bmatrix}\oplus\begin{bmatrix} k_1\oplus k_2 \\ \overline{k_1\oplus k_2}\end{bmatrix}$	$k_1^*=k_1$ $k_2^*=k_1\oplus k_2$
2	$O_2^k=\begin{bmatrix} x_1\cdot\bar{k}_1\oplus x_2\cdot k_1 \\ x_1\cdot k_1\oplus x_2\cdot\bar{k}_1\end{bmatrix}\oplus\begin{bmatrix} k_1\oplus k_2 \\ \overline{k_1\oplus k_2}\end{bmatrix}$	$O_2^d=\begin{bmatrix} x_1\cdot\bar{k}_1\oplus x_2\cdot k_1 \\ x_1\cdot k_1\oplus x_2\cdot\bar{k}_1\end{bmatrix}\oplus\begin{bmatrix} k_2 \\ \bar{k}_2\end{bmatrix}$	$k_1^*=k_1$ $k_2^*=k_1\oplus k_2$
3	$O_3^k=\begin{bmatrix} x_1\cdot(\overline{k_1\oplus k_2})\oplus x_2\cdot(k_1\oplus k_2) \\ x_1\cdot(k_1\oplus k_2)\oplus x_2\cdot(\overline{k_1\oplus k_2})\end{bmatrix}\oplus\begin{bmatrix} k_1 \\ \bar{k}_1\end{bmatrix}$	$O_3^d=\begin{bmatrix} x_1\cdot(\overline{k_1\oplus k_2})\oplus x_2\cdot(k_1\oplus k_2) \\ x_1\cdot(k_1\oplus k_2)\oplus x_2\cdot(\overline{k_1\oplus k_2})\end{bmatrix}\oplus\begin{bmatrix} k_2 \\ \bar{k}_2\end{bmatrix}$	$k_1^*=k_2$ $k_2^*=k_1$
4	$O_4^k=\begin{bmatrix} x_1\cdot\bar{k}_2\oplus x_2\cdot k_2 \\ x_1\cdot k_2\oplus x_2\cdot\bar{k}_2\end{bmatrix}\oplus\begin{bmatrix} k_1 \\ \bar{k}_1\end{bmatrix}$	$O_4^d=\begin{bmatrix} x_1\cdot\bar{k}_2\oplus x_2\cdot k_2 \\ x_1\cdot k_2\oplus x_2\cdot\bar{k}_2\end{bmatrix}\oplus\begin{bmatrix} k_1\oplus k_2 \\ \overline{k_1\oplus k_2}\end{bmatrix}$	$k_1^*=k_1\oplus k_2$ $k_2^*=k_2$
5	$O_5^k=\begin{bmatrix} x_1\cdot\bar{k}_2\oplus x_2\cdot k_2 \\ x_1\cdot k_2\oplus x_2\cdot\bar{k}_2\end{bmatrix}\oplus\begin{bmatrix} k_1\oplus k_2 \\ \overline{k_1\oplus k_2}\end{bmatrix}$	$O_5^d=\begin{bmatrix} x_1\cdot\bar{k}_2\oplus x_2\cdot k_2 \\ x_1\cdot k_2\oplus x_2\cdot\bar{k}_2\end{bmatrix}\oplus\begin{bmatrix} k_1 \\ \bar{k}_1\end{bmatrix}$	$k_1^*=k_1\oplus k_2$ $k_2^*=k_2$
6	$O_6^k=\begin{bmatrix} x_1\cdot(\overline{k_1\oplus k_2})\oplus x_2\cdot(k_1\oplus k_2) \\ x_1\cdot(k_1\oplus k_2)\oplus x_2\cdot(\overline{k_1\oplus k_2})\end{bmatrix}\oplus\begin{bmatrix} k_2 \\ \bar{k}_2\end{bmatrix}$	$O_6^k=\begin{bmatrix} x_1\cdot(\overline{k_1\oplus k_2})\oplus x_2\cdot(k_1\oplus k_2) \\ x_1\cdot(k_1\oplus k_2)\oplus x_2\cdot(\overline{k_1\oplus k_2})\end{bmatrix}\oplus\begin{bmatrix} k_1 \\ \bar{k}_1\end{bmatrix}$	$k_1^*=k_2$ $k_2^*=k_1$
7	$O_7^k=\begin{bmatrix} x_1\cdot\bar{k}_1\oplus x_2\cdot k_1 \\ x_1\cdot k_1\oplus x_2\cdot\bar{k}_1\end{bmatrix}\oplus\begin{bmatrix} \overline{k_1\oplus k_2} \\ k_1\oplus k_2\end{bmatrix}$	$O_7^d=\begin{bmatrix} x_1\cdot\bar{k}_1\oplus x_2\cdot k_1 \\ x_1\cdot k_1\oplus x_2\cdot\bar{k}_1\end{bmatrix}\oplus\begin{bmatrix} \bar{k}_2 \\ k_2\end{bmatrix}$	$k_1^*=k_1$ $k_2^*=k_1\oplus k_2$
8	$O_8^k=\begin{bmatrix} x_1\cdot\bar{k}_1\oplus x_2\cdot k_1 \\ x_1\cdot k_1\oplus x_2\cdot\bar{k}_1\end{bmatrix}\oplus\begin{bmatrix} \bar{k}_2 \\ k_2\end{bmatrix}$	$O_8^d=\begin{bmatrix} x_1\cdot\bar{k}_1\oplus x_2\cdot k_1 \\ x_1\cdot k_1\oplus x_2\cdot\bar{k}_1\end{bmatrix}\oplus\begin{bmatrix} \overline{k_1\oplus k_2} \\ k_1\oplus k_2\end{bmatrix}$	$k_1^*=k_1$ $k_2^*=k_1\oplus k_2$

Продовження таблиці 2.5

1	2	3	4
9	$O_9^k = \begin{bmatrix} x_1 \cdot (\overline{k_1 \oplus k_2}) \oplus x_2 \cdot (k_1 \oplus k_2) \\ x_1 \cdot (k_1 \oplus k_2) \oplus x_2 \cdot (\overline{k_1 \oplus k_2}) \end{bmatrix} \oplus \begin{bmatrix} \bar{k}_2 \\ k_2 \end{bmatrix}$	$O_9^d = \begin{bmatrix} x_1 \cdot (\overline{k_1 \oplus k_2}) \oplus x_2 \cdot (k_1 \oplus k_2) \\ x_1 \cdot (k_1 \oplus k_2) \oplus x_2 \cdot (\overline{k_1 \oplus k_2}) \end{bmatrix} \oplus \begin{bmatrix} \bar{k}_1 \\ k_1 \end{bmatrix}$	$k_1^* = k_2$ $k_2^* = k_1$
10	$O_{10}^k = \begin{bmatrix} x_1 \cdot \bar{k}_2 \oplus x_2 \cdot k_2 \\ x_1 \cdot k_2 \oplus x_2 \cdot \bar{k}_2 \end{bmatrix} \oplus \begin{bmatrix} \bar{k}_2 \\ k_2 \end{bmatrix}$	$O_{10}^d = \begin{bmatrix} x_1 \cdot \bar{k}_2 \oplus x_2 \cdot k_2 \\ x_1 \cdot k_2 \oplus x_2 \cdot \bar{k}_2 \end{bmatrix} \oplus \begin{bmatrix} \bar{k}_1 \\ k_1 \end{bmatrix}$	$k_1^* = k_1 \oplus k_2$ $k_2^* = k_2$
11	$O_{11}^k = \begin{bmatrix} x_1 \cdot \bar{k}_2 \oplus x_2 \cdot k_2 \\ x_1 \cdot k_2 \oplus x_2 \cdot \bar{k}_2 \end{bmatrix} \oplus \begin{bmatrix} \bar{k}_1 \\ k_1 \end{bmatrix}$	$O_{11}^d = \begin{bmatrix} x_1 \cdot \bar{k}_2 \oplus x_2 \cdot k_2 \\ x_1 \cdot k_2 \oplus x_2 \cdot \bar{k}_2 \end{bmatrix} \oplus \begin{bmatrix} \bar{k}_2 \\ k_2 \end{bmatrix}$	$k_1^* = k_1 \oplus k_2$ $k_2^* = k_2$
12	$O_{12}^k = \begin{bmatrix} x_1 \cdot (\overline{k_1 \oplus k_2}) \oplus x_2 \cdot (k_1 \oplus k_2) \\ x_1 \cdot (k_1 \oplus k_2) \oplus x_2 \cdot (\overline{k_1 \oplus k_2}) \end{bmatrix} \oplus \begin{bmatrix} \bar{k}_1 \\ k_1 \end{bmatrix}$	$O_{12}^d = \begin{bmatrix} x_1 \cdot (\overline{k_1 \oplus k_2}) \oplus x_2 \cdot (k_1 \oplus k_2) \\ x_1 \cdot (k_1 \oplus k_2) \oplus x_2 \cdot (\overline{k_1 \oplus k_2}) \end{bmatrix} \oplus \begin{bmatrix} \bar{k}_2 \\ k_2 \end{bmatrix}$	$k_1^* = k_2$ $k_2^* = k_1$
13	$O_{13}^k = \begin{bmatrix} x_1 \cdot (k_1 \oplus k_2) \oplus x_2 \cdot (\overline{k_1 \oplus k_2}) \\ x_1 \cdot (\overline{k_1 \oplus k_2}) \oplus x_2 \cdot (k_1 \oplus k_2) \end{bmatrix} \oplus \begin{bmatrix} k_2 \\ \bar{k}_2 \end{bmatrix}$	$O_{13}^d = \begin{bmatrix} x_1 \cdot (k_1 \oplus k_2) \oplus x_2 \cdot (\overline{k_1 \oplus k_2}) \\ x_1 \cdot (\overline{k_1 \oplus k_2}) \oplus x_2 \cdot (k_1 \oplus k_2) \end{bmatrix} \oplus \begin{bmatrix} \bar{k}_1 \\ k_1 \end{bmatrix}$	$k_1^* = \bar{k}_2$ $k_2^* = \bar{k}_1$
14	$O_{14}^k = \begin{bmatrix} x_1 \cdot k_2 \oplus x_2 \cdot \bar{k}_2 \\ x_1 \cdot \bar{k}_2 \oplus x_2 \cdot k_2 \end{bmatrix} \oplus \begin{bmatrix} k_2 \\ \bar{k}_2 \end{bmatrix}$	$O_{14}^d = \begin{bmatrix} x_1 \cdot k_2 \oplus x_2 \cdot \bar{k}_2 \\ x_1 \cdot \bar{k}_2 \oplus x_2 \cdot k_2 \end{bmatrix} \oplus \begin{bmatrix} k_1 \\ \bar{k}_1 \end{bmatrix}$	$k_1^* = \overline{k_1 \oplus k_2}$ $k_2^* = k_2$
15	$O_{15}^k = \begin{bmatrix} x_1 \cdot k_2 \oplus x_2 \cdot \bar{k}_2 \\ x_1 \cdot \bar{k}_2 \oplus x_2 \cdot k_2 \end{bmatrix} \oplus \begin{bmatrix} k_1 \\ \bar{k}_1 \end{bmatrix}$	$O_{15}^d = \begin{bmatrix} x_1 \cdot k_2 \oplus x_2 \cdot \bar{k}_2 \\ x_1 \cdot \bar{k}_2 \oplus x_2 \cdot k_2 \end{bmatrix} \oplus \begin{bmatrix} \overline{k_1 \oplus k_2} \\ k_1 \oplus k_2 \end{bmatrix}$	$k_1^* = \overline{k_1 \oplus k_2}$ $k_2^* = k_2$
16	$O_{16}^k = \begin{bmatrix} x_1 \cdot (k_1 \oplus k_2) \oplus x_2 \cdot (\overline{k_1 \oplus k_2}) \\ x_1 \cdot (\overline{k_1 \oplus k_2}) \oplus x_2 \cdot (k_1 \oplus k_2) \end{bmatrix} \oplus \begin{bmatrix} k_1 \\ \bar{k}_1 \end{bmatrix}$	$O_{16}^d = \begin{bmatrix} x_1 \cdot (k_1 \oplus k_2) \oplus x_2 \cdot (\overline{k_1 \oplus k_2}) \\ x_1 \cdot (\overline{k_1 \oplus k_2}) \oplus x_2 \cdot (k_1 \oplus k_2) \end{bmatrix} \oplus \begin{bmatrix} \bar{k}_2 \\ k_2 \end{bmatrix}$	$k_1^* = \bar{k}_2$ $k_2^* = \bar{k}_1$
17	$O_{17}^k = \begin{bmatrix} x_1 \cdot k_1 \oplus x_2 \cdot \bar{k}_1 \\ x_1 \cdot \bar{k}_1 \oplus x_2 \cdot k_1 \end{bmatrix} \oplus \begin{bmatrix} k_1 \oplus k_2 \\ \overline{k_1 \oplus k_2} \end{bmatrix}$	$O_{17}^d = \begin{bmatrix} x_1 \cdot k_1 \oplus x_2 \cdot \bar{k}_1 \\ x_1 \cdot \bar{k}_1 \oplus x_2 \cdot k_1 \end{bmatrix} \oplus \begin{bmatrix} \bar{k}_2 \\ k_2 \end{bmatrix}$	$k_1^* = k_1$ $k_2^* = \overline{k_1 \oplus k_2}$
18	$O_{18}^k = \begin{bmatrix} x_1 \cdot k_1 \oplus x_2 \cdot \bar{k}_1 \\ x_1 \cdot \bar{k}_1 \oplus x_2 \cdot k_1 \end{bmatrix} \oplus \begin{bmatrix} k_2 \\ \bar{k}_2 \end{bmatrix}$	$O_{18}^d = \begin{bmatrix} x_1 \cdot k_1 \oplus x_2 \cdot \bar{k}_1 \\ x_1 \cdot \bar{k}_1 \oplus x_2 \cdot k_1 \end{bmatrix} \oplus \begin{bmatrix} \overline{k_1 \oplus k_2} \\ k_1 \oplus k_2 \end{bmatrix}$	$k_1^* = k_1$ $k_2^* = \overline{k_1 \oplus k_2}$
19	$O_{19}^k = \begin{bmatrix} x_1 \cdot \bar{k}_2 \oplus x_2 \cdot k_2 \\ x_1 \cdot k_2 \oplus x_2 \cdot \bar{k}_2 \end{bmatrix} \oplus \begin{bmatrix} k_1 \\ \bar{k}_1 \end{bmatrix}$	$O_{19}^d = \begin{bmatrix} x_1 \cdot \bar{k}_2 \oplus x_2 \cdot k_2 \\ x_1 \cdot k_2 \oplus x_2 \cdot \bar{k}_2 \end{bmatrix} \oplus \begin{bmatrix} k_2 \\ \bar{k}_2 \end{bmatrix}$	$k_1^* = \overline{k_1 \oplus k_2}$ $k_2^* = k_2$
20	$O_{20}^k = \begin{bmatrix} x_1 \cdot (k_1 \oplus k_2) \oplus x_2 \cdot (\overline{k_1 \oplus k_2}) \\ x_1 \cdot (\overline{k_1 \oplus k_2}) \oplus x_2 \cdot (k_1 \oplus k_2) \end{bmatrix} \oplus \begin{bmatrix} \bar{k}_1 \\ k_1 \end{bmatrix}$	$O_{20}^d = \begin{bmatrix} x_1 \cdot (k_1 \oplus k_2) \oplus x_2 \cdot (\overline{k_1 \oplus k_2}) \\ x_1 \cdot (\overline{k_1 \oplus k_2}) \oplus x_2 \cdot (k_1 \oplus k_2) \end{bmatrix} \oplus \begin{bmatrix} k_2 \\ \bar{k}_2 \end{bmatrix}$	$k_1^* = \bar{k}_2$ $k_2^* = \bar{k}_1$
21	$O_{21}^k = \begin{bmatrix} x_1 \cdot k_1 \oplus x_2 \cdot \bar{k}_1 \\ x_1 \cdot \bar{k}_1 \oplus x_2 \cdot k_1 \end{bmatrix} \oplus \begin{bmatrix} \overline{k_1 \oplus k_2} \\ k_1 \oplus k_2 \end{bmatrix}$	$O_{21}^d = \begin{bmatrix} x_1 \cdot k_1 \oplus x_2 \cdot \bar{k}_1 \\ x_1 \cdot \bar{k}_1 \oplus x_2 \cdot k_1 \end{bmatrix} \oplus \begin{bmatrix} k_2 \\ \bar{k}_2 \end{bmatrix}$	$k_1^* = k_1$ $k_2^* = \overline{k_1 \oplus k_2}$
22	$O_{22}^k = \begin{bmatrix} x_1 \cdot k_1 \oplus x_2 \cdot \bar{k}_1 \\ x_1 \cdot \bar{k}_1 \oplus x_2 \cdot k_1 \end{bmatrix} \oplus \begin{bmatrix} \bar{k}_2 \\ k_2 \end{bmatrix}$	$O_{22}^d = \begin{bmatrix} x_1 \cdot k_1 \oplus x_2 \cdot \bar{k}_1 \\ x_1 \cdot \bar{k}_1 \oplus x_2 \cdot k_1 \end{bmatrix} \oplus \begin{bmatrix} k_1 \oplus k_2 \\ \overline{k_1 \oplus k_2} \end{bmatrix}$	$k_1^* = k_1$ $k_2^* = \overline{k_1 \oplus k_2}$
23	$O_{23}^k = \begin{bmatrix} x_1 \cdot (k_1 \oplus k_2) \oplus x_2 \cdot (\overline{k_1 \oplus k_2}) \\ x_1 \cdot (\overline{k_1 \oplus k_2}) \oplus x_2 \cdot (k_1 \oplus k_2) \end{bmatrix} \oplus \begin{bmatrix} \bar{k}_2 \\ k_2 \end{bmatrix}$	$O_{23}^d = \begin{bmatrix} x_1 \cdot (k_1 \oplus k_2) \oplus x_2 \cdot (\overline{k_1 \oplus k_2}) \\ x_1 \cdot (\overline{k_1 \oplus k_2}) \oplus x_2 \cdot (k_1 \oplus k_2) \end{bmatrix} \oplus \begin{bmatrix} k_1 \\ \bar{k}_1 \end{bmatrix}$	$k_1^* = \bar{k}_2$ $k_2^* = \bar{k}_1$
24	$O_{24}^k = \begin{bmatrix} x_1 \cdot k_2 \oplus x_2 \cdot \bar{k}_2 \\ x_1 \cdot \bar{k}_2 \oplus x_2 \cdot k_2 \end{bmatrix} \oplus \begin{bmatrix} \overline{k_1 \oplus k_2} \\ k_1 \oplus k_2 \end{bmatrix}$	$O_{24}^d = \begin{bmatrix} x_1 \cdot k_2 \oplus x_2 \cdot \bar{k}_2 \\ x_1 \cdot \bar{k}_2 \oplus x_2 \cdot k_2 \end{bmatrix} \oplus \begin{bmatrix} k_1 \\ \bar{k}_1 \end{bmatrix}$	$k_1^* = \overline{k_1 \oplus k_2}$ $k_2^* = k_2$

Додатковий аналіз табл.2.5 показав, що деякі моделі автоматів побудови другого операнду оберненої операції повторюються. Проведемо узагальнення отриманих результатів синтезу обернених двохрозрядних двохоперандних операцій строгого стійкого криптоперетворення з урахуванням встановленого факту. Отримані результати додаткового дослідження наведені в табл. 2.6 [3].

Таблиця 2.6

Узагальнені результати синтезу операцій на основі встановлених взаємозв'язків

Пряма операція криптоперетворення	**Обернена операція криптоперетворення**	**Модель автомата побудови другого операнду оберненої операції**
1	**2**	**3**
$O_1^k=\begin{bmatrix} x_1\cdot\bar{k}_1\oplus x_2\cdot k_1 \\ x_1\cdot k_1\oplus x_2\cdot\bar{k}_1\end{bmatrix}\oplus\begin{bmatrix} k_2 \\ \bar{k}_2\end{bmatrix}$	$O_2^k=\begin{bmatrix} x_1\cdot\bar{k}_1\oplus x_2\cdot k_1 \\ x_1\cdot k_1\oplus x_2\cdot\bar{k}_1\end{bmatrix}\oplus\begin{bmatrix} k_1\oplus k_2 \\ \overline{k_1\oplus k_2}\end{bmatrix}$	$k_1^*=k_1,$ $k_2^*=k_1\oplus k_2$
$O_8^k=\begin{bmatrix} x_1\cdot\bar{k}_1\oplus x_2\cdot k_1 \\ x_1\cdot k_1\oplus x_2\cdot\bar{k}_1\end{bmatrix}\oplus\begin{bmatrix} \bar{k}_2 \\ k_2\end{bmatrix}$	$O_7^k=\begin{bmatrix} x_1\cdot\bar{k}_1\oplus x_2\cdot k_1 \\ x_1\cdot k_1\oplus x_2\cdot\bar{k}_1\end{bmatrix}\oplus\begin{bmatrix} \overline{k_1\oplus k_2} \\ k_1\oplus k_2\end{bmatrix}$	
$O_3^k=\begin{bmatrix} x_1\cdot(\overline{k_1\oplus k_2})\oplus x_2\cdot(k_1\oplus k_2) \\ x_1\cdot(k_1\oplus k_2)\oplus x_2\cdot(\overline{k_1\oplus k_2})\end{bmatrix}\oplus\begin{bmatrix} k_1 \\ \bar{k}_1\end{bmatrix}$	$O_6^k=\begin{bmatrix} x_1\cdot(\overline{k_1\oplus k_2})\oplus x_2\cdot(k_1\oplus k_2) \\ x_1\cdot(k_1\oplus k_2)\oplus x_2\cdot(\overline{k_1\oplus k_2})\end{bmatrix}\oplus\begin{bmatrix} k_2 \\ \bar{k}_2\end{bmatrix}$	$k_1^*=k_2,$ $k_2^*=k_1$
$O_{12}^k=\begin{bmatrix} x_1\cdot(\overline{k_1\oplus k_2})\oplus x_2\cdot(k_1\oplus k_2) \\ x_1\cdot(k_1\oplus k_2)\oplus x_2\cdot(\overline{k_1\oplus k_2})\end{bmatrix}\oplus\begin{bmatrix} \bar{k}_1 \\ k_1\end{bmatrix}$	$O_9^k=\begin{bmatrix} x_1\cdot(\overline{k_1\oplus k_2})\oplus x_2\cdot(k_1\oplus k_2) \\ x_1\cdot(k_1\oplus k_2)\oplus x_2\cdot(\overline{k_1\oplus k_2})\end{bmatrix}\oplus\begin{bmatrix} \bar{k}_2 \\ k_2\end{bmatrix}$	
$O_4^k=\begin{bmatrix} x_1\cdot\bar{k}_2\oplus x_2\cdot k_2 \\ x_1\cdot k_2\oplus x_2\cdot\bar{k}_2\end{bmatrix}\oplus\begin{bmatrix} k_1 \\ \bar{k}_1\end{bmatrix}$	$O_5^k=\begin{bmatrix} x_1\cdot\bar{k}_2\oplus x_2\cdot k_2 \\ x_1\cdot k_2\oplus x_2\cdot\bar{k}_2\end{bmatrix}\oplus\begin{bmatrix} k_1\oplus k_2 \\ \overline{k_1\oplus k_2}\end{bmatrix}$	$k_1^*=\overline{k_1\oplus k_2}$ $k_2^*=k_2$
$O_{15}^k=\begin{bmatrix} x_1\cdot k_2\oplus x_2\cdot\bar{k}_2 \\ x_1\cdot\bar{k}_2\oplus x_2\cdot k_2\end{bmatrix}\oplus\begin{bmatrix} k_1 \\ \bar{k}_1\end{bmatrix}$	$O_{24}^k=\begin{bmatrix} x_1\cdot k_2\oplus x_2\cdot\bar{k}_2 \\ x_1\cdot\bar{k}_2\oplus x_2\cdot k_2\end{bmatrix}\oplus\begin{bmatrix} \overline{k_1\oplus k_2} \\ k_1\oplus k_2\end{bmatrix}$	

Продовження таблиці 2.6

1	2	3
$O_{14}^k = \begin{bmatrix} x_1 \cdot k_2 \oplus x_2 \cdot \bar{k}_2 \\ x_1 \cdot \bar{k}_2 \oplus x_2 \cdot k_2 \end{bmatrix} \oplus \begin{bmatrix} k_2 \\ \bar{k}_2 \end{bmatrix}$	$O_{19}^k = \begin{bmatrix} x_1 \cdot \bar{k}_2 \oplus x_2 \cdot k_2 \\ x_1 \cdot k_2 \oplus x_2 \cdot \bar{k}_2 \end{bmatrix} \oplus \begin{bmatrix} k_1 \\ \bar{k}_1 \end{bmatrix}$	$k_1^* = k_1 \oplus k_2$ $k_2^* = k_2$
$O_{10}^k = \begin{bmatrix} x_1 \cdot \bar{k}_2 \oplus x_2 \cdot k_2 \\ x_1 \cdot k_2 \oplus x_2 \cdot \bar{k}_2 \end{bmatrix} \oplus \begin{bmatrix} \bar{k}_2 \\ k_2 \end{bmatrix}$	$O_{11}^k = \begin{bmatrix} x_1 \cdot \bar{k}_2 \oplus x_2 \cdot k_2 \\ x_1 \cdot k_2 \oplus x_2 \cdot \bar{k}_2 \end{bmatrix} \oplus \begin{bmatrix} \bar{k}_1 \\ k_1 \end{bmatrix}$	
$O_{16}^k = \begin{bmatrix} x_1 \cdot (k_1 \oplus k_2) \oplus x_2 \cdot \overline{(k_1 \oplus k_2)} \\ x_1 \cdot \overline{(k_1 \oplus k_2)} \oplus x_2 \cdot (k_1 \oplus k_2) \end{bmatrix} \oplus \begin{bmatrix} k_1 \\ \bar{k}_1 \end{bmatrix}$	$O_{23}^k = \begin{bmatrix} x_1 \cdot (k_1 \oplus k_2) \oplus x_2 \cdot \overline{(k_1 \oplus k_2)} \\ x_1 \cdot \overline{(k_1 \oplus k_2)} \oplus x_2 \cdot (k_1 \oplus k_2) \end{bmatrix} \oplus \begin{bmatrix} \bar{k}_2 \\ k_2 \end{bmatrix}$	$k_1^* = \bar{k}_2$ $k_2^* = \bar{k}_1$
$O_{20}^k = \begin{bmatrix} x_1 \cdot (k_1 \oplus k_2) \oplus x_2 \cdot \overline{(k_1 \oplus k_2)} \\ x_1 \cdot \overline{(k_1 \oplus k_2)} \oplus x_2 \cdot (k_1 \oplus k_2) \end{bmatrix} \oplus \begin{bmatrix} \bar{k}_1 \\ k_1 \end{bmatrix}$	$O_{13}^k = \begin{bmatrix} x_1 \cdot (k_1 \oplus k_2) \oplus x_2 \cdot \overline{(k_1 \oplus k_2)} \\ x_1 \cdot \overline{(k_1 \oplus k_2)} \oplus x_2 \cdot (k_1 \oplus k_2) \end{bmatrix} \oplus \begin{bmatrix} k_2 \\ \bar{k}_2 \end{bmatrix}$	
$O_{18}^k = \begin{bmatrix} x_1 \cdot k_1 \oplus x_2 \cdot \bar{k}_1 \\ x_1 \cdot \bar{k}_1 \oplus x_2 \cdot k_1 \end{bmatrix} \oplus \begin{bmatrix} k_2 \\ \bar{k}_2 \end{bmatrix}$	$O_{21}^k = \begin{bmatrix} x_1 \cdot k_1 \oplus x_2 \cdot \bar{k}_1 \\ x_1 \cdot \bar{k}_1 \oplus x_2 \cdot k_1 \end{bmatrix} \oplus \begin{bmatrix} \overline{k_1 \oplus k_2} \\ k_1 \oplus k_2 \end{bmatrix}$	$k_1^* = k_1$ $k_2^* = \overline{k_1 \oplus k_2}$
$O_{22}^k = \begin{bmatrix} x_1 \cdot k_1 \oplus x_2 \cdot \bar{k}_1 \\ x_1 \cdot \bar{k}_1 \oplus x_2 \cdot k_1 \end{bmatrix} \oplus \begin{bmatrix} \bar{k}_2 \\ k_2 \end{bmatrix}$	$O_{17}^k = \begin{bmatrix} x_1 \cdot k_1 \oplus x_2 \cdot \bar{k}_1 \\ x_1 \cdot \bar{k}_1 \oplus x_2 \cdot k_1 \end{bmatrix} \oplus \begin{bmatrix} k_1 \oplus k_2 \\ \overline{k_1 \oplus k_2} \end{bmatrix}$	

Наведена послідовність встановлення взаємозв'язків та математичних перетворень може розглядатися як розроблений метод синтезу обернених двохрозрядних двохоперандних операцій ССКК на основі перетворення другого операнда.

Виходячи з цього, метод синтезу двохрозрядних двохоперандних операцій ССКК, на основі перетворення другого операнда, полягає в наступному:

1. Побудувати групу математичних моделей двохрозрядних двохоперандних операцій ССКК.

2. Встановити відповідність в групі математичних моделей двохрозрядних двохоперандних операцій ССКК між прямими і оберненими операціями криптоперетворення.

3. На основі аналізу математичних моделей операцій прямого і оберненого криптоперетворення побудувати модель автомата побудови другого операнда оберненої операції.

4. На основі застосування моделі автомата побудови другого операнда оберненої операції, перетворити другий операнд заданої прямої операції

криптоперетворення, що забезпечить синтез обернених двохрозрядних двохоперандних операцій ССКК.

Алгоритм реалізації методу синтезу двохрозрядних двохоперандних операцій ССКК на основі перетворення другого операнда наведений на рис.2.1.

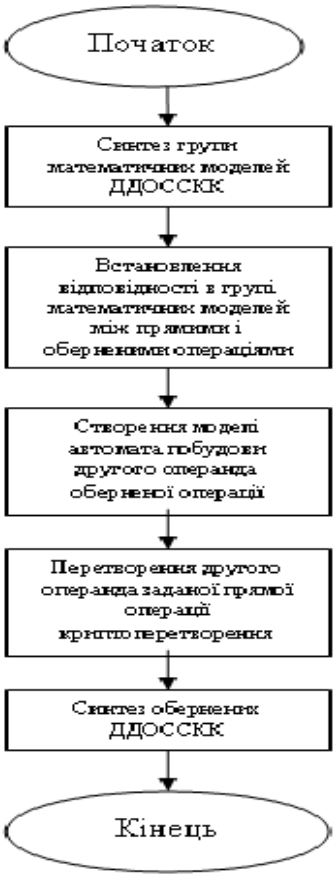


Рисунок 2.1. Блок-схема методу синтезу двохрозрядних двохоперандних операцій ССКК на основі перетворення другого операнда

Застосування оберненої двохрозрядної двохоперандної операції ССКК на основі перетворення другого операнда в методі підвищення стійкості і надійності потокового шифрування забезпечить створення нових якісних можливостей для розробників потокових шифрів.

Висновки з розділу 2

Вперше розроблено метод синтезу обернених двохрозрядних двохоперандних операцій ССКК на основі перетворення другого операнда, шляхом реалізації моделі автомата побудови другого операнда оберненої операції, що забезпечило можливість практичного застосування даних операцій.

1. Запропонована технологія дослідження взаємозв’язків між прямими і оберненими двохрозрядними двохоперандними операціями ССКК, яка забезпечує єдиний підхід для дослідження прямих та обернених операцій криптографічного перетворення інформації.

2. Досліджено і встановлено взаємозв’язки між прямими і оберненими операціями в групі двохрозрядних двохоперандних операцій ССКК.

3. На основі застосування запропонованої технології проведено синтез обернених двохрозрядних двохоперандних операцій ССКК, на основі встановлених взаємозв’язків.

4 Узагальнено результати дослідження взаємозв’язків між прямими та оберненими двохрозрядними двохоперандними операціями криптографічного кодування та сформульовано метод синтезу двохрозрядних двохоперандних операцій ССКК, на основі перетворення другого операнда.

5. Результати розділу опубліковано [3,4,6,8,10].

3 РОЗДІЛ

СИНТЕЗ ГРУПИ ДВОХРОЗРЯДНИХ ДВОХОПЕРАНДНИХ ОПЕРАЦІЙ СТРОГОГО СТІЙКОГО КРИПТОГРАФІЧНОГО КОДУВАННЯ НА ОСНОВІ ПЕРЕТВОРЕННЯ ДРУГОГО ОПЕРАНДА ВІДОМОЇ ОПЕРАЦІЇ

3.1 Синтез групи двохрозрядних двохоперандних операцій строгого стійкого криптографічного кодування на основі першої операції

Додатковий аналіз узагальнених результатів синтезу операцій на основі встановлених взаємозв'язків (табл.2.6) показав, що модель автомата побудови другого операнду оберненої операції, подібна до моделі групи двохрозрядних одноопераднних операцій криптографічного перетворення інформації [162]. Група двохрозрядних одноопераднних операцій криптографічного перетворення інформації наведена в табл. 3.1 [1,162].

Таблиця 3.1

Повна група двохрозрядних одноопераднних операцій криптографічного перетворення інформації

№ п/п	операція	№ п/п	операція	№ п/п	операція	№ п/п	операція
1	$F_{3,5}=\begin{bmatrix}x_1\\x_2\end{bmatrix}$	**7**	$F_{3,10}=\begin{bmatrix}x_1\\x_2\oplus 1\end{bmatrix}$	**13**	$F_{12,5}=\begin{bmatrix}x_1\oplus 1\\x_2\end{bmatrix}$	**19**	$F_{12,10}=\begin{bmatrix}x_1\oplus 1\\x_2\oplus 1\end{bmatrix}$
2	$F_{6,5}=\begin{bmatrix}x_1\oplus x_2\\x_2\end{bmatrix}$	**8**	$F_{6,10}=\begin{bmatrix}x_1\oplus x_2\\x_2\oplus 1\end{bmatrix}$	**14**	$F_{9,5}=\begin{bmatrix}x_1\oplus x_2\oplus 1\\x_2\end{bmatrix}$	**20**	$F_{9,10}=\begin{bmatrix}x_1\oplus x_2\oplus 1\\x_2\oplus 1\end{bmatrix}$
3	$F_{3,6}=\begin{bmatrix}x_1\\x_1\oplus x_2\end{bmatrix}$	**9**	$F_{3,9}=\begin{bmatrix}x_1\\x_1\oplus x_2\oplus 1\end{bmatrix}$	**15**	$F_{12,6}=\begin{bmatrix}x_1\oplus 1\\x_1\oplus x_2\end{bmatrix}$	**21**	$F_{12,9}=\begin{bmatrix}x_1\oplus 1\\x_1\oplus x_2\oplus 1\end{bmatrix}$
4	$F_{5,3}=\begin{bmatrix}x_2\\x_1\end{bmatrix}$	**10**	$F_{5,12}=\begin{bmatrix}x_2\\x_1\oplus 1\end{bmatrix}$	**16**	$F_{10,3}=\begin{bmatrix}x_2\oplus 1\\x_1\end{bmatrix}$	**22**	$F_{10,12}=\begin{bmatrix}x_2\oplus 1\\x_1\oplus 1\end{bmatrix}$
5	$F_{5,6}=\begin{bmatrix}x_2\\x_1\oplus x_2\end{bmatrix}$	**11**	$F_{5,9}=\begin{bmatrix}x_2\\x_1\oplus x_2\oplus 1\end{bmatrix}$	**17**	$F_{10,6}=\begin{bmatrix}x_2\oplus 1\\x_1\oplus x_2\end{bmatrix}$	**23**	$F_{10,9}=\begin{bmatrix}x_2\oplus 1\\x_1\oplus x_2\oplus 1\end{bmatrix}$
6	$F_{6,3}=\begin{bmatrix}x_1\oplus x_2\\x_1\end{bmatrix}$	**12**	$F_{6,12}=\begin{bmatrix}x_1\oplus x_2\\x_1\oplus 1\end{bmatrix}$	**18**	$F_{9,3}=\begin{bmatrix}x_1\oplus x_2\oplus 1\\x_1\end{bmatrix}$	**24**	$F_{9,12}=\begin{bmatrix}x_1\oplus x_2\oplus 1\\x_1\oplus 1\end{bmatrix}$

Так як наведені взаємозв'язки між прямими і оберненими операціями дозволяють синтезувати обернені операції, а кожна обернена операція, в свою чергу, є прямою операцією для іншої оберненої операції, то можна припустити що шляхом перетворення другого операнда одноопераднною операцією можливо синтезувати іншу операцію [9].

Перевіримо гіпотезу про те, що можна синтезувати ДДО ССКК на основі перетворення другого операнда.

Припустимо, що якщо над другим операндом двохопераднної операції строгого криптографічного кодування $O_1^k = \begin{bmatrix} x_1 \cdot \bar{k}_1 \oplus x_2 \cdot k_1 \\ x_1 \cdot k_1 \oplus x_2 \cdot \bar{k}_1 \end{bmatrix} \oplus \begin{bmatrix} k_2 \\ \bar{k}_2 \end{bmatrix}$ виконати одноопераднне криптографічне перетворення $F_{3,5} = \begin{bmatrix} x_1 \\ x_2 \end{bmatrix}$, то буде отримана операція строгого стійкого кодування $O_1^k = \begin{bmatrix} x_1 \cdot \bar{k}_1 \oplus x_2 \cdot k_1 \\ x_1 \cdot k_1 \oplus x_2 \cdot \bar{k}_1 \end{bmatrix} \oplus \begin{bmatrix} k_2 \\ \bar{k}_2 \end{bmatrix}$.

В результаті виконання даного перетворення отримуємо:

$$F_{3,5}(O_1^k) = \begin{cases} \begin{bmatrix} x_1 \\ x_2 \oplus 1 \end{bmatrix}, \text{ якщо } k_1 = 0; k_2 = 0 \\ \begin{bmatrix} x_1 \oplus 1 \\ x_2 \end{bmatrix}, \text{якщо } k_1 = 0; k_2 = 1 \\ \begin{bmatrix} x_2 \\ x_1 \oplus 1 \end{bmatrix}, \text{ якщо } k_1 = 1; k_2 = 0 \\ \begin{bmatrix} x_2 \oplus 1 \\ x_1 \end{bmatrix}, \text{якщо } k_1 = 1; k_2 = 1 \end{cases} = O_1^k = \begin{cases} \begin{bmatrix} x_1 \\ x_2 \oplus 1 \end{bmatrix}, \text{ якщо } k_1 = 0; k_2 = 0 \\ \begin{bmatrix} x_1 \oplus 1 \\ x_2 \end{bmatrix}, \text{якщо } k_1 = 0; k_2 = 1 \\ \begin{bmatrix} x_2 \\ x_1 \oplus 1 \end{bmatrix}, \text{ якщо } k_1 = 1; k_2 = 0 \\ \begin{bmatrix} x_2 \oplus 1 \\ x_1 \end{bmatrix}, \text{якщо } k_1 = 1; k_2 = 1 \end{cases} = O_1^k = \begin{bmatrix} x_1 \cdot \bar{k}_1 \oplus x_2 \cdot k_1 \\ x_1 \cdot k_1 \oplus x_2 \cdot \bar{k}_1 \end{bmatrix} \oplus \begin{bmatrix} k_2 \\ \bar{k}_2 \end{bmatrix} \quad (3.1).$$

Саме це й доводить, що шляхом перетворення другого операнда одноопераднною операцією можливо синтезувати іншу операцію [7].

За умови, що у випадку виконання над другим операндом двохопераднної операції строгого криптографічного кодування $O_1^k = \begin{bmatrix} x_1 \cdot \bar{k}_1 \oplus x_2 \cdot k_1 \\ x_1 \cdot k_1 \oplus x_2 \cdot \bar{k}_1 \end{bmatrix} \oplus \begin{bmatrix} k_2 \\ \bar{k}_2 \end{bmatrix}$ одноопераднне криптографічне перетворення $F_{6,5} = \begin{bmatrix} x_1 \oplus x_2 \\ x_2 \end{bmatrix}$, буде отримана операція строгого стійкого кодування $O_6^k = \begin{bmatrix} x_1 \cdot (\overline{k_1 \oplus k_2}) \oplus x_2 \cdot (k_1 \oplus k_2) \\ x_1 \cdot (k_1 \oplus k_2) \oplus x_2 \cdot (\overline{k_1 \oplus k_2}) \end{bmatrix} \oplus \begin{bmatrix} k_2 \\ \bar{k}_2 \end{bmatrix}$.

Таким чином отримуємо:

$$F_{6,5}(O_1^k)=\begin{cases}\begin{bmatrix}x_1\\ x_2\oplus 1\end{bmatrix}, \text{ якщо } k_1=0; k_2=0\\ \begin{bmatrix}x_2\oplus 1\\ x_1\end{bmatrix}, \text{якщо } k_1=1; k_2=1\\ \begin{bmatrix}x_2\\ x_1\oplus 1\end{bmatrix}, \text{ якщо } k_1=1; k_2=0\\ \begin{bmatrix}x_1\oplus 1\\ x_2\end{bmatrix}, \text{якщо } k_1=0; k_2=1\end{cases}=O_6^k=\begin{cases}\begin{bmatrix}x_1\\ x_2\oplus 1\end{bmatrix}, \text{ якщо } k_1=0; k_2=0\\ \begin{bmatrix}x_2\oplus 1\\ x_1\end{bmatrix}, \text{якщо } k_1=0; k_2=1\\ \begin{bmatrix}x_2\\ x_1\oplus 1\end{bmatrix}, \text{ якщо } k_1=1; k_2=0\\ \begin{bmatrix}x_1\oplus 1\\ x_2\end{bmatrix}, \text{якщо } k_1=1; k_2=1\end{cases}=O_6^k=\begin{bmatrix}x_1\cdot(\overline{k_1\oplus k_2})\oplus x_2\cdot(k_1\oplus k_2)\\ x_1\cdot(k_1\oplus k_2)\oplus x_2\cdot\overline{(k_1\oplus k_2)}\end{bmatrix}\oplus\begin{bmatrix}k_2\\ \bar{k}_2\end{bmatrix} \quad (3.2)$$

що й необхідно було довести.

У випадку виконання над другим операндом двохоперандної операції строгого криптографічного кодування $O_1^k=\begin{bmatrix}x_1\cdot\bar{k}_1\oplus x_2\cdot k_1\\ x_1\cdot k_1\oplus x_2\cdot\bar{k}_1\end{bmatrix}\oplus\begin{bmatrix}k_2\\ \bar{k}_2\end{bmatrix}$ одноопераднe криптографічне перетворення $F_{3,6}=\begin{bmatrix}x_1\\ x_1\oplus x_2\end{bmatrix}$, буде отримано операцію ССКК $O_2^k=\begin{bmatrix}x_1\cdot\bar{k}_1\oplus x_2\cdot k_1\\ x_1\cdot k_1\oplus x_2\cdot\bar{k}_1\end{bmatrix}\oplus\begin{bmatrix}k_1\oplus k_2\\ \overline{k_1\oplus k_2}\end{bmatrix}$.

Таким чином перетворення матиме наступний вигляд:

$$F_{3,6}(O_1^k)=\begin{cases}\begin{bmatrix}x_1\\ x_2\oplus 1\end{bmatrix}, \text{ якщо } k_1=0; k_2=0\\ \begin{bmatrix}x_1\oplus 1\\ x_2\end{bmatrix}, \text{якщо } k_1=0; k_2=1\\ \begin{bmatrix}x_2\oplus 1\\ x_1\end{bmatrix}, \text{ якщо } k_1=1; k_2=1\\ \begin{bmatrix}x_2\\ x_1\oplus 1\end{bmatrix}, \text{якщо } k_1=1; k_2=0\end{cases}=O_2^k=\begin{cases}\begin{bmatrix}x_1\\ x_2\oplus 1\end{bmatrix}, \text{ якщо } k_1=0; k_2=0\\ \begin{bmatrix}x_1\oplus 1\\ x_2\end{bmatrix}, \text{якщо } k_1=0; k_2=1\\ \begin{bmatrix}x_2\oplus 1\\ x_1\end{bmatrix}, \text{ якщо } k_1=1; k_2=0\\ \begin{bmatrix}x_2\\ x_1\oplus 1\end{bmatrix}, \text{якщо } k_1=1; k_2=1\end{cases}=O_2^k=\begin{bmatrix}x_1\cdot\bar{k}_1\oplus x_2\cdot k_1\\ x_1\cdot k_1\oplus x_2\cdot\bar{k}_1\end{bmatrix}\oplus\begin{bmatrix}k_1\oplus k_2\\ \overline{k_1\oplus k_2}\end{bmatrix} \quad (3.3)$$

що й показує правильність нашого твердження.

Якщо ж над другим операндом двохоперандної операції строгого криптографічного кодування $O_1^k=\begin{bmatrix}x_1\cdot\bar{k}_1\oplus x_2\cdot k_1\\ x_1\cdot k_1\oplus x_2\cdot\bar{k}_1\end{bmatrix}\oplus\begin{bmatrix}k_2\\ \bar{k}_2\end{bmatrix}$ виконати одноопераднe криптографічне перетворення $F_{5,3}=\begin{bmatrix}x_2\\ x_1\end{bmatrix}$, то у даному випадку буде отримана операція строгого стійкого кодування $O_4^k=\begin{bmatrix}x_1\cdot\bar{k}_2\oplus x_2\cdot k_2\\ x_1\cdot k_2\oplus x_2\cdot\bar{k}_2\end{bmatrix}\oplus\begin{bmatrix}k_1\\ \bar{k}_1\end{bmatrix}$.

Тобто дане перетворення матиме наступний вигляд:

$$F_{5,3}(O_1^k)=\begin{cases}\begin{bmatrix}x_1\\ x_2\oplus 1\end{bmatrix}, \text{ якщо } k_1=0;\ k_2=0\\ \begin{bmatrix}x_2\\ x_1\oplus 1\end{bmatrix}, \text{ якщо } k_1=1;\ k_2=0\\ \begin{bmatrix}x_1\oplus 1\\ x_2\end{bmatrix}, \text{якщо } k_1=0;\ k_2=1\\ \begin{bmatrix}x_1\oplus 1\\ x_2\end{bmatrix}, \text{якщо } k_1=1;\ k_2=1\end{cases} = O_4^k = \begin{cases}\begin{bmatrix}x_1\\ x_2\oplus 1\end{bmatrix}, \text{ якщо } k_1=0;\ k_2=0\\ \begin{bmatrix}x_2\\ x_1\oplus 1\end{bmatrix}, \text{якщо } k_1=0;\ k_2=1\\ \begin{bmatrix}x_1\oplus 1\\ x_2\end{bmatrix}, \text{ якщо } k_1=1;\ k_2=0\\ \begin{bmatrix}x_2\oplus 1\\ x_1\end{bmatrix}, \text{якщо } k_1=1;\ k_2=1\end{cases} = O_4^k = \begin{bmatrix}x_1\cdot\bar{k}_2\oplus x_2\cdot k_2\\ x_1\cdot k_2\oplus x_2\cdot\bar{k}_2\end{bmatrix}\oplus\begin{bmatrix}k_1\\ \bar{k}_1\end{bmatrix} \quad (3.4)$$

і показує, що наше твердження правильне.

У випадку, коли над другим операндом двохоперандної операції строгого криптографічного кодування $O_1^k=\begin{bmatrix}x_1\cdot\bar{k}_1\oplus x_2\cdot k_1\\ x_1\cdot k_1\oplus x_2\cdot\bar{k}_1\end{bmatrix}\oplus\begin{bmatrix}k_2\\ \bar{k}_2\end{bmatrix}$ виконується одноопераднe криптографічне перетворення $F_{5,6}=\begin{bmatrix}x_2\\ x_1\oplus x_2\end{bmatrix}$, буде отримана операція строгого стійкого кодування $O_5^k=\begin{bmatrix}x_1\cdot\bar{k}_2\oplus x_2\cdot k_2\\ x_1\cdot k_2\oplus x_2\cdot\bar{k}_2\end{bmatrix}\oplus\begin{bmatrix}k_1\oplus k_2\\ \overline{k_1\oplus k_2}\end{bmatrix}$.

Так як перетворення виглядає наступним чином:

$$F_{5,6}(O_1^k)=\begin{cases}\begin{bmatrix}x_1\\ x_2\oplus 1\end{bmatrix}, \text{ якщо } k_1=0;\ k_2=0\\ \begin{bmatrix}x_2\oplus 1\\ x_1\end{bmatrix}, \text{якщо } k_1=1;\ k_2=1\\ \begin{bmatrix}x_1\oplus 1\\ x_2\end{bmatrix}, \text{якщо } k_1=0;\ k_2=1\\ \begin{bmatrix}x_2\\ x_1\oplus 1\end{bmatrix}, \text{ якщо } k_1=1;\ k_2=0\end{cases} = O_5^k = \begin{cases}\begin{bmatrix}x_1\\ x_2\oplus 1\end{bmatrix}, \text{ якщо } k_1=0;\ k_2=0\\ \begin{bmatrix}x_2\oplus 1\\ x_1\end{bmatrix}, \text{якщо } k_1=0;\ k_2=1\\ \begin{bmatrix}x_1\oplus 1\\ x_2\end{bmatrix}, \text{ якщо } k_1=1;\ k_2=0\\ \begin{bmatrix}x_2\\ x_1\oplus 1\end{bmatrix}, \text{якщо } k_1=1;\ k_2=1\end{cases} = O_5^k = \begin{bmatrix}x_1\cdot\bar{k}_2\oplus x_2\cdot k_2\\ x_1\cdot k_2\oplus x_2\cdot\bar{k}_2\end{bmatrix}\oplus\begin{bmatrix}k_1\oplus k_2\\ \overline{k_1\oplus k_2}\end{bmatrix} \quad (3.5)$$

це доводить вірність нашого твердження.

Взявши операцію $O_1^k=\begin{bmatrix}x_1\cdot\bar{k}_1\oplus x_2\cdot k_1\\ x_1\cdot k_1\oplus x_2\cdot\bar{k}_1\end{bmatrix}\oplus\begin{bmatrix}k_2\\ \bar{k}_2\end{bmatrix}$ та виконавши над її другим операндом одноопераднe криптографічне перетворення $F_{6,3}=\begin{bmatrix}x_1\oplus x_2\\ x_1\end{bmatrix}$, отримуємо операцію строгого стійкого кодування $O_3^k=\begin{bmatrix}x_1\cdot(\overline{k_1\oplus k_2})\oplus x_2\cdot(k_1\oplus k_2)\\ x_1\cdot(k_1\oplus k_2)\oplus x_2\cdot(\overline{k_1\oplus k_2})\end{bmatrix}\oplus\begin{bmatrix}k_1\\ \bar{k}_1\end{bmatrix}$.

Осільки перетворення має наступний вигляд:

$$F_{6,3}(O_1^k)=\begin{cases}\begin{bmatrix}x_1\\ x_2\oplus 1\end{bmatrix}, \text{ якщо } k_1=0;\ k_2=0\\ \begin{bmatrix}x_2\\ x_1\oplus 1\end{bmatrix}, \text{якщо } k_1=1;\ k_2=0\\ \begin{bmatrix}x_2\oplus 1\\ x_1\end{bmatrix}, \text{якщо } k_1=1;\ k_2=1\\ \begin{bmatrix}x_1\oplus 1\\ x_2\end{bmatrix}, \text{якщо } k_1=0;\ k_2=1\end{cases}=O_3^k=\begin{cases}\begin{bmatrix}x_1\\ x_2\oplus 1\end{bmatrix}, \text{ якщо } k_1=0;\ k_2=0\\ \begin{bmatrix}x_2\\ x_1\oplus 1\end{bmatrix}, \text{якщо } k_1=0;\ k_2=1\\ \begin{bmatrix}x_2\oplus 1\\ x_1\end{bmatrix}, \text{якщо } k_1=1;\ k_2=0\\ \begin{bmatrix}x_1\oplus 1\\ x_2\end{bmatrix}, \text{якщо } k_1=1;\ k_2=1\end{cases}=O_3^k=\begin{bmatrix}x_1\cdot(\overline{k_1\oplus k_2})\oplus x_2\cdot(k_1\oplus k_2)\\ x_1\cdot(k_1\oplus k_2)\oplus x_2\cdot(\overline{k_1\oplus k_2})\end{bmatrix}\oplus\begin{bmatrix}k_1\\ \bar{k}_1\end{bmatrix} \quad (3.6)$$

це доводить правильність нашого твердження.

При одноопераднодному криптографічному перетворенні $F_{3,10}=\begin{bmatrix}x_1\\ x_2\oplus 1\end{bmatrix}$ над другим операндом двохоперандної операції $O_1^k=\begin{bmatrix}x_1\cdot\bar{k}_1\oplus x_2\cdot k_1\\ x_1\cdot k_1\oplus x_2\cdot\bar{k}_1\end{bmatrix}\oplus\begin{bmatrix}k_2\\ \bar{k}_2\end{bmatrix}$, буде отримана операція строгого стійкого кодування $O_8^k=\begin{bmatrix}x_1\cdot\bar{k}_1\oplus x_2\cdot k_1\\ x_1\cdot k_1\oplus x_2\cdot\bar{k}_1\end{bmatrix}\oplus\begin{bmatrix}\bar{k}_2\\ k_2\end{bmatrix}$.

Це показує перетворення:

$$F_{3,10}(O_1^k)=\begin{cases}\begin{bmatrix}x_1\oplus 1\\ x_2\end{bmatrix}, \text{якщо } k_1=0;\ k_2=1\\ \begin{bmatrix}x_1\\ x_2\oplus 1\end{bmatrix}, \text{ якщо } k_1=0;\ k_2=0\\ \begin{bmatrix}x_2\oplus 1\\ x_1\end{bmatrix}, \text{якщо } k_1=1;\ k_2=1\\ \begin{bmatrix}x_2\\ x_1\oplus 1\end{bmatrix}, \text{ якщо } k_1=1;\ k_2=0\end{cases}=O_8^k=\begin{cases}\begin{bmatrix}x_1\oplus 1\\ x_2\end{bmatrix}, \text{ якщо } k_1=0;\ k_2=0\\ \begin{bmatrix}x_1\\ x_2\oplus 1\end{bmatrix}, \text{якщо } k_1=0;\ k_2=1\\ \begin{bmatrix}x_2\oplus 1\\ x_1\end{bmatrix}, \text{ якщо } k_1=1;\ k_2=0\\ \begin{bmatrix}x_2\\ x_1\oplus 1\end{bmatrix}, \text{якщо } k_1=1;\ k_2=1\end{cases}=O_8^k=\begin{bmatrix}x_1\cdot\bar{k}_1\oplus x_2\cdot k_1\\ x_1\cdot k_1\oplus x_2\cdot\bar{k}_1\end{bmatrix}\oplus\begin{bmatrix}\bar{k}_2\\ k_2\end{bmatrix} \quad (3.7)$$

яке доводить правильність нашого твердження.

Якщо над другим операндом двохоперандної операції строгого криптографічного кодування $O_1^k=\begin{bmatrix}x_1\cdot\bar{k}_1\oplus x_2\cdot k_1\\ x_1\cdot k_1\oplus x_2\cdot\bar{k}_1\end{bmatrix}\oplus\begin{bmatrix}k_2\\ \bar{k}_2\end{bmatrix}$ виконати одноопераднде криптографічне перетворення $F_{6,10}=\begin{bmatrix}x_1\oplus x_2\\ x_2\oplus 1\end{bmatrix}$, то буде отримана операція строгого стійкого кодування $O_9^k=\begin{bmatrix}x_1\cdot(\overline{k_1\oplus k_2})\oplus x_2\cdot(k_1\oplus k_2)\\ x_1\cdot(k_1\oplus k_2)\oplus x_2\cdot(\overline{k_1\oplus k_2})\end{bmatrix}\oplus\begin{bmatrix}\bar{k}_2\\ k_2\end{bmatrix}$.

Так як перетворення виглядає наступним чином:

$$F_{6,10}(O_1^k)=\begin{cases}\begin{bmatrix}x_1\oplus 1\\ x_2\end{bmatrix}, якщо\ k_1=0;\ k_2=1\\ \begin{bmatrix}x_2\\ x_1\oplus 1\end{bmatrix}, якщо\ k_1=1;\ k_2=0\\ \begin{bmatrix}x_2\oplus 1\\ x_1\end{bmatrix}, якщо\ k_1=1;\ k_2=1\\ \begin{bmatrix}x_1\\ x_2\oplus 1\end{bmatrix}, якщо\ k_1=0;\ k_2=0\end{cases}=O_9^k=\begin{cases}\begin{bmatrix}x_1\oplus 1\\ x_2\end{bmatrix}, якщо\ k_1=0;\ k_2=0\\ \begin{bmatrix}x_2\\ x_1\oplus 1\end{bmatrix}, якщо\ k_1=0;\ k_2=1\\ \begin{bmatrix}x_2\oplus 1\\ x_1\end{bmatrix}, якщо\ k_1=1;\ k_2=0\\ \begin{bmatrix}x_1\\ x_2\oplus 1\end{bmatrix}, якщо\ k_1=1;\ k_2=1\end{cases}=O_9^k=\begin{bmatrix}x_1\cdot(\overline{k_1\oplus k_2})\oplus x_2\cdot(k_1\oplus k_2)\\ x_1\cdot(k_1\oplus k_2)\oplus x_2\cdot(\overline{k_1\oplus k_2})\end{bmatrix}\oplus\begin{bmatrix}\bar{k}_2\\ k_2\end{bmatrix} \quad (3.8)$$

Це й доводить правильність результату.

Якщо над другим операндом двохоперандної операції строгого криптографічного кодування $O_1^k=\begin{bmatrix}x_1\cdot\bar{k}_1\oplus x_2\cdot k_1\\ x_1\cdot k_1\oplus x_2\cdot\bar{k}_1\end{bmatrix}\oplus\begin{bmatrix}k_2\\ \bar{k}_2\end{bmatrix}$ виконати одноопераднде криптографічне перетворення $F_{3,9}=\begin{bmatrix}x_1\\ x_1\oplus x_2\oplus 1\end{bmatrix}$ то буде отримана операція строгого стійкого кодування $O_7^k=\begin{bmatrix}x_1\cdot\bar{k}_1\oplus x_2\cdot k_1\\ x_1\cdot k_1\oplus x_2\cdot\bar{k}_1\end{bmatrix}\oplus\begin{bmatrix}\overline{k_1\oplus k_2}\\ k_1\oplus k_2\end{bmatrix}$.

Так як:

$$F_{3,9}(O_1^k)=\begin{cases}\begin{bmatrix}x_1\oplus 1\\ x_2\end{bmatrix}, якщо\ k_1=0;\ k_2=1\\ \begin{bmatrix}x_1\\ x_2\oplus 1\end{bmatrix}, якщо\ k_1=0;\ k_2=0\\ \begin{bmatrix}x_2\\ x_1\oplus 1\end{bmatrix}, якщо\ k_1=1;\ k_2=0\\ \begin{bmatrix}x_2\oplus 1\\ x_1\end{bmatrix}, якщо\ k_1=1;\ k_2=1\end{cases}=O_7^k=\begin{cases}\begin{bmatrix}x_1\oplus 1\\ x_2\end{bmatrix}, якщо\ k_1=0;\ k_2=0\\ \begin{bmatrix}x_2\\ x_1\oplus 1\end{bmatrix}, якщо\ k_1=0;\ k_2=1\\ \begin{bmatrix}x_2\oplus 1\\ x_1\end{bmatrix}, якщо\ k_1=1;\ k_2=0\\ \begin{bmatrix}x_1\\ x_2\oplus 1\end{bmatrix}, якщо\ k_1=1;\ k_2=1\end{cases}=O_7^k=\begin{bmatrix}x_1\cdot\bar{k}_1\oplus x_2\cdot k_1\\ x_1\cdot k_1\oplus x_2\cdot\bar{k}_1\end{bmatrix}\oplus\begin{bmatrix}\overline{k_1\oplus k_2}\\ k_1\oplus k_2\end{bmatrix} \quad (3.9)$$

результат перетворення є доведенням твердження.

Якщо над другим операндом двохоперандної операції строгого криптографічного кодування $O_1^k=\begin{bmatrix}x_1\cdot\bar{k}_1\oplus x_2\cdot k_1\\ x_1\cdot k_1\oplus x_2\cdot\bar{k}_1\end{bmatrix}\oplus\begin{bmatrix}k_2\\ \bar{k}_2\end{bmatrix}$ виконати одноопераднде криптографічне перетворення $F_{5,12}=\begin{bmatrix}x_2\\ x_1\oplus 1\end{bmatrix}$, результатом буде отримана операція строгого стійкого кодування $O_{11}^k=\begin{bmatrix}x_1\cdot\bar{k}_2\oplus x_2\cdot k_2\\ x_1\cdot k_2\oplus x_2\cdot\bar{k}_2\end{bmatrix}\oplus\begin{bmatrix}\bar{k}_1\\ k_1\end{bmatrix}$.

Так як перетворення представлене:

$$F_{5,12}(O_1^k)=\begin{cases}\begin{bmatrix}x_1\oplus 1\\ x_2\end{bmatrix}, якщо\ k_1=0;\ k_2=1\\ \begin{bmatrix}x_2\oplus 1\\ x_1\end{bmatrix}, якщо\ k_1=1;\ k_2=1\\ \begin{bmatrix}x_1\\ x_2\oplus 1\end{bmatrix}, якщо\ k_1=0;\ k_2=0\\ \begin{bmatrix}x_2\\ x_1\oplus 1\end{bmatrix}, якщо\ k_1=1;\ k_2=0\end{cases}=O_{11}^k=\begin{cases}\begin{bmatrix}x_1\oplus 1\\ x_2\end{bmatrix}, якщо\ k_1=0;\ k_2=0\\ \begin{bmatrix}x_2\oplus 1\\ x_1\end{bmatrix}, якщо\ k_1=0;\ k_2=1\\ \begin{bmatrix}x_1\\ x_2\oplus 1\end{bmatrix}, якщо\ k_1=1;\ k_2=0\\ \begin{bmatrix}x_2\\ x_1\oplus 1\end{bmatrix}, якщо\ k_1=1;\ k_2=1\end{cases}=O_{11}^k=\begin{bmatrix}x_1\cdot\bar{k}_2\oplus x_2\cdot k_2\\ x_1\cdot k_2\oplus x_2\cdot\bar{k}_2\end{bmatrix}\oplus\begin{bmatrix}\bar{k}_1\\ k_1\end{bmatrix} \quad (3.10)$$

це відповідає твердженню.

Наступним одноопераднім перетворенням над другим операндом двохопераднної операції строгого криптографічного кодування $O_1^k=\begin{bmatrix}x_1\cdot\bar{k}_1\oplus x_2\cdot k_1\\ x_1\cdot k_1\oplus x_2\cdot\bar{k}_1\end{bmatrix}\oplus\begin{bmatrix}k_2\\ \bar{k}_2\end{bmatrix}$ буде $F_{5,9}=\begin{bmatrix}x_2\\ x_1\oplus x_2\oplus 1\end{bmatrix}$, при виконані якого, результатом буде отримана операція строгого стійкого кодування $O_{10}^k=\begin{bmatrix}x_1\cdot\bar{k}_2\oplus x_2\cdot k_2\\ x_1\cdot k_2\oplus x_2\cdot\bar{k}_2\end{bmatrix}\oplus\begin{bmatrix}\bar{k}_2\\ k_2\end{bmatrix}$.

Так як це перетворення матиме наступний вигляд:

$$F_{5,9}(O_1^k)=\begin{cases}\begin{bmatrix}x_1\oplus 1\\ x_2\end{bmatrix}, якщо\ k_1=0;\ k_2=1\\ \begin{bmatrix}x_2\\ x_1\oplus 1\end{bmatrix}, якщо\ k_1=1;\ k_2=0\\ \begin{bmatrix}x_1\\ x_2\oplus 1\end{bmatrix}, якщо\ k_1=0;\ k_2=0\\ \begin{bmatrix}x_2\oplus 1\\ x_1\end{bmatrix}, якщо\ k_1=1;\ k_2=1\end{cases}=O_{10}^k=\begin{cases}\begin{bmatrix}x_1\oplus 1\\ x_2\end{bmatrix}, якщо\ k_1=0;\ k_2=0\\ \begin{bmatrix}x_2\\ x_1\oplus 1\end{bmatrix}, якщо\ k_1=0;\ k_2=1\\ \begin{bmatrix}x_1\\ x_2\oplus 1\end{bmatrix}, якщо\ k_1=1;\ k_2=0\\ \begin{bmatrix}x_2\oplus 1\\ x_1\end{bmatrix}, якщо\ k_1=1;\ k_2=1\end{cases}=O_{11}^k=\begin{bmatrix}x_1\cdot\bar{k}_2\oplus x_2\cdot k_2\\ x_1\cdot k_2\oplus x_2\cdot\bar{k}_2\end{bmatrix}\oplus\begin{bmatrix}\bar{k}_1\\ k_1\end{bmatrix} \quad (3.11)$$

Результатом є доведенням нашого твердження.

Якщо над другим операндом двохопераднної операції строгого криптографічного кодування $O_1^k=\begin{bmatrix}x_1\cdot\bar{k}_1\oplus x_2\cdot k_1\\ x_1\cdot k_1\oplus x_2\cdot\bar{k}_1\end{bmatrix}\oplus\begin{bmatrix}k_2\\ \bar{k}_2\end{bmatrix}$ виконати одноопераднe криптографічне перетворення $F_{6,12}=\begin{bmatrix}x_1\oplus x_2\\ x_1\oplus 1\end{bmatrix}$, буде отримана операція строгого стійкого кодування $O_{12}^k=\begin{bmatrix}x_1\cdot(\overline{k_1\oplus k_2})\oplus x_2\cdot(k_1\oplus k_2)\\ x_1\cdot(k_1\oplus k_2)\oplus x_2\cdot\overline{(k_1\oplus k_2)}\end{bmatrix}\oplus\begin{bmatrix}\bar{k}_1\\ k_1\end{bmatrix}$.

Дане перетворення матиме наступний вигляд:

$$F_{6,12}(O_1^k)=\begin{cases}\begin{bmatrix}x_1\oplus 1\\ x_2\end{bmatrix}, якщо\ k_1=0;\ k_2=1\\ \begin{bmatrix}x_2\oplus 1\\ x_1\end{bmatrix}, якщо\ k_1=1;\ k_2=1\\ \begin{bmatrix}x_2\\ x_1\oplus 1\end{bmatrix}, якщо\ k_1=1;\ k_2=0\\ \begin{bmatrix}x_1\\ x_2\oplus 1\end{bmatrix}, якщо\ k_1=0;\ k_2=0\end{cases}=O_{12}^k=\begin{cases}\begin{bmatrix}x_1\oplus 1\\ x_2\end{bmatrix}, якщо\ k_1=0;\ k_2=0\\ \begin{bmatrix}x_2\oplus 1\\ x_1\end{bmatrix}, якщо\ k_1=0;\ k_2=1\\ \begin{bmatrix}x_2\\ x_1\oplus 1\end{bmatrix}, якщо\ k_1=1;\ k_2=0\\ \begin{bmatrix}x_1\\ x_2\oplus 1\end{bmatrix}, якщо\ k_1=1;\ k_2=1\end{cases}=O_{12}^k=\begin{bmatrix}x_1\cdot(\overline{k_1\oplus k_2})\oplus x_2\cdot(k_1\oplus k_2)\\ x_1\cdot(k_1\oplus k_2)\oplus x_2\cdot(\overline{k_1\oplus k_2})\end{bmatrix}\oplus\begin{bmatrix}\bar{k}_1\\ k_1\end{bmatrix} \quad (3.12)$$

що, власне, і потрібно було довести.

При виконанні над другим операндом двохоперандної операції строгого криптографічного кодування $O_1^k=\begin{bmatrix}x_1\cdot\bar{k}_1\oplus x_2\cdot k_1\\ x_1\cdot k_1\oplus x_2\cdot\bar{k}_1\end{bmatrix}\oplus\begin{bmatrix}k_2\\ \bar{k}_2\end{bmatrix}$ одноопераднe криптографічне перетворення $F_{12,5}=\begin{bmatrix}x_1\oplus 1\\ x_2\end{bmatrix}$, то буде отримана операція строгого стійкого кодування $O_{18}^k=\begin{bmatrix}x_1\cdot k_1\oplus x_2\cdot\bar{k}_1\\ x_1\cdot\bar{k}_1\oplus x_2\cdot k_1\end{bmatrix}\oplus\begin{bmatrix}k_2\\ \bar{k}_2\end{bmatrix}$.

Так як:

$$F_{12,5}(O_1^k)=\begin{cases}\begin{bmatrix}x_1\oplus 1\\ x_2\end{bmatrix}, якщо\ k_1=0;\ k_2=1\\ \begin{bmatrix}x_2\oplus 1\\ x_1\end{bmatrix}, якщо\ k_1=1;\ k_2=1\\ \begin{bmatrix}x_1\\ x_2\oplus 1\end{bmatrix}, якщо\ k_1=0;\ k_2=0\\ \begin{bmatrix}x_2\\ x_1\oplus 1\end{bmatrix}, якщо\ k_1=1;\ k_2=0\end{cases}=O_{18}^k=\begin{cases}\begin{bmatrix}x_2\\ x_1\oplus 1\end{bmatrix}, якщо\ k_1=0;\ k_2=0\\ \begin{bmatrix}x_2\oplus 1\\ x_1\end{bmatrix}, якщо\ k_1=0;\ k_2=1\\ \begin{bmatrix}x_1\\ x_2\oplus 1\end{bmatrix}, якщо\ k_1=1;\ k_2=0\\ \begin{bmatrix}x_1\oplus 1\\ x_2\end{bmatrix}, якщо\ k_1=1;\ k_2=1\end{cases}=O_{18}^k=\begin{bmatrix}x_1\cdot k_1\oplus x_2\cdot\bar{k}_1\\ x_1\cdot\bar{k}_1\oplus x_2\cdot k_1\end{bmatrix}\oplus\begin{bmatrix}k_2\\ \bar{k}_2\end{bmatrix} \quad (3.13)$$

отже, доведення вірне.

По аналогії з попередніми, вже виконаними, перетвореннями, виконаємо над другим операндом двохоперандної операції строгого криптографічного кодування $O_1^k=\begin{bmatrix}x_1\cdot\bar{k}_1\oplus x_2\cdot k_1\\ x_1\cdot k_1\oplus x_2\cdot\bar{k}_1\end{bmatrix}\oplus\begin{bmatrix}k_2\\ \bar{k}_2\end{bmatrix}$, одноопераднe криптографічне перетворення $F_{9,5}=\begin{bmatrix}x_1\oplus x_2\oplus 1\\ x_2\end{bmatrix}$, при якій буде отримана операція строгого стійкого кодування $O_{13}^k=\begin{bmatrix}x_1\cdot(k_1\oplus k_2)\oplus x_2\cdot(\overline{k_1\oplus k_2})\\ x_1\cdot(\overline{k_1\oplus k_2})\oplus x_2\cdot(k_1\oplus k_2)\end{bmatrix}\oplus\begin{bmatrix}k_2\\ \bar{k}_2\end{bmatrix}$.

Результат перетворення наступний:

$$F_{9,5}(O_1^k)=\begin{cases}\begin{bmatrix}x_2\\x_1\oplus 1\end{bmatrix}, \text{якщо } k_1=1;\ k_2=0\\ \begin{bmatrix}x_1\oplus 1\\x_2\end{bmatrix}, \text{якщо } k_1=0;\ k_2=1\\ \begin{bmatrix}x_1\\x_2\oplus 1\end{bmatrix}, \text{якщо } k_1=0;\ k_2=0\\ \begin{bmatrix}x_2\oplus 1\\x_1\end{bmatrix}, \text{якщо } k_1=1;\ k_2=1\end{cases}=O_{13}^k=\begin{cases}\begin{bmatrix}x_2\\x_1\oplus 1\end{bmatrix}, \text{якщо } k_1=0;\ k_2=0\\ \begin{bmatrix}x_1\oplus 1\\x_2\end{bmatrix}, \text{якщо } k_1=0;\ k_2=1\\ \begin{bmatrix}x_1\\x_2\oplus 1\end{bmatrix}, \text{якщо } k_1=1;\ k_2=0\\ \begin{bmatrix}x_2\oplus 1\\x_1\end{bmatrix}, \text{якщо } k_1=1;\ k_2=1\end{cases}=O_{13}^k=\begin{bmatrix}x_1\cdot(k_1\oplus k_2)\oplus x_2\cdot\overline{(k_1\oplus k_2)}\\ x_1\cdot\overline{(k_1\oplus k_2)}\oplus x_2\cdot(k_1\oplus k_2)\end{bmatrix}\oplus\begin{bmatrix}k_2\\\bar{k}_2\end{bmatrix} \quad (3.14)$$

що і потрібно було довести.

Якщо над другим операндом двохоперандної операції строгого криптографічного кодування $O_1^k=\begin{bmatrix}x_1\cdot\bar{k}_1\oplus x_2\cdot k_1\\ x_1\cdot k_1\oplus x_2\cdot\bar{k}_1\end{bmatrix}\oplus\begin{bmatrix}k_2\\\bar{k}_2\end{bmatrix}$ виконати одноопераднe криптографічне перетворення $F_{12,6}=\begin{bmatrix}x_1\oplus 1\\x_1\oplus x_2\end{bmatrix}$ то буде отримана операція строгого стійкого кодування $O_{17}^k=\begin{bmatrix}x_1\cdot k_1\oplus x_2\cdot\bar{k}_1\\ x_1\cdot\bar{k}_1\oplus x_2\cdot k_1\end{bmatrix}\oplus\begin{bmatrix}k_1\oplus k_2\\\overline{k_1\oplus k_2}\end{bmatrix}$.

Так як:

$$F_{12,6}(O_1^k)=\begin{cases}\begin{bmatrix}x_2\\x_1\oplus 1\end{bmatrix}, \text{якщо } k_1=1;\ k_2=0\\ \begin{bmatrix}x_2\oplus 1\\x_1\end{bmatrix}, \text{якщо } k_1=1;\ k_2=1\\ \begin{bmatrix}x_1\oplus 1\\x_2\end{bmatrix}, \text{якщо } k_1=0;\ k_2=1\\ \begin{bmatrix}x_1\\x_2\oplus 1\end{bmatrix}, \text{якщо } k_1=0;\ k_2=0\end{cases}=O_{17}^k=\begin{cases}\begin{bmatrix}x_2\\x_1\oplus 1\end{bmatrix}, \text{якщо } k_1=0;\ k_2=0\\ \begin{bmatrix}x_2\oplus 1\\x_1\end{bmatrix}, \text{якщо } k_1=0;\ k_2=1\\ \begin{bmatrix}x_1\oplus 1\\x_2\end{bmatrix}, \text{якщо } k_1=1;\ k_2=0\\ \begin{bmatrix}x_1\\x_2\oplus 1\end{bmatrix}, \text{якщо } k_1=1;\ k_2=1\end{cases}=O_{17}^k=\begin{bmatrix}x_1\cdot k_1\oplus x_2\cdot\bar{k}_1\\ x_1\cdot\bar{k}_1\oplus x_2\cdot k_1\end{bmatrix}\oplus\begin{bmatrix}k_1\oplus k_2\\\overline{k_1\oplus k_2}\end{bmatrix} \quad (3.15)$$

з цього виходить, що твердження вірне.

У випадку, коли над другим операндом двохоперандної операції строгого криптографічного кодування $O_1^k=\begin{bmatrix}x_1\cdot\bar{k}_1\oplus x_2\cdot k_1\\ x_1\cdot k_1\oplus x_2\cdot\bar{k}_1\end{bmatrix}\oplus\begin{bmatrix}k_2\\\bar{k}_2\end{bmatrix}$, виконується одноопераднe криптографічне перетворення $F_{10,3}=\begin{bmatrix}x_2\oplus 1\\x_1\end{bmatrix}$, буде отримана операція строгого стійкого кодування $O_{15}^k=\begin{bmatrix}x_1\cdot k_2\oplus x_2\cdot\bar{k}_2\\ x_1\cdot\bar{k}_2\oplus x_2\cdot k_2\end{bmatrix}\oplus\begin{bmatrix}k_1\\\bar{k}_1\end{bmatrix}$.

При виконанні даного перетворення:

$$F_{10,3}(O_1^k)=\begin{cases}\begin{bmatrix}x_2\\ x_1\oplus 1\end{bmatrix}, \text{ якщо } k_1=1;\ k_2=0\\ \begin{bmatrix}x_1\\ x_2\oplus 1\end{bmatrix}, \text{ якщо } k_1=0;\ k_2=0\\ \begin{bmatrix}x_2\oplus 1\\ x_1\end{bmatrix}, \text{якщо } k_1=1;\ k_2=1\\ \begin{bmatrix}x_1\oplus 1\\ x_2\end{bmatrix}, \text{якщо } k_1=0;\ k_2=1\end{cases}=O_{15}^k=\begin{cases}\begin{bmatrix}x_2\\ x_1\oplus 1\end{bmatrix}, \text{ якщо } k_1=0;\ k_2=0\\ \begin{bmatrix}x_1\\ x_2\oplus 1\end{bmatrix}, \text{якщо } k_1=0;\ k_2=1\\ \begin{bmatrix}x_2\oplus 1\\ x_1\end{bmatrix}, \text{ якщо } k_1=1;\ k_2=0\\ \begin{bmatrix}x_1\oplus 1\\ x_2\end{bmatrix}, \text{якщо } k_1=1;\ k_2=1\end{cases}=O_{15}^k=\begin{bmatrix}x_1\cdot k_2\oplus x_2\cdot \bar{k}_2\\ x_1\cdot \bar{k}_2\oplus x_2\cdot k_2\end{bmatrix}\oplus\begin{bmatrix}k_1\\ \bar{k}_1\end{bmatrix} \quad (3.16)$$

отримуємо результат, що доводить правильність твердження.

При виконанні над другим операндом двохоперандної операції строгого криптографічного кодування $O_1^k=\begin{bmatrix}x_1\cdot \bar{k}_1\oplus x_2\cdot k_1\\ x_1\cdot k_1\oplus x_2\cdot \bar{k}_1\end{bmatrix}\oplus\begin{bmatrix}k_2\\ \bar{k}_2\end{bmatrix}$ одноопераднe криптографічне перетворення $F_{10,6}=\begin{bmatrix}x_2\oplus 1\\ x_1\oplus x_2\end{bmatrix}$, буде отримана операція строгого стійкого кодування $O_{14}^k=\begin{bmatrix}x_1\cdot k_2\oplus x_2\cdot \bar{k}_2\\ x_1\cdot \bar{k}_2\oplus x_2\cdot k_2\end{bmatrix}\oplus\begin{bmatrix}k_2\\ \bar{k}_2\end{bmatrix}$.

Дане перетворення:

$$F_{10,6}(O_1^k)=\begin{cases}\begin{bmatrix}x_2\\ x_1\oplus 1\end{bmatrix}, \text{ якщо } k_1=1;\ k_2=0\\ \begin{bmatrix}x_1\oplus 1\\ x_2\end{bmatrix}, \text{якщо } k_1=0;\ k_2=1\\ \begin{bmatrix}x_2\oplus 1\\ x_1\end{bmatrix}, \text{якщо } k_1=1;\ k_2=1\\ \begin{bmatrix}x_1\\ x_2\oplus 1\end{bmatrix}, \text{ якщо } k_1=0;\ k_2=0\end{cases}=O_{14}^k=\begin{cases}\begin{bmatrix}x_2\\ x_1\oplus 1\end{bmatrix}, \text{ якщо } k_1=0;\ k_2=0\\ \begin{bmatrix}x_1\oplus 1\\ x_2\end{bmatrix}, \text{якщо } k_1=0;\ k_2=1\\ \begin{bmatrix}x_2\oplus 1\\ x_1\end{bmatrix}, \text{ якщо } k_1=1;\ k_2=0\\ \begin{bmatrix}x_1\\ x_2\oplus 1\end{bmatrix}, \text{якщо } k_1=1;\ k_2=1\end{cases}=O_{14}^k=\begin{bmatrix}x_1\cdot k_2\oplus x_2\cdot \bar{k}_2\\ x_1\cdot \bar{k}_2\oplus x_2\cdot k_2\end{bmatrix}\oplus\begin{bmatrix}k_2\\ \bar{k}_2\end{bmatrix} \quad (3.17)$$

Доводить правильність нашого твердження.

Якщо над другим операндом двохоперандної операції строгого криптографічного кодування $O_1^k=\begin{bmatrix}x_1\cdot \bar{k}_1\oplus x_2\cdot k_1\\ x_1\cdot k_1\oplus x_2\cdot \bar{k}_1\end{bmatrix}\oplus\begin{bmatrix}k_2\\ \bar{k}_2\end{bmatrix}$ виконати одноопераднe криптографічне перетворення $F_{9,3}=\begin{bmatrix}x_1\oplus x_2\oplus 1\\ x_1\end{bmatrix}$ то буде отримана операція строгого стійкого кодування $O_{16}^k=\begin{bmatrix}x_1\cdot(k_1\oplus k_2)\oplus x_2\cdot(\overline{k_1\oplus k_2})\\ x_1\cdot(\overline{k_1\oplus k_2})\oplus x_2\cdot(k_1\oplus k_2)\end{bmatrix}\oplus\begin{bmatrix}k_1\\ \bar{k}_1\end{bmatrix}$.

Так як перетворення матиме наступний вигляд:

$$F_{9,3}(O_1^k)=\begin{cases}\begin{bmatrix}x_2\\x_1\oplus 1\end{bmatrix}, \text{якщо } k_1=1;\ k_2=0\\ \begin{bmatrix}x_1\\x_2\oplus 1\end{bmatrix}, \text{якщо } k_1=0;\ k_2=0\\ \begin{bmatrix}x_1\oplus 1\\x_2\end{bmatrix}, \text{якщо } k_1=0;\ k_2=1\\ \begin{bmatrix}x_2\oplus 1\\x_1\end{bmatrix}, \text{якщо } k_1=1;\ k_2=1\end{cases}=O_{16}^k=\begin{cases}\begin{bmatrix}x_2\\x_1\oplus 1\end{bmatrix}, \text{якщо } k_1=0;\ k_2=0\\ \begin{bmatrix}x_1\\x_2\oplus 1\end{bmatrix}, \text{якщо } k_1=0;\ k_2=1\\ \begin{bmatrix}x_1\oplus 1\\x_2\end{bmatrix}, \text{якщо } k_1=1;\ k_2=0\\ \begin{bmatrix}x_2\oplus 1\\x_1\end{bmatrix}, \text{якщо } k_1=1;\ k_2=1\end{cases}=O_{16}^k=\begin{bmatrix}x_1\cdot(k_1\oplus k_2)\oplus x_2\cdot\overline{(k_1\oplus k_2)}\\ x_1\cdot\overline{(k_1\oplus k_2)}\oplus x_2\cdot(k_1\oplus k_2)\end{bmatrix}\oplus\begin{bmatrix}k_1\\\bar{k}_1\end{bmatrix} \tag{3.18}$$

це і є доведенням.

У випадку виконання над другим операндом двохоперандної операції строгого криптографічного кодування $O_1^k=\begin{bmatrix}x_1\cdot\bar{k}_1\oplus x_2\cdot k_1\\ x_1\cdot k_1\oplus x_2\cdot\bar{k}_1\end{bmatrix}\oplus\begin{bmatrix}k_2\\\bar{k}_2\end{bmatrix}$ одноопераднього криптографічного перетворення $F_{12,10}=\begin{bmatrix}x_1\oplus 1\\x_2\oplus 1\end{bmatrix}$ отримується операція строгого стійкого кодування $O_{22}^k=\begin{bmatrix}x_1\cdot k_1\oplus x_2\cdot\bar{k}_1\\ x_1\cdot\bar{k}_1\oplus x_2\cdot k_1\end{bmatrix}\oplus\begin{bmatrix}\bar{k}_2\\k_2\end{bmatrix}$.

Так як перетворення має наступний вигляд:

$$F_{12,10}(O_1^k)=\begin{cases}\begin{bmatrix}x_2\oplus 1\\x_1\end{bmatrix}, \text{якщо } k_1=1;\ k_2=1\\ \begin{bmatrix}x_2\\x_1\oplus 1\end{bmatrix}, \text{якщо } k_1=1;\ k_2=0\\ \begin{bmatrix}x_1\oplus 1\\x_2\end{bmatrix}, \text{якщо } k_1=0;\ k_2=1\\ \begin{bmatrix}x_1\\x_2\oplus 1\end{bmatrix}, \text{якщо } k_1=0;\ k_2=0\end{cases}=O_{22}^k=\begin{cases}\begin{bmatrix}x_2\oplus 1\\x_1\end{bmatrix}, \text{якщо } k_1=0;\ k_2=0\\ \begin{bmatrix}x_2\\x_1\oplus 1\end{bmatrix}, \text{якщо } k_1=0;\ k_2=1\\ \begin{bmatrix}x_1\oplus 1\\x_2\end{bmatrix}, \text{якщо } k_1=1;\ k_2=0\\ \begin{bmatrix}x_1\\x_2\oplus 1\end{bmatrix}, \text{якщо } k_1=1;\ k_2=1\end{cases}=O_{22}^k=\begin{bmatrix}x_1\cdot k_1\oplus x_2\cdot\bar{k}_1\\ x_1\cdot\bar{k}_1\oplus x_2\cdot k_1\end{bmatrix}\oplus\begin{bmatrix}\bar{k}_2\\k_2\end{bmatrix} \tag{3.19}$$

це доводить правильність твердження.

Якщо над другим операндом двохоперандної операції строгого криптографічного кодування $O_1^k=\begin{bmatrix}x_1\cdot\bar{k}_1\oplus x_2\cdot k_1\\ x_1\cdot k_1\oplus x_2\cdot\bar{k}_1\end{bmatrix}\oplus\begin{bmatrix}k_2\\\bar{k}_2\end{bmatrix}$ виконати одноопераднe криптографічне перетворення $F_{9,10}=\begin{bmatrix}x_1\oplus x_2\oplus 1\\x_2\oplus 1\end{bmatrix}$, то результатом буде операція строгого стійкого кодування $O_{23}^k=\begin{bmatrix}x_1\cdot(k_1\oplus k_2)\oplus x_2\cdot\overline{(k_1\oplus k_2)}\\ x_1\cdot\overline{(k_1\oplus k_2)}\oplus x_2\cdot(k_1\oplus k_2)\end{bmatrix}\oplus\begin{bmatrix}\bar{k}_2\\k_2\end{bmatrix}$.

Це показує наступне перетворення:

$$F_{9,10}(O_1^k)=\begin{cases}\begin{bmatrix}x_2\oplus 1\\ x_1\end{bmatrix}, якщо\ k_1=1;\ k_2=1\\ \begin{bmatrix}x_1\\ x_2\oplus 1\end{bmatrix},\ якщо\ k_1=0;\ k_2=0\\ \begin{bmatrix}x_1\oplus 1\\ x_2\end{bmatrix}, якщо\ k_1=0;\ k_2=1\\ \begin{bmatrix}x_2\\ x_1\oplus 1\end{bmatrix}, якщо\ k_1=1;\ k_2=0\end{cases}=O_{23}^k=\begin{cases}\begin{bmatrix}x_2\oplus 1\\ x_1\end{bmatrix},\ якщо\ k_1=0;\ k_2=0\\ \begin{bmatrix}x_1\\ x_2\oplus 1\end{bmatrix}, якщо\ k_1=0;\ k_2=1\\ \begin{bmatrix}x_1\oplus 1\\ x_2\end{bmatrix},\ якщо\ k_1=1;\ k_2=0\\ \begin{bmatrix}x_2\\ x_1\oplus 1\end{bmatrix}, якщо\ k_1=1;\ k_2=1\end{cases}=O_{23}^k=\begin{bmatrix}x_1\cdot(k_1\oplus k_2)\oplus x_2\cdot\overline{(k_1\oplus k_2)}\\ x_1\cdot\overline{(k_1\oplus k_2)}\oplus x_2\cdot(k_1\oplus k_2)\end{bmatrix}\oplus\begin{bmatrix}\bar{k}_2\\ k_2\end{bmatrix} \quad (3.20)$$

отже, твердження доведено.

При дії одноопераднього криптографічного перетворення $F_{12,9}=\begin{bmatrix}x_1\oplus 1\\ x_1\oplus x_2\oplus 1\end{bmatrix}$ на другий операнд двохоперандної операції строгого криптографічного кодування $O_1^k=\begin{bmatrix}x_1\cdot\bar{k}_1\oplus x_2\cdot k_1\\ x_1\cdot k_1\oplus x_2\cdot\bar{k}_1\end{bmatrix}\oplus\begin{bmatrix}k_2\\ \bar{k}_2\end{bmatrix}$, буде отримана операція строгого стійкого кодування $O_{21}^k=\begin{bmatrix}x_1\cdot k_1\oplus x_2\cdot\bar{k}_1\\ x_1\cdot\bar{k}_1\oplus x_2\cdot k_1\end{bmatrix}\oplus\begin{bmatrix}\overline{k_1\oplus k_2}\\ k_1\oplus k_2\end{bmatrix}$.

Дане перетворення має вигляд:

$$F_{12,9}(O_1^k)=\begin{cases}\begin{bmatrix}x_1\oplus 1\\ x_2\end{bmatrix}, якщо\ k_1=0;\ k_2=1\\ \begin{bmatrix}x_2\oplus 1\\ x_1\end{bmatrix}, якщо\ k_1=1;\ k_2=1\\ \begin{bmatrix}x_1\\ x_2\oplus 1\end{bmatrix},\ якщо\ k_1=0;\ k_2=0\\ \begin{bmatrix}x_2\\ x_1\oplus 1\end{bmatrix}, якщо\ k_1=1;\ k_2=0\end{cases}=O_{21}^k=\begin{cases}\begin{bmatrix}x_2\oplus 1\\ x_1\end{bmatrix},\ якщо\ k_1=0;\ k_2=0\\ \begin{bmatrix}x_2\\ x_1\oplus 1\end{bmatrix}, якщо\ k_1=0;\ k_2=1\\ \begin{bmatrix}x_1\\ x_2\oplus 1\end{bmatrix},\ якщо\ k_1=1;\ k_2=0\\ \begin{bmatrix}x_1\oplus 1\\ x_2\end{bmatrix}, якщо\ k_1=1;\ k_2=1\end{cases}=O_{21}^k=\begin{bmatrix}x_1\cdot k_1\oplus x_2\cdot\bar{k}_1\\ x_1\cdot\bar{k}_1\oplus x_2\cdot k_1\end{bmatrix}\oplus\begin{bmatrix}\overline{k_1\oplus k_2}\\ k_1\oplus k_2\end{bmatrix} \quad (3.21)$$

що і необхідно було довести.

У випадку, коли над другим операндом двохоперандної операції строгого криптографічного кодування $O_1^k=\begin{bmatrix}x_1\cdot\bar{k}_1\oplus x_2\cdot k_1\\ x_1\cdot k_1\oplus x_2\cdot\bar{k}_1\end{bmatrix}\oplus\begin{bmatrix}k_2\\ \bar{k}_2\end{bmatrix}$ виконується одноопераднe криптографічне перетворення $F_{10,12}=\begin{bmatrix}x_2\oplus 1\\ x_1\oplus 1\end{bmatrix}$, в результаті буде отримана операція строгого стійкого кодування $O_{19}^k=\begin{bmatrix}x_1\cdot\bar{k}_2\oplus x_2\cdot k_2\\ x_1\cdot k_2\oplus x_2\cdot\bar{k}_2\end{bmatrix}\oplus\begin{bmatrix}k_1\\ \bar{k}_1\end{bmatrix}$.

Що доводить наступне перетворення:

$$F_{10,12}(O_1^k)=\begin{cases}\begin{bmatrix}x_2\oplus 1\\ x_1\end{bmatrix}, якщо\ k_1=1;\ k_2=1\\ \begin{bmatrix}x_1\oplus 1\\ x_2\end{bmatrix}, якщо\ k_1=0;\ k_2=1\\ \begin{bmatrix}x_2\\ x_1\oplus 1\end{bmatrix}, якщо\ k_1=1;\ k_2=0\\ \begin{bmatrix}x_1\\ x_2\oplus 1\end{bmatrix}, якщо\ k_1=0;\ k_2=0\end{cases}=O_{19}^k=\begin{cases}\begin{bmatrix}x_2\oplus 1\\ x_1\end{bmatrix}, якщо\ k_1=0;\ k_2=0\\ \begin{bmatrix}x_1\oplus 1\\ x_2\end{bmatrix}, якщо\ k_1=0;\ k_2=1\\ \begin{bmatrix}x_2\\ x_1\oplus 1\end{bmatrix}, якщо\ k_1=1;\ k_2=0\\ \begin{bmatrix}x_1\\ x_2\oplus 1\end{bmatrix}, якщо\ k_1=1;\ k_2=1\end{cases}=O_{19}^k=\begin{bmatrix}x_1\cdot\bar{k}_2\oplus x_2\cdot k_2\\ x_1\cdot k_2\oplus x_2\cdot\bar{k}_2\end{bmatrix}\oplus\begin{bmatrix}k_1\\ \bar{k}_1\end{bmatrix} \quad (3.22)$$

Якщо над другим операндом двохоперандної операції строгого криптографічного кодування $O_1^k=\begin{bmatrix}x_1\cdot\bar{k}_1\oplus x_2\cdot k_1\\ x_1\cdot k_1\oplus x_2\cdot\bar{k}_1\end{bmatrix}\oplus\begin{bmatrix}k_2\\ \bar{k}_2\end{bmatrix}$ виконати одноопераднe криптографічне перетворення $F_{10,9}=\begin{bmatrix}x_2\oplus 1\\ x_1\oplus x_2\oplus 1\end{bmatrix}$, буде отримана операція строгого стійкого кодування $O_{24}^k=\begin{bmatrix}x_1\cdot k_2\oplus x_2\cdot\bar{k}_2\\ x_1\cdot\bar{k}_2\oplus x_2\cdot k_2\end{bmatrix}\oplus\begin{bmatrix}\overline{k_1\oplus k_2}\\ k_1\oplus k_2\end{bmatrix}$.

Так як:

$$F_{10,9}(O_1^k)=\begin{cases}\begin{bmatrix}x_2\oplus 1\\ x_1\end{bmatrix}, якщо\ k_1=1;\ k_2=1\\ \begin{bmatrix}x_1\\ x_2\oplus 1\end{bmatrix}, якщо\ k_1=0;\ k_2=0\\ \begin{bmatrix}x_2\\ x_1\oplus 1\end{bmatrix}, якщо\ k_1=1;\ k_2=0\\ \begin{bmatrix}x_1\oplus 1\\ x_2\end{bmatrix}, якщо\ k_1=0;\ k_2=1\end{cases}=O_{24}^k=\begin{cases}\begin{bmatrix}x_2\oplus 1\\ x_1\end{bmatrix}, якщо\ k_1=0;\ k_2=0\\ \begin{bmatrix}x_1\\ x_2\oplus 1\end{bmatrix}, якщо\ k_1=0;\ k_2=1\\ \begin{bmatrix}x_2\\ x_1\oplus 1\end{bmatrix}, якщо\ k_1=1;\ k_2=0\\ \begin{bmatrix}x_1\oplus 1\\ x_2\end{bmatrix}, якщо\ k_1=1;\ k_2=1\end{cases}=O_{24}^k=\begin{bmatrix}x_1\cdot k_2\oplus x_2\cdot\bar{k}_2\\ x_1\cdot\bar{k}_2\oplus x_2\cdot k_2\end{bmatrix}\oplus\begin{bmatrix}\overline{k_1\oplus k_2}\\ k_1\oplus k_2\end{bmatrix} \quad (3.23)$$

це доводить дане твердження.

При виконанні над другим операндом двохоперандної операції строгого криптографічного кодування $O_1^k=\begin{bmatrix}x_1\cdot\bar{k}_1\oplus x_2\cdot k_1\\ x_1\cdot k_1\oplus x_2\cdot\bar{k}_1\end{bmatrix}\oplus\begin{bmatrix}k_2\\ \bar{k}_2\end{bmatrix}$ одноопераднoго криптографічного перетворення $F=\begin{bmatrix}x_1\oplus x_2\oplus 1\\ x_1\oplus 1\end{bmatrix}$**,** отримана операція строгого стійкого кодування $O_{20}^k=\begin{bmatrix}x_1\cdot(k_1\oplus k_2)\oplus x_2\cdot(\overline{k_1\oplus k_2})\\ x_1\cdot(\overline{k_1\oplus k_2})\oplus x_2\cdot(k_1\oplus k_2)\end{bmatrix}\oplus\begin{bmatrix}\bar{k}_1\\ k_1\end{bmatrix}$.

Саме це доводить наступне:

$$F_{9,12}(O_1^k)=\begin{cases}\begin{bmatrix}x_2\oplus 1\\ x_1\end{bmatrix}, якщо\ k_1=1;\ k_2=1\\ \begin{bmatrix}x_1\oplus 1\\ x_2\end{bmatrix}, якщо\ k_1=0;\ k_2=1\\ \begin{bmatrix}x_1\\ x_2\oplus 1\end{bmatrix}, якщо\ k_1=0;\ k_2=0\\ \begin{bmatrix}x_2\\ x_1\oplus 1\end{bmatrix}, якщо\ k_1=1;\ k_2=0\end{cases}=O_{20}^k=\begin{cases}\begin{bmatrix}x_2\oplus 1\\ x_1\end{bmatrix}, якщо\ k_1=0;\ k_2=0\\ \begin{bmatrix}x_1\oplus 1\\ x_2\end{bmatrix}, якщо\ k_1=0;\ k_2=1\\ \begin{bmatrix}x_1\\ x_2\oplus 1\end{bmatrix}, якщо\ k_1=1;\ k_2=0\\ \begin{bmatrix}x_2\\ x_1\oplus 1\end{bmatrix}, якщо\ k_1=1;\ k_2=1\end{cases}=O_{20}^k=\begin{bmatrix}x_1\cdot(k_1\oplus k_2)\oplus x_2\cdot\overline{(k_1\oplus k_2)}\\ x_1\cdot\overline{(k_1\oplus k_2)}\oplus x_2\cdot(k_1\oplus k_2)\end{bmatrix}\oplus\begin{bmatrix}\bar{k}_1\\ k_1\end{bmatrix} \quad (3.24)$$

Згідно отриманих результатів, при яких виконувалось перетворення другого операнда відомої операції за допомогою одноопераднної операції, можна стверджувати, що на основі операції $O_1^k=\begin{bmatrix}x_1\cdot\bar{k}_1\oplus x_2\cdot k_1\\ x_1\cdot k_1\oplus x_2\cdot\bar{k}_1\end{bmatrix}\oplus\begin{bmatrix}k_2\\ \bar{k}_2\end{bmatrix}$ можна отримати повну групу двохрозрядних двохоперандних операцій ССКК.

3.2 Синтез групи двохрозрядних двохоперандних операцій ССКК на основі другої операції

Перевіримо правильність отриманого результату синтезом групи двохрозрядних двохоперандних операції ССК на основі операції $O_2^k=\begin{bmatrix}x_1\cdot\bar{k}_1\oplus x_2\cdot k_1\\ x_1\cdot k_1\oplus x_2\cdot\bar{k}_1\end{bmatrix}\oplus\begin{bmatrix}k_1\oplus k_2\\ \overline{k_1\oplus k_2}\end{bmatrix}$.

Якщо виконати одноопераднe криптографічне перетворення $F_{3,5}=\begin{bmatrix}x_1\\ x_2\end{bmatrix}$ над другим операндом двохоперандної операції строгого криптографічного кодування $O_2^k=\begin{bmatrix}x_1\cdot\bar{k}_1\oplus x_2\cdot k_1\\ x_1\cdot k_1\oplus x_2\cdot\bar{k}_1\end{bmatrix}\oplus\begin{bmatrix}k_1\oplus k_2\\ \overline{k_1\oplus k_2}\end{bmatrix}$, то буде отримана операція строгого стійкого криптографічного кодування $O_2^k=\begin{bmatrix}x_1\cdot\bar{k}_1\oplus x_2\cdot k_1\\ x_1\cdot k_1\oplus x_2\cdot\bar{k}_1\end{bmatrix}\oplus\begin{bmatrix}k_1\oplus k_2\\ \overline{k_1\oplus k_2}\end{bmatrix}$.

Так як перетворення має наступний вигляд:

$$F_{3,5}(O_2^k)=\begin{cases}\begin{bmatrix}x_1\\ x_2\oplus 1\end{bmatrix}, & якщо\ k_1=0;\ k_2=0\\ \begin{bmatrix}x_1\oplus 1\\ x_2\end{bmatrix}, & якщо\ k_1=0;\ k_2=1\\ \begin{bmatrix}x_2\oplus 1\\ x_1\end{bmatrix}, & якщо\ k_1=1;\ k_2=0\\ \begin{bmatrix}x_2\\ x_1\oplus 1\end{bmatrix}, & якщо\ k_1=1;\ k_2=1\end{cases}=O_2^k=\begin{cases}\begin{bmatrix}x_1\\ x_2\oplus 1\end{bmatrix}, & якщо\ k_1=0;\ k_2=0\\ \begin{bmatrix}x_1\oplus 1\\ x_2\end{bmatrix}, & якщо\ k_1=0;\ k_2=1\\ \begin{bmatrix}x_2\oplus 1\\ x_1\end{bmatrix}, & якщо\ k_1=1;\ k_2=0\\ \begin{bmatrix}x_2\\ x_1\oplus 1\end{bmatrix}, & якщо\ k_1=1;\ k_2=1\end{cases}\quad O_1^k=\begin{bmatrix}x_1\cdot\bar{k}_1\oplus x_2\cdot k_1\\ x_1\cdot k_1\oplus x_2\cdot\bar{k}_1\end{bmatrix}\oplus\begin{bmatrix}k_2\\ \bar{k}_2\end{bmatrix} \tag{3.25}$$

саме це підтверджує вірність твердження.

У випадку, коли над другим операндом двохоперандної операції строгого криптографічного кодування $O_2^k=\begin{bmatrix}x_1\cdot\bar{k}_1\oplus x_2\cdot k_1\\ x_1\cdot k_1\oplus x_2\cdot\bar{k}_1\end{bmatrix}\oplus\begin{bmatrix}k_1\oplus k_2\\ \overline{k_1\oplus k_2}\end{bmatrix}$ виконати одноопераднe криптографічне перетворення $F_{6,5}=\begin{bmatrix}x_1\oplus x_2\\ x_2\end{bmatrix}$ то буде отримана операція строгого стійкого кодування $O_3^k=\begin{bmatrix}x_1\cdot(\overline{k_1\oplus k_2})\oplus x_2\cdot(k_1\oplus k_2)\\ x_1\cdot(k_1\oplus k_2)\oplus x_2\cdot(\overline{k_1\oplus k_2})\end{bmatrix}\oplus\begin{bmatrix}k_1\\ \bar{k}_1\end{bmatrix}$.

Оскільки:

$$F_{6,5}(O_2^k)=\begin{cases}\begin{bmatrix}x_1\\ x_2\oplus 1\end{bmatrix}, & якщо\ k_1=0;\ k_2=0\\ \begin{bmatrix}x_2\\ x_1\oplus 1\end{bmatrix}, & якщо\ k_1=1;\ k_2=1\\ \begin{bmatrix}x_2\oplus 1\\ x_1\end{bmatrix}, & якщо\ k_1=1;\ k_2=0\\ \begin{bmatrix}x_1\oplus 1\\ x_2\end{bmatrix}, & якщо\ k_1=0;\ k_2=1\end{cases}=O_3^k=\begin{cases}\begin{bmatrix}x_1\\ x_2\oplus 1\end{bmatrix}, & якщо\ k_1=0;\ k_2=0\\ \begin{bmatrix}x_2\\ x_1\oplus 1\end{bmatrix}, & якщо\ k_1=0;\ k_2=1\\ \begin{bmatrix}x_2\oplus 1\\ x_1\end{bmatrix}, & якщо\ k_1=1;\ k_2=0\\ \begin{bmatrix}x_1\oplus 1\\ x_2\end{bmatrix}, & якщо\ k_1=1;\ k_2=1\end{cases}=O_3^k=\begin{bmatrix}x_1\cdot(\overline{k_1\oplus k_2})\oplus x_2\cdot(k_1\oplus k_2)\\ x_1\cdot(k_1\oplus k_2)\oplus x_2\cdot(\overline{k_1\oplus k_2})\end{bmatrix}\oplus\begin{bmatrix}k_1\\ \bar{k}_1\end{bmatrix} \tag{3.26}$$

що й необхідно було довести.

При одноопераднoму криптографічному перетворенні $F_{3,6}=\begin{bmatrix}x_1\\ x_1\oplus x_2\end{bmatrix}$ над другим операндом двохоперандної операції строгого криптографічного кодування $O_2^k=\begin{bmatrix}x_1\cdot\bar{k}_1\oplus x_2\cdot k_1\\ x_1\cdot k_1\oplus x_2\cdot\bar{k}_1\end{bmatrix}\oplus\begin{bmatrix}k_1\oplus k_2\\ \overline{k_1\oplus k_2}\end{bmatrix}$, то результатом буде отримана операція строгого стійкого кодування $O_1^k=\begin{bmatrix}x_1\cdot\bar{k}_1\oplus x_2\cdot k_1\\ x_1\cdot k_1\oplus x_2\cdot\bar{k}_1\end{bmatrix}\oplus\begin{bmatrix}k_2\\ \bar{k}_2\end{bmatrix}$.

Перетворення матиме наступний вигляд:

$$F_{3,6}(O_2^k)=\begin{cases}\begin{bmatrix}x_1\\ x_2\oplus 1\end{bmatrix}, якщо\ k_1=0;\ k_2=0\\ \begin{bmatrix}x_1\oplus 1\\ x_2\end{bmatrix}, якщо\ k_1=0;\ k_2=1\\ \begin{bmatrix}x_2\oplus 1\\ x_1\end{bmatrix}, якщо\ k_1=1;\ k_2=1\\ \begin{bmatrix}x_2\\ x_1\oplus 1\end{bmatrix}, якщо\ k_1=1;\ k_2=0\end{cases}=O_1^k=\begin{cases}\begin{bmatrix}x_1\\ x_2\oplus 1\end{bmatrix}, якщо\ k_1=0;\ k_2=0\\ \begin{bmatrix}x_1\oplus 1\\ x_2\end{bmatrix}, якщо\ k_1=0;\ k_2=1\\ \begin{bmatrix}x_2\oplus 1\\ x_1\end{bmatrix}, якщо\ k_1=1;\ k_2=0\\ \begin{bmatrix}x_2\\ x_1\oplus 1\end{bmatrix}, якщо\ k_1=1;\ k_2=1\end{cases}=O_1^k=\begin{bmatrix}x_1\cdot\bar{k}_1\oplus x_2\cdot k_1\\ x_1\cdot k_1\oplus x_2\cdot\bar{k}_1\end{bmatrix}\oplus\begin{bmatrix}k_2\\ \bar{k}_2\end{bmatrix} \quad (3.27)$$

що вказує на вірність твердження.

У випадку, при якому над другим операндом двохоперандної операції строгого криптографічного кодування $O_2^k=\begin{bmatrix}x_1\cdot\bar{k}_1\oplus x_2\cdot k_1\\ x_1\cdot k_1\oplus x_2\cdot\bar{k}_1\end{bmatrix}\oplus\begin{bmatrix}k_1\oplus k_2\\ \overline{k_1\oplus k_2}\end{bmatrix}$ буде виконано одноопераднe криптографічне перетворення $F_{5,3}=\begin{bmatrix}x_2\\ x_1\end{bmatrix}$, то буде одержана операція строгого стійкого кодування $O_5^k=\begin{bmatrix}x_1\cdot\bar{k}_2\oplus x_2\cdot k_2\\ x_1\cdot k_2\oplus x_2\cdot\bar{k}_2\end{bmatrix}\oplus\begin{bmatrix}k_1\oplus k_2\\ \overline{k_1\oplus k_2}\end{bmatrix}$.

У випадку перетворення:

$$F_{5,3}(O_2^k)=\begin{cases}\begin{bmatrix}x_1\\ x_2\oplus 1\end{bmatrix}, якщо\ k_1=0;\ k_2=0\\ \begin{bmatrix}x_2\oplus 1\\ x_1\end{bmatrix}, якщо\ k_1=1;\ k_2=0\\ \begin{bmatrix}x_1\oplus 1\\ x_2\end{bmatrix}, якщо\ k_1=0;\ k_2=1\\ \begin{bmatrix}x_2\\ x_1\oplus 1\end{bmatrix}, якщо\ k_1=1;\ k_2=1\end{cases}=O_5^k=\begin{cases}\begin{bmatrix}x_1\\ x_2\oplus 1\end{bmatrix}, якщо\ k_1=0;\ k_2=0\\ \begin{bmatrix}x_2\oplus 1\\ x_1\end{bmatrix}, якщо\ k_1=0;\ k_2=1\\ \begin{bmatrix}x_1\oplus 1\\ x_2\end{bmatrix}, якщо\ k_1=1;\ k_2=0\\ \begin{bmatrix}x_2\\ x_1\oplus 1\end{bmatrix}, якщо\ k_1=1;\ k_2=1\end{cases}=O_5^k=\begin{bmatrix}x_1\cdot\bar{k}_2\oplus x_2\cdot k_2\\ x_1\cdot k_2\oplus x_2\cdot\bar{k}_2\end{bmatrix}\oplus\begin{bmatrix}k_1\oplus k_2\\ \overline{k_1\oplus k_2}\end{bmatrix} \quad (3.28)$$

воно показує, що наше доведення вірне.

Якщо над другим операндом двохоперандної операції строгого криптографічного кодування $O_2^k=\begin{bmatrix}x_1\cdot\bar{k}_1\oplus x_2\cdot k_1\\ x_1\cdot k_1\oplus x_2\cdot\bar{k}_1\end{bmatrix}\oplus\begin{bmatrix}k_1\oplus k_2\\ \overline{k_1\oplus k_2}\end{bmatrix}$ виконати

одноопераднe криптографічне перетворення $F_{5,6}=\begin{bmatrix} x_2 \\ x_1 \oplus x_2 \end{bmatrix}$, буде отримана операція строгого стійкого кодування $O_4^k=\begin{bmatrix} x_1 \cdot \bar{k}_2 \oplus x_2 \cdot k_2 \\ x_1 \cdot k_2 \oplus x_2 \cdot \bar{k}_2 \end{bmatrix} \oplus \begin{bmatrix} k_1 \\ \bar{k}_1 \end{bmatrix}$.

Так як дане перетворення матиме наступний вигляд:

$$F_{5,6}(O_2^k)=\begin{cases} \begin{bmatrix} x_1 \\ x_2 \oplus 1 \end{bmatrix}, \text{ якщо } k_1=0; k_2=0 \\ \begin{bmatrix} x_2 \\ x_1 \oplus 1 \end{bmatrix}, \text{якщо } k_1=1; k_2=1 \\ \begin{bmatrix} x_1 \oplus 1 \\ x_2 \end{bmatrix}, \text{якщо } k_1=0; k_2=1 \\ \begin{bmatrix} x_2 \oplus 1 \\ x_1 \end{bmatrix}, \text{ якщо } k_1=1; k_2=0 \end{cases} = O_4^k = \begin{cases} \begin{bmatrix} x_1 \\ x_2 \oplus 1 \end{bmatrix}, \text{ якщо } k_1=0; k_2=0 \\ \begin{bmatrix} x_2 \\ x_1 \oplus 1 \end{bmatrix}, \text{якщо } k_1=0; k_2=1 \\ \begin{bmatrix} x_1 \oplus 1 \\ x_2 \end{bmatrix}, \text{ якщо } k_1=1; k_2=0 \\ \begin{bmatrix} x_2 \oplus 1 \\ x_1 \end{bmatrix}, \text{якщо } k_1=1; k_2=1 \end{cases} = O_4^k = \begin{bmatrix} x_1 \cdot \bar{k}_2 \oplus x_2 \cdot k_2 \\ x_1 \cdot k_2 \oplus x_2 \cdot \bar{k}_2 \end{bmatrix} \oplus \begin{bmatrix} k_1 \\ \bar{k}_1 \end{bmatrix} \quad (3.29)$$

це доводить вірність нашого твердження.

У випадку виконання одноопераднього криптографічного перетворення $F_{6,3}=\begin{bmatrix} x_1 \oplus x_2 \\ x_1 \end{bmatrix}$ над другим операндом двохоперандної операції строгого криптографічного кодування $O_2^k=\begin{bmatrix} x_1 \cdot \bar{k}_1 \oplus x_2 \cdot k_1 \\ x_1 \cdot k_1 \oplus x_2 \cdot \bar{k}_1 \end{bmatrix} \oplus \begin{bmatrix} k_1 \oplus k_2 \\ \overline{k_1 \oplus k_2} \end{bmatrix}$, буде отримана операція строгого стійкого кодування $O_6^k=\begin{bmatrix} x_1 \cdot (\overline{k_1 \oplus k_2}) \oplus x_2 \cdot (k_1 \oplus k_2) \\ x_1 \cdot (k_1 \oplus k_2) \oplus x_2 \cdot (\overline{k_1 \oplus k_2}) \end{bmatrix} \oplus \begin{bmatrix} k_2 \\ \bar{k}_2 \end{bmatrix}$.

Так як:

$$F_{6,3}(O_2^k)=\begin{cases} \begin{bmatrix} x_1 \\ x_2 \oplus 1 \end{bmatrix}, \text{ якщо } k_1=0; k_2=0 \\ \begin{bmatrix} x_2 \oplus 1 \\ x_1 \end{bmatrix}, \text{ якщо } k_1=1; k_2=0 \\ \begin{bmatrix} x_2 \\ x_1 \oplus 1 \end{bmatrix}, \text{якщо } k_1=1; k_2=1 \\ \begin{bmatrix} x_1 \oplus 1 \\ x_2 \end{bmatrix}, \text{якщо } k_1=0; k_2=1 \end{cases} = O_6^k = \begin{cases} \begin{bmatrix} x_1 \\ x_2 \oplus 1 \end{bmatrix}, \text{ якщо } k_1=0; k_2=0 \\ \begin{bmatrix} x_2 \oplus 1 \\ x_1 \end{bmatrix}, \text{якщо } k_1=0; k_2=1 \\ \begin{bmatrix} x_2 \\ x_1 \oplus 1 \end{bmatrix}, \text{ якщо } k_1=1; k_2=0 \\ \begin{bmatrix} x_1 \oplus 1 \\ x_2 \end{bmatrix}, \text{якщо } k_1=1; k_2=1 \end{cases} = O_6^k = \begin{bmatrix} x_1 \cdot (\overline{k_1 \oplus k_2}) \oplus x_2 \cdot (k_1 \oplus k_2) \\ x_1 \cdot (k_1 \oplus k_2) \oplus x_2 \cdot (\overline{k_1 \oplus k_2}) \end{bmatrix} \oplus \begin{bmatrix} k_2 \\ \bar{k}_2 \end{bmatrix} \quad (3.30)$$

що і потрібно було довести.

При виконанні над другим операндом двохоперандної операції строгого криптографічного кодування $O_2^k = \begin{bmatrix} x_1 \cdot \bar{k}_1 \oplus x_2 \cdot k_1 \\ x_1 \cdot k_1 \oplus x_2 \cdot \bar{k}_1 \end{bmatrix} \oplus \begin{bmatrix} k_1 \oplus k_2 \\ \overline{k_1 \oplus k_2} \end{bmatrix}$ одноопераднього криптографічного перетворення $F_{3,10} = \begin{bmatrix} x_1 \\ x_2 \oplus 1 \end{bmatrix}$, то буде отримана операція строгого стійкого кодування $O_7^k = \begin{bmatrix} x_1 \cdot \bar{k}_1 \oplus x_2 \cdot k_1 \\ x_1 \cdot k_1 \oplus x_2 \cdot \bar{k}_1 \end{bmatrix} \oplus \begin{bmatrix} \overline{k_1 \oplus k_2} \\ k_1 \oplus k_2 \end{bmatrix}$.

Дане перетворення:

$$F_{3,10}(O_2^k) = \begin{cases} \begin{bmatrix} x_1 \oplus 1 \\ x_2 \end{bmatrix}, \text{якщо } k_1 = 0; k_2 = 1 \\ \begin{bmatrix} x_1 \\ x_2 \oplus 1 \end{bmatrix}, \text{якщо } k_1 = 0; k_2 = 0 \\ \begin{bmatrix} x_2 \\ x_1 \oplus 1 \end{bmatrix}, \text{якщо } k_1 = 1; k_2 = 1 \\ \begin{bmatrix} x_2 \oplus 1 \\ x_1 \end{bmatrix}, \text{якщо } k_1 = 1; k_2 = 0 \end{cases} = O_7^k = \begin{cases} \begin{bmatrix} x_1 \oplus 1 \\ x_2 \end{bmatrix}, \text{якщо } k_1 = 0; k_2 = 0 \\ \begin{bmatrix} x_1 \\ x_2 \oplus 1 \end{bmatrix}, \text{якщо } k_1 = 0; k_2 = 1 \\ \begin{bmatrix} x_2 \\ x_1 \oplus 1 \end{bmatrix}, \text{якщо } k_1 = 1; k_2 = 0 \\ \begin{bmatrix} x_2 \oplus 1 \\ x_1 \end{bmatrix}, \text{якщо } k_1 = 1; k_2 = 1 \end{cases} = O_7^k = \begin{bmatrix} x_1 \cdot \bar{k}_1 \oplus x_2 \cdot k_1 \\ x_1 \cdot k_1 \oplus x_2 \cdot \bar{k}_1 \end{bmatrix} \oplus \begin{bmatrix} \overline{k_1 \oplus k_2} \\ k_1 \oplus k_2 \end{bmatrix} \quad (3.31)$$

показує вірність твердження.

При дії на другий операнд двохоперандної операції строгого криптографічного кодування $O_2^k = \begin{bmatrix} x_1 \cdot \bar{k}_1 \oplus x_2 \cdot k_1 \\ x_1 \cdot k_1 \oplus x_2 \cdot \bar{k}_1 \end{bmatrix} \oplus \begin{bmatrix} k_1 \oplus k_2 \\ \overline{k_1 \oplus k_2} \end{bmatrix}$ одноопераднім криптографічним перетворенням $F_{6,10} = \begin{bmatrix} x_1 \oplus x_2 \\ x_2 \oplus 1 \end{bmatrix}$ то буде отримана операція строгого стійкого кодування $O_{12}^k = \begin{bmatrix} x_1 \cdot (\overline{k_1 \oplus k_2}) \oplus x_2 \cdot (k_1 \oplus k_2) \\ x_1 \cdot (k_1 \oplus k_2) \oplus x_2 \cdot (\overline{k_1 \oplus k_2}) \end{bmatrix} \oplus \begin{bmatrix} \bar{k}_1 \\ k_1 \end{bmatrix}$.

Так як перетворення має наступний вигляд:

$$F_{6,10}(O_2^k) = \begin{cases} \begin{bmatrix} x_1 \oplus 1 \\ x_2 \end{bmatrix}, \text{якщо } k_1 = 0; k_2 = 1 \\ \begin{bmatrix} x_2 \oplus 1 \\ x_1 \end{bmatrix}, \text{якщо } k_1 = 1; k_2 = 0 \\ \begin{bmatrix} x_2 \\ x_1 \oplus 1 \end{bmatrix}, \text{якщо } k_1 = 1; k_2 = 1 \\ \begin{bmatrix} x_1 \\ x_2 \oplus 1 \end{bmatrix}, \text{якщо } k_1 = 0; k_2 = 0 \end{cases} = O_{12}^k = \begin{cases} \begin{bmatrix} x_1 \oplus 1 \\ x_2 \end{bmatrix}, \text{якщо } k_1 = 0; k_2 = 0 \\ \begin{bmatrix} x_2 \oplus 1 \\ x_1 \end{bmatrix}, \text{якщо } k_1 = 0; k_2 = 1 \\ \begin{bmatrix} x_2 \\ x_1 \oplus 1 \end{bmatrix}, \text{якщо } k_1 = 1; k_2 = 0 \\ \begin{bmatrix} x_1 \\ x_2 \oplus 1 \end{bmatrix}, \text{якщо } k_1 = 1; k_2 = 1 \end{cases} = O_{12}^k = \begin{bmatrix} x_1 \cdot (\overline{k_1 \oplus k_2}) \oplus x_2 \cdot (k_1 \oplus k_2) \\ x_1 \cdot (k_1 \oplus k_2) \oplus x_2 \cdot (\overline{k_1 \oplus k_2}) \end{bmatrix} \oplus \begin{bmatrix} \bar{k}_1 \\ k_1 \end{bmatrix} \quad (3.32)$$

це доводить правильність нашого твердження

Якщо над другим операндом двохоперандної операції строгого криптографічного кодування $O_2^k=\begin{bmatrix} x_1\cdot\bar{k}_1\oplus x_2\cdot k_1 \\ x_1\cdot k_1\oplus x_2\cdot\bar{k}_1 \end{bmatrix}\oplus\begin{bmatrix} k_1\oplus k_2 \\ \overline{k_1\oplus k_2} \end{bmatrix}$ виконати наступне одноопераднде криптографічне перетворення $F_{3,9}=\begin{bmatrix} x_1 \\ x_1\oplus x_2\oplus 1 \end{bmatrix}$, в результаті отримуємо операцію строгого стійкого криптографічного кодування $O_8^k=\begin{bmatrix} x_1\cdot\bar{k}_1\oplus x_2\cdot k_1 \\ x_1\cdot k_1\oplus x_2\cdot\bar{k}_1 \end{bmatrix}\oplus\begin{bmatrix} \bar{k}_2 \\ k_2 \end{bmatrix}$.

Так як:

$$F_{3,9}(O_2^k)=\begin{cases}\begin{bmatrix} x_1\oplus 1 \\ x_2 \end{bmatrix}, якщо\ k_1=0;\ k_2=1 \\ \begin{bmatrix} x_1 \\ x_2\oplus 1 \end{bmatrix}, якщо\ k_1=0;\ k_2=0 \\ \begin{bmatrix} x_2\oplus 1 \\ x_1 \end{bmatrix}, якщо\ k_1=1;\ k_2=1 \\ \begin{bmatrix} x_2 \\ x_1\oplus 1 \end{bmatrix}, якщо\ k_1=1;\ k_2=0\end{cases}=O_8^k=\begin{cases}\begin{bmatrix} x_1\oplus 1 \\ x_2 \end{bmatrix}, якщо\ k_1=0;\ k_2=0 \\ \begin{bmatrix} x_1 \\ x_2\oplus 1 \end{bmatrix}, якщо\ k_1=0;\ k_2=1 \\ \begin{bmatrix} x_2\oplus 1 \\ x_1 \end{bmatrix}, якщо\ k_1=1;\ k_2=0 \\ \begin{bmatrix} x_2 \\ x_1\oplus 1 \end{bmatrix}, якщо\ k_1=1;\ k_2=1\end{cases}=O_8^k=\begin{bmatrix} x_1\cdot\bar{k}_1\oplus x_2\cdot k_1 \\ x_1\cdot k_1\oplus x_2\cdot\bar{k}_1 \end{bmatrix}\oplus\begin{bmatrix} \bar{k}_2 \\ k_2 \end{bmatrix} \quad (3.33)$$

що й потрібно було довести.

Виконавши одноопераднде криптографічне перетворення $F_{5,12}=\begin{bmatrix} x_2 \\ x_1\oplus 1 \end{bmatrix}$ над другим операндом двохоперандної операції строгого криптографічного кодування $O_2^k=\begin{bmatrix} x_1\cdot\bar{k}_1\oplus x_2\cdot k_1 \\ x_1\cdot k_1\oplus x_2\cdot\bar{k}_1 \end{bmatrix}\oplus\begin{bmatrix} k_1\oplus k_2 \\ \overline{k_1\oplus k_2} \end{bmatrix}$, буде отримана операція строгого стійкого кодування $O_{10}^k=\begin{bmatrix} x_1\cdot\bar{k}_2\oplus x_2\cdot k_2 \\ x_1\cdot k_2\oplus x_2\cdot\bar{k}_2 \end{bmatrix}\oplus\begin{bmatrix} \bar{k}_2 \\ k_2 \end{bmatrix}$.

Це доводить наступне перетворення:

$$F_{5,12}(O_2^k)=\begin{cases}\begin{bmatrix} x_1\oplus 1 \\ x_2 \end{bmatrix}, якщо\ k_1=0;\ k_2=1 \\ \begin{bmatrix} x_2 \\ x_1\oplus 1 \end{bmatrix}, якщо\ k_1=1;\ k_2=0 \\ \begin{bmatrix} x_1 \\ x_2\oplus 1 \end{bmatrix}, якщо\ k_1=0;\ k_2=0 \\ \begin{bmatrix} x_2\oplus 1 \\ x_1 \end{bmatrix}, якщо\ k_1=1;\ k_2=1\end{cases}=O_{10}^k=\begin{cases}\begin{bmatrix} x_1\oplus 1 \\ x_2 \end{bmatrix}, якщо\ k_1=0;\ k_2=0 \\ \begin{bmatrix} x_2 \\ x_1\oplus 1 \end{bmatrix}, якщо\ k_1=0;\ k_2=1 \\ \begin{bmatrix} x_1 \\ x_2\oplus 1 \end{bmatrix}, якщо\ k_1=1;\ k_2=0 \\ \begin{bmatrix} x_2\oplus 1 \\ x_1 \end{bmatrix}, якщо\ k_1=1;\ k_2=1\end{cases}=O_{10}^k=\begin{bmatrix} x_1\cdot\bar{k}_2\oplus x_2\cdot k_2 \\ x_1\cdot k_2\oplus x_2\cdot\bar{k}_2 \end{bmatrix}\oplus\begin{bmatrix} \bar{k}_2 \\ k_2 \end{bmatrix} \quad (3.34)$$

Якщо над другим операндом двохоперандної операції строгого криптографічного кодування $O_2^k = \begin{bmatrix} x_1 \cdot \bar{k}_1 \oplus x_2 \cdot k_1 \\ x_1 \cdot k_1 \oplus x_2 \cdot \bar{k}_1 \end{bmatrix} \oplus \begin{bmatrix} k_1 \oplus k_2 \\ \overline{k_1 \oplus k_2} \end{bmatrix}$ виконати одноопераднe криптографічне перетворення $F_{5,9} = \begin{bmatrix} x_2 \\ x_1 \oplus x_2 \oplus 1 \end{bmatrix}$, то буде отримана операція строгого стійкого кодування $O_{11}^k = \begin{bmatrix} x_1 \cdot \bar{k}_2 \oplus x_2 \cdot k_2 \\ x_1 \cdot k_2 \oplus x_2 \cdot \bar{k}_2 \end{bmatrix} \oplus \begin{bmatrix} \bar{k}_1 \\ k_1 \end{bmatrix}$.

Так як:

$$F_{5,9}(O_2^k) = \begin{cases} \begin{bmatrix} x_1 \oplus 1 \\ x_2 \end{bmatrix}, якщо\ k_1 = 0; k_2 = 1 \\ \begin{bmatrix} x_2 \oplus 1 \\ x_1 \end{bmatrix}, якщо\ k_1 = 1; k_2 = 1 \\ \begin{bmatrix} x_1 \\ x_2 \oplus 1 \end{bmatrix}, якщо\ k_1 = 0; k_2 = 0 \\ \begin{bmatrix} x_2 \\ x_1 \oplus 1 \end{bmatrix}, якщо\ k_1 = 1; k_2 = 0 \end{cases} = O_{11}^k = \begin{cases} \begin{bmatrix} x_1 \oplus 1 \\ x_2 \end{bmatrix}, якщо\ k_1 = 0; k_2 = 0 \\ \begin{bmatrix} x_2 \oplus 1 \\ x_1 \end{bmatrix}, якщо\ k_1 = 0; k_2 = 1 \\ \begin{bmatrix} x_1 \\ x_2 \oplus 1 \end{bmatrix}, якщо\ k_1 = 1; k_2 = 0 \\ \begin{bmatrix} x_2 \\ x_1 \oplus 1 \end{bmatrix}, якщо\ k_1 = 1; k_2 = 1 \end{cases} = O_{11}^k = \begin{bmatrix} x_1 \cdot \bar{k}_2 \oplus x_2 \cdot k_2 \\ x_1 \cdot k_2 \oplus x_2 \cdot \bar{k}_2 \end{bmatrix} \oplus \begin{bmatrix} \bar{k}_1 \\ k_1 \end{bmatrix} \quad (3.35)$$

що і потрібно було довести.

Візьмемо наступну одноопераднy операцію $F_{6,12} = \begin{bmatrix} x_1 \oplus x_2 \\ x_1 \oplus 1 \end{bmatrix}$ та виконаємо за допомогою неї перетворення другого операнда двохоперандної операції строгого криптографічного кодування $O_2^k = \begin{bmatrix} x_1 \cdot \bar{k}_1 \oplus x_2 \cdot k_1 \\ x_1 \cdot k_1 \oplus x_2 \cdot \bar{k}_1 \end{bmatrix} \oplus \begin{bmatrix} k_1 \oplus k_2 \\ \overline{k_1 \oplus k_2} \end{bmatrix}$. В результаті буде отримана операція строгого стійкого кодування $O_9^k = \begin{bmatrix} x_1 \cdot (\overline{k_1 \oplus k_2}) \oplus x_2 \cdot (k_1 \oplus k_2) \\ x_1 \cdot (k_1 \oplus k_2) \oplus x_2 \cdot (\overline{k_1 \oplus k_2}) \end{bmatrix} \oplus \begin{bmatrix} \bar{k}_2 \\ k_2 \end{bmatrix}$.

Так як перетворення має наступний вигляд:

$$F_{6,12}(O_2^k) = \begin{cases} \begin{bmatrix} x_1 \oplus 1 \\ x_2 \end{bmatrix}, якщо\ k_1 = 0; k_2 = 1 \\ \begin{bmatrix} x_2 \\ x_1 \oplus 1 \end{bmatrix}, якщо\ k_1 = 1; k_2 = 0 \\ \begin{bmatrix} x_2 \oplus 1 \\ x_1 \end{bmatrix}, якщо\ k_1 = 1; k_2 = 1 \\ \begin{bmatrix} x_1 \\ x_2 \oplus 1 \end{bmatrix}, якщо\ k_1 = 0; k_2 = 0 \end{cases} = O_9^k = \begin{cases} \begin{bmatrix} x_1 \oplus 1 \\ x_2 \end{bmatrix}, якщо\ k_1 = 0; k_2 = 0 \\ \begin{bmatrix} x_2 \\ x_1 \oplus 1 \end{bmatrix}, якщо\ k_1 = 0; k_2 = 1 \\ \begin{bmatrix} x_2 \oplus 1 \\ x_1 \end{bmatrix}, якщо\ k_1 = 1; k_2 = 0 \\ \begin{bmatrix} x_1 \\ x_2 \oplus 1 \end{bmatrix}, якщо\ k_1 = 1; k_2 = 1 \end{cases} = O_9^k = \begin{bmatrix} x_1 \cdot (\overline{k_1 \oplus k_2}) \oplus x_2 \cdot (k_1 \oplus k_2) \\ x_1 \cdot (k_1 \oplus k_2) \oplus x_2 \cdot (\overline{k_1 \oplus k_2}) \end{bmatrix} \oplus \begin{bmatrix} \bar{k}_2 \\ k_2 \end{bmatrix} \quad (3.36)$$

це перетворення показує правильність нашого твердження.

Якщо над другим операндом двохоперандної операції строгого криптографічного кодування $O_2^k = \begin{bmatrix} x_1 \cdot \bar{k}_1 \oplus x_2 \cdot k_1 \\ x_1 \cdot k_1 \oplus x_2 \cdot \bar{k}_1 \end{bmatrix} \oplus \begin{bmatrix} k_1 \oplus k_2 \\ \overline{k_1 \oplus k_2} \end{bmatrix}$ виконати одноопераднe криптографічне перетворення $F_{12,5} = \begin{bmatrix} x_1 \oplus 1 \\ x_2 \end{bmatrix}$ то буде отримана операція строгого стійкого кодування $O_{21}^k = \begin{bmatrix} x_1 \cdot k_1 \oplus x_2 \cdot \bar{k}_1 \\ x_1 \cdot \bar{k}_1 \oplus x_2 \cdot k_1 \end{bmatrix} \oplus \begin{bmatrix} \overline{k_1 \oplus k_2} \\ k_1 \oplus k_2 \end{bmatrix}$.

Отже:

$$F_{12,5}(O_2^k) = \begin{cases} \begin{bmatrix} x_2 \oplus 1 \\ x_1 \end{bmatrix}, \text{якщо } k_1 = 1; k_2 = 1 \\ \begin{bmatrix} x_2 \\ x_1 \oplus 1 \end{bmatrix}, \text{якщо } k_1 = 1; k_2 = 0 \\ \begin{bmatrix} x_1 \\ x_2 \oplus 1 \end{bmatrix}, \text{якщо } k_1 = 0; k_2 = 0 \\ \begin{bmatrix} x_1 \oplus 1 \\ x_2 \end{bmatrix}, \text{якщо } k_1 = 0; k_2 = 1 \end{cases} = O_{21}^k = \begin{cases} \begin{bmatrix} x_2 \oplus 1 \\ x_1 \end{bmatrix}, \text{якщо } k_1 = 0; k_2 = 0 \\ \begin{bmatrix} x_2 \\ x_1 \oplus 1 \end{bmatrix}, \text{якщо } k_1 = 0; k_2 = 1 \\ \begin{bmatrix} x_1 \\ x_2 \oplus 1 \end{bmatrix}, \text{якщо } k_1 = 1; k_2 = 0 \\ \begin{bmatrix} x_1 \oplus 1 \\ x_2 \end{bmatrix}, \text{якщо } k_1 = 1; k_2 = 1 \end{cases} = O_{21}^k = \begin{bmatrix} x_1 \cdot k_1 \oplus x_2 \cdot \bar{k}_1 \\ x_1 \cdot \bar{k}_1 \oplus x_2 \cdot k_1 \end{bmatrix} \oplus \begin{bmatrix} \overline{k_1 \oplus k_2} \\ k_1 \oplus k_2 \end{bmatrix} \quad (3.37)$$

що й потрібно було довести.

Згідно попереднього перетворення проведемо над другим операндом двохоперандної операції строгого криптографічного кодування $O_2^k = \begin{bmatrix} x_1 \cdot \bar{k}_1 \oplus x_2 \cdot k_1 \\ x_1 \cdot k_1 \oplus x_2 \cdot \bar{k}_1 \end{bmatrix} \oplus \begin{bmatrix} k_1 \oplus k_2 \\ \overline{k_1 \oplus k_2} \end{bmatrix}$ одноопераднe криптографічне перетворення $F_{9,5} = \begin{bmatrix} x_1 \oplus x_2 \oplus 1 \\ x_2 \end{bmatrix}$. В результаті буде отримана операція строгого стійкого кодування $O_{20}^k = \begin{bmatrix} x_1 \cdot (k_1 \oplus k_2) \oplus x_2 \cdot (\overline{k_1 \oplus k_2}) \\ x_1 \cdot (\overline{k_1 \oplus k_2}) \oplus x_2 \cdot (k_1 \oplus k_2) \end{bmatrix} \oplus \begin{bmatrix} \bar{k}_1 \\ k_1 \end{bmatrix}$.

Наступне перетворення:

$$F_{9,5}(O_2^k)=\begin{cases}\begin{bmatrix}x_2\oplus 1\\ x_1\end{bmatrix}, якщо\ k_1=1;\ k_2=1\\ \begin{bmatrix}x_1\oplus 1\\ x_2\end{bmatrix}, якщо\ k_1=0;\ k_2=1\\ \begin{bmatrix}x_1\\ x_2\oplus 1\end{bmatrix},\ якщо\ k_1=0;\ k_2=0\\ \begin{bmatrix}x_2\\ x_1\oplus 1\end{bmatrix}, якщо\ k_1=1;\ k_2=0\end{cases}=O_{20}^k=\begin{cases}\begin{bmatrix}x_2\oplus 1\\ x_1\end{bmatrix},\ якщо\ k_1=0;\ k_2=0\\ \begin{bmatrix}x_1\oplus 1\\ x_2\end{bmatrix}, якщо\ k_1=0;\ k_2=1\\ \begin{bmatrix}x_1\\ x_2\oplus 1\end{bmatrix}, якщо\ k_1=1;\ k_2=0\\ \begin{bmatrix}x_2\\ x_1\oplus 1\end{bmatrix}, якщо\ k_1=1;\ k_2=1\end{cases}=O_{20}^k=\begin{bmatrix}x_1\cdot(k_1\oplus k_2)\oplus x_2\cdot\overline{(k_1\oplus k_2)}\\ x_1\cdot\overline{(k_1\oplus k_2)}\oplus x_2\cdot(k_1\oplus k_2)\end{bmatrix}\oplus\begin{bmatrix}\bar{k}_1\\ k_1\end{bmatrix} \quad (3.38)$$

доводить вірність твердження.

При виконанні над другим операндом двохоперандної операції строгого криптографічного кодування $O_2^k=\begin{bmatrix}x_1\cdot\bar{k}_1\oplus x_2\cdot k_1\\ x_1\cdot k_1\oplus x_2\cdot\bar{k}_1\end{bmatrix}\oplus\begin{bmatrix}k_1\oplus k_2\\ \overline{k_1\oplus k_2}\end{bmatrix}$ одноопераднe криптографічне перетворення $F_{12,6}=\begin{bmatrix}x_1\oplus 1\\ x_1\oplus x_2\end{bmatrix}$, буде отримана операція строгого стійкого кодування $O_{22}^k=\begin{bmatrix}x_1\cdot k_1\oplus x_2\cdot\bar{k}_1\\ x_1\cdot\bar{k}_1\oplus x_2\cdot k_1\end{bmatrix}\oplus\begin{bmatrix}\bar{k}_2\\ k_2\end{bmatrix}$.

Так як:

$$F_{12,6}(O_2^k)=\begin{cases}\begin{bmatrix}x_2\oplus 1\\ x_1\end{bmatrix}, якщо\ k_1=1;\ k_2=1\\ \begin{bmatrix}x_2\\ x_1\oplus 1\end{bmatrix}, якщо\ k_1=1;\ k_2=0\\ \begin{bmatrix}x_1\oplus 1\\ x_2\end{bmatrix}, якщо\ k_1=0;\ k_2=1\\ \begin{bmatrix}x_1\\ x_2\oplus 1\end{bmatrix},\ якщо\ k_1=0;\ k_2=0\end{cases}=O_{22}^k=\begin{cases}\begin{bmatrix}x_2\oplus 1\\ x_1\end{bmatrix},\ якщо\ k_1=0;\ k_2=0\\ \begin{bmatrix}x_2\\ x_1\oplus 1\end{bmatrix}, якщо\ k_1=0;\ k_2=1\\ \begin{bmatrix}x_1\oplus 1\\ x_2\end{bmatrix}, якщо\ k_1=1;\ k_2=0\\ \begin{bmatrix}x_1\\ x_2\oplus 1\end{bmatrix}, якщо\ k_1=1;\ k_2=1\end{cases}=O_{22}^k=\begin{bmatrix}x_1\cdot k_1\oplus x_2\cdot\bar{k}_1\\ x_1\cdot\bar{k}_1\oplus x_2\cdot k_1\end{bmatrix}\oplus\begin{bmatrix}\bar{k}_2\\ k_2\end{bmatrix} \quad (3.39)$$

що і потрібно було довести.

Одноопераднe криптографічне перетворення $F_{10,3}=\begin{bmatrix}x_2\oplus 1\\ x_1\end{bmatrix}$**,** при дії на другий операнд двохоперандної операції строгого криптографічного кодування $O_2^k=\begin{bmatrix}x_1\cdot\bar{k}_1\oplus x_2\cdot k_1\\ x_1\cdot k_1\oplus x_2\cdot\bar{k}_1\end{bmatrix}\oplus\begin{bmatrix}k_1\oplus k_2\\ \overline{k_1\oplus k_2}\end{bmatrix}$, дозволяє отримати операцію строгого стійкого кодування $O_{24}^k=\begin{bmatrix}x_1\cdot k_2\oplus x_2\cdot\bar{k}_2\\ x_1\cdot\bar{k}_2\oplus x_2\cdot k_2\end{bmatrix}\oplus\begin{bmatrix}\overline{k_1\oplus k_2}\\ k_1\oplus k_2\end{bmatrix}$.

Так як:

$$F_{10,3}(O_2^k)=\begin{cases}\begin{bmatrix}x_2\oplus 1\\ x_1\end{bmatrix}, якщо\ k_1=1;\ k_2=1\\ \begin{bmatrix}x_1\\ x_2\oplus 1\end{bmatrix}, якщо\ k_1=0;\ k_2=0\\ \begin{bmatrix}x_2\\ x_1\oplus 1\end{bmatrix}, якщо\ k_1=1;\ k_2=0\\ \begin{bmatrix}x_1\oplus 1\\ x_2\end{bmatrix}, якщо\ k_1=0;\ k_2=1\end{cases}=O_{24}^k=\begin{cases}\begin{bmatrix}x_2\oplus 1\\ x_1\end{bmatrix}, якщо\ k_1=0;\ k_2=0\\ \begin{bmatrix}x_1\\ x_2\oplus 1\end{bmatrix}, якщо\ k_1=0;\ k_2=1\\ \begin{bmatrix}x_2\\ x_1\oplus 1\end{bmatrix}, якщо\ k_1=1;\ k_2=0\\ \begin{bmatrix}x_1\oplus 1\\ x_2\end{bmatrix}, якщо\ k_1=1;\ k_2=1\end{cases}=O_{24}^k=\begin{bmatrix}x_1\cdot k_2\oplus x_2\cdot\bar{k}_2\\ x_1\cdot\bar{k}_2\oplus x_2\cdot k_2\end{bmatrix}\oplus\begin{bmatrix}\overline{k_1\oplus k_2}\\ k_1\oplus k_2\end{bmatrix} \quad (3.40)$$

це дозволяє показати вірність нашого твердження.

Якщо над другим операндом двохоперандної операції строгого стійкого криптографічного кодування $O_2^k=\begin{bmatrix}x_1\cdot\bar{k}_1\oplus x_2\cdot k_1\\ x_1\cdot k_1\oplus x_2\cdot\bar{k}_1\end{bmatrix}\oplus\begin{bmatrix}k_1\oplus k_2\\ \overline{k_1\oplus k_2}\end{bmatrix}$ виконати одноопераднe криптографічне перетворення $F_{10,6}=\begin{bmatrix}x_2\oplus 1\\ x_1\oplus x_2\end{bmatrix}$,то в результаті буде отримана операція строгого стійкого кодування $O_{19}^k=\begin{bmatrix}x_1\cdot\bar{k}_2\oplus x_2\cdot k_2\\ x_1\cdot k_2\oplus x_2\cdot\bar{k}_2\end{bmatrix}\oplus\begin{bmatrix}k_1\\ \bar{k}_1\end{bmatrix}$.

Вигляд даного перетворення буде наступним:

$$F_{10,6}(O_2^k)=\begin{cases}\begin{bmatrix}x_2\oplus 1\\ x_1\end{bmatrix}, якщо\ k_1=1;\ k_2=1\\ \begin{bmatrix}x_1\oplus 1\\ x_2\end{bmatrix}, якщо\ k_1=0;\ k_2=1\\ \begin{bmatrix}x_2\\ x_1\oplus 1\end{bmatrix}, якщо\ k_1=1;\ k_2=0\\ \begin{bmatrix}x_1\\ x_2\oplus 1\end{bmatrix}, якщо\ k_1=0;\ k_2=0\end{cases}=O_{19}^k=\begin{cases}\begin{bmatrix}x_2\oplus 1\\ x_1\end{bmatrix}, якщо\ k_1=0;\ k_2=0\\ \begin{bmatrix}x_1\oplus 1\\ x_2\end{bmatrix}, якщо\ k_1=0;\ k_2=1\\ \begin{bmatrix}x_2\\ x_1\oplus 1\end{bmatrix}, якщо\ k_1=1;\ k_2=0\\ \begin{bmatrix}x_1\\ x_2\oplus 1\end{bmatrix}, якщо\ k_1=1;\ k_2=1\end{cases}=O_{19}^k=\begin{bmatrix}x_1\cdot\bar{k}_2\oplus x_2\cdot k_2\\ x_1\cdot k_2\oplus x_2\cdot\bar{k}_2\end{bmatrix}\oplus\begin{bmatrix}k_1\\ \bar{k}_1\end{bmatrix} \quad (3.41)$$

що і потрібно було довести.

У разі виконання одноопераднoго криптографічного перетворення $F_{9,3}=\begin{bmatrix}x_1\oplus x_2\oplus 1\\ x_1\end{bmatrix}$ над другим операндом двохоперандної операції строгого криптографічного кодування $O_2^k=\begin{bmatrix}x_1\cdot\bar{k}_1\oplus x_2\cdot k_1\\ x_1\cdot k_1\oplus x_2\cdot\bar{k}_1\end{bmatrix}\oplus\begin{bmatrix}k_1\oplus k_2\\ \overline{k_1\oplus k_2}\end{bmatrix}$, отримуємо операцію

строгого стійкого криптографічного кодування $O_{23}^k = \begin{bmatrix} x_1 \cdot (k_1 \oplus k_2) \oplus x_2 \cdot (\overline{k_1 \oplus k_2}) \\ x_1 \cdot (\overline{k_1 \oplus k_2}) \oplus x_2 \cdot (k_1 \oplus k_2) \end{bmatrix} \oplus \begin{bmatrix} \bar{k}_2 \\ k_2 \end{bmatrix}$.

Так як:

$$F_{9,3}(O_2^k) = \begin{cases} \begin{bmatrix} x_2 \oplus 1 \\ x_1 \end{bmatrix}, \text{якщо } k_1 = 1; k_2 = 1 \\ \begin{bmatrix} x_1 \\ x_2 \oplus 1 \end{bmatrix}, \text{ якщо } k_1 = 0; k_2 = 0 \\ \begin{bmatrix} x_1 \oplus 1 \\ x_2 \end{bmatrix}, \text{якщо } k_1 = 0; k_2 = 1 \\ \begin{bmatrix} x_2 \\ x_1 \oplus 1 \end{bmatrix}, \text{ якщо } k_1 = 1; k_2 = 0 \end{cases} = O_{23}^k = \begin{cases} \begin{bmatrix} x_2 \oplus 1 \\ x_1 \end{bmatrix}, \text{ якщо } k_1 = 0; k_2 = 0 \\ \begin{bmatrix} x_1 \\ x_2 \oplus 1 \end{bmatrix}, \text{якщо } k_1 = 0; k_2 = 1 \\ \begin{bmatrix} x_1 \oplus 1 \\ x_2 \end{bmatrix}, \text{ якщо } k_1 = 1; k_2 = 0 \\ \begin{bmatrix} x_2 \\ x_1 \oplus 1 \end{bmatrix}, \text{якщо } k_1 = 1; k_2 = 1 \end{cases} = O_{23}^k = \begin{bmatrix} x_1 \cdot (k_1 \oplus k_2) \oplus x_2 \cdot (\overline{k_1 \oplus k_2}) \\ x_1 \cdot (\overline{k_1 \oplus k_2}) \oplus x_2 \cdot (k_1 \oplus k_2) \end{bmatrix} \oplus \begin{bmatrix} \bar{k}_2 \\ k_2 \end{bmatrix} \quad (3.42)$$

це доводить твердження.

Якщо над другим операндом двохоперандної операції строгого криптографічного кодування $O_2^k = \begin{bmatrix} x_1 \cdot \bar{k}_1 \oplus x_2 \cdot k_1 \\ x_1 \cdot k_1 \oplus x_2 \cdot \bar{k}_1 \end{bmatrix} \oplus \begin{bmatrix} k_1 \oplus k_2 \\ \overline{k_1 \oplus k_2} \end{bmatrix}$ виконати одноопераднe криптографічне перетворення $F_{12,10} = \begin{bmatrix} x_1 \oplus 1 \\ x_2 \oplus 1 \end{bmatrix}$ то буде отримана операція строгого стійкого кодування $O_{17}^k = \begin{bmatrix} x_1 \cdot k_1 \oplus x_2 \cdot \bar{k}_1 \\ x_1 \cdot \bar{k}_1 \oplus x_2 \cdot k_1 \end{bmatrix} \oplus \begin{bmatrix} k_1 \oplus k_2 \\ \overline{k_1 \oplus k_2} \end{bmatrix}$.

Так як:

$$F_{12,10}(O_2^k) = \begin{cases} \begin{bmatrix} x_2 \\ x_1 \oplus 1 \end{bmatrix}, \text{ якщо } k_1 = 1; k_2 = 0 \\ \begin{bmatrix} x_2 \oplus 1 \\ x_1 \end{bmatrix}, \text{якщо } k_1 = 1; k_2 = 1 \\ \begin{bmatrix} x_1 \oplus 1 \\ x_2 \end{bmatrix}, \text{якщо } k_1 = 0; k_2 = 1 \\ \begin{bmatrix} x_1 \\ x_2 \oplus 1 \end{bmatrix}, \text{ якщо } k_1 = 0; k_2 = 0 \end{cases} = O_{17}^k = \begin{cases} \begin{bmatrix} x_2 \\ x_1 \oplus 1 \end{bmatrix}, \text{ якщо } k_1 = 0; k_2 = 0 \\ \begin{bmatrix} x_2 \oplus 1 \\ x_1 \end{bmatrix}, \text{якщо } k_1 = 0; k_2 = 1 \\ \begin{bmatrix} x_1 \oplus 1 \\ x_2 \end{bmatrix}, \text{ якщо } k_1 = 1; k_2 = 0 \\ \begin{bmatrix} x_1 \\ x_2 \oplus 1 \end{bmatrix}, \text{якщо } k_1 = 1; k_2 = 1 \end{cases} = O_{17}^k = \begin{bmatrix} x_1 \cdot k_1 \oplus x_2 \cdot \bar{k}_1 \\ x_1 \cdot \bar{k}_1 \oplus x_2 \cdot k_1 \end{bmatrix} \oplus \begin{bmatrix} k_1 \oplus k_2 \\ \overline{k_1 \oplus k_2} \end{bmatrix} \quad (3.43)$$

що і потрібно було довести.

Виконавши над другим операндом двохоперандної операції строгого криптографічного кодування $O_2^k = \begin{bmatrix} x_1 \cdot \bar{k}_1 \oplus x_2 \cdot k_1 \\ x_1 \cdot k_1 \oplus x_2 \cdot \bar{k}_1 \end{bmatrix} \oplus \begin{bmatrix} k_1 \oplus k_2 \\ \overline{k_1 \oplus k_2} \end{bmatrix}$ одноопераднe

криптографічне перетворення $F_{9,10}=\begin{bmatrix} x_1 \oplus x_2 \oplus 1 \\ x_2 \oplus 1 \end{bmatrix}$,в результаті буде отримана операція строгого стійкого криптографічного кодування $O_{16}^{k}=\begin{bmatrix} x_1 \cdot (k_1 \oplus k_2) \oplus x_2 \cdot (\overline{k_1 \oplus k_2}) \\ x_1 \cdot (\overline{k_1 \oplus k_2}) \oplus x_2 \cdot (k_1 \oplus k_2) \end{bmatrix} \oplus \begin{bmatrix} k_1 \\ \bar{k}_1 \end{bmatrix}$.

Так як:

$$F_{9,10}(O_2^k)=\begin{cases} \begin{bmatrix} x_2 \\ x_1 \oplus 1 \end{bmatrix}, \text{якщо } k_1=1; k_2=0 \\ \begin{bmatrix} x_1 \\ x_2 \oplus 1 \end{bmatrix}, \text{якщо } k_1=0; k_2=0 \\ \begin{bmatrix} x_1 \oplus 1 \\ x_2 \end{bmatrix}, \text{якщо } k_1=0; k_2=1 \\ \begin{bmatrix} x_2 \oplus 1 \\ x_1 \end{bmatrix}, \text{якщо } k_1=1; k_2=1 \end{cases} = O_{16}^{k} = \begin{cases} \begin{bmatrix} x_2 \\ x_1 \oplus 1 \end{bmatrix}, \text{якщо } k_1=0; k_2=0 \\ \begin{bmatrix} x_1 \\ x_2 \oplus 1 \end{bmatrix}, \text{якщо } k_1=0; k_2=1 \\ \begin{bmatrix} x_1 \oplus 1 \\ x_2 \end{bmatrix}, \text{якщо } k_1=1; k_2=0 \\ \begin{bmatrix} x_2 \oplus 1 \\ x_1 \end{bmatrix}, \text{якщо } k_1=1; k_2=1 \end{cases} = O_{16}^{k}=\begin{bmatrix} x_1 \cdot (k_1 \oplus k_2) \oplus x_2 \cdot (\overline{k_1 \oplus k_2}) \\ x_1 \cdot (\overline{k_1 \oplus k_2}) \oplus x_2 \cdot (k_1 \oplus k_2) \end{bmatrix} \oplus \begin{bmatrix} k_1 \\ \bar{k}_1 \end{bmatrix} \quad (3.44)$$

що і потрібно було довести.

У випадку, коли над другим операндом двохоперандної операції строгого криптографічного кодування $O_2^k=\begin{bmatrix} x_1 \cdot \bar{k}_1 \oplus x_2 \cdot k_1 \\ x_1 \cdot k_1 \oplus x_2 \cdot \bar{k}_1 \end{bmatrix} \oplus \begin{bmatrix} k_1 \oplus k_2 \\ \overline{k_1 \oplus k_2} \end{bmatrix}$ виконати одноопераднe криптографічне перетворення $F_{12,9}=\begin{bmatrix} x_1 \oplus 1 \\ x_1 \oplus x_2 \oplus 1 \end{bmatrix}$, буде отримана операція строгого стійкого кодування $O_{18}^{k}=\begin{bmatrix} x_1 \cdot k_1 \oplus x_2 \cdot \bar{k}_1 \\ x_1 \cdot \bar{k}_1 \oplus x_2 \cdot k_1 \end{bmatrix} \oplus \begin{bmatrix} k_2 \\ \bar{k}_2 \end{bmatrix}$.

Так як:

$$F_{12,9}(O_2^k)=\begin{cases} \begin{bmatrix} x_2 \\ x_1 \oplus 1 \end{bmatrix}, \text{якщо } k_1=1; k_2=0 \\ \begin{bmatrix} x_2 \oplus 1 \\ x_1 \end{bmatrix}, \text{якщо } k_1=1; k_2=1 \\ \begin{bmatrix} x_1 \\ x_2 \oplus 1 \end{bmatrix}, \text{якщо } k_1=0; k_2=0 \\ \begin{bmatrix} x_1 \oplus 1 \\ x_2 \end{bmatrix}, \text{якщо } k_1=0; k_2=1 \end{cases} = O_{18}^{k} = \begin{cases} \begin{bmatrix} x_2 \\ x_1 \oplus 1 \end{bmatrix}, \text{якщо } k_1=0; k_2=0 \\ \begin{bmatrix} x_2 \oplus 1 \\ x_1 \end{bmatrix}, \text{якщо } k_1=0; k_2=1 \\ \begin{bmatrix} x_1 \\ x_2 \oplus 1 \end{bmatrix}, \text{якщо } k_1=1; k_2=0 \\ \begin{bmatrix} x_1 \oplus 1 \\ x_2 \end{bmatrix}, \text{якщо } k_1=1; k_2=1 \end{cases} = O_{18}^{k}=\begin{bmatrix} x_1 \cdot k_1 \oplus x_2 \cdot \bar{k}_1 \\ x_1 \cdot \bar{k}_1 \oplus x_2 \cdot k_1 \end{bmatrix} \oplus \begin{bmatrix} k_2 \\ \bar{k}_2 \end{bmatrix} \quad (3.45)$$

що й доведено.

При виконанні над другим операндом двохоперандної операції строгого криптографічного кодування $O_2^k = \begin{bmatrix} x_1 \cdot \bar{k}_1 \oplus x_2 \cdot k_1 \\ x_1 \cdot k_1 \oplus x_2 \cdot \bar{k}_1 \end{bmatrix} \oplus \begin{bmatrix} k_1 \oplus k_2 \\ \overline{k_1 \oplus k_2} \end{bmatrix}$ одноопераднe криптографічне перетворення $F_{10,12} = \begin{bmatrix} x_2 \oplus 1 \\ x_1 \oplus 1 \end{bmatrix}$, отримана операція строгого стійкого кодування $O_{14}^k = \begin{bmatrix} x_1 \cdot k_2 \oplus x_2 \cdot \bar{k}_2 \\ x_1 \cdot \bar{k}_2 \oplus x_2 \cdot k_2 \end{bmatrix} \oplus \begin{bmatrix} k_2 \\ \bar{k}_2 \end{bmatrix}$.

Так як:

$$F_{10,12}(O_2^k) = \begin{cases} \begin{bmatrix} x_2 \\ x_1 \oplus 1 \end{bmatrix}, \text{якщо } k_1 = 1; k_2 = 0 \\ \begin{bmatrix} x_1 \oplus 1 \\ x_2 \end{bmatrix}, \text{якщо } k_1 = 0; k_2 = 1 \\ \begin{bmatrix} x_2 \oplus 1 \\ x_1 \end{bmatrix}, \text{якщо } k_1 = 1; k_2 = 1 \\ \begin{bmatrix} x_1 \\ x_2 \oplus 1 \end{bmatrix}, \text{якщо } k_1 = 0; k_2 = 0 \end{cases} = O_{14}^k = \begin{cases} \begin{bmatrix} x_2 \\ x_1 \oplus 1 \end{bmatrix}, \text{якщо } k_1 = 0; k_2 = 0 \\ \begin{bmatrix} x_1 \oplus 1 \\ x_2 \end{bmatrix}, \text{якщо } k_1 = 0; k_2 = 1 \\ \begin{bmatrix} x_2 \oplus 1 \\ x_1 \end{bmatrix}, \text{якщо } k_1 = 1; k_2 = 0 \\ \begin{bmatrix} x_1 \\ x_2 \oplus 1 \end{bmatrix}, \text{якщо } k_1 = 1; k_2 = 1 \end{cases} = O_{14}^k = \begin{bmatrix} x_1 \cdot k_2 \oplus x_2 \cdot \bar{k}_2 \\ x_1 \cdot \bar{k}_2 \oplus x_2 \cdot k_2 \end{bmatrix} \oplus \begin{bmatrix} k_2 \\ \bar{k}_2 \end{bmatrix} \quad (3.46)$$

що і потрібно було довести.

Якщо над другим операндом двохоперандної операції строгого криптографічного кодування $O_2^k = \begin{bmatrix} x_1 \cdot \bar{k}_1 \oplus x_2 \cdot k_1 \\ x_1 \cdot k_1 \oplus x_2 \cdot \bar{k}_1 \end{bmatrix} \oplus \begin{bmatrix} k_1 \oplus k_2 \\ \overline{k_1 \oplus k_2} \end{bmatrix}$ виконати одноопераднe криптографічне перетворення $F_{10,9} = \begin{bmatrix} x_2 \oplus 1 \\ x_1 \oplus x_2 \oplus 1 \end{bmatrix}$, то буде отримана операція строгого стійкого кодування $O_{15}^k = \begin{bmatrix} x_1 \cdot k_2 \oplus x_2 \cdot \bar{k}_2 \\ x_1 \cdot \bar{k}_2 \oplus x_2 \cdot k_2 \end{bmatrix} \oplus \begin{bmatrix} k_1 \\ \bar{k}_1 \end{bmatrix}$.

Тобто перетворення виглядатиме наступним чином:

$$F_{10,9}(O_2^k)=\begin{cases}\begin{bmatrix}x_2\\x_1\oplus 1\end{bmatrix}, \text{якщо } k_1=1;\ k_2=0\\ \begin{bmatrix}x_1\\x_2\oplus 1\end{bmatrix}, \text{ якщо } k_1=0;\ k_2=0\\ \begin{bmatrix}x_2\oplus 1\\x_1\end{bmatrix}, \text{якщо } k_1=1;\ k_2=1\\ \begin{bmatrix}x_1\oplus 1\\x_2\end{bmatrix}, \text{якщо } k_1=0;\ k_2=1\end{cases}=O_{15}^k=\begin{cases}\begin{bmatrix}x_2\\x_1\oplus 1\end{bmatrix}, \text{ якщо } k_1=0;\ k_2=0\\ \begin{bmatrix}x_1\\x_2\oplus 1\end{bmatrix}, \text{якщо } k_1=0;\ k_2=1\\ \begin{bmatrix}x_2\oplus 1\\x_1\end{bmatrix}, \text{ якщо } k_1=1;\ k_2=0\\ \begin{bmatrix}x_1\oplus 1\\x_2\end{bmatrix}, \text{якщо } k_1=1;\ k_2=1\end{cases}=O_{15}^k=\begin{bmatrix}x_1\cdot k_2\oplus x_2\cdot\bar{k}_2\\ x_1\cdot\bar{k}_2\oplus x_2\cdot k_2\end{bmatrix}\oplus\begin{bmatrix}k_1\\\bar{k}_1\end{bmatrix} \quad (3.47)$$

зокрема, саме це й необхідно було довести.

Якщо над другим операндом двохоперандної операції строгого криптографічного кодування $O_2^k=\begin{bmatrix}x_1\cdot\bar{k}_1\oplus x_2\cdot k_1\\ x_1\cdot k_1\oplus x_2\cdot\bar{k}_1\end{bmatrix}\oplus\begin{bmatrix}k_1\oplus k_2\\ \overline{k_1\oplus k_2}\end{bmatrix}$ виконати одноопераднe криптографічне перетворення $F=\begin{bmatrix}x_1\oplus x_2\oplus 1\\ x_1\oplus 1\end{bmatrix}$, то буде отримана операція строгого стійкого кодування $O_{13}^k=\begin{bmatrix}x_1\cdot(k_1\oplus k_2)\oplus x_2\cdot(\overline{k_1\oplus k_2})\\ x_1\cdot(\overline{k_1\oplus k_2})\oplus x_2\cdot(k_1\oplus k_2)\end{bmatrix}\oplus\begin{bmatrix}k_2\\\bar{k}_2\end{bmatrix}$.

Перетворення набуває наступного вигляду:

$$F_{9,12}(O_2^k)=\begin{cases}\begin{bmatrix}x_2\\x_1\oplus 1\end{bmatrix}, \text{якщо } k_1=1;\ k_2=0\\ \begin{bmatrix}x_1\oplus 1\\x_2\end{bmatrix}, \text{якщо } k_1=0;\ k_2=1\\ \begin{bmatrix}x_1\\x_2\oplus 1\end{bmatrix}, \text{якщо } k_1=0;\ k_2=0\\ \begin{bmatrix}x_2\oplus 1\\x_1\end{bmatrix}, \text{якщо } k_1=1;\ k_2=1\end{cases}=O_{13}^k=\begin{cases}\begin{bmatrix}x_2\\x_1\oplus 1\end{bmatrix}, \text{якщо } k_1=0;\ k_2=0\\ \begin{bmatrix}x_1\oplus 1\\x_2\end{bmatrix}, \text{якщо } k_1=0;\ k_2=1\\ \begin{bmatrix}x_1\\x_2\oplus 1\end{bmatrix}, \text{якщо } k_1=1;\ k_2=0\\ \begin{bmatrix}x_2\oplus 1\\x_1\end{bmatrix}, \text{якщо } k_1=1;\ k_2=1\end{cases}=O_{13}^k=\begin{bmatrix}x_1\cdot(k_1\oplus k_2)\oplus x_2\cdot(\overline{k_1\oplus k_2})\\ x_1\cdot(\overline{k_1\oplus k_2})\oplus x_2\cdot(k_1\oplus k_2)\end{bmatrix}\oplus\begin{bmatrix}k_2\\\bar{k}_2\end{bmatrix} \quad (3.48)$$

що показує правильність доведення.

Даний процес синтезу групи двохрозрядних двохопераднихоперацій строгого криптографічного кодування показує, що з операції $O_2^k=\begin{bmatrix}x_1\cdot\bar{k}_1\oplus x_2\cdot k_1\\ x_1\cdot k_1\oplus x_2\cdot\bar{k}_1\end{bmatrix}\oplus\begin{bmatrix}k_1\oplus k_2\\ \overline{k_1\oplus k_2}\end{bmatrix}$ можна отримати повну групу операцій, при дії на другий операнд двохрозрядною одноопераднoю операцією шляхом перестановки.

3.3 Синтез групи двохрозрядних двохоперандних операцій строгого криптографічного кодування на основі третьої операції

Якщо над другим операндом двохоперандної операції строгого криптографічного кодування $O_3^k = \begin{bmatrix} x_1 \cdot (\overline{k_1 \oplus k_2}) \oplus x_2 \cdot (k_1 \oplus k_2) \\ x_1 \cdot (k_1 \oplus k_2) \oplus x_2 \cdot (\overline{k_1 \oplus k_2}) \end{bmatrix} \oplus \begin{bmatrix} k_1 \\ \bar{k}_1 \end{bmatrix}$ виконати одноопераднe криптографічне перетворення $F_{3,5} = \begin{bmatrix} x_1 \\ x_2 \end{bmatrix}$, то буде отримана операція строгого стійкого кодування $O_3^k = \begin{bmatrix} x_1 \cdot (\overline{k_1 \oplus k_2}) \oplus x_2 \cdot (k_1 \oplus k_2) \\ x_1 \cdot (k_1 \oplus k_2) \oplus x_2 \cdot (\overline{k_1 \oplus k_2}) \end{bmatrix} \oplus \begin{bmatrix} k_1 \\ \bar{k}_1 \end{bmatrix}$.

Оскільки криптографічне перетворення матиме наступний вигляд:

$$F_{3,5}(O_3^k) = \begin{cases} \begin{bmatrix} x_1 \\ x_2 \oplus 1 \end{bmatrix}, якщо\ k_1 = 0; k_2 = 0 \\ \begin{bmatrix} x_2 \\ x_1 \oplus 1 \end{bmatrix}, якщо\ k_1 = 0; k_2 = 1 \\ \begin{bmatrix} x_2 \oplus 1 \\ x_1 \end{bmatrix}, якщо\ k_1 = 1; k_2 = 0 \\ \begin{bmatrix} x_1 \oplus 1 \\ x_2 \end{bmatrix}, якщо\ k_1 = 1; k_2 = 1 \end{cases} = O_3^k = \begin{cases} \begin{bmatrix} x_1 \\ x_2 \oplus 1 \end{bmatrix}, якщо\ k_1 = 0; k_2 = 0 \\ \begin{bmatrix} x_2 \\ x_1 \oplus 1 \end{bmatrix}, якщо\ k_1 = 0; k_2 = 1 \\ \begin{bmatrix} x_2 \oplus 1 \\ x_1 \end{bmatrix}, якщо\ k_1 = 1; k_2 = 0 \\ \begin{bmatrix} x_1 \oplus 1 \\ x_2 \end{bmatrix}, якщо\ k_1 = 1; k_2 = 1 \end{cases} = O_3^k = \begin{bmatrix} x_1 \cdot (\overline{k_1 \oplus k_2}) \oplus x_2 \cdot (k_1 \oplus k_2) \\ x_1 \cdot (k_1 \oplus k_2) \oplus x_2 \cdot (\overline{k_1 \oplus k_2}) \end{bmatrix} \oplus \begin{bmatrix} k_1 \\ \bar{k}_1 \end{bmatrix} \quad (3.49)$$

це підтверджує, що наше твердження вірне.

Якщо над другим операндом двохоперандної операції строгого криптографічного кодування $O_3^k = \begin{bmatrix} x_1 \cdot (\overline{k_1 \oplus k_2}) \oplus x_2 \cdot (k_1 \oplus k_2) \\ x_1 \cdot (k_1 \oplus k_2) \oplus x_2 \cdot (\overline{k_1 \oplus k_2}) \end{bmatrix} \oplus \begin{bmatrix} k_1 \\ \bar{k}_1 \end{bmatrix}$ виконати одноопераднe криптографічне перетворення $F_{6,5} = \begin{bmatrix} x_1 \oplus x_2 \\ x_2 \end{bmatrix}$, то буде отримана операція строгого стійкого кодування $O_{13}^k = \begin{bmatrix} x_1 \cdot (k_1 \oplus k_2) \oplus x_2 \cdot (\overline{k_1 \oplus k_2}) \\ x_1 \cdot (\overline{k_1 \oplus k_2}) \oplus x_2 \cdot (k_1 \oplus k_2) \end{bmatrix} \oplus \begin{bmatrix} k_2 \\ \bar{k}_2 \end{bmatrix}$.

Так як:

$$F_{6,5}(O_3^k)=\begin{cases}\begin{bmatrix}x_1\\ x_2\oplus 1\end{bmatrix}, якщо\ k_1=0;\ k_2=0\\ \begin{bmatrix}x_1\oplus 1\\ x_2\end{bmatrix}, якщо\ k_1=1;\ k_2=1\\ \begin{bmatrix}x_2\oplus 1\\ x_1\end{bmatrix}, якщо\ k_1=1;\ k_2=0\\ \begin{bmatrix}x_2\\ x_1\oplus 1\end{bmatrix}, якщо\ k_1=0;\ k_2=1\end{cases}=O_2^k=\begin{cases}\begin{bmatrix}x_1\\ x_2\oplus 1\end{bmatrix}, якщо\ k_1=0;\ k_2=0\\ \begin{bmatrix}x_1\oplus 1\\ x_2\end{bmatrix}, якщо\ k_1=0;\ k_2=1\\ \begin{bmatrix}x_2\oplus 1\\ x_1\end{bmatrix}, якщо\ k_1=1;\ k_2=0\\ \begin{bmatrix}x_2\\ x_1\oplus 1\end{bmatrix}, якщо\ k_1=1;\ k_2=1\end{cases}=O_2^k=\begin{bmatrix}x_1\cdot\bar{k}_1\oplus x_2\cdot k_1\\ x_1\cdot k_1\oplus x_2\cdot\bar{k}_1\end{bmatrix}\oplus\begin{bmatrix}k_1\oplus k_2\\ \overline{k_1\oplus k_2}\end{bmatrix} \quad (3.50)$$

що і потрібно було довести.

Якщо над другим операндом двохрозрядної двохоперандної операції строгого криптографічного кодування $O_3^k=\begin{bmatrix}x_1\cdot(\overline{k_1\oplus k_2})\oplus x_2\cdot(k_1\oplus k_2)\\ x_1\cdot(k_1\oplus k_2)\oplus x_2\cdot(\overline{k_1\oplus k_2})\end{bmatrix}\oplus\begin{bmatrix}k_1\\ \bar{k}_1\end{bmatrix}$ виконати одноопераднe криптографічне перетворення $F_{3,6}=\begin{bmatrix}x_1\\ x_1\oplus x_2\end{bmatrix}$, то буде отримана операція строгого стійкого кодування $O_4^k=\begin{bmatrix}x_1\cdot\bar{k}_2\oplus x_2\cdot k_2\\ x_1\cdot k_2\oplus x_2\cdot\bar{k}_2\end{bmatrix}\oplus\begin{bmatrix}k_1\\ \bar{k}_1\end{bmatrix}$.

Так як:

$$F_{3,6}(O_3^k)=\begin{cases}\begin{bmatrix}x_1\\ x_2\oplus 1\end{bmatrix}, якщо\ k_1=0;\ k_2=0\\ \begin{bmatrix}x_2\\ x_1\oplus 1\end{bmatrix}, якщо\ k_1=0;\ k_2=1\\ \begin{bmatrix}x_1\oplus 1\\ x_2\end{bmatrix}, якщо\ k_1=1;\ k_2=1\\ \begin{bmatrix}x_2\oplus 1\\ x_1\end{bmatrix}, якщо\ k_1=1;\ k_2=0\end{cases}=O_4^k=\begin{cases}\begin{bmatrix}x_1\\ x_2\oplus 1\end{bmatrix}, якщо\ k_1=0;\ k_2=0\\ \begin{bmatrix}x_2\\ x_1\oplus 1\end{bmatrix}, якщо\ k_1=0;\ k_2=1\\ \begin{bmatrix}x_1\oplus 1\\ x_2\end{bmatrix}, якщо\ k_1=1;\ k_2=0\\ \begin{bmatrix}x_2\oplus 1\\ x_1\end{bmatrix}, якщо\ k_1=1;\ k_2=1\end{cases}=O_4^k=\begin{bmatrix}x_1\cdot\bar{k}_2\oplus x_2\cdot k_2\\ x_1\cdot k_2\oplus x_2\cdot\bar{k}_2\end{bmatrix}\oplus\begin{bmatrix}k_1\\ \bar{k}_1\end{bmatrix} \quad (3.51)$$

що і потрібно було довести.

Якщо над другим операндом двохоперандної операції строгого криптографічного кодування $O_3^k=\begin{bmatrix}x_1\cdot(\overline{k_1\oplus k_2})\oplus x_2\cdot(k_1\oplus k_2)\\ x_1\cdot(k_1\oplus k_2)\oplus x_2\cdot(\overline{k_1\oplus k_2})\end{bmatrix}\oplus\begin{bmatrix}k_1\\ \bar{k}_1\end{bmatrix}$ виконати одноопераднe криптографічне перетворення $F_{5,3}=\begin{bmatrix}x_2\\ x_1\end{bmatrix}$, то буде отримана операція строгого стійкого кодування $O_6^k=\begin{bmatrix}x_1\cdot(\overline{k_1\oplus k_2})\oplus x_2\cdot(k_1\oplus k_2)\\ x_1\cdot(k_1\oplus k_2)\oplus x_2\cdot(\overline{k_1\oplus k_2})\end{bmatrix}\oplus\begin{bmatrix}k_2\\ \bar{k}_2\end{bmatrix}$.

Так як:

$$F_{5,3}(O_3^k)=\begin{cases}\begin{bmatrix}x_1\\x_2\oplus 1\end{bmatrix}, якщо\ k_1=0;k_2=0\\ \begin{bmatrix}x_2\oplus 1\\x_1\end{bmatrix}, якщо\ k_1=1;k_2=0\\ \begin{bmatrix}x_2\\x_1\oplus 1\end{bmatrix}, якщо\ k_1=0;k_2=1\\ \begin{bmatrix}x_1\oplus 1\\x_2\end{bmatrix}, якщо\ k_1=1;k_2=1\end{cases}=O_6^k=\begin{cases}\begin{bmatrix}x_1\\x_2\oplus 1\end{bmatrix}, якщо\ k_1=0;k_2=0\\ \begin{bmatrix}x_2\oplus 1\\x_1\end{bmatrix}, якщо\ k_1=0;k_2=1\\ \begin{bmatrix}x_2\\x_1\oplus 1\end{bmatrix}, якщо\ k_1=1;k_2=0\\ \begin{bmatrix}x_1\oplus 1\\x_2\end{bmatrix}, якщо\ k_1=1;k_2=1\end{cases}=O_6^k=\begin{bmatrix}x_1\cdot(\overline{k_1\oplus k_2})\oplus x_2\cdot(k_1\oplus k_2)\\ x_1\cdot(k_1\oplus k_2)\oplus x_2\cdot(\overline{k_1\oplus k_2})\end{bmatrix}\oplus\begin{bmatrix}k_2\\\bar{k}_2\end{bmatrix} \quad (3.52)$$

що і доводить вірність отриманого результату.

По аналогії виконаємо над другим операндом двохоперандної операції строгого криптографічного кодування $O_3^k=\begin{bmatrix}x_1\cdot(\overline{k_1\oplus k_2})\oplus x_2\cdot(k_1\oplus k_2)\\ x_1\cdot(k_1\oplus k_2)\oplus x_2\cdot(\overline{k_1\oplus k_2})\end{bmatrix}\oplus\begin{bmatrix}k_1\\\bar{k}_1\end{bmatrix}$ виконати одноопераднe криптографічне перетворення $F_{5,6}=\begin{bmatrix}x_2\\x_1\oplus x_2\end{bmatrix}$, то буде отримана операція строгого стійкого кодування $O_1^k=\begin{bmatrix}x_1\cdot\bar{k}_1\oplus x_2\cdot k_1\\ x_1\cdot k_1\oplus x_2\cdot\bar{k}_1\end{bmatrix}\oplus\begin{bmatrix}k_2\\\bar{k}_2\end{bmatrix}$.

Перетворення операції виглядає наступним чином:

$$F_{5,6}(O_3^k)=\begin{cases}\begin{bmatrix}x_1\\x_2\oplus 1\end{bmatrix}, якщо\ k_1=0;k_2=0\\ \begin{bmatrix}x_1\oplus 1\\x_2\end{bmatrix}, якщо\ k_1=1;k_2=1\\ \begin{bmatrix}x_2\\x_1\oplus 1\end{bmatrix}, якщо\ k_1=0;k_2=1\\ \begin{bmatrix}x_2\oplus 1\\x_1\end{bmatrix}, якщо\ k_1=1;k_2=0\end{cases}=O_1^k=\begin{cases}\begin{bmatrix}x_1\\x_2\oplus 1\end{bmatrix}, якщо\ k_1=0;k_2=0\\ \begin{bmatrix}x_1\oplus 1\\x_2\end{bmatrix}, якщо\ k_1=0;k_2=1\\ \begin{bmatrix}x_2\\x_1\oplus 1\end{bmatrix}, якщо\ k_1=1;k_2=0\\ \begin{bmatrix}x_2\oplus 1\\x_1\end{bmatrix}, якщо\ k_1=1;k_2=1\end{cases}=O_1^k=\begin{bmatrix}x_1\cdot\bar{k}_1\oplus x_2\cdot k_1\\ x_1\cdot k_1\oplus x_2\cdot\bar{k}_1\end{bmatrix}\oplus\begin{bmatrix}k_2\\\bar{k}_2\end{bmatrix} \quad (3.53)$$

що і потрібно було довести.

Оскільки над другим операндом двохоперандної операції строгого криптографічного кодування $O_3^k=\begin{bmatrix}x_1\cdot(\overline{k_1\oplus k_2})\oplus x_2\cdot(k_1\oplus k_2)\\ x_1\cdot(k_1\oplus k_2)\oplus x_2\cdot(\overline{k_1\oplus k_2})\end{bmatrix}\oplus\begin{bmatrix}k_1\\\bar{k}_1\end{bmatrix}$ було виконано одноопераднe криптографічне перетворення $F_{6,3}=\begin{bmatrix}x_1\oplus x_2\\x_1\end{bmatrix}$, то в результаті буде отримана операція строгого стійкого кодування $O_5^k=\begin{bmatrix}x_1\cdot\bar{k}_2\oplus x_2\cdot k_2\\ x_1\cdot k_2\oplus x_2\cdot\bar{k}_2\end{bmatrix}\oplus\begin{bmatrix}k_1\oplus k_2\\\overline{k_1\oplus k_2}\end{bmatrix}$.

Так як:

$$F_{6,3}(O_3^k)=\begin{cases}\begin{bmatrix}x_1\\ x_2\oplus 1\end{bmatrix}, \text{ якщо } k_1=0;\ k_2=0\\ \begin{bmatrix}x_2\oplus 1\\ x_1\end{bmatrix}, \text{якщо } k_1=1;\ k_2=0\\ \begin{bmatrix}x_1\oplus 1\\ x_2\end{bmatrix}, \text{якщо } k_1=1;\ k_2=1\\ \begin{bmatrix}x_2\\ x_1\oplus 1\end{bmatrix}, \text{якщо } k_1=0;\ k_2=1\end{cases}=O_5^k=\begin{cases}\begin{bmatrix}x_1\\ x_2\oplus 1\end{bmatrix}, \text{ якщо } k_1=0;\ k_2=0\\ \begin{bmatrix}x_2\oplus 1\\ x_1\end{bmatrix}, \text{якщо } k_1=0;\ k_2=1\\ \begin{bmatrix}x_1\oplus 1\\ x_2\end{bmatrix}, \text{якщо } k_1=1;\ k_2=0\\ \begin{bmatrix}x_2\\ x_1\oplus 1\end{bmatrix}, \text{якщо } k_1=1;\ k_2=1\end{cases}=O_5^k=\begin{bmatrix}x_1\cdot\bar{k}_2\oplus x_2\cdot k_2\\ x_1\cdot k_2\oplus x_2\cdot\bar{k}_2\end{bmatrix}\oplus\begin{bmatrix}k_1\oplus k_2\\ \overline{k_1\oplus k_2}\end{bmatrix} \quad (3.54)$$

що й доведено.

Якщо над другим операндом двохоперандної операції строгого криптографічного кодування $O_3^k=\begin{bmatrix}x_1\cdot(\overline{k_1\oplus k_2})\oplus x_2\cdot(k_1\oplus k_2)\\ x_1\cdot(k_1\oplus k_2)\oplus x_2\cdot(\overline{k_1\oplus k_2})\end{bmatrix}\oplus\begin{bmatrix}k_1\\ \bar{k}_1\end{bmatrix}$ виконати одноопераднe криптографічне перетворення $F_{3,10}=\begin{bmatrix}x_1\\ x_2\oplus 1\end{bmatrix}$, то буде отримана операція строгого стійкого кодування $O_{16}^k=\begin{bmatrix}x_1\cdot(k_1\oplus k_2)\oplus x_2\cdot(\overline{k_1\oplus k_2})\\ x_1\cdot(\overline{k_1\oplus k_2})\oplus x_2\cdot(k_1\oplus k_2)\end{bmatrix}\oplus\begin{bmatrix}k_1\\ \bar{k}_1\end{bmatrix}$.

Так як:

$$F_{3,10}(O_3^k)=\begin{cases}\begin{bmatrix}x_2\\ x_1\oplus 1\end{bmatrix}, \text{якщо } k_1=0;\ k_2=1\\ \begin{bmatrix}x_1\\ x_2\oplus 1\end{bmatrix}, \text{ якщо } k_1=0;\ k_2=0\\ \begin{bmatrix}x_1\oplus 1\\ x_2\end{bmatrix}, \text{якщо } k_1=1;\ k_2=1\\ \begin{bmatrix}x_2\oplus 1\\ x_1\end{bmatrix}, \text{якщо } k_1=1;\ k_2=0\end{cases}=O_{16}^k=\begin{cases}\begin{bmatrix}x_2\\ x_1\oplus 1\end{bmatrix}, \text{ якщо } k_1=0;\ k_2=0\\ \begin{bmatrix}x_1\\ x_2\oplus 1\end{bmatrix}, \text{якщо } k_1=0;\ k_2=1\\ \begin{bmatrix}x_1\oplus 1\\ x_2\end{bmatrix}, \text{якщо } k_1=1;\ k_2=0\\ \begin{bmatrix}x_2\oplus 1\\ x_1\end{bmatrix}, \text{якщо } k_1=1;\ k_2=1\end{cases}=O_{16}^k=\begin{bmatrix}x_1\cdot(k_1\oplus k_2)\oplus x_2\cdot(\overline{k_1\oplus k_2})\\ x_1\cdot(\overline{k_1\oplus k_2})\oplus x_2\cdot(k_1\oplus k_2)\end{bmatrix}\oplus\begin{bmatrix}k_1\\ \bar{k}_1\end{bmatrix} \quad (3.55)$$

що і потрібно було довести.

У випадку, коли над другим операндом двохоперандної операції строгого криптографічного кодування $O_3^k=\begin{bmatrix}x_1\cdot(\overline{k_1\oplus k_2})\oplus x_2\cdot(k_1\oplus k_2)\\ x_1\cdot(k_1\oplus k_2)\oplus x_2\cdot(\overline{k_1\oplus k_2})\end{bmatrix}\oplus\begin{bmatrix}k_1\\ \bar{k}_1\end{bmatrix}$ виконати одноопераднe криптографічне перетворення $F_{6,10}=\begin{bmatrix}x_1\oplus x_2\\ x_2\oplus 1\end{bmatrix}$, то буде отримана операція строгого стійкого кодування $O_{17}^k=\begin{bmatrix}x_1\cdot k_1\oplus x_2\cdot\bar{k}_1\\ x_1\cdot\bar{k}_1\oplus x_2\cdot k_1\end{bmatrix}\oplus\begin{bmatrix}k_1\oplus k_2\\ \overline{k_1\oplus k_2}\end{bmatrix}$.

Отже, перетворення даних операцій набуває наступного вигляду:

$$F_{6,10}(O_3^k)=\begin{cases}\begin{bmatrix}x_2\\ x_1\oplus 1\end{bmatrix}, якщо\ k_1=0;\ k_2=1\\ \begin{bmatrix}x_2\oplus 1\\ x_1\end{bmatrix}, якщо\ k_1=1;\ k_2=0\\ \begin{bmatrix}x_1\oplus 1\\ x_2\end{bmatrix}, якщо\ k_1=1;\ k_2=1\\ \begin{bmatrix}x_1\\ x_2\oplus 1\end{bmatrix}, якщо\ k_1=0;\ k_2=0\end{cases}=O_{17}^k=\begin{cases}\begin{bmatrix}x_2\\ x_1\oplus 1\end{bmatrix}, якщо\ k_1=0;\ k_2=0\\ \begin{bmatrix}x_2\oplus 1\\ x_1\end{bmatrix}, якщо\ k_1=0;\ k_2=1\\ \begin{bmatrix}x_1\oplus 1\\ x_2\end{bmatrix}, якщо\ k_1=1;\ k_2=0\\ \begin{bmatrix}x_1\\ x_2\oplus 1\end{bmatrix}, якщо\ k_1=1;\ k_2=1\end{cases}=O_{17}^k=\begin{bmatrix}x_1\cdot k_1\oplus x_2\cdot\bar{k}_1\\ x_1\cdot\bar{k}_1\oplus x_2\cdot k_1\end{bmatrix}\oplus\begin{bmatrix}k_1\oplus k_2\\ \overline{k_1\oplus k_2}\end{bmatrix} \quad (3.56)$$

що, саме, й потрібно було довести.

Якщо над другим операндом двохоперандної операції строгого криптографічного кодування $O_3^k=\begin{bmatrix}x_1\cdot(\overline{k_1\oplus k_2})\oplus x_2\cdot(k_1\oplus k_2)\\ x_1\cdot(k_1\oplus k_2)\oplus x_2\cdot(\overline{k_1\oplus k_2})\end{bmatrix}\oplus\begin{bmatrix}k_1\\ \bar{k}_1\end{bmatrix}$ виконати одноопераднe криптографічне перетворення $F_{3,9}=\begin{bmatrix}x_1\\ x_1\oplus x_2\oplus 1\end{bmatrix}$, то буде отримана операція строгого стійкого кодування $O_{13}^k=\begin{bmatrix}x_1\cdot(k_1\oplus k_2)\oplus x_2\cdot(\overline{k_1\oplus k_2})\\ x_1\cdot(\overline{k_1\oplus k_2})\oplus x_2\cdot(k_1\oplus k_2)\end{bmatrix}\oplus\begin{bmatrix}k_2\\ \bar{k}_2\end{bmatrix}$.

Так як:

$$F_{3,9}(O_3^k)=\begin{cases}\begin{bmatrix}x_2\\ x_1\oplus 1\end{bmatrix}, якщо\ k_1=0;\ k_2=1\\ \begin{bmatrix}x_1\\ x_2\oplus 1\end{bmatrix}, якщо\ k_1=0;\ k_2=0\\ \begin{bmatrix}x_2\oplus 1\\ x_1\end{bmatrix}, якщо\ k_1=1;\ k_2=0\\ \begin{bmatrix}x_1\oplus 1\\ x_2\end{bmatrix}, якщо\ k_1=1;\ k_2=1\end{cases}=O_{15}^k=\begin{cases}\begin{bmatrix}x_2\\ x_1\oplus 1\end{bmatrix}, якщо\ k_1=0;\ k_2=0\\ \begin{bmatrix}x_1\\ x_2\oplus 1\end{bmatrix}, якщо\ k_1=0;\ k_2=1\\ \begin{bmatrix}x_2\oplus 1\\ x_1\end{bmatrix}, якщо\ k_1=1;\ k_2=0\\ \begin{bmatrix}x_1\oplus 1\\ x_2\end{bmatrix}, якщо\ k_1=1;\ k_2=1\end{cases}=O_{15}^k=\begin{bmatrix}x_1\cdot k_2\oplus x_2\cdot\bar{k}_2\\ x_1\cdot\bar{k}_2\oplus x_2\cdot k_2\end{bmatrix}\oplus\begin{bmatrix}k_1\\ \bar{k}_1\end{bmatrix} \quad (3.57)$$

що і потрібно було довести.

Якщо над другим операндом двохоперандної операції строгого криптографічного кодування $O_3^k=\begin{bmatrix}x_1\cdot(\overline{k_1\oplus k_2})\oplus x_2\cdot(k_1\oplus k_2)\\ x_1\cdot(k_1\oplus k_2)\oplus x_2\cdot(\overline{k_1\oplus k_2})\end{bmatrix}\oplus\begin{bmatrix}k_1\\ \bar{k}_1\end{bmatrix}$ виконати одноопераднe криптографічне перетворення $F_{5,12}=\begin{bmatrix}x_2\\ x_1\oplus 1\end{bmatrix}$, то буде отримана операція строгого стійкого кодування $O_{13}^k=\begin{bmatrix}x_1\cdot(k_1\oplus k_2)\oplus x_2\cdot(\overline{k_1\oplus k_2})\\ x_1\cdot(\overline{k_1\oplus k_2})\oplus x_2\cdot(k_1\oplus k_2)\end{bmatrix}\oplus\begin{bmatrix}k_2\\ \bar{k}_2\end{bmatrix}$.

Так як:

$$F_{5,12}(O_3^k)=\begin{cases}\begin{bmatrix}x_2\\ x_1\oplus 1\end{bmatrix}, якщо\ k_1=0;\ k_2=1\\ \begin{bmatrix}x_1\oplus 1\\ x_2\end{bmatrix}, якщо\ k_1=1;\ k_2=1\\ \begin{bmatrix}x_1\\ x_2\oplus 1\end{bmatrix}, якщо\ k_1=0;\ k_2=0\\ \begin{bmatrix}x_2\oplus 1\\ x_1\end{bmatrix}, якщо\ k_1=1;\ k_2=0\end{cases}=O_{13}^k=\begin{cases}\begin{bmatrix}x_2\\ x_1\oplus 1\end{bmatrix}, якщо\ k_1=0;\ k_2=0\\ \begin{bmatrix}x_1\oplus 1\\ x_2\end{bmatrix}, якщо\ k_1=0;\ k_2=1\\ \begin{bmatrix}x_1\\ x_2\oplus 1\end{bmatrix}, якщо\ k_1=1;\ k_2=0\\ \begin{bmatrix}x_2\oplus 1\\ x_1\end{bmatrix}, якщо\ k_1=1;\ k_2=1\end{cases}=O_{13}^k=\begin{bmatrix}x_1\cdot(k_1\oplus k_2)\oplus x_2\cdot(\overline{k_1\oplus k_2})\\ x_1\cdot(\overline{k_1\oplus k_2})\oplus x_2\cdot(k_1\oplus k_2)\end{bmatrix}\oplus\begin{bmatrix}k_2\\ \bar{k}_2\end{bmatrix} \quad (3.58)$$

що й потрібно було довести.

У разі виконання над другим операндом двохоперандної операції строгого криптографічного кодування $O_3^k=\begin{bmatrix}x_1\cdot(\overline{k_1\oplus k_2})\oplus x_2\cdot(k_1\oplus k_2)\\ x_1\cdot(k_1\oplus k_2)\oplus x_2\cdot(\overline{k_1\oplus k_2})\end{bmatrix}\oplus\begin{bmatrix}k_1\\ \bar{k}_1\end{bmatrix}$ виконати одноопераднe криптографічне перетворення $F_{5,9}=\begin{bmatrix}x_2\\ x_1\oplus x_2\oplus 1\end{bmatrix}$, то буде отримана операція строгого стійкого кодування $O_{18}^k=\begin{bmatrix}x_1\cdot k_1\oplus x_2\cdot\bar{k}_1\\ x_1\cdot\bar{k}_1\oplus x_2\cdot k_1\end{bmatrix}\oplus\begin{bmatrix}k_2\\ \bar{k}_2\end{bmatrix}$.

Так як:

$$F_{5,9}(O_3^k)=\begin{cases}\begin{bmatrix}x_2\\ x_1\oplus 1\end{bmatrix}, якщо\ k_1=0;\ k_2=1\\ \begin{bmatrix}x_2\oplus 1\\ x_1\end{bmatrix}, якщо\ k_1=1;\ k_2=0\\ \begin{bmatrix}x_1\\ x_2\oplus 1\end{bmatrix}, якщо\ k_1=0;\ k_2=0\\ \begin{bmatrix}x_1\oplus 1\\ x_2\end{bmatrix}, якщо\ k_1=1;\ k_2=1\end{cases}=O_{18}^k=\begin{cases}\begin{bmatrix}x_2\\ x_1\oplus 1\end{bmatrix}, якщо\ k_1=0;\ k_2=0\\ \begin{bmatrix}x_2\oplus 1\\ x_1\end{bmatrix}, якщо\ k_1=0;\ k_2=1\\ \begin{bmatrix}x_1\\ x_2\oplus 1\end{bmatrix}, якщо\ k_1=1;\ k_2=0\\ \begin{bmatrix}x_1\oplus 1\\ x_2\end{bmatrix}, якщо\ k_1=1;\ k_2=1\end{cases}=O_{18}^k=\begin{bmatrix}x_1\cdot k_1\oplus x_2\cdot\bar{k}_1\\ x_1\cdot\bar{k}_1\oplus x_2\cdot k_1\end{bmatrix}\oplus\begin{bmatrix}k_2\\ \bar{k}_2\end{bmatrix} \quad (3.59)$$

що і потрібно було довести.

Якщо над другим операндом двохоперандної операції строгого криптографічного кодування $O_3^k=\begin{bmatrix}x_1\cdot(\overline{k_1\oplus k_2})\oplus x_2\cdot(k_1\oplus k_2)\\ x_1\cdot(k_1\oplus k_2)\oplus x_2\cdot(\overline{k_1\oplus k_2})\end{bmatrix}\oplus\begin{bmatrix}k_1\\ \bar{k}_1\end{bmatrix}$ виконати одноопераднe криптографічне перетворення $F_{6,12}=\begin{bmatrix}x_1\oplus x_2\\ x_1\oplus 1\end{bmatrix}$, то буде отримана операція строгого стійкого кодування $O_{14}^k=\begin{bmatrix}x_1\cdot k_2\oplus x_2\cdot\bar{k}_2\\ x_1\cdot\bar{k}_2\oplus x_2\cdot k_2\end{bmatrix}\oplus\begin{bmatrix}k_2\\ \bar{k}_2\end{bmatrix}$.

Так як перетворення набуває наступного вигляду:

$$F_{6,12}(O_3^k)=\begin{cases}\begin{bmatrix}x_2\\ x_1\oplus 1\end{bmatrix}, якщо\ k_1=0;\ k_2=1\\ \begin{bmatrix}x_1\oplus 1\\ x_2\end{bmatrix}, якщо\ k_1=1;\ k_2=1\\ \begin{bmatrix}x_2\oplus 1\\ x_1\end{bmatrix}, якщо\ k_1=1;\ k_2=0\\ \begin{bmatrix}x_1\\ x_2\oplus 1\end{bmatrix}, якщо\ k_1=0;\ k_2=0\end{cases}=O_{14}^k=\begin{cases}\begin{bmatrix}x_2\\ x_1\oplus 1\end{bmatrix}, якщо\ k_1=0;\ k_2=0\\ \begin{bmatrix}x_1\oplus 1\\ x_2\end{bmatrix}, якщо\ k_1=0;\ k_2=1\\ \begin{bmatrix}x_2\oplus 1\\ x_1\end{bmatrix}, якщо\ k_1=1;\ k_2=0\\ \begin{bmatrix}x_1\\ x_2\oplus 1\end{bmatrix}, якщо\ k_1=1;\ k_2=1\end{cases}=O_{14}^k=\begin{bmatrix}x_1\cdot k_2\oplus x_2\cdot\bar{k}_2\\ x_1\cdot\bar{k}_2\oplus x_2\cdot k_2\end{bmatrix}\oplus\begin{bmatrix}k_2\\ \bar{k}_2\end{bmatrix} \tag{3.60}$$

це означає, що було доведено потрібне.

Якщо над другим операндом двохоперандної операції строгого криптографічного кодування $O_3^k=\begin{bmatrix}x_1\cdot(\overline{k_1\oplus k_2})\oplus x_2\cdot(k_1\oplus k_2)\\ x_1\cdot(k_1\oplus k_2)\oplus x_2\cdot(\overline{k_1\oplus k_2})\end{bmatrix}\oplus\begin{bmatrix}k_1\\ \bar{k}_1\end{bmatrix}$ виконати одноопераднe криптографічне перетворення $F_{12,5}=\begin{bmatrix}x_1\oplus 1\\ x_2\end{bmatrix}$, то буде отримана операція строгого стійкого кодування $O_{20}^k=\begin{bmatrix}x_1\cdot(k_1\oplus k_2)\oplus x_2\cdot(\overline{k_1\oplus k_2})\\ x_1\cdot(\overline{k_1\oplus k_2})\oplus x_2\cdot(k_1\oplus k_2)\end{bmatrix}$.

Так як:

$$F_{12,5}(O_3^k)=\begin{cases}\begin{bmatrix}x_2\oplus 1\\ x_1\end{bmatrix}, якщо\ k_1=1;\ k_2=0\\ \begin{bmatrix}x_1\oplus 1\\ x_2\end{bmatrix}, якщо\ k_1=1;\ k_2=1\\ \begin{bmatrix}x_1\\ x_2\oplus 1\end{bmatrix}, якщо\ k_1=0;\ k_2=0\\ \begin{bmatrix}x_2\\ x_1\oplus 1\end{bmatrix}, якщо\ k_1=0;\ k_2=1\end{cases}=O_{20}^k=\begin{cases}\begin{bmatrix}x_2\oplus 1\\ x_1\end{bmatrix}, якщо\ k_1=1;\ k_2=0\\ \begin{bmatrix}x_1\oplus 1\\ x_2\end{bmatrix}, якщо\ k_1=1;\ k_2=1\\ \begin{bmatrix}x_1\\ x_2\oplus 1\end{bmatrix}, якщо\ k_1=0;\ k_2=0\\ \begin{bmatrix}x_2\\ x_1\oplus 1\end{bmatrix}, якщо\ k_1=0;\ k_2=1\end{cases}=O_{20}^k=\begin{bmatrix}x_1\cdot(k_1\oplus k_2)\oplus x_2\cdot(\overline{k_1\oplus k_2})\\ x_1\cdot(\overline{k_1\oplus k_2})\oplus x_2\cdot(k_1\oplus k_2)\end{bmatrix}\oplus\begin{bmatrix}\bar{k}_1\\ k_1\end{bmatrix} \tag{3.61}$$

саме це й потрібно було довести і потрібно було довести.

Якщо над другим операндом двохоперандної операції строгого криптографічного кодування $O_3^k=\begin{bmatrix}x_1\cdot(\overline{k_1\oplus k_2})\oplus x_2\cdot(k_1\oplus k_2)\\ x_1\cdot(k_1\oplus k_2)\oplus x_2\cdot(\overline{k_1\oplus k_2})\end{bmatrix}\oplus\begin{bmatrix}k_1\\ \bar{k}_1\end{bmatrix}$ виконати одноопераднe криптографічне перетворення $F_{9,5}=\begin{bmatrix}x_1\oplus x_2\oplus 1\\ x_2\end{bmatrix}$, то буде отримана операція строгого стійкого кодування $O_{21}^k=\begin{bmatrix}x_1\cdot k_1\oplus x_2\cdot\bar{k}_1\\ x_1\cdot\bar{k}_1\oplus x_2\cdot k_1\end{bmatrix}\oplus\begin{bmatrix}\overline{k_1\oplus k_2}\\ k_1\oplus k_2\end{bmatrix}$.

Так як:

$$F_{9,5}(O_3^k)=\begin{cases}\begin{bmatrix}x_2\oplus 1\\ x_1\end{bmatrix}, \text{якщо } k_1=1;\ k_2=0\\ \begin{bmatrix}x_2\\ x_1\oplus 1\end{bmatrix}, \text{якщо } k_1=0;\ k_2=1\\ \begin{bmatrix}x_1\\ x_2\oplus 1\end{bmatrix}, \text{якщо } k_1=0;\ k_2=0\\ \begin{bmatrix}x_1\oplus 1\\ x_2\end{bmatrix}, \text{якщо } k_1=1;\ k_2=1\end{cases}=O_{21}^k=\begin{cases}\begin{bmatrix}x_2\oplus 1\\ x_1\end{bmatrix}, \text{якщо } k_1=1;\ k_2=0\\ \begin{bmatrix}x_2\\ x_1\oplus 1\end{bmatrix}, \text{якщо } k_1=0;\ k_2=1\\ \begin{bmatrix}x_1\\ x_2\oplus 1\end{bmatrix}, \text{якщо } k_1=0;\ k_2=0\\ \begin{bmatrix}x_1\oplus 1\\ x_2\end{bmatrix}, \text{якщо } k_1=1;\ k_2=1\end{cases}=O_{21}^k=\begin{bmatrix}x_1\cdot k_1\oplus x_2\cdot\bar{k}_1\\ x_1\cdot\bar{k}_1\oplus x_2\cdot k_1\end{bmatrix}\oplus\begin{bmatrix}\overline{k_1\oplus k_2}\\ k_1\oplus k_2\end{bmatrix} \quad (3.62)$$

що і потрібно було довести.

Аналогічно попереднім прикладам, виконаємо наступне одноопераднде криптографічне перетворення $F_{12,6}=\begin{bmatrix}x_1\oplus 1\\ x_1\oplus x_2\end{bmatrix}$ над другим операндом двохопераднді операції строгого стійкого криптографічного кодування $O_3^k=\begin{bmatrix}x_1\cdot(\overline{k_1\oplus k_2})\oplus x_2\cdot(k_1\oplus k_2)\\ x_1\cdot(k_1\oplus k_2)\oplus x_2\cdot(\overline{k_1\oplus k_2})\end{bmatrix}\oplus\begin{bmatrix}k_1\\ \bar{k}_1\end{bmatrix}$, що, в результаті, дає можливість отримати операцію строгого стійкого кодування $O_{19}^k=\begin{bmatrix}x_1\cdot\bar{k}_2\oplus x_2\cdot k_2\\ x_1\cdot k_2\oplus x_2\cdot\bar{k}_2\end{bmatrix}\oplus\begin{bmatrix}k_1\\ \bar{k}_1\end{bmatrix}$.

Так як:

$$F_{12,6}(O_3^k)=\begin{cases}\begin{bmatrix}x_2\oplus 1\\ x_1\end{bmatrix}, \text{якщо } k_1=1;\ k_2=0\\ \begin{bmatrix}x_1\oplus 1\\ x_2\end{bmatrix}, \text{якщо } k_1=1;\ k_2=1\\ \begin{bmatrix}x_2\\ x_1\oplus 1\end{bmatrix}, \text{якщо } k_1=0;\ k_2=1\\ \begin{bmatrix}x_1\\ x_2\oplus 1\end{bmatrix}, \text{якщо } k_1=0;\ k_2=0\end{cases}=O_{19}^k=\begin{cases}\begin{bmatrix}x_2\oplus 1\\ x_1\end{bmatrix}, \text{якщо } k_1=1;\ k_2=0\\ \begin{bmatrix}x_1\oplus 1\\ x_2\end{bmatrix}, \text{якщо } k_1=1;\ k_2=1\\ \begin{bmatrix}x_2\\ x_1\oplus 1\end{bmatrix}, \text{якщо } k_1=0;\ k_2=1\\ \begin{bmatrix}x_1\\ x_2\oplus 1\end{bmatrix}, \text{якщо } k_1=0;\ k_2=0\end{cases}=O_{19}^k=\begin{bmatrix}x_1\cdot\bar{k}_2\oplus x_2\cdot k_2\\ x_1\cdot k_2\oplus x_2\cdot\bar{k}_2\end{bmatrix}\oplus\begin{bmatrix}k_1\\ \bar{k}_1\end{bmatrix} \quad (3.63)$$

що і потрібно було довести.

У випадку, коли над другим операндом двохопераднді операції строгого криптографічного кодування $O_3^k=\begin{bmatrix}x_1\cdot(\overline{k_1\oplus k_2})\oplus x_2\cdot(k_1\oplus k_2)\\ x_1\cdot(k_1\oplus k_2)\oplus x_2\cdot(\overline{k_1\oplus k_2})\end{bmatrix}\oplus\begin{bmatrix}k_1\\ \bar{k}_1\end{bmatrix}$ виконати одноопераднде криптографічне перетворення $F_{10,3}=\begin{bmatrix}x_2\oplus 1\\ x_1\end{bmatrix}$, то буде

отримана операція строгого стійкого кодування $O_{23}^k = \begin{bmatrix} x_1 \cdot (k_1 \oplus k_2) \oplus x_2 \cdot (\overline{k_1 \oplus k_2}) \\ x_1 \cdot (\overline{k_1 \oplus k_2}) \oplus x_2 \cdot (k_1 \oplus k_2) \end{bmatrix} \oplus \begin{bmatrix} \bar{k}_2 \\ k_2 \end{bmatrix}$.

Оскільки перетворення вигладає наступним чином:

$$F_{10,3}(O_3^k) = \begin{cases} \begin{bmatrix} x_2 \oplus 1 \\ x_1 \end{bmatrix}, \text{якщо } k_1 = 1; k_2 = 0 \\ \begin{bmatrix} x_1 \\ x_2 \oplus 1 \end{bmatrix}, \text{якщо } k_1 = 0; k_2 = 0 \\ \begin{bmatrix} x_1 \oplus 1 \\ x_2 \end{bmatrix}, \text{якщо } k_1 = 1; k_2 = 1 \\ \begin{bmatrix} x_2 \\ x_1 \oplus 1 \end{bmatrix}, \text{якщо } k_1 = 0; k_2 = 1 \end{cases} = O_{23}^k = \begin{cases} \begin{bmatrix} x_2 \oplus 1 \\ x_1 \end{bmatrix}, \text{якщо } k_1 = 1; k_2 = 0 \\ \begin{bmatrix} x_1 \\ x_2 \oplus 1 \end{bmatrix}, \text{якщо } k_1 = 0; k_2 = 0 \\ \begin{bmatrix} x_1 \oplus 1 \\ x_2 \end{bmatrix}, \text{якщо } k_1 = 1; k_2 = 1 \\ \begin{bmatrix} x_2 \\ x_1 \oplus 1 \end{bmatrix}, \text{якщо } k_1 = 0; k_2 = 1 \end{cases} = O_{23}^k = \begin{bmatrix} x_1 \cdot (k_1 \oplus k_2) \oplus x_2 \cdot (\overline{k_1 \oplus k_2}) \\ x_1 \cdot (\overline{k_1 \oplus k_2}) \oplus x_2 \cdot (k_1 \oplus k_2) \end{bmatrix} \oplus \begin{bmatrix} \bar{k}_2 \\ k_2 \end{bmatrix} \quad (3.64)$$

це й доводить наше твердження.

Якщо над другим операндом двохоперандної операції строгого криптографічного кодування $O_3^k = \begin{bmatrix} x_1 \cdot (\overline{k_1 \oplus k_2}) \oplus x_2 \cdot (k_1 \oplus k_2) \\ x_1 \cdot (k_1 \oplus k_2) \oplus x_2 \cdot (\overline{k_1 \oplus k_2}) \end{bmatrix} \oplus \begin{bmatrix} k_1 \\ \bar{k}_1 \end{bmatrix}$ виконати одноопераднe криптографічне перетворення $F_{10,6} = \begin{bmatrix} x_2 \oplus 1 \\ x_1 \oplus x_2 \end{bmatrix}$, то буде отримана операція строгого стійкого кодування $O_{22}^k = \begin{bmatrix} x_1 \cdot k_1 \oplus x_2 \cdot \bar{k}_1 \\ x_1 \cdot \bar{k}_1 \oplus x_2 \cdot k_1 \end{bmatrix} \oplus \begin{bmatrix} \bar{k}_2 \\ k_2 \end{bmatrix}$.

Отже:

$$F_{10,6}(O_3^k) = \begin{cases} \begin{bmatrix} x_2 \oplus 1 \\ x_1 \end{bmatrix}, \text{якщо } k_1 = 1; k_2 = 0 \\ \begin{bmatrix} x_2 \\ x_1 \oplus 1 \end{bmatrix}, \text{якщо } k_1 = 0; k_2 = 1 \\ \begin{bmatrix} x_1 \oplus 1 \\ x_2 \end{bmatrix}, \text{якщо } k_1 = 1; k_2 = 1 \\ \begin{bmatrix} x_1 \\ x_2 \oplus 1 \end{bmatrix}, \text{якщо } k_1 = 0; k_2 = 0 \end{cases} = O_{22}^k = \begin{cases} \begin{bmatrix} x_2 \oplus 1 \\ x_1 \end{bmatrix}, \text{якщо } k_1 = 1; k_2 = 0 \\ \begin{bmatrix} x_2 \\ x_1 \oplus 1 \end{bmatrix}, \text{якщо } k_1 = 0; k_2 = 1 \\ \begin{bmatrix} x_1 \oplus 1 \\ x_2 \end{bmatrix}, \text{якщо } k_1 = 1; k_2 = 1 \\ \begin{bmatrix} x_1 \\ x_2 \oplus 1 \end{bmatrix}, \text{якщо } k_1 = 0; k_2 = 0 \end{cases} = O_{22}^k = \begin{bmatrix} x_1 \cdot k_1 \oplus x_2 \cdot \bar{k}_1 \\ x_1 \cdot \bar{k}_1 \oplus x_2 \cdot k_1 \end{bmatrix} \oplus \begin{bmatrix} \bar{k}_2 \\ k_2 \end{bmatrix} \quad (3.65)$$

саме це і необхідно було довести.

При виконанні над другим операндом двохоперандної операції строгого криптографічного кодування $O_3^k = \begin{bmatrix} x_1 \cdot (\overline{k_1 \oplus k_2}) \oplus x_2 \cdot (k_1 \oplus k_2) \\ x_1 \cdot (k_1 \oplus k_2) \oplus x_2 \cdot (\overline{k_1 \oplus k_2}) \end{bmatrix} \oplus \begin{bmatrix} k_1 \\ \bar{k}_1 \end{bmatrix}$

одноопераднe криптографічне перетворення $F_{9,3}=\begin{bmatrix} x_1 \oplus x_2 \oplus 1 \\ x_1 \end{bmatrix}$, то буде отримана операція строгого стійкого кодування $O_{22}^k = \begin{bmatrix} x_1 \cdot k_1 \oplus x_2 \cdot \bar{k}_1 \\ x_1 \cdot \bar{k}_1 \oplus x_2 \cdot k_1 \end{bmatrix} \oplus \begin{bmatrix} \bar{k}_2 \\ k_2 \end{bmatrix}$.

Перетворення набуває наступного вигляду:

$$F_{9,3}(O_3^k)=\begin{cases} \begin{bmatrix} x_2 \oplus 1 \\ x_1 \end{bmatrix}, \text{якщо } k_1=1;\ k_2=0 \\ \begin{bmatrix} x_2 \\ x_1 \oplus 1 \end{bmatrix}, \text{якщо } k_1=0;\ k_2=1 \\ \begin{bmatrix} x_1 \oplus 1 \\ x_2 \end{bmatrix}, \text{якщо } k_1=1;\ k_2=1 \\ \begin{bmatrix} x_1 \\ x_2 \oplus 1 \end{bmatrix}, \text{якщо } k_1=0;\ k_2=0 \end{cases} = O_{22}^k = \begin{cases} \begin{bmatrix} x_2 \oplus 1 \\ x_1 \end{bmatrix}, \text{якщо } k_1=1;\ k_2=0 \\ \begin{bmatrix} x_2 \\ x_1 \oplus 1 \end{bmatrix}, \text{якщо } k_1=0;\ k_2=1 \\ \begin{bmatrix} x_1 \oplus 1 \\ x_2 \end{bmatrix}, \text{якщо } k_1=1;\ k_2=1 \\ \begin{bmatrix} x_1 \\ x_2 \oplus 1 \end{bmatrix}, \text{якщо } k_1=0;\ k_2=0 \end{cases} = O_{22}^k = \begin{bmatrix} x_1 \cdot k_1 \oplus x_2 \cdot \bar{k}_1 \\ x_1 \cdot \bar{k}_1 \oplus x_2 \cdot k_1 \end{bmatrix} \oplus \begin{bmatrix} \bar{k}_2 \\ k_2 \end{bmatrix} \quad (3.66)$$

що і потрібно було довести.

Якщо над другим операндом двохоперандної операції строгого криптографічного кодування $O_3^k = \begin{bmatrix} x_1 \cdot (\overline{k_1 \oplus k_2}) \oplus x_2 \cdot (k_1 \oplus k_2) \\ x_1 \cdot (k_1 \oplus k_2) \oplus x_2 \cdot (\overline{k_1 \oplus k_2}) \end{bmatrix} \oplus \begin{bmatrix} k_1 \\ \bar{k}_1 \end{bmatrix}$ виконати одноопераднe криптографічне перетворення $F_{12,10}=\begin{bmatrix} x_1 \oplus 1 \\ x_2 \oplus 1 \end{bmatrix}$, то буде отримана операція строгого стійкого кодування $O_{22}^k = \begin{bmatrix} x_1 \cdot k_1 \oplus x_2 \cdot \bar{k}_1 \\ x_1 \cdot \bar{k}_1 \oplus x_2 \cdot k_1 \end{bmatrix} \oplus \begin{bmatrix} \bar{k}_2 \\ k_2 \end{bmatrix}$.

Дане перетворення показує вірність нашого твердження:

$$F_{12,10}(O_3^k)=\begin{cases} \begin{bmatrix} x_1 \oplus 1 \\ x_2 \end{bmatrix}, \text{якщо } k_1=1;\ k_2=1 \\ \begin{bmatrix} x_2 \oplus 1 \\ x_1 \end{bmatrix}, \text{якщо } k_1=1;\ k_2=0 \\ \begin{bmatrix} x_2 \\ x_1 \oplus 1 \end{bmatrix}, \text{якщо } k_1=0;\ k_2=1 \\ \begin{bmatrix} x_1 \\ x_2 \oplus 1 \end{bmatrix}, \text{якщо } k_1=0;\ k_2=0 \end{cases} = O_{12}^k = \begin{cases} \begin{bmatrix} x_1 \oplus 1 \\ x_2 \end{bmatrix}, \text{якщо } k_1=1;\ k_2=1 \\ \begin{bmatrix} x_2 \oplus 1 \\ x_1 \end{bmatrix}, \text{якщо } k_1=1;\ k_2=0 \\ \begin{bmatrix} x_2 \\ x_1 \oplus 1 \end{bmatrix}, \text{якщо } k_1=0;\ k_2=1 \\ \begin{bmatrix} x_1 \\ x_2 \oplus 1 \end{bmatrix}, \text{якщо } k_1=0;\ k_2=0 \end{cases} = O_{12}^k = \begin{bmatrix} x_1 \cdot (\overline{k_1 \oplus k_2}) \oplus x_2 \cdot (k_1 \oplus k_2) \\ x_1 \cdot (k_1 \oplus k_2) \oplus x_2 \cdot (\overline{k_1 \oplus k_2}) \end{bmatrix} \oplus \begin{bmatrix} \bar{k}_1 \\ k_1 \end{bmatrix} \quad (3.67)$$

Якщо над другим операндом двохоперандної операції строгого криптографічного кодування $O_3^k = \begin{bmatrix} x_1 \cdot (\overline{k_1 \oplus k_2}) \oplus x_2 \cdot (k_1 \oplus k_2) \\ x_1 \cdot (k_1 \oplus k_2) \oplus x_2 \cdot (\overline{k_1 \oplus k_2}) \end{bmatrix} \oplus \begin{bmatrix} k_1 \\ \bar{k}_1 \end{bmatrix}$ виконати

одноопераднe криптографічне перетворення $F_{9,10}=\begin{bmatrix} x_1 \oplus x_2 \oplus 1 \\ x_2 \oplus 1 \end{bmatrix}$, то буде отримана операція строгого стійкого кодування $O_7^k=\begin{bmatrix} x_1 \cdot \bar{k}_1 \oplus x_2 \cdot k_1 \\ x_1 \cdot k_1 \oplus x_2 \cdot \bar{k}_1 \end{bmatrix} \oplus \begin{bmatrix} \overline{k_1 \oplus k_2} \\ k_1 \oplus k_2 \end{bmatrix}$.

Так як перетворення операцій має наступний вигляд:

$$F_{9,10}(O_3^k)=\begin{cases} \begin{bmatrix} x_1 \oplus 1 \\ x_2 \end{bmatrix}, якщо\ k_1=1;\ k_2=1 \\ \begin{bmatrix} x_1 \\ x_2 \oplus 1 \end{bmatrix},\ якщо\ k_1=0;\ k_2=0 \\ \begin{bmatrix} x_2 \\ x_1 \oplus 1 \end{bmatrix}, якщо\ k_1=0;\ k_2=1 \\ \begin{bmatrix} x_2 \oplus 1 \\ x_1 \end{bmatrix},\ якщо\ k_1=1;\ k_2=0 \end{cases} = O_7^k = \begin{cases} \begin{bmatrix} x_1 \oplus 1 \\ x_2 \end{bmatrix},\ якщо\ k_1=0;\ k_2=0 \\ \begin{bmatrix} x_1 \\ x_2 \oplus 1 \end{bmatrix}, якщо\ k_1=0;\ k_2=1 \\ \begin{bmatrix} x_2 \\ x_1 \oplus 1 \end{bmatrix},\ якщо\ k_1=1;\ k_2=0 \\ \begin{bmatrix} x_2 \oplus 1 \\ x_1 \end{bmatrix}, якщо\ k_1=1;\ k_2=1 \end{cases} = O_7^k = \begin{bmatrix} x_1 \cdot \bar{k}_1 \oplus x_2 \cdot k_1 \\ x_1 \cdot k_1 \oplus x_2 \cdot \bar{k}_1 \end{bmatrix} \oplus \begin{bmatrix} \overline{k_1 \oplus k_2} \\ k_1 \oplus k_2 \end{bmatrix} \quad (3.68)$$

це доводить вірність нашого твердження.

Виконаємо над другим операндом двохоперандної операції строгого криптографічного кодування $O_3^k=\begin{bmatrix} x_1 \cdot (\overline{k_1 \oplus k_2}) \oplus x_2 \cdot (k_1 \oplus k_2) \\ x_1 \cdot (k_1 \oplus k_2) \oplus x_2 \cdot \overline{(k_1 \oplus k_2)} \end{bmatrix} \oplus \begin{bmatrix} k_1 \\ \bar{k}_1 \end{bmatrix}$ виконати одноопераднe криптографічне перетворення $F_{12,9}=\begin{bmatrix} x_1 \oplus 1 \\ x_1 \oplus x_2 \oplus 1 \end{bmatrix}$, то буде отримана операція строгого стійкого кодування $O_{11}^k=\begin{bmatrix} x_1 \cdot \bar{k}_2 \oplus x_2 \cdot k_2 \\ x_1 \cdot k_2 \oplus x_2 \cdot \bar{k}_2 \end{bmatrix} \oplus \begin{bmatrix} \bar{k}_1 \\ k_1 \end{bmatrix}$.

Оскільки:

$$F_{12,9}(O_3^k)=\begin{cases} \begin{bmatrix} x_1 \oplus 1 \\ x_2 \end{bmatrix}, якщо\ k_1=1;\ k_2=1 \\ \begin{bmatrix} x_2 \oplus 1 \\ x_1 \end{bmatrix},\ якщо\ k_1=1;\ k_2=0 \\ \begin{bmatrix} x_1 \\ x_2 \oplus 1 \end{bmatrix},\ якщо\ k_1=0;\ k_2=0 \\ \begin{bmatrix} x_2 \\ x_1 \oplus 1 \end{bmatrix}, якщо\ k_1=0;\ k_2=1 \end{cases} = O_{11}^k = \begin{cases} \begin{bmatrix} x_1 \oplus 1 \\ x_2 \end{bmatrix}, якщо\ k_1=1;\ k_2=1 \\ \begin{bmatrix} x_2 \oplus 1 \\ x_1 \end{bmatrix},\ якщо\ k_1=1;\ k_2=0 \\ \begin{bmatrix} x_1 \\ x_2 \oplus 1 \end{bmatrix},\ якщо\ k_1=0;\ k_2=0 \\ \begin{bmatrix} x_2 \\ x_1 \oplus 1 \end{bmatrix}, якщо\ k_1=0;\ k_2=1 \end{cases} = O_{11}^k = \begin{bmatrix} x_1 \cdot \bar{k}_2 \oplus x_2 \cdot k_2 \\ x_1 \cdot k_2 \oplus x_2 \cdot \bar{k}_2 \end{bmatrix} \oplus \begin{bmatrix} \bar{k}_1 \\ k_1 \end{bmatrix} \quad (3.69)$$

саме це й потрібно було довести.

При виконанні одноопераднoго криптографічного перетворення $F_{10,12}=\begin{bmatrix} x_2 \oplus 1 \\ x_1 \oplus 1 \end{bmatrix}$ над другим операндом двохоперандної операції строгого

криптографічного кодування $O_3^k = \begin{bmatrix} x_1 \cdot (\overline{k_1 \oplus k_2}) \oplus x_2 \cdot (k_1 \oplus k_2) \\ x_1 \cdot (k_1 \oplus k_2) \oplus x_2 \cdot (\overline{k_1 \oplus k_2}) \end{bmatrix} \oplus \begin{bmatrix} k_1 \\ \bar{k}_1 \end{bmatrix}$, отримуємо операцію строгого стійкого кодування $O_9^k = \begin{bmatrix} x_1 \cdot (\overline{k_1 \oplus k_2}) \oplus x_2 \cdot (k_1 \oplus k_2) \\ x_1 \cdot (k_1 \oplus k_2) \oplus x_2 \cdot (\overline{k_1 \oplus k_2}) \end{bmatrix} \oplus \begin{bmatrix} \bar{k}_2 \\ k_2 \end{bmatrix}$.

Отже, перетворення має наступний вигляд:

$$F_{10,12}(O_3^k) = \begin{cases} \begin{bmatrix} x_1 \oplus 1 \\ x_2 \end{bmatrix}, якщо\ k_1 = 1; k_2 = 1 \\ \begin{bmatrix} x_2 \\ x_1 \oplus 1 \end{bmatrix}, якщо\ k_1 = 0; k_2 = 1 \\ \begin{bmatrix} x_2 \oplus 1 \\ x_1 \end{bmatrix}, якщо\ k_1 = 1; k_2 = 0 \\ \begin{bmatrix} x_1 \\ x_2 \oplus 1 \end{bmatrix}, якщо\ k_1 = 0; k_2 = 0 \end{cases} = O_9^k = \begin{cases} \begin{bmatrix} x_1 \oplus 1 \\ x_2 \end{bmatrix}, якщо\ k_1 = 1; k_2 = 1 \\ \begin{bmatrix} x_2 \\ x_1 \oplus 1 \end{bmatrix}, якщо\ k_1 = 0; k_2 = 1 \\ \begin{bmatrix} x_2 \oplus 1 \\ x_1 \end{bmatrix}, якщо\ k_1 = 1; k_2 = 0 \\ \begin{bmatrix} x_1 \\ x_2 \oplus 1 \end{bmatrix}, якщо\ k_1 = 0; k_2 = 0 \end{cases} = O_9^k = \begin{bmatrix} x_1 \cdot (\overline{k_1 \oplus k_2}) \oplus x_2 \cdot (k_1 \oplus k_2) \\ x_1 \cdot (k_1 \oplus k_2) \oplus x_2 \cdot (\overline{k_1 \oplus k_2}) \end{bmatrix} \oplus \begin{bmatrix} \bar{k}_2 \\ k_2 \end{bmatrix} \quad (3.70)$$

що й доводить вірність твердження.

Якщо над другим операндом двохоперандної операції строгого криптографічного кодування $O_3^k = \begin{bmatrix} x_1 \cdot (\overline{k_1 \oplus k_2}) \oplus x_2 \cdot (k_1 \oplus k_2) \\ x_1 \cdot (k_1 \oplus k_2) \oplus x_2 \cdot (\overline{k_1 \oplus k_2}) \end{bmatrix} \oplus \begin{bmatrix} k_1 \\ \bar{k}_1 \end{bmatrix}$ виконати одноопераднде криптографічне перетворення $F_{10,9} = \begin{bmatrix} x_2 \oplus 1 \\ x_1 \oplus x_2 \oplus 1 \end{bmatrix}$, то буде отримана операція строгого стійкого криптографічного кодування $O_8^k = \begin{bmatrix} x_1 \cdot \bar{k}_1 \oplus x_2 \cdot k_1 \\ x_1 \cdot k_1 \oplus x_2 \cdot \bar{k}_1 \end{bmatrix} \oplus \begin{bmatrix} \bar{k}_2 \\ k_2 \end{bmatrix}$.

Згідно даної операції отримуємо наступне перетворення:

$$F_{10,9}(O_3^k) = \begin{cases} \begin{bmatrix} x_1 \oplus 1 \\ x_2 \end{bmatrix}, якщо\ k_1 = 1; k_2 = 1 \\ \begin{bmatrix} x_1 \\ x_2 \oplus 1 \end{bmatrix}, якщо\ k_1 = 0; k_2 = 0 \\ \begin{bmatrix} x_2 \oplus 1 \\ x_1 \end{bmatrix}, якщо\ k_1 = 1; k_2 = 0 \\ \begin{bmatrix} x_2 \\ x_1 \oplus 1 \end{bmatrix}, якщо\ k_1 = 0; k_2 = 1 \end{cases} = O_8^k = \begin{cases} \begin{bmatrix} x_1 \oplus 1 \\ x_2 \end{bmatrix}, якщо\ k_1 = 1; k_2 = 1 \\ \begin{bmatrix} x_1 \\ x_2 \oplus 1 \end{bmatrix}, якщо\ k_1 = 0; k_2 = 0 \\ \begin{bmatrix} x_2 \oplus 1 \\ x_1 \end{bmatrix}, якщо\ k_1 = 1; k_2 = 0 \\ \begin{bmatrix} x_2 \\ x_1 \oplus 1 \end{bmatrix}, якщо\ k_1 = 0; k_2 = 1 \end{cases} = O_8^k = \begin{bmatrix} x_1 \cdot \bar{k}_1 \oplus x_2 \cdot k_1 \\ x_1 \cdot k_1 \oplus x_2 \cdot \bar{k}_1 \end{bmatrix} \oplus \begin{bmatrix} \bar{k}_2 \\ k_2 \end{bmatrix} \quad (3.71)$$

саме це і потрібно було довести.

Оскільки наступна двохрозрядна одноопераднда операція представлена $F_{9,12}=\begin{bmatrix} x_1 \oplus x_2 \oplus 1 \\ x_1 \oplus 1 \end{bmatrix}$, виконаємо перетворення другого операнда двохоперандної операції строгого криптографічного кодування $O_3^k=\begin{bmatrix} x_1 \cdot (\overline{k_1 \oplus k_2}) \oplus x_2 \cdot (k_1 \oplus k_2) \\ x_1 \cdot (k_1 \oplus k_2) \oplus x_2 \cdot \overline{(k_1 \oplus k_2)} \end{bmatrix} \oplus \begin{bmatrix} k_1 \\ \bar{k}_1 \end{bmatrix}$ за допомогою неї. Внаслідок цього отримано нову операцію строгого стійкого кодування $O_{10}^k=\begin{bmatrix} x_1 \cdot \bar{k}_2 \oplus x_2 \cdot k_2 \\ x_1 \cdot k_2 \oplus x_2 \cdot \bar{k}_2 \end{bmatrix} \oplus \begin{bmatrix} \bar{k}_2 \\ k_2 \end{bmatrix}$.

Так як перетворення має наступний вигляд:

$$F_{9,12}(O_3^k)=\begin{cases} \begin{bmatrix} x_1 \oplus 1 \\ x_2 \end{bmatrix}, якщо\ k_1=1; k_2=1 \\ \begin{bmatrix} x_2 \\ x_1 \oplus 1 \end{bmatrix}, якщо\ k_1=0; k_2=1 \\ \begin{bmatrix} x_1 \\ x_2 \oplus 1 \end{bmatrix}, якщо\ k_1=0; k_2=0 \\ \begin{bmatrix} x_2 \oplus 1 \\ x_1 \end{bmatrix}, якщо\ k_1=1; k_2=0 \end{cases} = O_{10}^k = \begin{cases} \begin{bmatrix} x_1 \oplus 1 \\ x_2 \end{bmatrix}, якщо\ k_1=1; k_2=1 \\ \begin{bmatrix} x_2 \\ x_1 \oplus 1 \end{bmatrix}, якщо\ k_1=0; k_2=1 \\ \begin{bmatrix} x_1 \\ x_2 \oplus 1 \end{bmatrix}, якщо\ k_1=0; k_2=0 \\ \begin{bmatrix} x_2 \oplus 1 \\ x_1 \end{bmatrix}, якщо\ k_1=1; k_2=0 \end{cases} = O_{10}^k = \begin{bmatrix} x_1 \cdot \bar{k}_2 \oplus x_2 \cdot k_2 \\ x_1 \cdot k_2 \oplus x_2 \cdot \bar{k}_2 \end{bmatrix} \oplus \begin{bmatrix} \bar{k}_2 \\ k_2 \end{bmatrix} \quad (3.72)$$

це й доводить вірність нашого твердження.

Дані операції перетворення показують, що з однієї операції $O_3^k=\begin{bmatrix} x_1 \cdot (\overline{k_1 \oplus k_2}) \oplus x_2 \cdot (k_1 \oplus k_2) \\ x_1 \cdot (k_1 \oplus k_2) \oplus x_2 \cdot \overline{(k_1 \oplus k_2)} \end{bmatrix} \oplus \begin{bmatrix} k_1 \\ \bar{k}_1 \end{bmatrix}$, можна отримати повну групу двохрозрядних двохоперандних операцій ССКК.

3.4 Метод синтезу групи двохрозрядних двохоперандних операцій строгого криптографічного кодування на основі заданої операції.

Розглянемо синтез групи двохрозрядних двохоперандних операцій строгого криптографічного кодування на основі четвертої операції, яка представлена у наступному вигляді $O_4^k = \begin{bmatrix} x_1 \cdot \bar{k}_2 \oplus x_2 \cdot k_2 \\ x_1 \cdot k_2 \oplus x_2 \cdot \bar{k}_2 \end{bmatrix} \oplus \begin{bmatrix} k_1 \\ \bar{k}_1 \end{bmatrix}$.

Зокрема, якщо над другим операндом двохоперандної операції строгого криптографічного кодування $O_4^k = \begin{bmatrix} x_1 \cdot \bar{k}_2 \oplus x_2 \cdot k_2 \\ x_1 \cdot k_2 \oplus x_2 \cdot \bar{k}_2 \end{bmatrix} \oplus \begin{bmatrix} k_1 \\ \bar{k}_1 \end{bmatrix}$ виконати одноопераднe криптографічне перетворення $F_{3,5} = \begin{bmatrix} x_1 \\ x_2 \end{bmatrix}$, то буде отримана операція строгого стійкого кодування $O_4^k = \begin{bmatrix} x_1 \cdot \bar{k}_2 \oplus x_2 \cdot k_2 \\ x_1 \cdot k_2 \oplus x_2 \cdot \bar{k}_2 \end{bmatrix} \oplus \begin{bmatrix} k_1 \\ \bar{k}_1 \end{bmatrix}$.

Так як:

$$F_{3,5}(O_4^k) = \begin{cases} \begin{bmatrix} x_1 \\ x_2 \oplus 1 \end{bmatrix}, \text{ якщо } k_1 = 0; k_2 = 0 \\ \begin{bmatrix} x_2 \\ x_1 \oplus 1 \end{bmatrix}, \text{якщо } k_1 = 0; k_2 = 1 \\ \begin{bmatrix} x_1 \oplus 1 \\ x_2 \end{bmatrix}, \text{ якщо } k_1 = 1; k_2 = 0 \\ \begin{bmatrix} x_2 \oplus 1 \\ x_1 \end{bmatrix}, \text{якщо } k_1 = 1; k_2 = 1 \end{cases} = O_4^k = \begin{cases} \begin{bmatrix} x_1 \\ x_2 \oplus 1 \end{bmatrix}, \text{ якщо } k_1 = 0; k_2 = 0 \\ \begin{bmatrix} x_2 \\ x_1 \oplus 1 \end{bmatrix}, \text{якщо } k_1 = 0; k_2 = 1 \\ \begin{bmatrix} x_1 \oplus 1 \\ x_2 \end{bmatrix}, \text{ якщо } k_1 = 1; k_2 = 0 \\ \begin{bmatrix} x_2 \oplus 1 \\ x_1 \end{bmatrix}, \text{якщо } k_1 = 1; k_2 = 1 \end{cases} = O_4^k = \begin{bmatrix} x_1 \cdot \bar{k}_2 \oplus x_2 \cdot k_2 \\ x_1 \cdot k_2 \oplus x_2 \cdot \bar{k}_2 \end{bmatrix} \oplus \begin{bmatrix} k_1 \\ \bar{k}_1 \end{bmatrix} \quad (3.73)$$

це і потрібно було довести.

При виконанні над другим операндом двохоперандної операції строгого криптографічного кодування $O_4^k = \begin{bmatrix} x_1 \cdot \bar{k}_2 \oplus x_2 \cdot k_2 \\ x_1 \cdot k_2 \oplus x_2 \cdot \bar{k}_2 \end{bmatrix} \oplus \begin{bmatrix} k_1 \\ \bar{k}_1 \end{bmatrix}$ одноопераднoго криптографічного перетворення $F_{6,5} = \begin{bmatrix} x_1 \oplus x_2 \\ x_2 \end{bmatrix}$, в результаті буде отримана операція строгого стійкого кодування $O_5^k = \begin{bmatrix} x_1 \cdot \bar{k}_2 \oplus x_2 \cdot k_2 \\ x_1 \cdot k_2 \oplus x_2 \cdot \bar{k}_2 \end{bmatrix} \oplus \begin{bmatrix} k_1 \oplus k_2 \\ \overline{k_1 \oplus k_2} \end{bmatrix}$.

Оскільки перетворення має наступний вигляд:

$$F_{6,5}(O_4^k)=\begin{cases}\begin{bmatrix}x_1\\x_2\oplus 1\end{bmatrix}, \text{ якщо } k_1=0;\ k_2=0\\ \begin{bmatrix}x_2\oplus 1\\x_1\end{bmatrix}, \text{якщо } k_1=1;\ k_2=1\\ \begin{bmatrix}x_1\oplus 1\\x_2\end{bmatrix}, \text{ якщо } k_1=1;\ k_2=0\\ \begin{bmatrix}x_2\\x_1\oplus 1\end{bmatrix}, \text{якщо } k_1=1;\ k_2=1\end{cases}=O_5^k=\begin{cases}\begin{bmatrix}x_1\\x_2\oplus 1\end{bmatrix}, \text{ якщо } k_1=0;\ k_2=0\\ \begin{bmatrix}x_2\oplus 1\\x_1\end{bmatrix}, \text{якщо } k_1=1;\ k_2=1\\ \begin{bmatrix}x_1\oplus 1\\x_2\end{bmatrix}, \text{ якщо } k_1=1;\ k_2=0\\ \begin{bmatrix}x_2\\x_1\oplus 1\end{bmatrix}, \text{якщо } k_1=1;\ k_2=1\end{cases}=O_5^k=\begin{bmatrix}x_1\cdot\bar{k}_2\oplus x_2\cdot k_2\\ x_1\cdot k_2\oplus x_2\cdot\bar{k}_2\end{bmatrix}\oplus\begin{bmatrix}k_1\oplus k_2\\ \overline{k_1\oplus k_2}\end{bmatrix} \tag{3.74}$$

це доводить наше твердження.

Якщо над другим операндом двохоперандної операції строгого криптографічного кодування $O_4^k=\begin{bmatrix}x_1\cdot\bar{k}_2\oplus x_2\cdot k_2\\ x_1\cdot k_2\oplus x_2\cdot\bar{k}_2\end{bmatrix}\oplus\begin{bmatrix}k_1\\ \bar{k}_1\end{bmatrix}$ виконати одноопераднде криптографічне перетворення $F_{3,6}=\begin{bmatrix}x_1\\ x_1\oplus x_2\end{bmatrix}$, то буде отримана операція строгого стійкого кодування $O_3^k=\begin{bmatrix}x_1\cdot(\overline{k_1\oplus k_2})\oplus x_2\cdot(k_1\oplus k_2)\\ x_1\cdot(k_1\oplus k_2)\oplus x_2\cdot(\overline{k_1\oplus k_2})\end{bmatrix}\oplus\begin{bmatrix}k_1\\ \bar{k}_1\end{bmatrix}$.

Так як:

$$F_{3,6}(O_4^k)=\begin{cases}\begin{bmatrix}x_1\\x_2\oplus 1\end{bmatrix}, \text{ якщо } k_1=0;\ k_2=0\\ \begin{bmatrix}x_2\\x_1\oplus 1\end{bmatrix}, \text{якщо } k_1=0;\ k_2=1\\ \begin{bmatrix}x_1\oplus 1\\x_2\end{bmatrix}, \text{ якщо } k_1=1;\ k_2=0\\ \begin{bmatrix}x_2\oplus 1\\x_1\end{bmatrix}, \text{якщо } k_1=1;\ k_2=1\end{cases}=O_3^k=\begin{cases}\begin{bmatrix}x_1\\x_2\oplus 1\end{bmatrix}, \text{ якщо } k_1=0;\ k_2=0\\ \begin{bmatrix}x_2\\x_1\oplus 1\end{bmatrix}, \text{якщо } k_1=0;\ k_2=1\\ \begin{bmatrix}x_2\oplus 1\\x_1\end{bmatrix}, \text{якщо } k_1=1;\ k_2=1\\ \begin{bmatrix}x_1\oplus 1\\x_2\end{bmatrix}, \text{ якщо } k_1=1;\ k_2=0\end{cases}=O_3^k=\begin{bmatrix}x_1\cdot(\overline{k_1\oplus k_2})\oplus x_2\cdot(k_1\oplus k_2)\\ x_1\cdot(k_1\oplus k_2)\oplus x_2\cdot(\overline{k_1\oplus k_2})\end{bmatrix}\oplus\begin{bmatrix}k_1\\ \bar{k}_1\end{bmatrix} \tag{3.75}$$

отже, це показує, що наше твердження вірне.

При виконанні одноопераднього криптографічного перетворення $F_{5,3}=\begin{bmatrix}x_2\\ x_1\end{bmatrix}$, над другим операндом двохоперандної операції строгого криптографічного кодування $O_4^k=\begin{bmatrix}x_1\cdot\bar{k}_2\oplus x_2\cdot k_2\\ x_1\cdot k_2\oplus x_2\cdot\bar{k}_2\end{bmatrix}\oplus\begin{bmatrix}k_1\\ \bar{k}_1\end{bmatrix}$, отримана операція строгого стійкого кодування $O_1^k=\begin{bmatrix}x_1\cdot\bar{k}_1\oplus x_2\cdot k_1\\ x_1\cdot k_1\oplus x_2\cdot\bar{k}_1\end{bmatrix}\oplus\begin{bmatrix}k_2\\ \bar{k}_2\end{bmatrix}$.

Внаслідок перетворення отримуємо наступне:

$$F_{5,3}(O_4^k)=\begin{cases}\begin{bmatrix}x_1\\ x_2\oplus 1\end{bmatrix}, якщо\ k_1=0;\ k_2=0\\ \begin{bmatrix}x_1\oplus 1\\ x_2\end{bmatrix}, якщо\ k_1=1;\ k_2=0\\ \begin{bmatrix}x_2\\ x_1\oplus 1\end{bmatrix}, якщо\ k_1=0;\ k_2=1\\ \begin{bmatrix}x_2\oplus 1\\ x_1\end{bmatrix}, якщо\ k_1=1;\ k_2=1\end{cases}=O_1^k=\begin{cases}\begin{bmatrix}x_1\\ x_2\oplus 1\end{bmatrix}, якщо\ k_1=0;\ k_2=0\\ \begin{bmatrix}x_1\oplus 1\\ x_2\end{bmatrix}, якщо\ k_1=1;\ k_2=0\\ \begin{bmatrix}x_2\\ x_1\oplus 1\end{bmatrix}, якщо\ k_1=0;\ k_2=1\\ \begin{bmatrix}x_2\oplus 1\\ x_1\end{bmatrix}, якщо\ k_1=1;\ k_2=1\end{cases}=O_1^k=\begin{bmatrix}x_1\cdot\bar{k}_1\oplus x_2\cdot k_1\\ x_1\cdot k_1\oplus x_2\cdot\bar{k}_1\end{bmatrix}\oplus\begin{bmatrix}k_2\\ \bar{k}_2\end{bmatrix} \quad (3.76)$$

що і потрібно було довести.

У випадку виконання над другим операндом двохоперандної операції строгого криптографічного кодування $O_4^k=\begin{bmatrix}x_1\cdot\bar{k}_2\oplus x_2\cdot k_2\\ x_1\cdot k_2\oplus x_2\cdot\bar{k}_2\end{bmatrix}\oplus\begin{bmatrix}k_1\\ \bar{k}_1\end{bmatrix}$ одноопераднього криптографічного перетворення $F_{5,6}=\begin{bmatrix}x_2\\ x_1\oplus x_2\end{bmatrix}$, то буде отримана операція строгого стійкого кодування $O_6^k=\begin{bmatrix}x_1\cdot(\overline{k_1\oplus k_2})\oplus x_2\cdot(k_1\oplus k_2)\\ x_1\cdot(k_1\oplus k_2)\oplus x_2\cdot(\overline{k_1\oplus k_2})\end{bmatrix}\oplus\begin{bmatrix}k_2\\ \bar{k}_2\end{bmatrix}$.

Так як:

$$F_{5,6}(O_4^k)=\begin{cases}\begin{bmatrix}x_1\\ x_2\oplus 1\end{bmatrix}, якщо\ k_1=0;\ k_2=0\\ \begin{bmatrix}x_2\oplus 1\\ x_1\end{bmatrix}, якщо\ k_1=1;\ k_2=1\\ \begin{bmatrix}x_2\\ x_1\oplus 1\end{bmatrix}, якщо\ k_1=0;\ k_2=1\\ \begin{bmatrix}x_1\oplus 1\\ x_2\end{bmatrix}, якщо\ k_1=1;\ k_2=0\end{cases}=O_6^k=\begin{cases}\begin{bmatrix}x_1\\ x_2\oplus 1\end{bmatrix}, якщо\ k_1=0;\ k_2=0\\ \begin{bmatrix}x_2\oplus 1\\ x_1\end{bmatrix}, якщо\ k_1=1;\ k_2=1\\ \begin{bmatrix}x_2\\ x_1\oplus 1\end{bmatrix}, якщо\ k_1=0;\ k_2=1\\ \begin{bmatrix}x_1\oplus 1\\ x_2\end{bmatrix}, якщо\ k_1=1;\ k_2=0\end{cases}=O_6^k=\begin{bmatrix}x_1\cdot(\overline{k_1\oplus k_2})\oplus x_2\cdot(k_1\oplus k_2)\\ x_1\cdot(k_1\oplus k_2)\oplus x_2\cdot(\overline{k_1\oplus k_2})\end{bmatrix}\oplus\begin{bmatrix}k_2\\ \bar{k}_2\end{bmatrix} \quad (3.77)$$

саме це і потрібно було довести.

Внаслідок наступного перетворення другого операнда двохоперандної операції строгого криптографічного кодування $O_4^k=\begin{bmatrix}x_1\cdot\bar{k}_2\oplus x_2\cdot k_2\\ x_1\cdot k_2\oplus x_2\cdot\bar{k}_2\end{bmatrix}\oplus\begin{bmatrix}k_1\\ \bar{k}_1\end{bmatrix}$ одноопераднною операцією $F_{6,3}=\begin{bmatrix}x_1\oplus x_2\\ x_1\end{bmatrix}$, буде отримана операція строгого стійкого кодування $O_2^k=\begin{bmatrix}x_1\cdot\bar{k}_1\oplus x_2\cdot k_1\\ x_1\cdot k_1\oplus x_2\cdot\bar{k}_1\end{bmatrix}\oplus\begin{bmatrix}k_1\oplus k_2\\ \overline{k_1\oplus k_2}\end{bmatrix}$.

Так як:

$$F_{6,3}(O_4^k)=\begin{cases}\begin{bmatrix}x_1\\ x_2\oplus 1\end{bmatrix}, \text{ якщо } k_1=0;\ k_2=0\\ \begin{bmatrix}x_1\oplus 1\\ x_2\end{bmatrix}, \text{ якщо } k_1=1;\ k_2=0\\ \begin{bmatrix}x_2\oplus 1\\ x_1\end{bmatrix}, \text{якщо } k_1=1;\ k_2=1\\ \begin{bmatrix}x_2\\ x_1\oplus 1\end{bmatrix}, \text{якщо } k_1=1;\ k_2=1\end{cases}=O_2^k=\begin{cases}\begin{bmatrix}x_1\\ x_2\oplus 1\end{bmatrix}, \text{ якщо } k_1=0;\ k_2=0\\ \begin{bmatrix}x_1\oplus 1\\ x_2\end{bmatrix}, \text{ якщо } k_1=1;\ k_2=0\\ \begin{bmatrix}x_2\oplus 1\\ x_1\end{bmatrix}, \text{якщо } k_1=1;\ k_2=1\\ \begin{bmatrix}x_2\\ x_1\oplus 1\end{bmatrix}, \text{якщо } k_1=1;\ k_2=1\end{cases}=O_2^k=\begin{bmatrix}x_1\cdot\bar{k}_1\oplus x_2\cdot k_1\\ x_1\cdot k_1\oplus x_2\cdot\bar{k}_1\end{bmatrix}\oplus\begin{bmatrix}k_1\oplus k_2\\ \overline{k_1\oplus k_2}\end{bmatrix} \quad (3.78)$$

що і потрібно було довести.

Якщо над другим операндом двохоперандної операції строгого криптографічного кодування $O_4^k=\begin{bmatrix}x_1\cdot\bar{k}_2\oplus x_2\cdot k_2\\ x_1\cdot k_2\oplus x_2\cdot\bar{k}_2\end{bmatrix}\oplus\begin{bmatrix}k_1\\ \bar{k}_1\end{bmatrix}$ виконати одноопераднде криптографічне перетворення $F_{3,10}=\begin{bmatrix}x_1\\ x_2\oplus 1\end{bmatrix}$, то буде отримана операція строгого стійкого кодування $O_{15}^k=\begin{bmatrix}x_1\cdot k_2\oplus x_2\cdot\bar{k}_2\\ x_1\cdot\bar{k}_2\oplus x_2\cdot k_2\end{bmatrix}\oplus\begin{bmatrix}k_1\\ \bar{k}_1\end{bmatrix}$.

Так як:

$$F_{3,10}(O_4^k)=\begin{cases}\begin{bmatrix}x_2\\ x_1\oplus 1\end{bmatrix}, \text{ якщо } k_1=0;\ k_2=0\\ \begin{bmatrix}x_1\\ x_2\oplus 1\end{bmatrix}, \text{якщо } k_1=0;\ k_2=1\\ \begin{bmatrix}x_2\oplus 1\\ x_1\end{bmatrix}, \text{якщо } k_1=1;\ k_2=1\\ \begin{bmatrix}x_1\oplus 1\\ x_2\end{bmatrix}, \text{якщо } k_1=1;\ k_2=0\end{cases}=O_{15}^k=\begin{cases}\begin{bmatrix}x_2\\ x_1\oplus 1\end{bmatrix}, \text{ якщо } k_1=0;\ k_2=0\\ \begin{bmatrix}x_1\\ x_2\oplus 1\end{bmatrix}, \text{якщо } k_1=0;\ k_2=1\\ \begin{bmatrix}x_2\oplus 1\\ x_1\end{bmatrix}, \text{якщо } k_1=1;\ k_2=1\\ \begin{bmatrix}x_1\oplus 1\\ x_2\end{bmatrix}, \text{якщо } k_1=1;\ k_2=0\end{cases}=O_{15}^k=\begin{bmatrix}x_1\cdot k_2\oplus x_2\cdot\bar{k}_2\\ x_1\cdot\bar{k}_2\oplus x_2\cdot k_2\end{bmatrix}\oplus\begin{bmatrix}k_1\\ \bar{k}_1\end{bmatrix} \quad (3.79)$$

що і потрібно було довести.

За умови, якщо над другим операндом двохоперандної операції строгого криптографічного кодування $O_4^k=\begin{bmatrix}x_1\cdot\bar{k}_2\oplus x_2\cdot k_2\\ x_1\cdot k_2\oplus x_2\cdot\bar{k}_2\end{bmatrix}\oplus\begin{bmatrix}k_1\\ \bar{k}_1\end{bmatrix}$ виконати одноопераднде криптографічне перетворення $F_{6,10}=\begin{bmatrix}x_1\oplus x_2\\ x_2\oplus 1\end{bmatrix}$, то буде отримана операція строгого стійкого кодування $O_{14}^k=\begin{bmatrix}x_1\cdot k_2\oplus x_2\cdot\bar{k}_2\\ x_1\cdot\bar{k}_2\oplus x_2\cdot k_2\end{bmatrix}\oplus\begin{bmatrix}k_2\\ \bar{k}_2\end{bmatrix}$.

Так як:

$$F_{6,10}(O_4^k)=\begin{cases}\begin{bmatrix}x_2\\x_1\oplus 1\end{bmatrix}, якщо\ k_1=0;\ k_2=0\\ \begin{bmatrix}x_1\oplus 1\\x_2\end{bmatrix}, якщо\ k_1=1;\ k_2=0\\ \begin{bmatrix}x_2\oplus 1\\x_1\end{bmatrix}, якщо\ k_1=1;\ k_2=1\\ \begin{bmatrix}x_1\\x_2\oplus 1\end{bmatrix}, якщо\ k_1=1;\ k_2=1\end{cases}=O_{14}^k=\begin{cases}\begin{bmatrix}x_2\\x_1\oplus 1\end{bmatrix}, якщо\ k_1=0;\ k_2=0\\ \begin{bmatrix}x_1\oplus 1\\x_2\end{bmatrix}, якщо\ k_1=1;\ k_2=0\\ \begin{bmatrix}x_2\oplus 1\\x_1\end{bmatrix}, якщо\ k_1=1;\ k_2=1\\ \begin{bmatrix}x_1\\x_2\oplus 1\end{bmatrix}, якщо\ k_1=1;\ k_2=1\end{cases}=O_{14}^k=\begin{bmatrix}x_1\cdot k_2\oplus x_2\cdot\bar{k}_2\\x_1\cdot\bar{k}_2\oplus x_2\cdot k_2\end{bmatrix}\oplus\begin{bmatrix}k_2\\\bar{k}_2\end{bmatrix}$$

(3.80)

отже, це те, що потрібно було довести.

Якщо над другим операндом двохоперандної операції строгого криптографічного кодування $O_4^k=\begin{bmatrix}x_1\cdot\bar{k}_2\oplus x_2\cdot k_2\\x_1\cdot k_2\oplus x_2\cdot\bar{k}_2\end{bmatrix}\oplus\begin{bmatrix}k_1\\\bar{k}_1\end{bmatrix}$ виконати одноопераднe криптографічне перетворення $F_{3,9}=\begin{bmatrix}x_1\\x_1\oplus x_2\oplus 1\end{bmatrix}$, то буде отримана операція строгого стійкого кодування $O_{16}^k=\begin{bmatrix}x_1\cdot(k_1\oplus k_2)\oplus x_2\cdot(\overline{k_1\oplus k_2})\\x_1\cdot(\overline{k_1\oplus k_2})\oplus x_2\cdot(k_1\oplus k_2)\end{bmatrix}\oplus\begin{bmatrix}k_1\\\bar{k}_1\end{bmatrix}$.

Так як:

$$F_{3,9}(O_4^k)=\begin{cases}\begin{bmatrix}x_2\\x_1\oplus 1\end{bmatrix}, якщо\ k_1=0;\ k_2=0\\ \begin{bmatrix}x_1\\x_2\oplus 1\end{bmatrix}, якщо\ k_1=0;\ k_2=1\\ \begin{bmatrix}x_1\oplus 1\\x_2\end{bmatrix}, якщо\ k_1=1;\ k_2=0\\ \begin{bmatrix}x_2\oplus 1\\x_1\end{bmatrix}, якщо\ k_1=1;\ k_2=1\end{cases}=O_{16}^k=\begin{cases}\begin{bmatrix}x_2\\x_1\oplus 1\end{bmatrix}, якщо\ k_1=0;\ k_2=0\\ \begin{bmatrix}x_1\\x_2\oplus 1\end{bmatrix}, якщо\ k_1=0;\ k_2=1\\ \begin{bmatrix}x_1\oplus 1\\x_2\end{bmatrix}, якщо\ k_1=1;\ k_2=0\\ \begin{bmatrix}x_2\oplus 1\\x_1\end{bmatrix}, якщо\ k_1=1;\ k_2=1\end{cases}=O_{16}^k=\begin{bmatrix}x_1\cdot(k_1\oplus k_2)\oplus x_2\cdot(\overline{k_1\oplus k_2})\\x_1\cdot(\overline{k_1\oplus k_2})\oplus x_2\cdot(k_1\oplus k_2)\end{bmatrix}\oplus\begin{bmatrix}k_1\\\bar{k}_1\end{bmatrix}\quad(3.81)$$

це й потрібно було довести.

У випадку, коли над другим операндом двохоперандної операції строгого криптографічного кодування $O_4^k=\begin{bmatrix}x_1\cdot\bar{k}_2\oplus x_2\cdot k_2\\x_1\cdot k_2\oplus x_2\cdot\bar{k}_2\end{bmatrix}\oplus\begin{bmatrix}k_1\\\bar{k}_1\end{bmatrix}$ виконано одноопераднe криптографічне перетворення $F_{5,12}=\begin{bmatrix}x_2\\x_1\oplus 1\end{bmatrix}$, результатом буде отримана операція строгого стійкого кодування $O_{18}^k=\begin{bmatrix}x_1\cdot k_1\oplus x_2\cdot\bar{k}_1\\x_1\cdot\bar{k}_1\oplus x_2\cdot k_1\end{bmatrix}\oplus\begin{bmatrix}k_2\\\bar{k}_2\end{bmatrix}$.

Так як:

$$F_{5,12}(O_4^k)=\begin{cases}\begin{bmatrix}x_2\\ x_1\oplus 1\end{bmatrix}, якщо\ k_1=0;\ k_2=0\\ \begin{bmatrix}x_2\oplus 1\\ x_1\end{bmatrix}, якщо\ k_1=1;\ k_2=1\\ \begin{bmatrix}x_1\\ x_2\oplus 1\end{bmatrix}, якщо\ k_1=1;\ k_2=0\\ \begin{bmatrix}x_1\oplus 1\\ x_2\end{bmatrix}, якщо\ k_1=1;\ k_2=0\end{cases}=O_{18}^k=\begin{cases}\begin{bmatrix}x_2\\ x_1\oplus 1\end{bmatrix}, якщо\ k_1=0;\ k_2=0\\ \begin{bmatrix}x_2\oplus 1\\ x_1\end{bmatrix}, якщо\ k_1=1;\ k_2=1\\ \begin{bmatrix}x_1\\ x_2\oplus 1\end{bmatrix}, якщо\ k_1=1;\ k_2=0\\ \begin{bmatrix}x_1\oplus 1\\ x_2\end{bmatrix}, якщо\ k_1=1;\ k_2=0\end{cases}=O_{18}^k=\begin{bmatrix}x_1\cdot k_1\oplus x_2\cdot\bar{k}_1\\ x_1\cdot\bar{k}_1\oplus x_2\cdot k_1\end{bmatrix}\oplus\begin{bmatrix}k_2\\ \bar{k}_2\end{bmatrix}\quad(3.82)$$

саме це потрібно було довести.

Якщо над другим операндом двохоперандної операції строгого стійкого криптографічного кодування $O_4^k=\begin{bmatrix}x_1\cdot\bar{k}_2\oplus x_2\cdot k_2\\ x_1\cdot k_2\oplus x_2\cdot\bar{k}_2\end{bmatrix}\oplus\begin{bmatrix}k_1\\ \bar{k}_1\end{bmatrix}$ виконати одноопераднe криптографічне перетворення $F_{5,9}=\begin{bmatrix}x_2\\ x_1\oplus x_2\oplus 1\end{bmatrix}$, то буде отримана операція строгого стійкого кодування $O_{13}^k=\begin{bmatrix}x_1\cdot(k_1\oplus k_2)\oplus x_2\cdot(\overline{k_1\oplus k_2})\\ x_1\cdot(\overline{k_1\oplus k_2})\oplus x_2\cdot(k_1\oplus k_2)\end{bmatrix}\oplus\begin{bmatrix}k_2\\ \bar{k}_2\end{bmatrix}$.

Так як перетворення набуває наступного винляду:

$$F_{5,9}(O_4^k)=\begin{cases}\begin{bmatrix}x_2\\ x_1\oplus 1\end{bmatrix}, якщо\ k_1=0;\ k_2=0\\ \begin{bmatrix}x_1\oplus 1\\ x_2\end{bmatrix}, якщо\ k_1=1;\ k_2=0\\ \begin{bmatrix}x_1\\ x_2\oplus 1\end{bmatrix}, якщо\ k_1=1;\ k_2=0\\ \begin{bmatrix}x_2\oplus 1\\ x_1\end{bmatrix}, якщо\ k_1=1;\ k_2=1\end{cases}=O_{13}^k=\begin{cases}\begin{bmatrix}x_2\\ x_1\oplus 1\end{bmatrix}, якщо\ k_1=0;\ k_2=0\\ \begin{bmatrix}x_1\oplus 1\\ x_2\end{bmatrix}, якщо\ k_1=1;\ k_2=0\\ \begin{bmatrix}x_1\\ x_2\oplus 1\end{bmatrix}, якщо\ k_1=1;\ k_2=0\\ \begin{bmatrix}x_2\oplus 1\\ x_1\end{bmatrix}, якщо\ k_1=1;\ k_2=1\end{cases}=O_{13}^k=\begin{bmatrix}x_1\cdot(k_1\oplus k_2)\oplus x_2\cdot(\overline{k_1\oplus k_2})\\ x_1\cdot(\overline{k_1\oplus k_2})\oplus x_2\cdot(k_1\oplus k_2)\end{bmatrix}\oplus\begin{bmatrix}k_2\\ \bar{k}_2\end{bmatrix}\quad(3.83)$$

це вказує на правильність твердження.

Якщо над другим операндом двохоперандної операції строгого криптографічного кодування $O_4^k=\begin{bmatrix}x_1\cdot\bar{k}_2\oplus x_2\cdot k_2\\ x_1\cdot k_2\oplus x_2\cdot\bar{k}_2\end{bmatrix}\oplus\begin{bmatrix}k_1\\ \bar{k}_1\end{bmatrix}$ виконати одноопераднe криптографічне перетворення $F_{6,12}=\begin{bmatrix}x_1\oplus x_2\\ x_1\oplus 1\end{bmatrix}$, то буде отримана операція строгого стійкого кодування $O_{17}^k=\begin{bmatrix}x_1\cdot k_1\oplus x_2\cdot\bar{k}_1\\ x_1\cdot\bar{k}_1\oplus x_2\cdot k_1\end{bmatrix}\oplus\begin{bmatrix}k_1\oplus k_2\\ \overline{k_1\oplus k_2}\end{bmatrix}$.

Оскільки:

$$F_{6,12}(O_4^k)=\begin{cases}\begin{bmatrix}x_2\\ x_1\oplus 1\end{bmatrix}, & якщо\ k_1=0;\ k_2=0\\ \begin{bmatrix}x_2\oplus 1\\ x_1\end{bmatrix}, & якщо\ k_1=1;\ k_2=1\\ \begin{bmatrix}x_1\oplus 1\\ x_2\end{bmatrix}, & якщо\ k_1=1;\ k_2=0\\ \begin{bmatrix}x_1\\ x_2\oplus 1\end{bmatrix}, & якщо\ k_1=1;\ k_2=1\end{cases}=O_{17}^k=\begin{cases}\begin{bmatrix}x_2\\ x_1\oplus 1\end{bmatrix}, & якщо\ k_1=0;\ k_2=0\\ \begin{bmatrix}x_2\oplus 1\\ x_1\end{bmatrix}, & якщо\ k_1=1;\ k_2=1\\ \begin{bmatrix}x_1\oplus 1\\ x_2\end{bmatrix}, & якщо\ k_1=1;\ k_2=0\\ \begin{bmatrix}x_1\\ x_2\oplus 1\end{bmatrix}, & якщо\ k_1=1;\ k_2=1\end{cases}=O_{17}^k=\begin{bmatrix}x_1\cdot k_1\oplus x_2\cdot\bar{k}_1\\ x_1\cdot\bar{k}_1\oplus x_2\cdot k_1\end{bmatrix}\oplus\begin{bmatrix}k_1\oplus k_2\\ \overline{k_1\oplus k_2}\end{bmatrix} \tag{3.84}$$

це доводить наше твердження.

Якщо над другим операндом двохоперандної операції строгого криптографічного кодування $O_4^k=\begin{bmatrix}x_1\cdot\bar{k}_2\oplus x_2\cdot k_2\\ x_1\cdot k_2\oplus x_2\cdot\bar{k}_2\end{bmatrix}\oplus\begin{bmatrix}k_1\\ \bar{k}_1\end{bmatrix}$ виконати одноопераднe криптографічне перетворення $F_{12,5}=\begin{bmatrix}x_1\oplus 1\\ x_2\end{bmatrix}$, то буде отримана операція строгого стійкого кодування $O_{11}^k=\begin{bmatrix}x_1\cdot\bar{k}_2\oplus x_2\cdot k_2\\ x_1\cdot k_2\oplus x_2\cdot\bar{k}_2\end{bmatrix}\oplus\begin{bmatrix}\bar{k}_1\\ k_1\end{bmatrix}$.

Так як:

$$F_{12,5}(O_4^k)=\begin{cases}\begin{bmatrix}x_1\oplus 1\\ x_2\end{bmatrix}, & якщо\ k_1=1;\ k_2=0\\ \begin{bmatrix}x_2\oplus 1\\ x_1\end{bmatrix}, & якщо\ k_1=1;\ k_2=1\\ \begin{bmatrix}x_1\\ x_2\oplus 1\end{bmatrix}, & якщо\ k_1=0;\ k_2=0\\ \begin{bmatrix}x_2\\ x_1\oplus 1\end{bmatrix}, & якщо\ k_1=0;\ k_2=1\end{cases}=O_{11}^k=\begin{cases}\begin{bmatrix}x_1\oplus 1\\ x_2\end{bmatrix}, & якщо\ k_1=1;\ k_2=0\\ \begin{bmatrix}x_2\oplus 1\\ x_1\end{bmatrix}, & якщо\ k_1=1;\ k_2=1\\ \begin{bmatrix}x_1\\ x_2\oplus 1\end{bmatrix}, & якщо\ k_1=0;\ k_2=0\\ \begin{bmatrix}x_2\\ x_1\oplus 1\end{bmatrix}, & якщо\ k_1=0;\ k_2=1\end{cases}=O_{11}^k=\begin{bmatrix}x_1\cdot\bar{k}_2\oplus x_2\cdot k_2\\ x_1\cdot k_2\oplus x_2\cdot\bar{k}_2\end{bmatrix}\oplus\begin{bmatrix}\bar{k}_1\\ k_1\end{bmatrix} \tag{3.85}$$

Що і потрібно було довести.

Якщо над другим операндом двохоперандної операції строгого криптографічного кодування $O_4^k=\begin{bmatrix}x_1\cdot\bar{k}_2\oplus x_2\cdot k_2\\ x_1\cdot k_2\oplus x_2\cdot\bar{k}_2\end{bmatrix}\oplus\begin{bmatrix}k_1\\ \bar{k}_1\end{bmatrix}$ виконати одноопераднe криптографічне перетворення $F_{9,5}=\begin{bmatrix}x_1\oplus x_2\oplus 1\\ x_2\end{bmatrix}$, то буде отримана операція строгого стійкого кодування $O_{10}^k=\begin{bmatrix}x_1\cdot\bar{k}_2\oplus x_2\cdot k_2\\ x_1\cdot k_2\oplus x_2\cdot\bar{k}_2\end{bmatrix}\oplus\begin{bmatrix}\bar{k}_2\\ k_2\end{bmatrix}$.

Так як:

$$F_{9,5}(O_4^k)=\begin{cases}\begin{bmatrix}x_1\\ x_2\oplus 1\end{bmatrix}, \text{ якщо } k_1=0;\ k_2=0\\ \begin{bmatrix}x_2\\ x_1\oplus 1\end{bmatrix}, \text{якщо } k_1=0;\ k_2=1\\ \begin{bmatrix}x_1\oplus 1\\ x_2\end{bmatrix}, \text{ якщо } k_1=1;\ k_2=0\\ \begin{bmatrix}x_2\oplus 1\\ x_1\end{bmatrix}, \text{якщо } k_1=1;\ k_2=1\end{cases}=O_{10}^k=\begin{cases}\begin{bmatrix}x_1\oplus 1\\ x_2\end{bmatrix}, \text{якщо } k_1=1;\ k_2=0\\ \begin{bmatrix}x_2\\ x_1\oplus 1\end{bmatrix}, \text{якщо } k_1=0;\ k_2=1\\ \begin{bmatrix}x_1\\ x_2\oplus 1\end{bmatrix}, \text{ якщо } k_1=0;\ k_2=0\\ \begin{bmatrix}x_2\oplus 1\\ x_1\end{bmatrix}, \text{якщо } k_1=1;\ k_2=1\end{cases}=O_{10}^k=\begin{bmatrix}x_1\cdot\bar{k}_2\oplus x_2\cdot k_2\\ x_1\cdot k_2\oplus x_2\cdot\bar{k}_2\end{bmatrix}\oplus\begin{bmatrix}\bar{k}_2\\ k_2\end{bmatrix} \quad (3.86)$$

що і потрібно було довести.

Якщо над другим операндом двохоперандної операції строгого криптографічного кодування $O_4^k=\begin{bmatrix}x_1\cdot\bar{k}_2\oplus x_2\cdot k_2\\ x_1\cdot k_2\oplus x_2\cdot\bar{k}_2\end{bmatrix}\oplus\begin{bmatrix}k_1\\ \bar{k}_1\end{bmatrix}$ виконати одноопераднe криптографічне перетворення $F_{12,6}=\begin{bmatrix}x_1\oplus 1\\ x_1\oplus x_2\end{bmatrix}$, то буде отримана операція строгого стійкого кодування $O_{12}^k=\begin{bmatrix}x_1\cdot(\overline{k_1\oplus k_2})\oplus x_2\cdot(k_1\oplus k_2)\\ x_1\cdot(k_1\oplus k_2)\oplus x_2\cdot(\overline{k_1\oplus k_2})\end{bmatrix}\oplus\begin{bmatrix}\bar{k}_1\\ k_1\end{bmatrix}$.

Так як:

$$F_{12,6}(O_4^k)=\begin{cases}\begin{bmatrix}x_1\oplus 1\\ x_2\end{bmatrix}, \text{ якщо } k_1=1;\ k_2=0\\ \begin{bmatrix}x_2\oplus 1\\ x_1\end{bmatrix}, \text{якщо } k_1=1;\ k_2=1\\ \begin{bmatrix}x_2\\ x_1\oplus 1\end{bmatrix}, \text{якщо } k_1=0;\ k_2=1\\ \begin{bmatrix}x_1\\ x_2\oplus 1\end{bmatrix}, \text{ якщо } k_1=0;\ k_2=0\end{cases}=O_{12}^k=\begin{cases}\begin{bmatrix}x_1\oplus 1\\ x_2\end{bmatrix}, \text{ якщо } k_1=1;\ k_2=0\\ \begin{bmatrix}x_2\oplus 1\\ x_1\end{bmatrix}, \text{якщо } k_1=1;\ k_2=1\\ \begin{bmatrix}x_2\\ x_1\oplus 1\end{bmatrix}, \text{якщо } k_1=0;\ k_2=1\\ \begin{bmatrix}x_1\\ x_2\oplus 1\end{bmatrix}, \text{ якщо } k_1=0;\ k_2=0\end{cases}=O_{12}^k=\begin{bmatrix}x_1\cdot(\overline{k_1\oplus k_2})\oplus x_2\cdot(k_1\oplus k_2)\\ x_1\cdot(k_1\oplus k_2)\oplus x_2\cdot(\overline{k_1\oplus k_2})\end{bmatrix}\oplus\begin{bmatrix}\bar{k}_1\\ k_1\end{bmatrix} \quad (3.87)$$

це й потрібно було довести.

При виконанні над другим операндом двохоперандної операції строгого криптографічного кодування $O_4^k=\begin{bmatrix}x_1\cdot\bar{k}_2\oplus x_2\cdot k_2\\ x_1\cdot k_2\oplus x_2\cdot\bar{k}_2\end{bmatrix}\oplus\begin{bmatrix}k_1\\ \bar{k}_1\end{bmatrix}$ одноопераднe криптографічне перетворення $F_{10,3}=\begin{bmatrix}x_2\oplus 1\\ x_1\end{bmatrix}$, то буде отримана операція строгого стійкого кодування $O_8^k=\begin{bmatrix}x_1\cdot\bar{k}_1\oplus x_2\cdot k_1\\ x_1\cdot k_1\oplus x_2\cdot\bar{k}_1\end{bmatrix}\oplus\begin{bmatrix}\bar{k}_2\\ k_2\end{bmatrix}$.

У випадку наступного перетворення:

$$F_{10,3}(O_4^k)=\begin{cases}\begin{bmatrix}x_1\oplus 1\\ x_2\end{bmatrix}, \text{якщо } k_1=1;\ k_2=0\\ \begin{bmatrix}x_1\\ x_2\oplus 1\end{bmatrix}, \text{ якщо } k_1=0;\ k_2=0\\ \begin{bmatrix}x_2\oplus 1\\ x_1\end{bmatrix}, \text{якщо } k_1=1;\ k_2=1\\ \begin{bmatrix}x_2\\ x_1\oplus 1\end{bmatrix}, \text{якщо } k_1=0;\ k_2=1\end{cases}=O_8^k=\begin{cases}\begin{bmatrix}x_1\oplus 1\\ x_2\end{bmatrix}, \text{якщо } k_1=1;\ k_2=0\\ \begin{bmatrix}x_1\\ x_2\oplus 1\end{bmatrix}, \text{ якщо } k_1=0;\ k_2=0\\ \begin{bmatrix}x_2\oplus 1\\ x_1\end{bmatrix}, \text{якщо } k_1=1;\ k_2=1\\ \begin{bmatrix}x_2\\ x_1\oplus 1\end{bmatrix}, \text{якщо } k_1=0;\ k_2=1\end{cases}=O_8^k=\begin{bmatrix}x_1\cdot\bar{k}_1\oplus x_2\cdot k_1\\ x_1\cdot k_1\oplus x_2\cdot\bar{k}_1\end{bmatrix}\oplus\begin{bmatrix}\bar{k}_2\\ k_2\end{bmatrix} \quad (3.88)$$

показано, що наше твердження вірне.

Якщо над другим операндом двохоперандної операції строгого криптографічного кодування $O_4^k=\begin{bmatrix}x_1\cdot\bar{k}_2\oplus x_2\cdot k_2\\ x_1\cdot k_2\oplus x_2\cdot\bar{k}_2\end{bmatrix}\oplus\begin{bmatrix}k_1\\ \bar{k}_1\end{bmatrix}$ виконати одноопераднде криптографічне перетворення $F_{10,6}=\begin{bmatrix}x_2\oplus 1\\ x_1\oplus x_2\end{bmatrix}$, то буде отримана операція строгого стійкого кодування $O_9^k=\begin{bmatrix}x_1\cdot(\overline{k_1\oplus k_2})\oplus x_2\cdot(k_1\oplus k_2)\\ x_1\cdot(k_1\oplus k_2)\oplus x_2\cdot(\overline{k_1\oplus k_2})\end{bmatrix}\oplus\begin{bmatrix}\bar{k}_2\\ k_2\end{bmatrix}$.

Так як:

$$F_{10,6}(O_4^k)=\begin{cases}\begin{bmatrix}x_1\oplus 1\\ x_2\end{bmatrix}, \text{якщо } k_1=1;\ k_2=0\\ \begin{bmatrix}x_2\\ x_1\oplus 1\end{bmatrix}, \text{якщо } k_1=0;\ k_2=1\\ \begin{bmatrix}x_2\oplus 1\\ x_1\end{bmatrix}, \text{якщо } k_1=1;\ k_2=1\\ \begin{bmatrix}x_1\\ x_2\oplus 1\end{bmatrix}, \text{ якщо } k_1=0;\ k_2=0\end{cases}=O_9^k=\begin{cases}\begin{bmatrix}x_1\oplus 1\\ x_2\end{bmatrix}, \text{якщо } k_1=1;\ k_2=0\\ \begin{bmatrix}x_2\\ x_1\oplus 1\end{bmatrix}, \text{якщо } k_1=0;\ k_2=1\\ \begin{bmatrix}x_2\oplus 1\\ x_1\end{bmatrix}, \text{якщо } k_1=1;\ k_2=1\\ \begin{bmatrix}x_1\\ x_2\oplus 1\end{bmatrix}, \text{ якщо } k_1=0;\ k_2=0\end{cases}=O_9^k=\begin{bmatrix}x_1\cdot(\overline{k_1\oplus k_2})\oplus x_2\cdot(k_1\oplus k_2)\\ x_1\cdot(k_1\oplus k_2)\oplus x_2\cdot(\overline{k_1\oplus k_2})\end{bmatrix}\oplus\begin{bmatrix}\bar{k}_2\\ k_2\end{bmatrix} \quad (3.89)$$

що і потрібно було довести.

Якщо над другим операндом двохоперандної операції строгого криптографічного кодування $O_4^k=\begin{bmatrix}x_1\cdot\bar{k}_2\oplus x_2\cdot k_2\\ x_1\cdot k_2\oplus x_2\cdot\bar{k}_2\end{bmatrix}\oplus\begin{bmatrix}k_1\\ \bar{k}_1\end{bmatrix}$ виконати одноопераднде криптографічне перетворення $F_{9,3}=\begin{bmatrix}x_1\oplus x_2\oplus 1\\ x_1\end{bmatrix}$, то буде отримана операція строгого стійкого кодування $O_7^k=\begin{bmatrix}x_1\cdot\bar{k}_1\oplus x_2\cdot k_1\\ x_1\cdot k_1\oplus x_2\cdot\bar{k}_1\end{bmatrix}\oplus\begin{bmatrix}\overline{k_1\oplus k_2}\\ k_1\oplus k_2\end{bmatrix}$.

Так як:

$$F_{9,3}(O_4^k)=\begin{cases}\begin{bmatrix}x_1\oplus 1\\ x_2\end{bmatrix}, \text{якщо } k_1=1;\ k_2=0\\ \begin{bmatrix}x_1\\ x_2\oplus 1\end{bmatrix}, \text{якщо } k_1=0;\ k_2=0\\ \begin{bmatrix}x_2\\ x_1\oplus 1\end{bmatrix}, \text{якщо } k_1=0;\ k_2=1\\ \begin{bmatrix}x_2\oplus 1\\ x_1\end{bmatrix}, \text{якщо } k_1=1;\ k_2=1\end{cases}=O_7^k=\begin{cases}\begin{bmatrix}x_1\oplus 1\\ x_2\end{bmatrix}, \text{якщо } k_1=1;\ k_2=0\\ \begin{bmatrix}x_1\\ x_2\oplus 1\end{bmatrix}, \text{якщо } k_1=0;\ k_2=0\\ \begin{bmatrix}x_2\\ x_1\oplus 1\end{bmatrix}, \text{якщо } k_1=0;\ k_2=1\\ \begin{bmatrix}x_2\oplus 1\\ x_1\end{bmatrix}, \text{якщо } k_1=1;\ k_2=1\end{cases}=O_7^k=\begin{bmatrix}x_1\cdot\bar{k}_1\oplus x_2\cdot k_1\\ x_1\cdot k_1\oplus x_2\cdot\bar{k}_1\end{bmatrix}\oplus\begin{bmatrix}\overline{k_1\oplus k_2}\\ k_1\oplus k_2\end{bmatrix} \tag{3.90}$$

це і потрібно було довести.

Якщо над другим операндом двохоперандної операції строгого криптографічного кодування $O_4^k=\begin{bmatrix}x_1\cdot\bar{k}_2\oplus x_2\cdot k_2\\ x_1\cdot k_2\oplus x_2\cdot\bar{k}_2\end{bmatrix}\oplus\begin{bmatrix}k_1\\ \bar{k}_1\end{bmatrix}$ виконати одноопераднe криптографічне перетворення $F_{12,10}=\begin{bmatrix}x_1\oplus 1\\ x_2\oplus 1\end{bmatrix}$, то буде отримана операція строгого стійкого кодування $O_{19}^k=\begin{bmatrix}x_1\cdot\bar{k}_2\oplus x_2\cdot k_2\\ x_1\cdot k_2\oplus x_2\cdot\bar{k}_2\end{bmatrix}\oplus\begin{bmatrix}k_1\\ \bar{k}_1\end{bmatrix}$.

Так як:

$$F_{12,10}(O_4^k)=\begin{cases}\begin{bmatrix}x_2\oplus 1\\ x_1\end{bmatrix}, \text{якщо } k_1=1;\ k_2=1\\ \begin{bmatrix}x_1\oplus 1\\ x_2\end{bmatrix}, \text{якщо } k_1=1;\ k_2=0\\ \begin{bmatrix}x_2\\ x_1\oplus 1\end{bmatrix}, \text{якщо } k_1=0;\ k_2=1\\ \begin{bmatrix}x_1\\ x_2\oplus 1\end{bmatrix}, \text{якщо } k_1=0;\ k_2=0\end{cases}=O_{19}^k=\begin{cases}\begin{bmatrix}x_2\oplus 1\\ x_1\end{bmatrix}, \text{якщо } k_1=1;\ k_2=1\\ \begin{bmatrix}x_1\oplus 1\\ x_2\end{bmatrix}, \text{якщо } k_1=1;\ k_2=0\\ \begin{bmatrix}x_2\\ x_1\oplus 1\end{bmatrix}, \text{якщо } k_1=0;\ k_2=1\\ \begin{bmatrix}x_1\\ x_2\oplus 1\end{bmatrix}, \text{якщо } k_1=0;\ k_2=0\end{cases}=O_{19}^k=\begin{bmatrix}x_1\cdot\bar{k}_2\oplus x_2\cdot k_2\\ x_1\cdot k_2\oplus x_2\cdot\bar{k}_2\end{bmatrix}\oplus\begin{bmatrix}k_1\\ \bar{k}_1\end{bmatrix} \tag{3.91}$$

Це показує, що твердження вірне.

Якщо над другим операндом двохоперандної операції строгого криптографічного кодування $O_4^k=\begin{bmatrix}x_1\cdot\bar{k}_2\oplus x_2\cdot k_2\\ x_1\cdot k_2\oplus x_2\cdot\bar{k}_2\end{bmatrix}\oplus\begin{bmatrix}k_1\\ \bar{k}_1\end{bmatrix}$ виконати одноопераднe криптографічне перетворення $F_{9,10}=\begin{bmatrix}x_1\oplus x_2\oplus 1\\ x_2\oplus 1\end{bmatrix}$, то буде отримана операція строгого стійкого кодування $O_{24}^k=\begin{bmatrix}x_1\cdot k_2\oplus x_2\cdot\bar{k}_2\\ x_1\cdot\bar{k}_2\oplus x_2\cdot k_2\end{bmatrix}\oplus\begin{bmatrix}\overline{k_1\oplus k_2}\\ k_1\oplus k_2\end{bmatrix}$.

Так як:

$$F_{9,10}(O_4^k)=\begin{cases}\begin{bmatrix}x_2\oplus 1\\ x_1\end{bmatrix}, якщо\ k_1=1;\ k_2=1\\ \begin{bmatrix}x_1\\ x_2\oplus 1\end{bmatrix}, якщо\ k_1=0;\ k_2=1\\ \begin{bmatrix}x_2\\ x_1\oplus 1\end{bmatrix}, якщо\ k_1=1;\ k_2=0\\ \begin{bmatrix}x_1\oplus 1\\ x_1\end{bmatrix}, якщо\ k_1=1;\ k_2=0\end{cases}=O_{24}^k=\begin{cases}\begin{bmatrix}x_2\oplus 1\\ x_1\end{bmatrix}, якщо\ k_1=1;\ k_2=1\\ \begin{bmatrix}x_1\\ x_2\oplus 1\end{bmatrix}, якщо\ k_1=0;\ k_2=1\\ \begin{bmatrix}x_2\\ x_1\oplus 1\end{bmatrix}, якщо\ k_1=1;\ k_2=0\\ \begin{bmatrix}x_1\oplus 1\\ x_1\end{bmatrix}, якщо\ k_1=1;\ k_2=0\end{cases}=O_{24}^k=\begin{bmatrix}x_1\cdot k_2\oplus x_2\cdot\bar{k}_2\\ x_1\cdot\bar{k}_2\oplus x_2\cdot k_2\end{bmatrix}\oplus\begin{bmatrix}\overline{k_1\oplus k_2}\\ k_1\oplus k_2\end{bmatrix} \quad (3.92)$$

це й потрібно було довести.

Якщо над другим операндом двохоперандної операції строгого криптографічного кодування $O_4^k=\begin{bmatrix}x_1\cdot\bar{k}_2\oplus x_2\cdot k_2\\ x_1\cdot k_2\oplus x_2\cdot\bar{k}_2\end{bmatrix}\oplus\begin{bmatrix}k_1\\ \bar{k}_1\end{bmatrix}$ виконати одноопераднде криптографічне перетворення $F_{12,9}=\begin{bmatrix}x_1\oplus 1\\ x_1\oplus x_2\oplus 1\end{bmatrix}$, то буде отримана операція строгого стійкого кодування $O_{20}^k=\begin{bmatrix}x_1\cdot(k_1\oplus k_2)\oplus x_2\cdot(\overline{k_1\oplus k_2})\\ x_1\cdot(\overline{k_1\oplus k_2})\oplus x_2\cdot(k_1\oplus k_2)\end{bmatrix}\oplus\begin{bmatrix}\bar{k}_1\\ k_1\end{bmatrix}$.

Так як:

$$F_{12,9}(O_4^k)=\begin{cases}\begin{bmatrix}x_2\oplus 1\\ x_1\end{bmatrix}, якщо\ k_1=1;\ k_2=1\\ \begin{bmatrix}x_1\oplus 1\\ x_1\end{bmatrix}, якщо\ k_1=1;\ k_2=0\\ \begin{bmatrix}x_1\\ x_2\oplus 1\end{bmatrix}, якщо\ k_1=0;\ k_2=0\\ \begin{bmatrix}x_2\\ x_1\oplus 1\end{bmatrix}, якщо\ k_1=0;\ k_2=1\end{cases}=O_{20}^k=\begin{cases}\begin{bmatrix}x_2\oplus 1\\ x_1\end{bmatrix}, якщо\ k_1=1;\ k_2=1\\ \begin{bmatrix}x_1\oplus 1\\ x_1\end{bmatrix}, якщо\ k_1=1;\ k_2=0\\ \begin{bmatrix}x_1\\ x_2\oplus 1\end{bmatrix}, якщо\ k_1=0;\ k_2=0\\ \begin{bmatrix}x_2\\ x_1\oplus 1\end{bmatrix}, якщо\ k_1=0;\ k_2=1\end{cases}=O_{20}^k=\begin{bmatrix}x_1\cdot(k_1\oplus k_2)\oplus x_2\cdot(\overline{k_1\oplus k_2})\\ x_1\cdot(\overline{k_1\oplus k_2})\oplus x_2\cdot(k_1\oplus k_2)\end{bmatrix}\oplus\begin{bmatrix}\bar{k}_1\\ k_1\end{bmatrix} \quad (3.93)$$

це і потребувало доведення.

Виконання одноопераднього криптографічного перетворення $F_{10,12}=\begin{bmatrix}x_2\oplus 1\\ x_1\oplus 1\end{bmatrix}$ над другим операндом двохоперандної операції строгого криптографічного кодування $O_4^k=\begin{bmatrix}x_1\cdot\bar{k}_2\oplus x_2\cdot k_2\\ x_1\cdot k_2\oplus x_2\cdot\bar{k}_2\end{bmatrix}\oplus\begin{bmatrix}k_1\\ \bar{k}_1\end{bmatrix}$ то буде отримана операція строгого стійкого кодування $O_{22}^k=\begin{bmatrix}x_1\cdot k_1\oplus x_2\cdot\bar{k}_1\\ x_1\cdot\bar{k}_1\oplus x_2\cdot k_1\end{bmatrix}\oplus\begin{bmatrix}\bar{k}_2\\ k_2\end{bmatrix}$.

Так як:

$$F_{10,12}(O_4^k)=\begin{cases}\begin{bmatrix}x_1\\x_2\oplus 1\end{bmatrix}, \text{ якщо } k_1=0;\ k_2=0\\ \begin{bmatrix}x_2\\x_1\oplus 1\end{bmatrix}, \text{якщо } k_1=0;\ k_2=1\\ \begin{bmatrix}x_1\oplus 1\\x_2\end{bmatrix}, \text{ якщо } k_1=1;\ k_2=0\\ \begin{bmatrix}x_2\oplus 1\\x_1\end{bmatrix}, \text{якщо } k_1=1;\ k_2=1\end{cases}=O_{22}^k=\begin{cases}\begin{bmatrix}x_2\oplus 1\\x_1\end{bmatrix}, \text{якщо } k_1=1;\ k_2=1\\ \begin{bmatrix}x_2\\x_1\oplus 1\end{bmatrix}, \text{якщо } k_1=0;\ k_2=1\\ \begin{bmatrix}x_1\oplus 1\\x_2\end{bmatrix}, \text{ якщо } k_1=1;\ k_2=0\\ \begin{bmatrix}x_1\\x_2\oplus 1\end{bmatrix}, \text{ якщо } k_1=0;\ k_2=0\end{cases}=O_{22}^k=\begin{bmatrix}x_1\cdot k_1\oplus x_2\cdot\bar{k}_1\\x_1\cdot\bar{k}_1\oplus x_2\cdot k_1\end{bmatrix}\oplus\begin{bmatrix}\bar{k}_2\\k_2\end{bmatrix} \quad (3.94)$$

що і потрібно було довести.

Якщо над другим операндом двохоперандної операції строгого криптографічного кодування $O_4^k=\begin{bmatrix}x_1\cdot\bar{k}_2\oplus x_2\cdot k_2\\x_1\cdot k_2\oplus x_2\cdot\bar{k}_2\end{bmatrix}\oplus\begin{bmatrix}k_1\\\bar{k}_1\end{bmatrix}$ виконати одноопераднде криптографічне перетворення $F_{10,9}=\begin{bmatrix}x_2\oplus 1\\x_1\oplus x_2\oplus 1\end{bmatrix}$, то буде отримана операція строгого стійкого кодування $O_{23}^k=\begin{bmatrix}x_1\cdot(k_1\oplus k_2)\oplus x_2\cdot(\overline{k_1\oplus k_2})\\x_1\cdot(\overline{k_1\oplus k_2})\oplus x_2\cdot(k_1\oplus k_2)\end{bmatrix}\oplus\begin{bmatrix}\bar{k}_2\\k_2\end{bmatrix}$.

Оскільки:

$$F_{10,9}(O_4^k)=\begin{cases}\begin{bmatrix}x_2\oplus 1\\x_1\end{bmatrix}, \text{якщо } k_1=1;\ k_2=1\\ \begin{bmatrix}x_1\\x_2\oplus 1\end{bmatrix}, \text{ якщо } k_1=0;\ k_2=0\\ \begin{bmatrix}x_1\oplus 1\\x_2\end{bmatrix}, \text{якщо } k_1=1;\ k_2=0\\ \begin{bmatrix}x_2\\x_1\oplus 1\end{bmatrix}, \text{якщо } k_1=0;\ k_2=1\end{cases}=O_{23}^k=\begin{cases}\begin{bmatrix}x_2\oplus 1\\x_1\end{bmatrix}, \text{якщо } k_1=1;\ k_2=1\\ \begin{bmatrix}x_1\\x_2\oplus 1\end{bmatrix}, \text{ якщо } k_1=0;\ k_2=0\\ \begin{bmatrix}x_1\oplus 1\\x_2\end{bmatrix}, \text{якщо } k_1=1;\ k_2=0\\ \begin{bmatrix}x_2\\x_1\oplus 1\end{bmatrix}, \text{якщо } k_1=0;\ k_2=1\end{cases}=O_{23}^k=\begin{bmatrix}x_1\cdot(k_1\oplus k_2)\oplus x_2\cdot(\overline{k_1\oplus k_2})\\x_1\cdot(\overline{k_1\oplus k_2})\oplus x_2\cdot(k_1\oplus k_2)\end{bmatrix}\oplus\begin{bmatrix}\bar{k}_2\\k_2\end{bmatrix} \quad (3.95)$$

Це показує правильність нашого твердження.

Якщо над другим операндом двохоперандної операції строгого криптографічного кодування $O_4^k=\begin{bmatrix}x_1\cdot\bar{k}_2\oplus x_2\cdot k_2\\x_1\cdot k_2\oplus x_2\cdot\bar{k}_2\end{bmatrix}\oplus\begin{bmatrix}k_1\\\bar{k}_1\end{bmatrix}$ виконати одноопераднде криптографічне перетворення $F_{9,12}=\begin{bmatrix}x_1\oplus x_2\oplus 1\\x_1\oplus 1\end{bmatrix}$, то буде отримана операція строгого стійкого кодування $O_{21}^k=\begin{bmatrix}x_1\cdot k_1\oplus x_2\cdot\bar{k}_1\\x_1\cdot\bar{k}_1\oplus x_2\cdot k_1\end{bmatrix}\oplus\begin{bmatrix}\overline{k_1\oplus k_2}\\k_1\oplus k_2\end{bmatrix}$.

Так як:

$$F_{9,12}(O_4^k)=\begin{cases}\begin{bmatrix}x_2\oplus 1\\ x_1\end{bmatrix}, якщо\ k_1=1;\ k_2=1\\ \begin{bmatrix}x_2\\ x_1\oplus 1\end{bmatrix}, якщо\ k_1=0;\ k_2=1\\ \begin{bmatrix}x_1\\ x_2\oplus 1\end{bmatrix}, якщо\ k_1=0;\ k_2=0\\ \begin{bmatrix}x_1\oplus 1\\ x_2\end{bmatrix}, якщо\ k_1=1;\ k_2=0\end{cases}=O_{21}^k=\begin{cases}\begin{bmatrix}x_2\oplus 1\\ x_1\end{bmatrix}, якщо\ k_1=1;\ k_2=1\\ \begin{bmatrix}x_2\\ x_1\oplus 1\end{bmatrix}, якщо\ k_1=0;\ k_2=1\\ \begin{bmatrix}x_1\\ x_2\oplus 1\end{bmatrix}, якщо\ k_1=0;\ k_2=0\\ \begin{bmatrix}x_1\oplus 1\\ x_2\end{bmatrix}, якщо\ k_1=1;\ k_2=0\end{cases}=O_{21}^k=\begin{bmatrix}x_1\cdot k_1\oplus x_2\cdot\bar{k}_1\\ x_1\cdot\bar{k}_1\oplus x_2\cdot k_1\end{bmatrix}\oplus\begin{bmatrix}\overline{k_1\oplus k_2}\\ k_1\oplus k_2\end{bmatrix} \tag{3.96}$$

що і потрібно було довести.

Згідно отриманих результатів, можна стверджувати, що при виконанні операцій перестановок над $O_4^k=\begin{bmatrix}x_1\cdot\bar{k}_2\oplus x_2\cdot k_2\\ x_1\cdot k_2\oplus x_2\cdot\bar{k}_2\end{bmatrix}\oplus\begin{bmatrix}k_1\\ \bar{k}_1\end{bmatrix}$, на основі перетворення другого операнда шляхом двохрозрядної одноопераднної операції було синтезовано повну групу двохрозрядних двохоперандних операцій строгого криптографічного кодування.

Для наведених результатів дослідження досягнуто збільшення варіативності алгоритмів в 24 рази, так як даний метод гарантовано дозволяє синтезувати з будь якої операції 24 операції, які складають повну групу операцій в полі G_4 .

Виходячи з отриманих результатів дослідження, метод синтезу двохрозрядних двохоперандних операцій ССКК на основі перетворення другого операнда полягає в наступному:

1. Визначити математичну модель двохрозрядної двохоперандної операції ССКК на основі якої буде будуватися група операцій.

2. Провести синтез групи математичних моделей двохрозрядних одноопераднних операцій ССКК на основі застосування одного з відомих методів їх синтезу.

3. Вибрати першу математичну модель двохрозрядних одноопераднних операцій строгого стійкого криптографічного кодування.

4. Модифікувати визначену математичну модель двохрозрядної двохоперандної операції ССКК шляхом перетворення другого операнда даної

операції на основі виконання над нею вибраної одноопераднної операції ССКК.

5. Якщо вибрана математична модель двохрозрядних одноопераднних операцій ССКК не остання в синтезованій групі, тоді вибрати наступну модель і повернутися до пункту 4.

6. Перевірити завершення побудови групи двохрозрядних двохоперандних операцій ССКК на основі кількісного співпадіння отриманих двохоперандних і одноопераднних операцій.

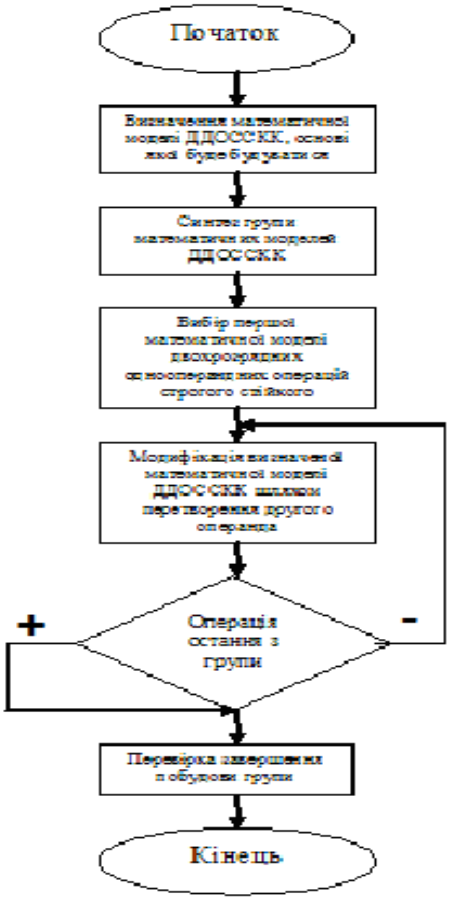


Рисунок 3.1. Блок-схема методу синтезу двохрозрядних двохоперандних операцій ССКК на основі перетворення другого операнда

Алгоритм реалізації методу синтезу двохрозрядних двохоперандних операцій ССКК на основі перетворення другого операнда наведений на рис.3.1.

Висновки з розділу 3

Вперше розроблено метод синтезу групи двохрозрядних двохоперандних операцій ССКК на основі перетворення другого операнда відомої операції шляхом виконання над ним двохрозрядної одноопераднної операції, що забезпечило можливість збільшення варіативності криптопримітивів при практичному застосуванні даних операцій.

1. Запропонована технологія синтезу групи двохрозрядних двохоперандних операцій строгого криптографічного кодування забезпечує побудову повної групи з 24 операцій на основі однієї відомої операції.

2. На основі застосування запропонованої технології проведено синтез груп двохрозрядних двохоперандних операцій ССКК на основі перетворення другого операнда відомої операції.

3. Запропонований та перевірений підхід синтезу групи двохрозрядних двохоперандних операцій ССКК на основі перетворення другого операнда відомої операції дозволив розробити метод синтезу групи двохрозрядних двохоперандних операцій ССКК на основі перетворення другого операнда відомої операції.

5. Результати розділу опубліковано [1,7,9].

РОЗДІЛ 4

МЕТОД ГЕНЕРАЦІЇ ПСЕВДОВИПАДКОВИХ ПОСЛІДОВНОСТЕЙ ДВОХРОЗРЯДНИХ ДВОХОПЕРАНДНИХ ОПЕРАЦІЙ СТРОГОГО СТІЙКОГО КРИПТОГРАФІЧНОГО КОДУВАННЯ НА ОСНОВІ ПЕРЕТВОРЕННЯ ДРУГОГО ОПЕРАНДА ТА ЙОГО РЕАЛІЗАЦІЯ

4.1 Розробка методу генерації псевдовипадкових послідовностей двохрозрядних двохоперандних операцій строгого стійкого криптографічного кодування на основі перетворення другого операнда

4.1.1 Узагальнення результатів синтезу групи операцій криптоперетворення

Узагальнимо результати синтезу групи операцій криптоперетворення на основі першої операції. Зокрема, згрупуємо дані операції згідно одноопераднних операцій, які діяли на другий операнд.

Узагальнені результати синтезу групи операцій криптоперетворення на основі першої операції наведені в табл.4.1.

Табл.4.1 показує, що при застосуванні методу синтезу двохрозрядних двохоперандних операцій ССКК на прикладі $O_1^k = \begin{bmatrix} x_1 \cdot \bar{k}_1 \oplus x_2 \cdot k_1 \\ x_1 \cdot k_1 \oplus x_2 \cdot \bar{k}_1 \end{bmatrix} \oplus \begin{bmatrix} k_2 \\ \bar{k}_2 \end{bmatrix}$ при перетворенні другого операнда шляхом дії на нього одноопераднної двохрозрядної операції можна отримати повну групу операцій.

Узагальнимо результати дослідження синтезу двохрозрядних двохоперандних операцій строгого стійкого криптографічного перетворення на прикладі операції криптографічного кодування $O_2^k = \begin{bmatrix} x_1 \cdot \bar{k}_1 \oplus x_2 \cdot k_1 \\ x_1 \cdot k_1 \oplus x_2 \cdot \bar{k}_1 \end{bmatrix} \oplus \begin{bmatrix} k_1 \oplus k_2 \\ \overline{k_1 \oplus k_2} \end{bmatrix}$. У табл. 4.2 показано отриману групу операцій криптоперетворення на основі O_2^k [2].

Таблиця 4.1

Зведені результати синтезу двохоперандних операції ССК на основі операції $O_1^k = \begin{bmatrix} x_1 \cdot \bar{k}_1 \oplus x_2 \cdot k_1 \\ x_1 \cdot k_1 \oplus x_2 \cdot \bar{k}_1 \end{bmatrix} \oplus \begin{bmatrix} k_2 \\ \bar{k}_2 \end{bmatrix}$

Операції перестановок	**Класифікатор операцій** $O_1^k = \begin{bmatrix} x_1 \cdot \bar{k}_1 \oplus x_2 \cdot k_1 \\ x_1 \cdot k_1 \oplus x_2 \cdot \bar{k}_1 \end{bmatrix} \oplus \begin{bmatrix} k_2 \\ \bar{k}_2 \end{bmatrix}$							
	1	$O_1^k = \begin{bmatrix} x_1 \cdot \bar{k}_1 \oplus x_2 \cdot k_1 \\ x_1 \cdot k_1 \oplus x_2 \cdot \bar{k}_1 \end{bmatrix} \oplus \begin{bmatrix} k_2 \\ \bar{k}_2 \end{bmatrix}$	7	$O_8^k = \begin{bmatrix} x_1 \cdot \bar{k}_1 \oplus x_2 \cdot k_1 \\ x_1 \cdot k_1 \oplus x_2 \cdot \bar{k}_1 \end{bmatrix} \oplus \begin{bmatrix} \bar{k}_2 \\ k_2 \end{bmatrix}$	13	$O_{18}^k = \begin{bmatrix} x_1 \cdot k_1 \oplus x_2 \cdot \bar{k}_1 \\ x_1 \cdot \bar{k}_1 \oplus x_2 \cdot k_1 \end{bmatrix} \oplus \begin{bmatrix} k_2 \\ \bar{k}_2 \end{bmatrix}$	19	$O_{22}^k = \begin{bmatrix} x_1 \cdot k_1 \oplus x_2 \cdot \bar{k}_1 \\ x_1 \cdot \bar{k}_1 \oplus x_2 \cdot k_1 \end{bmatrix} \oplus \begin{bmatrix} \bar{k}_2 \\ k_2 \end{bmatrix}$
	2	$O_6^k = \begin{bmatrix} x_1 \cdot (\overline{k_1 \oplus k_2}) \oplus x_2 \cdot (k_1 \oplus k_2) \\ x_1 \cdot (k_1 \oplus k_2) \oplus x_2 \cdot (\overline{k_1 \oplus k_2}) \end{bmatrix} \oplus \begin{bmatrix} k_2 \\ \bar{k}_2 \end{bmatrix}$	8	$O_9^k = \begin{bmatrix} x_1 \cdot (\overline{k_1 \oplus k_2}) \oplus x_2 \cdot (k_1 \oplus k_2) \\ x_1 \cdot (k_1 \oplus k_2) \oplus x_2 \cdot (\overline{k_1 \oplus k_2}) \end{bmatrix} \oplus \begin{bmatrix} \bar{k}_2 \\ k_2 \end{bmatrix}$	14	$O_{13}^k = \begin{bmatrix} x_1 \cdot (k_1 \oplus k_2) \oplus x_2 \cdot (\overline{k_1 \oplus k_2}) \\ x_1 \cdot (\overline{k_1 \oplus k_2}) \oplus x_2 \cdot (k_1 \oplus k_2) \end{bmatrix} \oplus \begin{bmatrix} k_2 \\ \bar{k}_2 \end{bmatrix}$	20	$O_{23}^k = \begin{bmatrix} x_1 \cdot (k_1 \oplus k_2) \oplus x_2 \cdot (\overline{k_1 \oplus k_2}) \\ x_1 \cdot (\overline{k_1 \oplus k_2}) \oplus x_2 \cdot (k_1 \oplus k_2) \end{bmatrix} \oplus \begin{bmatrix} \bar{k}_2 \\ k_2 \end{bmatrix}$
	3	$O_2^k = \begin{bmatrix} x_1 \cdot \bar{k}_1 \oplus x_2 \cdot k_1 \\ x_1 \cdot k_1 \oplus x_2 \cdot \bar{k}_1 \end{bmatrix} \oplus \begin{bmatrix} k_1 \oplus k_2 \\ \overline{k_1 \oplus k_2} \end{bmatrix}$	9	$O_7^k = \begin{bmatrix} x_1 \cdot \bar{k}_1 \oplus x_2 \cdot k_1 \\ x_1 \cdot k_1 \oplus x_2 \cdot \bar{k}_1 \end{bmatrix} \oplus \begin{bmatrix} \overline{k_1 \oplus k_2} \\ k_1 \oplus k_2 \end{bmatrix}$	15	$O_{17}^k = \begin{bmatrix} x_1 \cdot k_1 \oplus x_2 \cdot \bar{k}_1 \\ x_1 \cdot \bar{k}_1 \oplus x_2 \cdot k_1 \end{bmatrix} \oplus \begin{bmatrix} k_1 \oplus k_2 \\ \overline{k_1 \oplus k_2} \end{bmatrix}$	21	$O_{21}^k = \begin{bmatrix} x_1 \cdot k_1 \oplus x_2 \cdot \bar{k}_1 \\ x_1 \cdot \bar{k}_1 \oplus x_2 \cdot k_1 \end{bmatrix} \oplus \begin{bmatrix} \overline{k_1 \oplus k_2} \\ k_1 \oplus k_2 \end{bmatrix}$
	4	$O_4^k = \begin{bmatrix} x_1 \cdot \bar{k}_2 \oplus x_2 \cdot k_2 \\ x_1 \cdot k_2 \oplus x_2 \cdot \bar{k}_2 \end{bmatrix} \oplus \begin{bmatrix} k_1 \\ \bar{k}_1 \end{bmatrix}$	10	$O_{11}^k = \begin{bmatrix} x_1 \cdot \bar{k}_2 \oplus x_2 \cdot k_2 \\ x_1 \cdot k_2 \oplus x_2 \cdot \bar{k}_2 \end{bmatrix} \oplus \begin{bmatrix} \bar{k}_1 \\ k_1 \end{bmatrix}$	16	$O_{15}^k = \begin{bmatrix} x_1 \cdot k_2 \oplus x_2 \cdot \bar{k}_2 \\ x_1 \cdot \bar{k}_2 \oplus x_2 \cdot k_2 \end{bmatrix} \oplus \begin{bmatrix} k_1 \\ \bar{k}_1 \end{bmatrix}$	22	$O_{19}^k = \begin{bmatrix} x_1 \cdot \bar{k}_2 \oplus x_2 \cdot k_2 \\ x_1 \cdot k_2 \oplus x_2 \cdot \bar{k}_2 \end{bmatrix} \oplus \begin{bmatrix} k_1 \\ \bar{k}_1 \end{bmatrix}$
	5	$O_5^k = \begin{bmatrix} x_1 \cdot \bar{k}_2 \oplus x_2 \cdot k_2 \\ x_1 \cdot k_2 \oplus x_2 \cdot \bar{k}_2 \end{bmatrix} \oplus \begin{bmatrix} k_1 \oplus k_2 \\ \overline{k_1 \oplus k_2} \end{bmatrix}$	11	$O_{10}^k = \begin{bmatrix} x_1 \cdot \bar{k}_2 \oplus x_2 \cdot k_2 \\ x_1 \cdot k_2 \oplus x_2 \cdot \bar{k}_2 \end{bmatrix} \oplus \begin{bmatrix} \bar{k}_2 \\ k_2 \end{bmatrix}$	17	$O_{14}^k = \begin{bmatrix} x_1 \cdot k_2 \oplus x_2 \cdot \bar{k}_2 \\ x_1 \cdot \bar{k}_2 \oplus x_2 \cdot k_2 \end{bmatrix} \oplus \begin{bmatrix} k_2 \\ \bar{k}_2 \end{bmatrix}$	23	$O_{24}^k = \begin{bmatrix} x_1 \cdot k_2 \oplus x_2 \cdot \bar{k}_2 \\ x_1 \cdot \bar{k}_2 \oplus x_2 \cdot k_2 \end{bmatrix} \oplus \begin{bmatrix} \overline{k_1 \oplus k_2} \\ k_1 \oplus k_2 \end{bmatrix}$
	6	$O_3^k = \begin{bmatrix} x_1 \cdot (\overline{k_1 \oplus k_2}) \oplus x_2 \cdot (k_1 \oplus k_2) \\ x_1 \cdot (k_1 \oplus k_2) \oplus x_2 \cdot (\overline{k_1 \oplus k_2}) \end{bmatrix} \oplus \begin{bmatrix} k_1 \\ \bar{k}_1 \end{bmatrix}$	12	$O_{12}^k = \begin{bmatrix} x_1 \cdot (\overline{k_1 \oplus k_2}) \oplus x_2 \cdot (k_1 \oplus k_2) \\ x_1 \cdot (k_1 \oplus k_2) \oplus x_2 \cdot (\overline{k_1 \oplus k_2}) \end{bmatrix} \oplus \begin{bmatrix} \bar{k}_1 \\ k_1 \end{bmatrix}$	18	$O_{16}^k = \begin{bmatrix} x_1 \cdot (k_1 \oplus k_2) \oplus x_2 \cdot (\overline{k_1 \oplus k_2}) \\ x_1 \cdot (\overline{k_1 \oplus k_2}) \oplus x_2 \cdot (k_1 \oplus k_2) \end{bmatrix} \oplus \begin{bmatrix} k \\ \bar{k} \end{bmatrix}$	24	$O_{20}^k = \begin{bmatrix} x_1 \cdot (k_1 \oplus k_2) \oplus x_2 \cdot (\overline{k_1 \oplus k_2}) \\ x_1 \cdot (\overline{k_1 \oplus k_2}) \oplus x_2 \cdot (k_1 \oplus k_2) \end{bmatrix} \oplus \begin{bmatrix} \bar{k}_1 \\ k_1 \end{bmatrix}$

Таблиця 4.2

Зведені результати синтезу двохоперандних операції ССК на основі операції $O_2^k=\begin{bmatrix}x_1\cdot\bar{k}_1\oplus x_2\cdot k_1\\ x_1\cdot k_1\oplus x_2\cdot\bar{k}_1\end{bmatrix}\oplus\begin{bmatrix}k_1\oplus k_2\\ \overline{k_1\oplus k_2}\end{bmatrix}$

Операції перестановок	**Класифікатор операцій** $O_2^k=\begin{bmatrix}x_1\cdot\bar{k}_1\oplus x_2\cdot k_1\\ x_1\cdot k_1\oplus x_2\cdot\bar{k}_1\end{bmatrix}\oplus\begin{bmatrix}k_1\oplus k_2\\ \overline{k_1\oplus k_2}\end{bmatrix}$							
	1	$O_2^k=\begin{bmatrix}x_1\cdot\bar{k}_1\oplus x_2\cdot k_1\\ x_1\cdot k_1\oplus x_2\cdot\bar{k}_1\end{bmatrix}\oplus\begin{bmatrix}k_1\oplus k_2\\ \overline{k_1\oplus k_2}\end{bmatrix}$	7	$O_7^k=\begin{bmatrix}x_1\cdot\bar{k}_1\oplus x_2\cdot k_1\\ x_1\cdot k_1\oplus x_2\cdot\bar{k}_1\end{bmatrix}\oplus\begin{bmatrix}\overline{k_1\oplus k_2}\\ k_1\oplus k_2\end{bmatrix}$	13	$O_{21}^k=\begin{bmatrix}x_1\cdot k_1\oplus x_2\cdot\bar{k}_1\\ x_1\cdot\bar{k}_1\oplus x_2\cdot k_1\end{bmatrix}\oplus\begin{bmatrix}\overline{k_1\oplus k_2}\\ k_1\oplus k_2\end{bmatrix}$	19	$O_{17}^k=\begin{bmatrix}x_1\cdot k_1\oplus x_2\cdot\bar{k}_1\\ x_1\cdot\bar{k}_1\oplus x_2\cdot k_1\end{bmatrix}\oplus\begin{bmatrix}k_1\oplus k_2\\ \overline{k_1\oplus k_2}\end{bmatrix}$
	2	$O_3^k=\begin{bmatrix}x_1\cdot(\overline{k_1\oplus k_2})\oplus x_2\cdot(k_1\oplus k_2)\\ x_1\cdot(k_1\oplus k_2)\oplus x_2\cdot(\overline{k_1\oplus k_2})\end{bmatrix}\oplus\begin{bmatrix}k_1\\ \bar{k}_1\end{bmatrix}$	8	$O_{12}^k=\begin{bmatrix}x_1\cdot(\overline{k_1\oplus k_2})\oplus x_2\cdot(k_1\oplus k_2)\\ x_1\cdot(k_1\oplus k_2)\oplus x_2\cdot(\overline{k_1\oplus k_2})\end{bmatrix}\oplus\begin{bmatrix}\bar{k}_1\\ k_1\end{bmatrix}$	14	$O_{20}^k=\begin{bmatrix}x_1\cdot(k_1\oplus k_2)\oplus x_2\cdot(\overline{k_1\oplus k_2})\\ x_1\cdot(\overline{k_1\oplus k_2})\oplus x_2\cdot(k_1\oplus k_2)\end{bmatrix}\oplus\begin{bmatrix}\bar{k}_1\\ k_1\end{bmatrix}$	20	$O_{16}^k=\begin{bmatrix}x_1\cdot(k_1\oplus k_2)\oplus x_2\cdot(\overline{k_1\oplus k_2})\\ x_1\cdot(\overline{k_1\oplus k_2})\oplus x_2\cdot(k_1\oplus k_2)\end{bmatrix}\oplus\begin{bmatrix}k_1\\ \bar{k}_1\end{bmatrix}$
	3	$O_1^k=\begin{bmatrix}x_1\cdot\bar{k}_1\oplus x_2\cdot k_1\\ x_1\cdot k_1\oplus x_2\cdot\bar{k}_1\end{bmatrix}\oplus\begin{bmatrix}k_2\\ \bar{k}_2\end{bmatrix}$	9	$O_8^k=\begin{bmatrix}x_1\cdot\bar{k}_1\oplus x_2\cdot k_1\\ x_1\cdot k_1\oplus x_2\cdot\bar{k}_1\end{bmatrix}\oplus\begin{bmatrix}\bar{k}_2\\ k_2\end{bmatrix}$	15	$O_{22}^k=\begin{bmatrix}x_1\cdot k_1\oplus x_2\cdot\bar{k}_1\\ x_1\cdot\bar{k}_1\oplus x_2\cdot k_1\end{bmatrix}\oplus\begin{bmatrix}\bar{k}_2\\ k_2\end{bmatrix}$	21	$O_{18}^k=\begin{bmatrix}x_1\cdot k_1\oplus x_2\cdot\bar{k}_1\\ x_1\cdot\bar{k}_1\oplus x_2\cdot k_1\end{bmatrix}\oplus\begin{bmatrix}k_2\\ \bar{k}_2\end{bmatrix}$
	4	$O_5^k=\begin{bmatrix}x_1\cdot\bar{k}_2\oplus x_2\cdot k_2\\ x_1\cdot k_2\oplus x_2\cdot\bar{k}_2\end{bmatrix}\oplus\begin{bmatrix}k_1\oplus k_2\\ \overline{k_1\oplus k_2}\end{bmatrix}$	10	$O_{10}^k=\begin{bmatrix}x_1\cdot\bar{k}_2\oplus x_2\cdot k_2\\ x_1\cdot k_2\oplus x_2\cdot\bar{k}_2\end{bmatrix}\oplus\begin{bmatrix}\bar{k}_2\\ k_2\end{bmatrix}$	16	$O_{24}^k=\begin{bmatrix}x_1\cdot k_2\oplus x_2\cdot\bar{k}_2\\ x_1\cdot\bar{k}_2\oplus x_2\cdot k_2\end{bmatrix}\oplus\begin{bmatrix}\overline{k_1\oplus k_2}\\ k_1\oplus k_2\end{bmatrix}$	22	$O_{14}^k=\begin{bmatrix}x_1\cdot k_2\oplus x_2\cdot\bar{k}_2\\ x_1\cdot\bar{k}_2\oplus x_2\cdot k_2\end{bmatrix}\oplus\begin{bmatrix}k_2\\ \bar{k}_2\end{bmatrix}$
	5	$O_4^k=\begin{bmatrix}x_1\cdot\bar{k}_2\oplus x_2\cdot k_2\\ x_1\cdot k_2\oplus x_2\cdot\bar{k}_2\end{bmatrix}\oplus\begin{bmatrix}k_1\\ \bar{k}_1\end{bmatrix}$	11	$O_{11}^k=\begin{bmatrix}x_1\cdot\bar{k}_2\oplus x_2\cdot k_2\\ x_1\cdot k_2\oplus x_2\cdot\bar{k}_2\end{bmatrix}\oplus\begin{bmatrix}\bar{k}_1\\ k_1\end{bmatrix}$	17	$O_{19}^k=\begin{bmatrix}x_1\cdot\bar{k}_2\oplus x_2\cdot k_2\\ x_1\cdot k_2\oplus x_2\cdot\bar{k}_2\end{bmatrix}\oplus\begin{bmatrix}k_1\\ \bar{k}_1\end{bmatrix}$	23	$O_{15}^k=\begin{bmatrix}x_1\cdot k_2\oplus x_2\cdot\bar{k}_2\\ x_1\cdot\bar{k}_2\oplus x_2\cdot k_2\end{bmatrix}\oplus\begin{bmatrix}k_1\\ \bar{k}_1\end{bmatrix}$
	6	$O_6^k=\begin{bmatrix}x_1\cdot(\overline{k_1\oplus k_2})\oplus x_2\cdot(k_1\oplus k_2)\\ x_1\cdot(k_1\oplus k_2)\oplus x_2\cdot(\overline{k_1\oplus k_2})\end{bmatrix}\oplus\begin{bmatrix}k_2\\ \bar{k}_2\end{bmatrix}$	12	$O_9^k=\begin{bmatrix}x_1\cdot(\overline{k_1\oplus k_2})\oplus x_2\cdot(k_1\oplus k_2)\\ x_1\cdot(k_1\oplus k_2)\oplus x_2\cdot(\overline{k_1\oplus k_2})\end{bmatrix}\oplus\begin{bmatrix}\bar{k}_2\\ k_2\end{bmatrix}$	18	$O_{23}^k=\begin{bmatrix}x_1\cdot(k_1\oplus k_2)\oplus x_2\cdot(\overline{k_1\oplus k_2})\\ x_1\cdot(\overline{k_1\oplus k_2})\oplus x_2\cdot(k_1\oplus k_2)\end{bmatrix}\oplus\begin{bmatrix}\bar{k}_2\\ k_2\end{bmatrix}$	24	$O_{13}^k=\begin{bmatrix}x_1\cdot(k_1\oplus k_2)\oplus x_2\cdot(\overline{k_1\oplus k_2})\\ x_1\cdot(\overline{k_1\oplus k_2})\oplus x_2\cdot(k_1\oplus k_2)\end{bmatrix}\oplus\begin{bmatrix}k_2\\ \bar{k}_2\end{bmatrix}$

Для подальшого дослідження розглянемо результати методу синтезу двохрозрядних двохоперандних операцій ССКК на прикладі операції криптоперетворення $O_3^k = \begin{bmatrix} x_1 \cdot (\overline{k_1 \oplus k_2}) \oplus x_2 \cdot (k_1 \oplus k_2) \\ x_1 \cdot (k_1 \oplus k_2) \oplus x_2 \cdot (\overline{k_1 \oplus k_2}) \end{bmatrix} \oplus \begin{bmatrix} k_1 \\ \bar{k}_1 \end{bmatrix}$. Табл.4.3 показує отриману групу операцій на основі O_3^k .

Аналіз табл. 4.4 показує, що при виконанні одноопераднього криптографічного перетворення над другим операндом двохоперандної операції строгого криптографічного кодування $O_4^k = \begin{bmatrix} x_1 \cdot \bar{k}_2 \oplus x_2 \cdot k_2 \\ x_1 \cdot k_2 \oplus x_2 \cdot \bar{k}_2 \end{bmatrix} \oplus \begin{bmatrix} k_1 \\ \bar{k}_1 \end{bmatrix}$, отримуємо синтезовану групу двохрозрядних двохоперандних операцій ССКК [2].

Згідно даного дослідження можна зробити висновок, що з будь-якої з представлених двохрозрядних двохоперандних операцій криптографічного кодування можна отримати повну групу синтезованих двохрозрядних двохоперандних операцій криптографічного перетворення.

В результаті дослідження розроблено підхід до побудови двохрозрядних двохоперандних операцій ССКК на основі перетворення другого операнда.

Застосування групи одноопераднних операцій для перетворення другого операнда дозволяє отримати групу двохрозрядних двохоперандних операцій строгого стійкого криптоперетворення.

Розроблений підхід дозволяє значно спростити процес дослідження та синтезу групи операцій строгого стійкого криптоперетворення.

Таблиця 4.3

Зведені результати синтезу двохоперандних операції ССК на основі операції $O_3^k = \begin{bmatrix} x_1 \cdot (\overline{k_1 \oplus k_2}) \oplus x_2 \cdot (k_1 \oplus k_2) \\ x_1 \cdot (k_1 \oplus k_2) \oplus x_2 \cdot (\overline{k_1 \oplus k_2}) \end{bmatrix} \oplus \begin{bmatrix} k_1 \\ \bar{k}_1 \end{bmatrix}$

Операції перестановок	**Класифікатор операцій** $O_3^k = \begin{bmatrix} x_1 \cdot (\overline{k_1 \oplus k_2}) \oplus x_2 \cdot (k_1 \oplus k_2) \\ x_1 \cdot (k_1 \oplus k_2) \oplus x_2 \cdot (\overline{k_1 \oplus k_2}) \end{bmatrix} \oplus \begin{bmatrix} k_1 \\ \bar{k}_1 \end{bmatrix}$							
	1	$O_3^k = \begin{bmatrix} x_1 \cdot (\overline{k_1 \oplus k_2}) \oplus x_2 \cdot (k_1 \oplus k_2) \\ x_1 \cdot (k_1 \oplus k_2) \oplus x_2 \cdot (\overline{k_1 \oplus k_2}) \end{bmatrix} \oplus \begin{bmatrix} k_1 \\ \bar{k}_1 \end{bmatrix}$	7	$O_{16}^k = \begin{bmatrix} x_1 \cdot (k_1 \oplus k_2) \oplus x_2 \cdot (\overline{k_1 \oplus k_2}) \\ x_1 \cdot (\overline{k_1 \oplus k_2}) \oplus x_2 \cdot (k_1 \oplus k_2) \end{bmatrix} \oplus \begin{bmatrix} k_1 \\ \bar{k}_1 \end{bmatrix}$	13	$O_{20}^k = \begin{bmatrix} x_1 \cdot (k_1 \oplus k_2) \oplus x_2 \cdot (\overline{k_1 \oplus k_2}) \\ x_1 \cdot (\overline{k_1 \oplus k_2}) \oplus x_2 \cdot (k_1 \oplus k_2) \end{bmatrix}$	19	$O_{12}^k = \begin{bmatrix} x_1 \cdot (\overline{k_1 \oplus k_2}) \oplus x_2 \cdot (k_1 \oplus k_2) \\ x_1 \cdot (k_1 \oplus k_2) \oplus x_2 \cdot (\overline{k_1 \oplus k_2}) \end{bmatrix} \oplus \begin{bmatrix} \bar{k}_1 \\ k_1 \end{bmatrix}$
	2	$O_2^k = \begin{bmatrix} x_1 \cdot \bar{k}_1 \oplus x_2 \cdot k_1 \\ x_1 \cdot k_1 \oplus x_2 \cdot \bar{k}_1 \end{bmatrix} \oplus \begin{bmatrix} k_1 \oplus k_2 \\ \overline{k_1 \oplus k_2} \end{bmatrix}$	8	$O_{17}^k = \begin{bmatrix} x_1 \cdot k_1 \oplus x_2 \cdot \bar{k}_1 \\ x_1 \cdot \bar{k}_1 \oplus x_2 \cdot k_1 \end{bmatrix} \oplus \begin{bmatrix} k_1 \oplus k_2 \\ \overline{k_1 \oplus k_2} \end{bmatrix}$	14	$O_{21}^k = \begin{bmatrix} x_1 \cdot k_1 \oplus x_2 \cdot \bar{k}_1 \\ x_1 \cdot \bar{k}_1 \oplus x_2 \cdot k_1 \end{bmatrix} \oplus \begin{bmatrix} \overline{k_1 \oplus k_2} \\ k_1 \oplus k_2 \end{bmatrix}$	20	$O_7^k = \begin{bmatrix} x_1 \cdot \bar{k}_1 \oplus x_2 \cdot k_1 \\ x_1 \cdot k_1 \oplus x_2 \cdot \bar{k}_1 \end{bmatrix} \oplus \begin{bmatrix} \overline{k_1 \oplus k_2} \\ k_1 \oplus k_2 \end{bmatrix}$
	3	$O_4^k = \begin{bmatrix} x_1 \cdot \bar{k}_2 \oplus x_2 \cdot k_2 \\ x_1 \cdot k_2 \oplus x_2 \cdot \bar{k}_2 \end{bmatrix} \oplus \begin{bmatrix} k_1 \\ \bar{k}_1 \end{bmatrix}$	9	$O_{15}^k = \begin{bmatrix} x_1 \cdot k_2 \oplus x_2 \cdot \bar{k}_2 \\ x_1 \cdot \bar{k}_2 \oplus x_2 \cdot k_2 \end{bmatrix} \oplus \begin{bmatrix} k_1 \\ \bar{k}_1 \end{bmatrix}$	15	$O_{19}^k = \begin{bmatrix} x_1 \cdot \bar{k}_2 \oplus x_2 \cdot k_2 \\ x_1 \cdot k_2 \oplus x_2 \cdot \bar{k}_2 \end{bmatrix} \oplus \begin{bmatrix} k_1 \\ \bar{k}_1 \end{bmatrix}$	21	$O_{11}^k = \begin{bmatrix} x_1 \cdot \bar{k}_2 \oplus x_2 \cdot k_2 \\ x_1 \cdot k_2 \oplus x_2 \cdot \bar{k}_2 \end{bmatrix} \oplus \begin{bmatrix} \bar{k}_1 \\ k_1 \end{bmatrix}$
	4	$O_6^k = \begin{bmatrix} x_1 \cdot (\overline{k_1 \oplus k_2}) \oplus x_2 \cdot (k_1 \oplus k_2) \\ x_1 \cdot (k_1 \oplus k_2) \oplus x_2 \cdot (\overline{k_1 \oplus k_2}) \end{bmatrix} \oplus \begin{bmatrix} k_2 \\ \bar{k}_2 \end{bmatrix}$	10	$O_{13}^k = \begin{bmatrix} x_1 \cdot (k_1 \oplus k_2) \oplus x_2 \cdot (\overline{k_1 \oplus k_2}) \\ x_1 \cdot (\overline{k_1 \oplus k_2}) \oplus x_2 \cdot (k_1 \oplus k_2) \end{bmatrix} \oplus \begin{bmatrix} k_2 \\ \bar{k}_2 \end{bmatrix}$	16	$O_{23}^k = \begin{bmatrix} x_1 \cdot (k_1 \oplus k_2) \oplus x_2 \cdot (\overline{k_1 \oplus k_2}) \\ x_1 \cdot (\overline{k_1 \oplus k_2}) \oplus x_2 \cdot (k_1 \oplus k_2) \end{bmatrix} \oplus \begin{bmatrix} \bar{k}_2 \\ k_2 \end{bmatrix}$	22	$O_9^k = \begin{bmatrix} x_1 \cdot (\overline{k_1 \oplus k_2}) \oplus x_2 \cdot (k_1 \oplus k_2) \\ x_1 \cdot (k_1 \oplus k_2) \oplus x_2 \cdot (\overline{k_1 \oplus k_2}) \end{bmatrix} \oplus \begin{bmatrix} \bar{k}_2 \\ k_2 \end{bmatrix}$
	5	$O_1^k = \begin{bmatrix} x_1 \cdot \bar{k}_1 \oplus x_2 \cdot k_1 \\ x_1 \cdot k_1 \oplus x_2 \cdot \bar{k}_1 \end{bmatrix} \oplus \begin{bmatrix} k_2 \\ \bar{k}_2 \end{bmatrix}$	11	$O_{18}^k = \begin{bmatrix} x_1 \cdot k_1 \oplus x_2 \cdot \bar{k}_1 \\ x_1 \cdot \bar{k}_1 \oplus x_2 \cdot k_1 \end{bmatrix} \oplus \begin{bmatrix} k_2 \\ \bar{k}_2 \end{bmatrix}$	17	$O_{22}^k = \begin{bmatrix} x_1 \cdot k_1 \oplus x_2 \cdot \bar{k}_1 \\ x_1 \cdot \bar{k}_1 \oplus x_2 \cdot k_1 \end{bmatrix} \oplus \begin{bmatrix} \bar{k}_2 \\ k_2 \end{bmatrix}$	23	$O_8^k = \begin{bmatrix} x_1 \cdot \bar{k}_1 \oplus x_2 \cdot k_1 \\ x_1 \cdot k_1 \oplus x_2 \cdot \bar{k}_1 \end{bmatrix} \oplus \begin{bmatrix} \bar{k}_2 \\ k_2 \end{bmatrix}$
	6	$O_5^k = \begin{bmatrix} x_1 \cdot \bar{k}_2 \oplus x_2 \cdot k_2 \\ x_1 \cdot k_2 \oplus x_2 \cdot \bar{k}_2 \end{bmatrix} \oplus \begin{bmatrix} k_1 \oplus k_2 \\ \overline{k_1 \oplus k_2} \end{bmatrix}$	12	$O_{14}^k = \begin{bmatrix} x_1 \cdot k_2 \oplus x_2 \cdot \bar{k}_2 \\ x_1 \cdot \bar{k}_2 \oplus x_2 \cdot k_2 \end{bmatrix} \oplus \begin{bmatrix} k_2 \\ \bar{k}_2 \end{bmatrix}$	18	$O_{24}^k = \begin{bmatrix} x_1 \cdot k_2 \oplus x_2 \cdot \bar{k}_2 \\ x_1 \cdot \bar{k}_2 \oplus x_2 \cdot k_2 \end{bmatrix} \oplus \begin{bmatrix} \overline{k_1 \oplus k_2} \\ k_1 \oplus k_2 \end{bmatrix}$	24	$O_{10}^k = \begin{bmatrix} x_1 \cdot \bar{k}_2 \oplus x_2 \cdot k_2 \\ x_1 \cdot k_2 \oplus x_2 \cdot \bar{k}_2 \end{bmatrix} \oplus \begin{bmatrix} \bar{k}_2 \\ k_2 \end{bmatrix}$

Таблиця 4.4

Зведені результати синтезу двохоперандних операції ССК на основі операції $O_4^k = \begin{bmatrix} x_1 \cdot \bar{k}_2 \oplus x_2 \cdot k_2 \\ x_1 \cdot k_2 \oplus x_2 \cdot \bar{k}_2 \end{bmatrix} \oplus \begin{bmatrix} k_1 \\ \bar{k}_1 \end{bmatrix}$

Операції перестановок	**Класифікатор операцій** $O_4^k = \begin{bmatrix} x_1 \cdot \bar{k}_2 \oplus x_2 \cdot k_2 \\ x_1 \cdot k_2 \oplus x_2 \cdot \bar{k}_2 \end{bmatrix} \oplus \begin{bmatrix} k_1 \\ \bar{k}_1 \end{bmatrix}$							
	1	$O_4^k = \begin{bmatrix} x_1 \cdot \bar{k}_2 \oplus x_2 \cdot k_2 \\ x_1 \cdot k_2 \oplus x_2 \cdot \bar{k}_2 \end{bmatrix} \oplus \begin{bmatrix} k_1 \\ \bar{k}_1 \end{bmatrix}$	7	$O_{15}^k = \begin{bmatrix} x_1 \cdot k_2 \oplus x_2 \cdot \bar{k}_2 \\ x_1 \cdot \bar{k}_2 \oplus x_2 \cdot k_2 \end{bmatrix} \oplus \begin{bmatrix} k_1 \\ \bar{k}_1 \end{bmatrix}$	13	$O_{11}^k = \begin{bmatrix} x_1 \cdot \bar{k}_2 \oplus x_2 \cdot k_2 \\ x_1 \cdot k_2 \oplus x_2 \cdot \bar{k}_2 \end{bmatrix} \oplus \begin{bmatrix} \bar{k}_1 \\ k_1 \end{bmatrix}$	19	$O_{19}^k = \begin{bmatrix} x_1 \cdot \bar{k}_2 \oplus x_2 \cdot k_2 \\ x_1 \cdot k_2 \oplus x_2 \cdot \bar{k}_2 \end{bmatrix} \oplus \begin{bmatrix} k_1 \\ \bar{k}_1 \end{bmatrix}$
	2	$O_5^k = \begin{bmatrix} x_1 \cdot \bar{k}_2 \oplus x_2 \cdot k_2 \\ x_1 \cdot k_2 \oplus x_2 \cdot \bar{k}_2 \end{bmatrix} \oplus \begin{bmatrix} k_1 \oplus k_2 \\ \overline{k_1 \oplus k_2} \end{bmatrix}$	8	$O_{14}^k = \begin{bmatrix} x_1 \cdot k_2 \oplus x_2 \cdot \bar{k}_2 \\ x_1 \cdot \bar{k}_2 \oplus x_2 \cdot k_2 \end{bmatrix} \oplus \begin{bmatrix} k_2 \\ \bar{k}_2 \end{bmatrix}$	14	$O_{10}^k = \begin{bmatrix} x_1 \cdot \bar{k}_2 \oplus x_2 \cdot k_2 \\ x_1 \cdot k_2 \oplus x_2 \cdot \bar{k}_2 \end{bmatrix} \oplus \begin{bmatrix} \bar{k}_2 \\ k_2 \end{bmatrix}$	20	$O_{24}^k = \begin{bmatrix} x_1 \cdot k_2 \oplus x_2 \cdot \bar{k}_2 \\ x_1 \cdot \bar{k}_2 \oplus x_2 \cdot k_2 \end{bmatrix} \oplus \begin{bmatrix} \overline{k_1 \oplus k_2} \\ k_1 \oplus k_2 \end{bmatrix}$
	3	$O_3^k = \begin{bmatrix} x_1 \cdot \overline{(k_1 \oplus k_2)} \oplus x_2 \cdot (k_1 \oplus k_2) \\ x_1 \cdot (k_1 \oplus k_2) \oplus x_2 \cdot \overline{(k_1 \oplus k_2)} \end{bmatrix} \oplus \begin{bmatrix} k_1 \\ \bar{k}_1 \end{bmatrix}$	9	$O_{16}^k = \begin{bmatrix} x_1 \cdot (k_1 \oplus k_2) \oplus x_2 \cdot \overline{(k_1 \oplus k_2)} \\ x_1 \cdot \overline{(k_1 \oplus k_2)} \oplus x_2 \cdot (k_1 \oplus k_2) \end{bmatrix} \oplus \begin{bmatrix} k_1 \\ \bar{k}_1 \end{bmatrix}$	15	$O_{12}^k = \begin{bmatrix} x_1 \cdot \overline{(k_1 \oplus k_2)} \oplus x_2 \cdot (k_1 \oplus k_2) \\ x_1 \cdot (k_1 \oplus k_2) \oplus x_2 \cdot \overline{(k_1 \oplus k_2)} \end{bmatrix} \oplus \begin{bmatrix} \bar{k}_1 \\ k_1 \end{bmatrix}$	21	$O_{20}^k = \begin{bmatrix} x_1 \cdot (k_1 \oplus k_2) \oplus x_2 \cdot \overline{(k_1 \oplus k_2)} \\ x_1 \cdot \overline{(k_1 \oplus k_2)} \oplus x_2 \cdot (k_1 \oplus k_2) \end{bmatrix} \oplus \begin{bmatrix} \bar{k}_1 \\ k_1 \end{bmatrix}$
	4	$O_1^k = \begin{bmatrix} x_1 \cdot \bar{k}_1 \oplus x_2 \cdot k_1 \\ x_1 \cdot k_1 \oplus x_2 \cdot \bar{k}_1 \end{bmatrix} \oplus \begin{bmatrix} k_2 \\ \bar{k}_2 \end{bmatrix}$	10	$O_{18}^k = \begin{bmatrix} x_1 \cdot k_1 \oplus x_2 \cdot \bar{k}_1 \\ x_1 \cdot \bar{k}_1 \oplus x_2 \cdot k_1 \end{bmatrix} \oplus \begin{bmatrix} k_2 \\ \bar{k}_2 \end{bmatrix}$	16	$O_8^k = \begin{bmatrix} x_1 \cdot \bar{k}_1 \oplus x_2 \cdot k_1 \\ x_1 \cdot k_1 \oplus x_2 \cdot \bar{k}_1 \end{bmatrix} \oplus \begin{bmatrix} \bar{k}_2 \\ k_2 \end{bmatrix}$	22	$O_{22}^k = \begin{bmatrix} x_1 \cdot k_1 \oplus x_2 \cdot \bar{k}_1 \\ x_1 \cdot \bar{k}_1 \oplus x_2 \cdot k_1 \end{bmatrix} \oplus \begin{bmatrix} \bar{k}_2 \\ k_2 \end{bmatrix}$
	5	$O_6^k = \begin{bmatrix} x_1 \cdot \overline{(k_1 \oplus k_2)} \oplus x_2 \cdot (k_1 \oplus k_2) \\ x_1 \cdot (k_1 \oplus k_2) \oplus x_2 \cdot \overline{(k_1 \oplus k_2)} \end{bmatrix} \oplus \begin{bmatrix} k_2 \\ \bar{k}_2 \end{bmatrix}$	11	$O_{13}^k = \begin{bmatrix} x_1 \cdot (k_1 \oplus k_2) \oplus x_2 \cdot \overline{(k_1 \oplus k_2)} \\ x_1 \cdot \overline{(k_1 \oplus k_2)} \oplus x_2 \cdot (k_1 \oplus k_2) \end{bmatrix} \oplus \begin{bmatrix} k_2 \\ \bar{k}_2 \end{bmatrix}$	17	$O_9^k = \begin{bmatrix} x_1 \cdot \overline{(k_1 \oplus k_2)} \oplus x_2 \cdot (k_1 \oplus k_2) \\ x_1 \cdot (k_1 \oplus k_2) \oplus x_2 \cdot \overline{(k_1 \oplus k_2)} \end{bmatrix} \oplus \begin{bmatrix} \bar{k}_2 \\ k_2 \end{bmatrix}$	23	$O_{23}^k = \begin{bmatrix} x_1 \cdot (k_1 \oplus k_2) \oplus x_2 \cdot \overline{(k_1 \oplus k_2)} \\ x_1 \cdot \overline{(k_1 \oplus k_2)} \oplus x_2 \cdot (k_1 \oplus k_2) \end{bmatrix} \oplus \begin{bmatrix} \bar{k}_2 \\ k_2 \end{bmatrix}$
	6	$O_2^k = \begin{bmatrix} x_1 \cdot \bar{k}_1 \oplus x_2 \cdot k_1 \\ x_1 \cdot k_1 \oplus x_2 \cdot \bar{k}_1 \end{bmatrix} \oplus \begin{bmatrix} k_1 \oplus k_2 \\ \overline{k_1 \oplus k_2} \end{bmatrix}$	12	$O_{17}^k = \begin{bmatrix} x_1 \cdot k_1 \oplus x_2 \cdot \bar{k}_1 \\ x_1 \cdot \bar{k}_1 \oplus x_2 \cdot k_1 \end{bmatrix} \oplus \begin{bmatrix} k_1 \oplus k_2 \\ \overline{k_1 \oplus k_2} \end{bmatrix}$	18	$O_7^k = \begin{bmatrix} x_1 \cdot \bar{k}_1 \oplus x_2 \cdot k_1 \\ x_1 \cdot k_1 \oplus x_2 \cdot \bar{k}_1 \end{bmatrix} \oplus \begin{bmatrix} \overline{k_1 \oplus k_2} \\ k_1 \oplus k_2 \end{bmatrix}$	24	$O_{21}^k = \begin{bmatrix} x_1 \cdot k_1 \oplus x_2 \cdot \bar{k}_1 \\ x_1 \cdot \bar{k}_1 \oplus x_2 \cdot k_1 \end{bmatrix} \oplus \begin{bmatrix} k_1 \oplus k_2 \\ \overline{k_1 \oplus k_2} \end{bmatrix}$

4.1.2 Розробка методу генерації псевдовипадкових послідовностей двохрозрядних двохоперандних операцій строгого стійкого криптографічного кодування на основі перетворення другого операнда

Проведене дослідження показує можливість отримання групи операцій криптоперетворення з кожної двохрозрядної двохоперандної операції криптографічного кодування в межах даної групи, тобто генерацію послідовностей операцій криптоперетворення.

Побудова послідовностей двохрозрядних двохоперандних операцій строгого стійкого криптоперетворення на основі одноопераднних операцій призводить до побудови різних послідовностей операцій. В результаті даного дослідження було отримано генерацію груп з двохрозрядних двохоперандних операцій строгого стійкого криптоперетворення на основі використання одноопераднних операцій криптографічного кодування.

Результати даного дослідження представлені в табл.4.5 [2].

Сутність методу генерації псевдовипадкових послідовностей двохрозрядних двохоперандних операцій ССКК на основі перетворення другого операнда можна представити наступним алгоритмом:

1. Визначення заданої двохрозрядної двохоперандної операції ССКК на основі перетворення другого операнда.
2. Випадкова генерація групи одноопераднних двохрозрядних операції ССКК.
3. Модифікація заданої двохрозрядної двохоперандної операції шляхом перетворення другого операнда відомої операції за допомогою одноопераднної операції.
4. Перевірка отриманого результату модифікованої операції.
5. Модифікація отриманої операції шляхом виконання повторної операції перетворення другого операнда відомої операції за допомогою одноопераднної операції.
6. Перевірка отриманого результату правильного виконання операції перетворення над другим операном вибраної операції.
7. Пункти 3–6 повторюються до завершення використання повної групи модифікованих двохрозрядних двохоперандних операцій строгого стійкого криптографічного перетворення.

8. Пункти 2–7 повторюються до повного завершення криптоперетворення інформації.

На рис. 4.1 наведено блок-схему реалізації даного алгоритму.

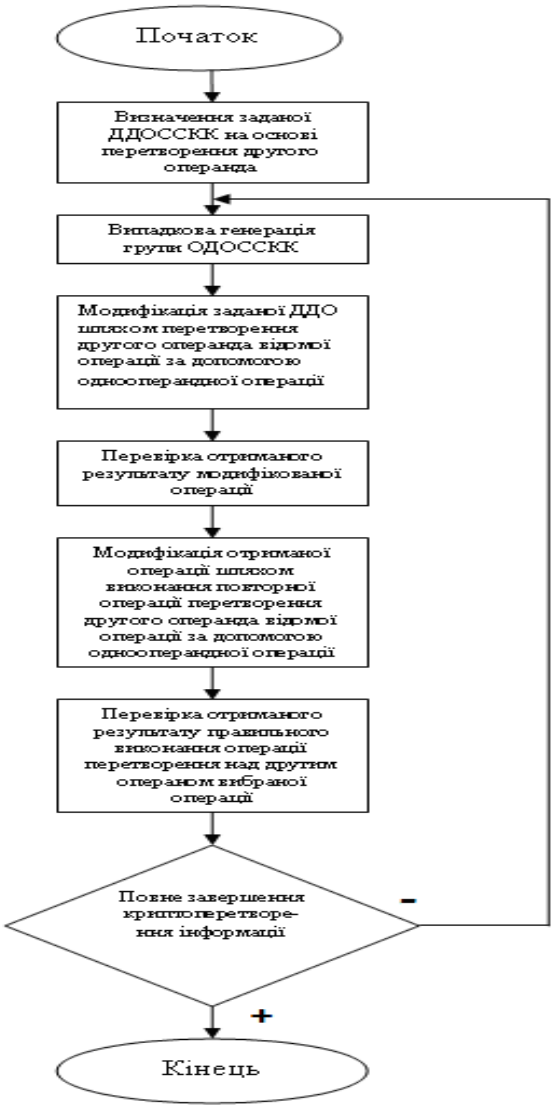


Рис. 4.5. Блок-схема реалізації алгоритму генерації псевдовипадкових послідовностей двохрозрядних двохоперандних операцій ССКК на основі перетворення другого операнда

Реалізація даного методу забезпечує псевдовипадковий синтез операцій криптоперетворення. Даний метод генерації псевдовипадкових послідовностей двохрозрядних двохоперандних операцій ССКК, на основі перетворення другого операнда доцільно використати при вдосконаленні методу підвищення криптостійкості і надійності потокового шифрування [2,5].

Таблиця 4.5

Генерація повної групи послідовностей операцій криптоперетворення

O	Операції перетворення																							
	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24
O_1^k	O_1^k	O_6^k	O_2^k	O_4^k	O_5^k	O_3^k	O_8^k	O_9^k	O_7^k	O_{11}^k	O_{10}^k	O_{12}^k	O_{18}^k	O_{13}^k	O_{17}^k	O_{15}^k	O_{14}^k	O_{16}^k	O_{22}^k	O_{23}^k	O_{21}^k	O_{19}^k	O_{24}^k	O_{20}^k
O_2^k	O_2^k	O_3^k	O_1^k	O_5^k	O_4^k	O_6^k	O_7^k	O_{12}^k	O_8^k	O_{10}^k	O_{11}^k	O_9^k	O_{21}^k	O_{20}^k	O_{22}^k	O_{24}^k	O_{19}^k	O_{23}^k	O_{17}^k	O_{16}^k	O_{18}^k	O_{14}^k	O_{15}^k	O_{13}^k
O_3^k	O_3^k	O_2^k	O_4^k	O_6^k	O_1^k	O_5^k	O_{16}^k	O_{17}^k	O_{15}^k	O_{13}^k	O_{18}^k	O_{14}^k	O_{20}^k	O_{21}^k	O_{19}^k	O_{23}^k	O_{22}^k	O_{24}^k	O_{12}^k	O_7^k	O_{11}^k	O_9^k	O_8^k	O_{10}^k
O_4^k	O_4^k	O_5^k	O_3^k	O_1^k	O_6^k	O_2^k	O_{15}^k	O_{14}^k	O_{16}^k	O_{18}^k	O_{13}^k	O_{17}^k	O_{11}^k	O_{10}^k	O_{12}^k	O_8^k	O_9^k	O_7^k	O_{19}^k	O_{24}^k	O_{20}^k	O_{22}^k	O_{23}^k	O_{21}^k
O_5^k	O_5^k	O_4^k	O_6^k	O_2^k	O_3^k	O_1^k	O_{24}^k	O_{19}^k	O_{23}^k	O_{21}^k	O_{20}^k	O_{22}^k	O_{10}^k	O_{11}^k	O_9^k	O_7^k	O_{12}^k	O_8^k	O_{14}^k	O_{15}^k	O_{13}^k	O_{17}^k	O_{16}^k	O_{18}^k
O_6^k	O_6^k	O_1^k	O_5^k	O_3^k	O_2^k	O_4^k	O_{23}^k	O_{22}^k	O_{24}^k	O_{20}^k	O_{21}^k	O_{19}^k	O_{13}^k	O_{18}^k	O_{14}^k	O_{16}^k	O_{17}^k	O_{15}^k	O_9^k	O_8^k	O_{10}^k	O_{12}^k	O_7^k	O_{11}^k
O_7^k	O_7^k	O_{12}^k	O_8^k	O_{10}^k	O_{11}^k	O_9^k	O_2^k	O_3^k	O_1^k	O_5^k	O_4^k	O_6^k	O_{17}^k	O_{16}^k	O_{18}^k	O_{14}^k	O_{15}^k	O_{13}^k	O_{21}^k	O_{20}^k	O_{22}^k	O_{24}^k	O_{19}^k	O_{23}^k
O_8^k	O_8^k	O_9^k	O_7^k	O_{11}^k	O_{10}^k	O_{12}^k	O_1^k	O_6^k	O_2^k	O_4^k	O_5^k	O_3^k	O_{22}^k	O_{23}^k	O_{21}^k	O_{19}^k	O_{24}^k	O_{20}^k	O_{18}^k	O_{13}^k	O_{17}^k	O_{15}^k	O_{14}^k	O_{16}^k
O_9^k	O_9^k	O_8^k	O_{10}^k	O_{12}^k	O_7^k	O_{11}^k	O_{13}^k	O_{18}^k	O_{14}^k	O_{16}^k	O_{17}^k	O_{15}^k	O_{23}^k	O_{22}^k	O_{24}^k	O_{20}^k	O_{21}^k	O_{19}^k	O_6^k	O_1^k	O_5^k	O_3^k	O_2^k	O_4^k
O_{10}^k	O_{10}^k	O_{11}^k	O_9^k	O_7^k	O_{12}^k	O_8^k	O_{14}^k	O_{15}^k	O_{13}^k	O_{17}^k	O_{16}^k	O_{18}^k	O_5^k	O_4^k	O_6^k	O_2^k	O_3^k	O_1^k	O_{24}^k	O_{19}^k	O_{23}^k	O_{21}^k	O_{20}^k	O_{22}^k
O_{11}^k	O_{11}^k	O_{10}^k	O_{12}^k	O_8^k	O_9^k	O_7^k	O_{19}^k	O_{24}^k	O_{20}^k	O_{22}^k	O_{23}^k	O_{21}^k	O_4^k	O_5^k	O_3^k	O_1^k	O_6^k	O_2^k	O_{15}^k	O_{14}^k	O_{16}^k	O_{18}^k	O_{13}^k	O_{17}^k
O_{12}^k	O_{12}^k	O_7^k	O_{11}^k	O_9^k	O_8^k	O_{10}^k	O_{20}^k	O_{21}^k	O_{19}^k	O_{23}^k	O_{22}^k	O_{24}^k	O_{16}^k	O_{17}^k	O_{15}^k	O_{13}^k	O_{18}^k	O_{14}^k	O_3^k	O_2^k	O_4^k	O_6^k	O_1^k	O_5^k
O_{13}^k	O_{13}^k	O_{18}^k	O_{14}^k	O_{16}^k	O_{17}^k	O_{15}^k	O_9^k	O_8^k	O_{10}^k	O_{12}^k	O_7^k	O_{11}^k	O_6^k	O_1^k	O_5^k	O_3^k	O_2^k	O_4^k	O_{23}^k	O_{22}^k	O_{24}^k	O_{20}^k	O_{21}^k	O_{19}^k
O_{14}^k	O_{14}^k	O_{15}^k	O_{13}^k	O_{17}^k	O_{16}^k	O_{18}^k	O_{10}^k	O_{11}^k	O_9^k	O_7^k	O_{12}^k	O_8^k	O_{24}^k	O_{19}^k	O_{23}^k	O_{21}^k	O_{20}^k	O_{22}^k	O_5^k	O_4^k	O_6^k	O_2^k	O_3^k	O_1^k
O_{15}^k	O_{15}^k	O_{14}^k	O_{16}^k	O_{18}^k	O_{13}^k	O_{17}^k	O_4^k	O_5^k	O_3^k	O_1^k	O_6^k	O_2^k	O_{19}^k	O_{24}^k	O_{20}^k	O_{22}^k	O_{23}^k	O_{21}^k	O_{11}^k	O_{10}^k	O_{12}^k	O_8^k	O_9^k	O_7^k
O_{16}^k	O_{16}^k	O_{17}^k	O_{15}^k	O_{13}^k	O_{18}^k	O_{14}^k	O_3^k	O_2^k	O_4^k	O_6^k	O_1^k	O_5^k	O_{12}^k	O_7^k	O_{11}^k	O_9^k	O_8^k	O_{10}^k	O_{20}^k	O_{21}^k	O_{19}^k	O_{23}^k	O_{22}^k	O_{24}^k
O_{17}^k	O_{17}^k	O_{16}^k	O_{18}^k	O_{14}^k	O_{15}^k	O_{13}^k	O_{21}^k	O_{20}^k	O_{22}^k	O_{24}^k	O_{19}^k	O_{23}^k	O_7^k	O_{12}^k	O_8^k	O_{10}^k	O_{11}^k	O_9^k	O_2^k	O_3^k	O_1^k	O_5^k	O_4^k	O_6^k
O_{18}^k	O_{18}^k	O_{13}^k	O_{17}^k	O_{15}^k	O_{14}^k	O_{16}^k	O_{22}^k	O_{23}^k	O_{21}^k	O_{19}^k	O_{24}^k	O_{20}^k	O_1^k	O_6^k	O_2^k	O_4^k	O_5^k	O_3^k	O_8^k	O_9^k	O_7^k	O_{11}^k	O_{10}^k	O_{12}^k
O_{19}^k	O_{19}^k	O_{24}^k	O_{20}^k	O_{22}^k	O_{23}^k	O_{21}^k	O_{11}^k	O_{10}^k	O_{12}^k	O_8^k	O_9^k	O_7^k	O_{15}^k	O_{14}^k	O_{16}^k	O_{18}^k	O_{13}^k	O_{17}^k	O_4^k	O_5^k	O_3^k	O_1^k	O_6^k	O_2^k
O_{20}^k	O_{20}^k	O_{21}^k	O_{19}^k	O_{23}^k	O_{22}^k	O_{24}^k	O_{12}^k	O_7^k	O_{11}^k	O_9^k	O_8^k	O_{10}^k	O_3^k	O_2^k	O_4^k	O_6^k	O_1^k	O_5^k	O_{16}^k	O_{17}^k	O_{15}^k	O_{13}^k	O_{18}^k	O_{14}^k
O_{21}^k	O_{21}^k	O_{20}^k	O_{22}^k	O_{24}^k	O_{19}^k	O_{23}^k	O_{17}^k	O_{16}^k	O_{18}^k	O_{14}^k	O_{15}^k	O_{13}^k	O_2^k	O_3^k	O_1^k	O_5^k	O_4^k	O_6^k	O_7^k	O_{12}^k	O_8^k	O_{10}^k	O_{11}^k	O_9^k
O_{22}^k	O_{22}^k	O_{23}^k	O_{21}^k	O_{19}^k	O_{24}^k	O_{20}^k	O_{18}^k	O_{13}^k	O_{17}^k	O_{15}^k	O_{14}^k	O_{16}^k	O_8^k	O_9^k	O_7^k	O_{11}^k	O_{10}^k	O_{12}^k	O_1^k	O_6^k	O_2^k	O_4^k	O_5^k	O_3^k
O_{23}^k	O_{23}^k	O_{22}^k	O_{24}^k	O_{20}^k	O_{21}^k	O_{19}^k	O_6^k	O_1^k	O_5^k	O_3^k	O_2^k	O_4^k	O_9^k	O_8^k	O_{10}^k	O_{12}^k	O_7^k	O_{11}^k	O_{13}^k	O_{18}^k	O_{14}^k	O_{16}^k	O_{17}^k	O_{15}^k
O_{24}^k	O_{24}^k	O_{19}^k	O_{23}^k	O_{21}^k	O_{20}^k	O_{22}^k	O_5^k	O_4^k	O_6^k	O_2^k	O_3^k	O_1^k	O_{14}^k	O_{15}^k	O_{13}^k	O_{17}^k	O_{16}^k	O_{18}^k	O_{10}^k	O_{11}^k	O_9^k	O_7^k	O_{12}^k	O_8^k

4.2 Генерації взаємопов'язаних псевдовипадкових послідовностей прямих і обернених двохрозрядних двохоперандних операцій строгого стійкого криптографічного кодування на основі перетворення другого операнда

Дослідимо можливість спрощення синтезу двохрозрядних двохоперандних операцій ССКК шляхом перетворення другого операнда. Візьмемо двохрозрядну двохоперандну операцію ССКК даного представлення $O_1^k = \begin{bmatrix} x_1 \cdot \bar{k}_1 \oplus x_2 \cdot k_1 \\ x_1 \cdot k_1 \oplus x_2 \cdot \bar{k}_1 \end{bmatrix} \oplus \begin{bmatrix} k_2 \\ \bar{k}_2 \end{bmatrix}$ [2].

Для знаходження обернених двохрозрядних двохоперандних операцій ССКК необхідно провести перетворення другого операнда за допомогою одноопераднних операцій.

В роботі доведено, що на основі перетворення другого операнда за допомогою одноопераднних операцій буде отримано повну групу двозоперандних операцій, якій належать всі прямі і відповідні їм обернені операції.

Провівши аналіз будови двохоперандної операції, можна стверждувати, що вона реалізує чотири одноопераднді операції. Основною умовою для її виконання є значення другого операнда. Враховуючи це, можна допустити, що при однаковій зміні умов реалізації одноопераднних операцій в прямому і оберненому криптоперетвореннi буде отримана нова пара взаємопов'язаних операцій придатна для застосування в криптографії.

Перевіримо правильність нашого твердження на прикладі групи операцій криптографічного перетворення на основі O_1^k [2].

Візьмемо двохрозрядну двохоперандну операцію ССКК у вигляді $O_1^k = \begin{bmatrix} x_1 \cdot \bar{k}_1 \oplus x_2 \cdot k_1 \\ x_1 \cdot k_1 \oplus x_2 \cdot \bar{k}_1 \end{bmatrix} \oplus \begin{bmatrix} k_2 \\ \bar{k}_2 \end{bmatrix}$ та виконаємо над другим операндом одноопераднде перетворення $F_{3,5} = \begin{bmatrix} y_1 \\ y_2 \end{bmatrix}$, у якому (y_1) – це k_1, а (y_2) – це k_2.

В результаті отримуємо наступне перетворення:

$$F_{3,5}\left(O_1^k\right) = \begin{bmatrix} x_1 \cdot \bar{y}_1 \oplus x_2 \cdot y_1 \\ x_1 \cdot y_1 \oplus x_2 \cdot \bar{y}_1 \end{bmatrix} \oplus \begin{bmatrix} y_2 \\ \bar{y}_2 \end{bmatrix} = O_1^{d_1},$$

де $O_1^{d_1}$ – це операція декодування, на основі перетворення другого операнда двохрозрядної двохоперандної операції одноопераднною операцією.

Тобто, в результаті перетворення отримуємо операцію $O_1^{d_1}$, що відповідає операції O_1^k.

В подальшому виконаємо ще одне перетворення $F_{3,5} = \begin{bmatrix} y_1 \\ y_2 \end{bmatrix}$ над отриманою операцією, яка відповідає $O_1^k = \begin{bmatrix} x_1 \cdot \bar{k}_1 \oplus x_2 \cdot k_1 \\ x_1 \cdot k_1 \oplus x_2 \cdot \bar{k}_1 \end{bmatrix} \oplus \begin{bmatrix} k_2 \\ \bar{k}_2 \end{bmatrix}$. В результаті отримуємо наступне:

$$F_{3,5}\left(O_1^{d_1}\right) = \begin{bmatrix} x_1 \cdot \bar{k}_1 \oplus x_2 \cdot k_1 \\ x_1 \cdot k_1 \oplus x_2 \cdot \bar{k}_1 \end{bmatrix} \oplus \begin{bmatrix} k_2 \\ \bar{k}_2 \end{bmatrix} = O_1^k$$

Таким чином в результаті подвійного перетворення $F_{3,5} = \begin{bmatrix} y_1 \\ y_2 \end{bmatrix}$ з O_1^k отримуємо $O_1^k = \begin{bmatrix} x_1 \cdot \bar{k}_1 \oplus x_2 \cdot k_1 \\ x_1 \cdot k_1 \oplus x_2 \cdot \bar{k}_1 \end{bmatrix} \oplus \begin{bmatrix} k_2 \\ \bar{k}_2 \end{bmatrix}$.

Візьмемо двохрозрядну двохоперандну операцію строгого стійкого криптографічного перетворення такого представлення $O_1^k = \begin{bmatrix} x_1 \cdot \bar{k}_1 \oplus x_2 \cdot k_1 \\ x_1 \cdot k_1 \oplus x_2 \cdot \bar{k}_1 \end{bmatrix} \oplus \begin{bmatrix} k_2 \\ \bar{k}_2 \end{bmatrix}$ та виконаємо над другим операндом одноопераднде перетворення $F_{6,5} = \begin{bmatrix} y_1 \oplus y_2 \\ y_2 \end{bmatrix}$, у якому $(y_1 \oplus y_2)$ – це k_1, а y_2 – це k_2.

В результаті даного перетворення отримуємо:

$$F_{6,5}(O_1^k)=\begin{bmatrix} x_1\cdot(\overline{(y_1\oplus y_2)\oplus y_2})\oplus x_2\cdot((y_1\oplus y_2)\oplus y_2) \\ x_1\cdot((y_1\oplus y_2)\oplus y_2)\oplus x_2\cdot(\overline{(y_1\oplus y_2)\oplus y_2}) \end{bmatrix}\oplus\begin{bmatrix} y_2 \\ \bar{y}_2 \end{bmatrix}=O_1^{d_2}\ .$$

Тобто в результаті перетворення отримуємо операцію $O_1^{d_2}$,що, в свою чергу відповідає O_6^k .

В процесі подальшого двохрозрядного одноопераднього перетворення $F_{6,5}=\begin{bmatrix} y_1\oplus y_2 \\ y_2 \end{bmatrix}$ над $O_1^{d_2}=\begin{bmatrix} x_1\cdot(\overline{(y_1\oplus y_2)\oplus y_2})\oplus x_2\cdot((y_1\oplus y_2)\oplus y_2) \\ x_1\cdot((y_1\oplus y_2)\oplus y_2)\oplus x_2\cdot(\overline{(y_1\oplus y_2)\oplus y_2}) \end{bmatrix}\oplus\begin{bmatrix} y_2 \\ \bar{y}_2 \end{bmatrix}$ отримуємо наступне:

$$F_{6,5}(O_1^{d_2})=\begin{bmatrix} x_1\cdot\bar{k}_1\oplus x_2\cdot k_1 \\ x_1\cdot k_1\oplus x_2\cdot\bar{k}_1 \end{bmatrix}\oplus\begin{bmatrix} k_2 \\ \bar{k}_2 \end{bmatrix}=O_1^k\ ,$$

Таким чином в результаті подвійного перетворення $F_{6,5}=\begin{bmatrix} y_1\oplus y_2 \\ y_2 \end{bmatrix}$ з O_1^k отримуємо $O_1^k=\begin{bmatrix} x_1\cdot\bar{k}_1\oplus x_2\cdot k_1 \\ x_1\cdot k_1\oplus x_2\cdot\bar{k}_1 \end{bmatrix}\oplus\begin{bmatrix} k_2 \\ \bar{k}_2 \end{bmatrix}$.

Візьмемо двохрозрядну двохоперандну операцію строгого стійкого криптографічного перетворення такого представлення $O_1^k=\begin{bmatrix} x_1\cdot\bar{k}_1\oplus x_2\cdot k_1 \\ x_1\cdot k_1\oplus x_2\cdot\bar{k}_1 \end{bmatrix}\oplus\begin{bmatrix} k_2 \\ \bar{k}_2 \end{bmatrix}$ та виконаємо над другим операндом одноопераднe перетворення $F_{3,6}=\begin{bmatrix} y_1 \\ y_1\oplus y_2 \end{bmatrix}$, у якому (y_1) – це k_1 , а ($y_1\oplus y_2$) – це k_2 .

В результаті даного перетворення отримуємо:

$$F_{3,6}(O_1^k)=\begin{bmatrix} x_1\cdot\overline{y_1}\oplus x_2\cdot y_1 \\ x_1\cdot y_1\oplus x_2\cdot\overline{y_1} \end{bmatrix}\oplus\begin{bmatrix} (y_1\oplus y_2) \\ \overline{(y_1\oplus y_2)} \end{bmatrix}=O_1^{d_3}\ .$$

Тобто в результаті перетворення отримуємо операцію $O_1^{d_3}$,що, в свою чергу відповідає O_2^k .

В процесі подальшого двохрозрядного одноопераднього перетворення $F_{3,6}=\begin{bmatrix} y_1 \\ y_1\oplus y_2 \end{bmatrix}$ над $O_1^{d_3}=\begin{bmatrix} x_1\cdot\overline{y_1}\oplus x_2\cdot y_1 \\ x_1\cdot y_1\oplus x_2\cdot\overline{y_1} \end{bmatrix}\oplus\begin{bmatrix} (y_1\oplus y_2) \\ \overline{(y_1\oplus y_2)} \end{bmatrix}$ отримуємо наступне:

$$F_{3,6}(O_1^{d_3})=\begin{bmatrix} x_1\cdot\bar{k}_1\oplus x_2\cdot k_1 \\ x_1\cdot k_1\oplus x_2\cdot\bar{k}_1 \end{bmatrix}\oplus\begin{bmatrix} k_2 \\ \bar{k}_2 \end{bmatrix}=O_1^k\ ,$$

Таким чином в результаті подвійного перетворення $F_{3,6}=\begin{bmatrix} y_1 \\ y_1 \oplus y_2 \end{bmatrix}$ з O_1^k отримуємо $O_1^k=\begin{bmatrix} x_1 \cdot \bar{k}_1 \oplus x_2 \cdot k_1 \\ x_1 \cdot k_1 \oplus x_2 \cdot \bar{k}_1 \end{bmatrix} \oplus \begin{bmatrix} k_2 \\ \bar{k}_2 \end{bmatrix}$.

Візьмемо двохрозрядну двохоперандну операцію строгого стійкого криптографічного перетворення такого представлення $O_1^k=\begin{bmatrix} x_1 \cdot \bar{k}_1 \oplus x_2 \cdot k_1 \\ x_1 \cdot k_1 \oplus x_2 \cdot \bar{k}_1 \end{bmatrix} \oplus \begin{bmatrix} k_2 \\ \bar{k}_2 \end{bmatrix}$ та виконаємо над другим операндом одноопераднe перетворення $F_{5,3}=\begin{bmatrix} y_2 \\ y_1 \end{bmatrix}$, у якому ($y_2$) – це k_1, а (y_1) – це k_2.

В результаті даного перетворення отримуємо:

$$F_{5,3}(O_1^k)=\begin{bmatrix} x_1 \cdot \overline{y_2} \oplus x_2 \cdot y_2 \\ x_1 \cdot y_2 \oplus x_2 \cdot \overline{y_2} \end{bmatrix} \oplus \begin{bmatrix} y_1 \\ \overline{y_1} \end{bmatrix} = O_1^{d_4} .$$

Тобто в результаті перетворення отримуємо операцію $O_1^{d_4}$,що, в свою чергу відповідає $O_4^k=\begin{bmatrix} x_1 \cdot \bar{k}_2 \oplus x_2 \cdot k_2 \\ x_1 \cdot k_2 \oplus x_2 \cdot \bar{k}_2 \end{bmatrix} \oplus \begin{bmatrix} k_1 \\ \bar{k}_1 \end{bmatrix}$.

В процесі подальшого двохрозрядного одноопераднoго перетворення $F_{5,3}=\begin{bmatrix} y_2 \\ y_1 \end{bmatrix}$ над $O_1^{d_3}=\begin{bmatrix} x_1 \cdot \overline{y_1} \oplus x_2 \cdot y_1 \\ x_1 \cdot y_1 \oplus x_2 \cdot \overline{y_1} \end{bmatrix} \oplus \begin{bmatrix} (y_1 \oplus y_2) \\ \overline{(y_1 \oplus y_2)} \end{bmatrix}$ отримуємо наступне:

$$F_{5,3}(O_1^{d_4})= \begin{bmatrix} x_1 \cdot \bar{k}_1 \oplus x_2 \cdot k_1 \\ x_1 \cdot k_1 \oplus x_2 \cdot \bar{k}_1 \end{bmatrix} \oplus \begin{bmatrix} k_2 \\ \bar{k}_2 \end{bmatrix} = O_1^k ,$$

Таким чином в результаті подвійного перетворення $F_{5,3}=\begin{bmatrix} y_2 \\ y_1 \end{bmatrix}$ з O_1^k отримуємо $O_1^k=\begin{bmatrix} x_1 \cdot \bar{k}_1 \oplus x_2 \cdot k_1 \\ x_1 \cdot k_1 \oplus x_2 \cdot \bar{k}_1 \end{bmatrix} \oplus \begin{bmatrix} k_2 \\ \bar{k}_2 \end{bmatrix}$.

Візьмемо двохрозрядну двохоперандну операцію строгого стійкого криптографічного перетворення такого представлення $O_1^k=\begin{bmatrix} x_1 \cdot \bar{k}_1 \oplus x_2 \cdot k_1 \\ x_1 \cdot k_1 \oplus x_2 \cdot \bar{k}_1 \end{bmatrix} \oplus \begin{bmatrix} k_2 \\ \bar{k}_2 \end{bmatrix}$ та виконаємо над другим операндом одноопераднe перетворення $F_{5,6}=\begin{bmatrix} y_2 \\ y_1 \oplus y_2 \end{bmatrix}$, у якому ($y_2$) – це k_1, а ($y_1 \oplus y_2$) – це k_2.

В результаті даного перетворення отримуємо:

$$F_{5,6}(O_1^k)=\begin{bmatrix} x_1\cdot\overline{y_2}\oplus x_2\cdot y_2 \\ x_1\cdot y_2\oplus x_2\cdot\overline{y_2}\end{bmatrix}\oplus\begin{bmatrix}(y_1\oplus y_2)\\ \overline{(y_1\oplus y_2)}\end{bmatrix}=O_1^{d_5}\ .$$

Тобто в результаті перетворення отримуємо операцію $O_1^{d_5}$,що, в свою чергу відповідає $O_5^k=\begin{bmatrix} x_1\cdot\bar{k}_2\oplus x_2\cdot k_2 \\ x_1\cdot k_2\oplus x_2\cdot\bar{k}_2\end{bmatrix}\oplus\begin{bmatrix}k_1\oplus k_2\\ \overline{k_1\oplus k_2}\end{bmatrix}$.

В процесі подальшого двохрозрядного одноопераднього перетворення $F_{5,6}=\begin{bmatrix} y_2 \\ y_1\oplus y_2\end{bmatrix}$ над $O_1^{d_5}=\begin{bmatrix} x_1\cdot\overline{y_1}\oplus x_2\cdot y_1 \\ x_1\cdot y_1\oplus x_2\cdot\overline{y_1}\end{bmatrix}\oplus\begin{bmatrix}(y_1\oplus y_2)\\ \overline{(y_1\oplus y_2)}\end{bmatrix}$ отримуємо наступне:

$$F_{5,6}(O_1^{d_5})=\begin{bmatrix} x_1\cdot\bar{k}_1\oplus x_2\cdot k_1 \\ x_1\cdot k_1\oplus x_2\cdot\bar{k}_1\end{bmatrix}\oplus\begin{bmatrix}k_2\\ \bar{k}_2\end{bmatrix}=O_1^k\ ,$$

Таким чином в результаті подвійного перетворення $F_{5,6}=\begin{bmatrix} y_2 \\ y_1\oplus y_2\end{bmatrix}$ з O_1^k отримуємо $O_1^k=\begin{bmatrix} x_1\cdot\bar{k}_1\oplus x_2\cdot k_1 \\ x_1\cdot k_1\oplus x_2\cdot\bar{k}_1\end{bmatrix}\oplus\begin{bmatrix}k_2\\ \bar{k}_2\end{bmatrix}$.

Візьмемо двохрозрядну двохоперандну операцію строгого стійкого криптографічного перетворення такого представлення $O_1^k=\begin{bmatrix} x_1\cdot\bar{k}_1\oplus x_2\cdot k_1 \\ x_1\cdot k_1\oplus x_2\cdot\bar{k}_1\end{bmatrix}\oplus\begin{bmatrix}k_2\\ \bar{k}_2\end{bmatrix}$ та виконаємо над другим операндом одноопераднe перетворення $F_{6,3}=\begin{bmatrix} y_1\oplus y_2 \\ y_1\end{bmatrix}$, у якому $(y_1\oplus y_2)$ – це k_1, а (y_1) – це k_2.

В результаті даного перетворення отримуємо:

$$F_{6,5}(O_1^k)=\begin{bmatrix} x_1\cdot\overline{(y_1\oplus y_2)}\oplus x_2\cdot(y_1\oplus y_2) \\ x_1\cdot(y_1\oplus y_2)\oplus x_2\cdot\overline{(y_1\oplus y_2)}\end{bmatrix}\oplus\begin{bmatrix}y_1\\ \overline{y_1}\end{bmatrix}=O_1^{d_6}\ .$$

Тобто в результаті перетворення отримуємо операцію $O_1^{d_6}$,що, в свою чергу відповідає $O_3^k=\begin{bmatrix} x_1\cdot\overline{(k_1\oplus k_2)}\oplus x_2\cdot(k_1\oplus k_2) \\ x_1\cdot(k_1\oplus k_2)\oplus x_2\cdot\overline{(k_1\oplus k_2)}\end{bmatrix}\oplus\begin{bmatrix}k_1\\ \bar{k}_1\end{bmatrix}$.

В процесі подальшого двохрозрядного одноопераднього перетворення $F_{6,3}=\begin{bmatrix} y_1\oplus y_2 \\ y_1\end{bmatrix}$ над $O_1^{d_6}=\begin{bmatrix} x_1\cdot\overline{(y_1\oplus y_2)}\oplus x_2\cdot(y_1\oplus y_2) \\ x_1\cdot(y_1\oplus y_2)\oplus x_2\cdot\overline{(y_1\oplus y_2)}\end{bmatrix}\oplus\begin{bmatrix}y_1\\ \overline{y_1}\end{bmatrix}$ отримуємо наступне:

$$F_{6,5}(O_1^{d_6}) = \begin{bmatrix} x_1 \cdot \bar{k}_1 \oplus x_2 \cdot k_1 \\ x_1 \cdot k_1 \oplus x_2 \cdot \bar{k}_1 \end{bmatrix} \oplus \begin{bmatrix} k_2 \\ \bar{k}_2 \end{bmatrix} = O_1^k \ ,$$

Таким чином в результаті подвійного перетворення $F_{6,3} = \begin{bmatrix} y_1 \oplus y_2 \\ y_1 \end{bmatrix}$ з O_1^k отримуємо $O_1^k = \begin{bmatrix} x_1 \cdot \bar{k}_1 \oplus x_2 \cdot k_1 \\ x_1 \cdot k_1 \oplus x_2 \cdot \bar{k}_1 \end{bmatrix} \oplus \begin{bmatrix} k_2 \\ \bar{k}_2 \end{bmatrix}$.

Візьмемо двохрозрядну двохоперандну операцію строгого стійкого криптографічного перетворення такого представлення $O_1^k = \begin{bmatrix} x_1 \cdot \bar{k}_1 \oplus x_2 \cdot k_1 \\ x_1 \cdot k_1 \oplus x_2 \cdot \bar{k}_1 \end{bmatrix} \oplus \begin{bmatrix} k_2 \\ \bar{k}_2 \end{bmatrix}$ та виконаємо над другим операндом одноопераднe перетворення $F_{3,10} = \begin{bmatrix} y_1 \\ y_2 \oplus 1 \end{bmatrix}$, у якому (y_1) – це k_1, а $(y_2 \oplus 1)$ – це k_2.

В результаті даного перетворення отримуємо:

$$F_{3,10}(O_1^k) = \begin{bmatrix} x_1 \cdot \overline{y_1} \oplus x_2 \cdot y_1 \\ x_1 \cdot y_1 \oplus x_2 \cdot \overline{y_1} \end{bmatrix} \oplus \begin{bmatrix} (y_2 \oplus 1) \\ \overline{(y_2 \oplus 1)} \end{bmatrix} = O_1^{d_7} \ .$$

Тобто в результаті перетворення отримуємо операцію $O_1^{d_7}$,що, в свою чергу відповідає $O_8^k = \begin{bmatrix} x_1 \cdot \bar{k}_1 \oplus x_2 \cdot k_1 \\ x_1 \cdot k_1 \oplus x_2 \cdot \bar{k}_1 \end{bmatrix} \oplus \begin{bmatrix} \bar{k}_2 \\ k_2 \end{bmatrix}$.

В процесі подальшого двохрозрядного одноопераднoго перетворення $F_{3,10} = \begin{bmatrix} y_1 \\ y_2 \oplus 1 \end{bmatrix}$ над $O_1^{d_7} = \begin{bmatrix} x_1 \cdot \overline{y_1} \oplus x_2 \cdot y_1 \\ x_1 \cdot y_1 \oplus x_2 \cdot \overline{y_1} \end{bmatrix} \oplus \begin{bmatrix} (y_2 \oplus 1) \\ \overline{(y_2 \oplus 1)} \end{bmatrix}$ отримуємо наступне:

$$F_{3,10}(O_1^{d_7}) = \begin{bmatrix} x_1 \cdot \bar{k}_1 \oplus x_2 \cdot k_1 \\ x_1 \cdot k_1 \oplus x_2 \cdot \bar{k}_1 \end{bmatrix} \oplus \begin{bmatrix} k_2 \\ \bar{k}_2 \end{bmatrix} = O_1^k \ .$$

Таким чином в результаті подвійного перетворення $F_{3,10} = \begin{bmatrix} y_1 \\ y_2 \oplus 1 \end{bmatrix}$ з O_1^k отримуємо $O_1^k = \begin{bmatrix} x_1 \cdot \bar{k}_1 \oplus x_2 \cdot k_1 \\ x_1 \cdot k_1 \oplus x_2 \cdot \bar{k}_1 \end{bmatrix} \oplus \begin{bmatrix} k_2 \\ \bar{k}_2 \end{bmatrix}$.

Візьмемо двохрозрядну двохоперандну операцію строгого стійкого криптографічного перетворення такого представлення $O_1^k = \begin{bmatrix} x_1 \cdot \bar{k}_1 \oplus x_2 \cdot k_1 \\ x_1 \cdot k_1 \oplus x_2 \cdot \bar{k}_1 \end{bmatrix} \oplus \begin{bmatrix} k_2 \\ \bar{k}_2 \end{bmatrix}$ та

виконаємо над другим операндом одноопераднe перетворення $F_{6,10}=\begin{bmatrix} y_1 \oplus y_2 \\ y_2 \oplus 1 \end{bmatrix}$,

у якому $(y_1 \oplus y_2)$ – це k_1, а $(y_2 \oplus 1)$ – це k_2.

В результаті даного перетворення отримуємо:

$$F_{6,10}(O_1^k)=\begin{bmatrix} x_1 \cdot \overline{(y_1 \oplus y_2)} \oplus x_2 \cdot (y_1 \oplus y_2) \\ x_1 \cdot (y_1 \oplus y_2) \oplus x_2 \cdot \overline{(y_1 \oplus y_2)} \end{bmatrix} \oplus \begin{bmatrix} (y_2 \oplus 1) \\ \overline{(y_2 \oplus 1)} \end{bmatrix} = O_1^{d_8} .$$

Тобто в результаті перетворення отримуємо операцію $O_1^{d_8}$,що, в свою чергу відповідає $O_9^k=\begin{bmatrix} x_1 \cdot (\overline{k_1 \oplus k_2}) \oplus x_2 \cdot (k_1 \oplus k_2) \\ x_1 \cdot (k_1 \oplus k_2) \oplus x_2 \cdot \overline{(k_1 \oplus k_2)} \end{bmatrix} \oplus \begin{bmatrix} \bar{k}_2 \\ k_2 \end{bmatrix}$.

В процесі подальшого двохрозрядного одноопераднoго перетворення $F_{6,10}=\begin{bmatrix} y_1 \oplus y_2 \\ y_2 \oplus 1 \end{bmatrix}$ над $O_1^{d_8}=\begin{bmatrix} x_1 \cdot \overline{(y_1 \oplus y_2)} \oplus x_2 \cdot (y_1 \oplus y_2) \\ x_1 \cdot (y_1 \oplus y_2) \oplus x_2 \cdot \overline{(y_1 \oplus y_2)} \end{bmatrix} \oplus \begin{bmatrix} (y_2 \oplus 1) \\ \overline{(y_2 \oplus 1)} \end{bmatrix}$ отримуємо наступне:

$$F_{6,5}(O_1^{d_8})= \begin{bmatrix} x_1 \cdot \bar{k}_1 \oplus x_2 \cdot k_1 \\ x_1 \cdot k_1 \oplus x_2 \cdot \bar{k}_1 \end{bmatrix} \oplus \begin{bmatrix} k_2 \\ \bar{k}_2 \end{bmatrix} = O_1^k ,$$

Таким чином в результаті подвійного перетворення $F_{6,10}=\begin{bmatrix} y_1 \oplus y_2 \\ y_2 \oplus 1 \end{bmatrix}$ з O_1^k отримуємо $O_1^k=\begin{bmatrix} x_1 \cdot \bar{k}_1 \oplus x_2 \cdot k_1 \\ x_1 \cdot k_1 \oplus x_2 \cdot \bar{k}_1 \end{bmatrix} \oplus \begin{bmatrix} k_2 \\ \bar{k}_2 \end{bmatrix}$.

Візьмемо двохрозрядну двохоперандну операцію строгого стійкого криптографічного перетворення такого представлення $O_1^k=\begin{bmatrix} x_1 \cdot \bar{k}_1 \oplus x_2 \cdot k_1 \\ x_1 \cdot k_1 \oplus x_2 \cdot \bar{k}_1 \end{bmatrix} \oplus \begin{bmatrix} k_2 \\ \bar{k}_2 \end{bmatrix}$ та виконаємо над другим операндом одноопераднe перетворення $F_{3,9}=\begin{bmatrix} y_1 \\ y_1 \oplus y_2 \oplus 1 \end{bmatrix}$, у якому (y_1) – це k_1, а $(y_1 \oplus y_2 \oplus 1)$ – це k_2.

В результаті даного перетворення отримуємо:

$$F_{3,9}(O_1^k)=\begin{bmatrix} x_1 \cdot \overline{y_1} \oplus x_2 \cdot y_1 \\ x_1 \cdot y_1 \oplus x_2 \cdot \overline{y_1} \end{bmatrix} \oplus \begin{bmatrix} (y_1 \oplus y_2 \oplus 1) \\ \overline{(y_1 \oplus y_2 \oplus 1)} \end{bmatrix} = O_1^{d_9} .$$

Тобто в результаті перетворення отримуємо операцію $O_1^{d_9}$,що, в свою чергу відповідає $O_7^k=\begin{bmatrix} x_1 \cdot \bar{k}_1 \oplus x_2 \cdot k_1 \\ x_1 \cdot k_1 \oplus x_2 \cdot \bar{k}_1 \end{bmatrix} \oplus \begin{bmatrix} \overline{k_1 \oplus k_2} \\ k_1 \oplus k_2 \end{bmatrix}$.

В процесі подальшого двохрозрядного одноопераднього перетворення $F_{3,9}=\begin{bmatrix} y_1 \\ y_1 \oplus y_2 \oplus 1 \end{bmatrix}$ над $O_1^{d_9}=\begin{bmatrix} x_1 \cdot \overline{y_1} \oplus x_2 \cdot y_1 \\ x_1 \cdot y_1 \oplus x_2 \cdot \overline{y_1} \end{bmatrix} \oplus \begin{bmatrix} (y_1 \oplus y_2 \oplus 1) \\ \overline{(y_1 \oplus y_2 \oplus 1)} \end{bmatrix}$ отримуємо наступне:

$$F_{3,9}(O_1^{d_3}) = \begin{bmatrix} x_1 \cdot \bar{k}_1 \oplus x_2 \cdot k_1 \\ x_1 \cdot k_1 \oplus x_2 \cdot \bar{k}_1 \end{bmatrix} \oplus \begin{bmatrix} k_2 \\ \bar{k}_2 \end{bmatrix} = O_1^k \ ,$$

Таким чином в результаті подвійного перетворення $F_{3,9}=\begin{bmatrix} y_1 \\ y_1 \oplus y_2 \oplus 1 \end{bmatrix}$ з O_1^k отримуємо $O_1^k=\begin{bmatrix} x_1 \cdot \bar{k}_1 \oplus x_2 \cdot k_1 \\ x_1 \cdot k_1 \oplus x_2 \cdot \bar{k}_1 \end{bmatrix} \oplus \begin{bmatrix} k_2 \\ \bar{k}_2 \end{bmatrix}$.

Візьмемо двохрозрядну двохоперандну операцію строгого стійкого криптографічного перетворення такого представлення $O_1^k=\begin{bmatrix} x_1 \cdot \bar{k}_1 \oplus x_2 \cdot k_1 \\ x_1 \cdot k_1 \oplus x_2 \cdot \bar{k}_1 \end{bmatrix} \oplus \begin{bmatrix} k_2 \\ \bar{k}_2 \end{bmatrix}$ та виконаємо над другим операндом одноопераднe перетворення $F_{5,12}=\begin{bmatrix} y_2 \\ y_1 \oplus 1 \end{bmatrix}$, у якому (y_2) – це k_1, а $(y_1 \oplus 1)$ – це k_2.

В результаті даного перетворення отримуємо:

$$F_{5,12}(O_1^k)=\begin{bmatrix} x_1 \cdot \overline{y_2} \oplus x_2 \cdot y_2 \\ x_1 \cdot y_2 \oplus x_2 \cdot \overline{y_2} \end{bmatrix} \oplus \begin{bmatrix} (y_1 \oplus 1) \\ \overline{(y_1 \oplus 1)} \end{bmatrix} = O_1^{d_{10}} \ .$$

Тобто в результаті перетворення отримуємо операцію $O_1^{d_{10}}$,що, в свою чергу відповідає $O_{11}^k=\begin{bmatrix} x_1 \cdot \bar{k}_2 \oplus x_2 \cdot k_2 \\ x_1 \cdot k_2 \oplus x_2 \cdot \bar{k}_2 \end{bmatrix} \oplus \begin{bmatrix} \bar{k}_1 \\ k_1 \end{bmatrix}$.

В процесі подальшого двохрозрядного одноопераднього перетворення $F_{5,12}=\begin{bmatrix} y_2 \\ y_1 \oplus 1 \end{bmatrix}$ над $O_1^{d_{10}}=\begin{bmatrix} x_1 \cdot \overline{y_2} \oplus x_2 \cdot y_2 \\ x_1 \cdot y_2 \oplus x_2 \cdot \overline{y_2} \end{bmatrix} \oplus \begin{bmatrix} (y_1 \oplus 1) \\ \overline{(y_1 \oplus 1)} \end{bmatrix}$ отримуємо наступне:

$$F_{5,12}(O_1^{d_{10}}) = \begin{bmatrix} x_1 \cdot \bar{k}_1 \oplus x_2 \cdot k_1 \\ x_1 \cdot k_1 \oplus x_2 \cdot \bar{k}_1 \end{bmatrix} \oplus \begin{bmatrix} k_2 \\ \bar{k}_2 \end{bmatrix} = O_1^k \ ,$$

Таким чином в результаті подвійного перетворення $F_{5,12}=\begin{bmatrix} y_2 \\ y_1 \oplus 1 \end{bmatrix}$ з O_1^k отримуємо $O_1^k=\begin{bmatrix} x_1 \cdot \bar{k}_1 \oplus x_2 \cdot k_1 \\ x_1 \cdot k_1 \oplus x_2 \cdot \bar{k}_1 \end{bmatrix} \oplus \begin{bmatrix} k_2 \\ \bar{k}_2 \end{bmatrix}$.

Візьмемо двохрозрядну двохоперандну операцію строгого стійкого криптографічного перетворення такого представлення $O_1^k = \begin{bmatrix} x_1 \cdot \bar{k}_1 \oplus x_2 \cdot k_1 \\ x_1 \cdot k_1 \oplus x_2 \cdot \bar{k}_1 \end{bmatrix} \oplus \begin{bmatrix} k_2 \\ \bar{k}_2 \end{bmatrix}$ та виконаємо над другим операндом одноопераднде перетворення $F_{5,9} = \begin{bmatrix} y_2 \\ y_1 \oplus y_2 \oplus 1 \end{bmatrix}$, у якому (y_1) – це k_1, а $(y_1 \oplus y_2 \oplus 1)$ – це k_2.

В результаті даного перетворення отримуємо:

$$F_{5,9}(O_1^k) = \begin{bmatrix} x_1 \cdot \overline{y_2} \oplus x_2 \cdot y_2 \\ x_1 \cdot y_2 \oplus x_2 \cdot \overline{y_2} \end{bmatrix} \oplus \begin{bmatrix} (y_1 \oplus y_2 \oplus 1) \\ \overline{(y_1 \oplus y_2 \oplus 1)} \end{bmatrix} = O_1^{d_{11}} .$$

Тобто в результаті перетворення отримуємо операцію $O_1^{d_{11}}$,що, в свою чергу відповідає $O_{10}^k = \begin{bmatrix} x_1 \cdot \bar{k}_2 \oplus x_2 \cdot k_2 \\ x_1 \cdot k_2 \oplus x_2 \cdot \bar{k}_2 \end{bmatrix} \oplus \begin{bmatrix} \bar{k}_2 \\ k_2 \end{bmatrix}$.

В процесі подальшого двохрозрядного одноопераднде перетворення $F_{5,9} = \begin{bmatrix} y_2 \\ y_1 \oplus y_2 \oplus 1 \end{bmatrix}$ над $O_1^{d_{11}} = \begin{bmatrix} x_1 \cdot \overline{y_2} \oplus x_2 \cdot y_2 \\ x_1 \cdot y_2 \oplus x_2 \cdot \overline{y_2} \end{bmatrix} \oplus \begin{bmatrix} (y_1 \oplus y_2 \oplus 1) \\ \overline{(y_1 \oplus y_2 \oplus 1)} \end{bmatrix}$ отримуємо наступне:

$$F_{5,9}(O_1^{d_3}) = \begin{bmatrix} x_1 \cdot \bar{k}_1 \oplus x_2 \cdot k_1 \\ x_1 \cdot k_1 \oplus x_2 \cdot \bar{k}_1 \end{bmatrix} \oplus \begin{bmatrix} k_2 \\ \bar{k}_2 \end{bmatrix} = O_1^k ,$$

Таким чином в результаті подвійного перетворення $F_{5,9} = \begin{bmatrix} y_2 \\ y_1 \oplus y_2 \oplus 1 \end{bmatrix}$ з O_1^k отримуємо $O_1^k = \begin{bmatrix} x_1 \cdot \bar{k}_1 \oplus x_2 \cdot k_1 \\ x_1 \cdot k_1 \oplus x_2 \cdot \bar{k}_1 \end{bmatrix} \oplus \begin{bmatrix} k_2 \\ \bar{k}_2 \end{bmatrix}$.

Візьмемо двохрозрядну двохоперандну операцію строгого стійкого криптографічного перетворення такого представлення $O_1^k = \begin{bmatrix} x_1 \cdot \bar{k}_1 \oplus x_2 \cdot k_1 \\ x_1 \cdot k_1 \oplus x_2 \cdot \bar{k}_1 \end{bmatrix} \oplus \begin{bmatrix} k_2 \\ \bar{k}_2 \end{bmatrix}$ та виконаємо над другим операндом одноопераднде перетворення $F_{6,12} = \begin{bmatrix} y_1 \oplus y_2 \\ y_1 \oplus 1 \end{bmatrix}$, у якому $(y_1 \oplus y_2)$ – це k_1, а $(y_1 \oplus 1)$ – це k_2.

В результаті даного перетворення отримуємо:

$$F_{6,12}(O_1^k) = \begin{bmatrix} x_1 \cdot \overline{(y_1 \oplus y_2)} \oplus x_2 \cdot (y_1 \oplus y_2) \\ x_1 \cdot (y_1 \oplus y_2) \oplus x_2 \cdot \overline{(y_1 \oplus y_2)} \end{bmatrix} \oplus \begin{bmatrix} (y_1 \oplus 1) \\ \overline{(y_1 \oplus 1)} \end{bmatrix} = O_1^{d_{12}} .$$

Тобто в результаті перетворення отримуємо операцію $O_1^{d_{12}}$,що, в свою чергу відповідає $O_{12}^k = \begin{bmatrix} x_1 \cdot (\overline{k_1 \oplus k_2}) \oplus x_2 \cdot (k_1 \oplus k_2) \\ x_1 \cdot (k_1 \oplus k_2) \oplus x_2 \cdot (\overline{k_1 \oplus k_2}) \end{bmatrix} \oplus \begin{bmatrix} \bar{k}_1 \\ k_1 \end{bmatrix}$.

В процесі подальшого двохрозрядного одноопераднього перетворення $F_{6,12} = \begin{bmatrix} y_1 \oplus y_2 \\ y_1 \oplus 1 \end{bmatrix}$ над $O_1^{d_{12}} = \begin{bmatrix} x_1 \cdot \overline{(y_1 \oplus y_2)} \oplus x_2 \cdot (y_1 \oplus y_2) \\ x_1 \cdot (y_1 \oplus y_2) \oplus x_2 \cdot \overline{(y_1 \oplus y_2)} \end{bmatrix} \oplus \begin{bmatrix} (y_1 \oplus 1) \\ \overline{(y_1 \oplus 1)} \end{bmatrix}$ отримуємо наступне:

$$F_{6,12}(O_1^{d_{12}}) = \begin{bmatrix} x_1 \cdot \bar{k}_1 \oplus x_2 \cdot k_1 \\ x_1 \cdot k_1 \oplus x_2 \cdot \bar{k}_1 \end{bmatrix} \oplus \begin{bmatrix} k_2 \\ \bar{k}_2 \end{bmatrix} = O_1^k \ ,$$

Таким чином в результаті подвійного перетворення $F_{6,12} = \begin{bmatrix} y_1 \oplus y_2 \\ y_1 \oplus 1 \end{bmatrix}$ з O_1^k отримуємо $O_1^k = \begin{bmatrix} x_1 \cdot \bar{k}_1 \oplus x_2 \cdot k_1 \\ x_1 \cdot k_1 \oplus x_2 \cdot \bar{k}_1 \end{bmatrix} \oplus \begin{bmatrix} k_2 \\ \bar{k}_2 \end{bmatrix}$.

Візьмемо двохрозрядну двохоперандну операцію строгого стійкого криптографічного перетворення такого представлення $O_1^k = \begin{bmatrix} x_1 \cdot \bar{k}_1 \oplus x_2 \cdot k_1 \\ x_1 \cdot k_1 \oplus x_2 \cdot \bar{k}_1 \end{bmatrix} \oplus \begin{bmatrix} k_2 \\ \bar{k}_2 \end{bmatrix}$ та виконаємо над другим операндом одноопераднe перетворення $F_{12,5} = \begin{bmatrix} y_1 \oplus 1 \\ y_2 \end{bmatrix}$, у якому $(y_1 \oplus 1)$ – це k_1, а (y_2) – це k_2.

В результаті даного перетворення отримуємо:

$$F_{12,5}(O_1^k) = \begin{bmatrix} x_1 \cdot \overline{(y_1 \oplus 1)} \oplus x_2 \cdot (y_1 \oplus 1) \\ x_1 \cdot (y_1 \oplus 1) \oplus x_2 \cdot \overline{(y_1 \oplus 1)} \end{bmatrix} \oplus \begin{bmatrix} y_2 \\ \overline{y_2} \end{bmatrix} = O_1^{d_{13}} \ .$$

Тобто в результаті перетворення отримуємо операцію $O_1^{d_{13}}$,що, в свою чергу відповідає $O_{18}^k = \begin{bmatrix} x_1 \cdot k_1 \oplus x_2 \cdot \bar{k}_1 \\ x_1 \cdot \bar{k}_1 \oplus x_2 \cdot k_1 \end{bmatrix} \oplus \begin{bmatrix} k_2 \\ \bar{k}_2 \end{bmatrix}$.

В процесі подальшого двохрозрядного одноопераднього перетворення $F_{12,5} = \begin{bmatrix} y_1 \oplus 1 \\ y_2 \end{bmatrix}$ над $O_1^{d_{13}} = \begin{bmatrix} x_1 \cdot \overline{(y_1 \oplus 1)} \oplus x_2 \cdot (y_1 \oplus 1) \\ x_1 \cdot (y_1 \oplus 1) \oplus x_2 \cdot \overline{(y_1 \oplus 1)} \end{bmatrix} \oplus \begin{bmatrix} y_2 \\ \overline{y_2} \end{bmatrix}$ отримуємо наступне:

$$F_{12,5}(O_1^{d_{13}}) = \begin{bmatrix} x_1 \cdot \bar{k}_1 \oplus x_2 \cdot k_1 \\ x_1 \cdot k_1 \oplus x_2 \cdot \bar{k}_1 \end{bmatrix} \oplus \begin{bmatrix} k_2 \\ \bar{k}_2 \end{bmatrix} = O_1^k \ ,$$

Таким чином в результаті подвійного перетворення $F_{12,5}=\begin{bmatrix} y_1 \oplus 1 \\ y_2 \end{bmatrix}$ з O_1^k отримуємо $O_1^k=\begin{bmatrix} x_1 \cdot \bar{k}_1 \oplus x_2 \cdot k_1 \\ x_1 \cdot k_1 \oplus x_2 \cdot \bar{k}_1 \end{bmatrix} \oplus \begin{bmatrix} k_2 \\ \bar{k}_2 \end{bmatrix}$.

Візьмемо двохрозрядну двохоперандну операцію строгого стійкого криптографічного перетворення такого представлення $O_1^k=\begin{bmatrix} x_1 \cdot \bar{k}_1 \oplus x_2 \cdot k_1 \\ x_1 \cdot k_1 \oplus x_2 \cdot \bar{k}_1 \end{bmatrix} \oplus \begin{bmatrix} k_2 \\ \bar{k}_2 \end{bmatrix}$ та виконаємо над другим операндом одноопераднe перетворення $F_{9,5}=\begin{bmatrix} y_1 \oplus y_2 \oplus 1 \\ y_2 \end{bmatrix}$, у якому $(y_1 \oplus y_2 \oplus 1)$ – це k_1, а (y_2) – це k_2.

В результаті даного перетворення отримуємо:

$$F_{9,5}(O_1^k)=\begin{bmatrix} x_1 \cdot \overline{(y_1 \oplus y_2 \oplus 1)} \oplus x_2 \cdot (y_1 \oplus y_2 \oplus 1) \\ x_1 \cdot (y_1 \oplus y_2 \oplus 1) \oplus x_2 \cdot \overline{(y_1 \oplus y_2 \oplus 1)} \end{bmatrix} \oplus \begin{bmatrix} y_2 \\ \overline{y_2} \end{bmatrix} = O_1^{d_{14}} .$$

Тобто в результаті перетворення отримуємо операцію $O_1^{d_{14}}$,що, в свою чергу відповідає $O_{13}^k=\begin{bmatrix} x_1 \cdot (k_1 \oplus k_2) \oplus x_2 \cdot \overline{(k_1 \oplus k_2)} \\ x_1 \cdot \overline{(k_1 \oplus k_2)} \oplus x_2 \cdot (k_1 \oplus k_2) \end{bmatrix} \oplus \begin{bmatrix} k_2 \\ \bar{k}_2 \end{bmatrix}$.

В процесі подальшого двохрозрядного одноопераднoго перетворення $F_{9,5}=\begin{bmatrix} y_1 \oplus y_2 \oplus 1 \\ y_2 \end{bmatrix}$ над $O_1^{d_{14}}=\begin{bmatrix} x_1 \cdot \overline{(y_1 \oplus y_2 \oplus 1)} \oplus x_2 \cdot (y_1 \oplus y_2 \oplus 1) \\ x_1 \cdot (y_1 \oplus y_2 \oplus 1) \oplus x_2 \cdot \overline{(y_1 \oplus y_2 \oplus 1)} \end{bmatrix} \oplus \begin{bmatrix} y_2 \\ \overline{y_2} \end{bmatrix}$ отримуємо наступне:

$$F_{6,5}(O_1^{d_3}) = \begin{bmatrix} x_1 \cdot \bar{k}_1 \oplus x_2 \cdot k_1 \\ x_1 \cdot k_1 \oplus x_2 \cdot \bar{k}_1 \end{bmatrix} \oplus \begin{bmatrix} k_2 \\ \bar{k}_2 \end{bmatrix} = O_1^k ,$$

Таким чином в результаті подвійного перетворення $F_{9,5}=\begin{bmatrix} y_1 \oplus y_2 \oplus 1 \\ y_2 \end{bmatrix}$ з O_1^k отримуємо $O_1^k=\begin{bmatrix} x_1 \cdot \bar{k}_1 \oplus x_2 \cdot k_1 \\ x_1 \cdot k_1 \oplus x_2 \cdot \bar{k}_1 \end{bmatrix} \oplus \begin{bmatrix} k_2 \\ \bar{k}_2 \end{bmatrix}$.

Візьмемо двохрозрядну двохоперандну операцію строгого стійкого криптографічного перетворення такого представлення $O_1^k=\begin{bmatrix} x_1 \cdot \bar{k}_1 \oplus x_2 \cdot k_1 \\ x_1 \cdot k_1 \oplus x_2 \cdot \bar{k}_1 \end{bmatrix} \oplus \begin{bmatrix} k_2 \\ \bar{k}_2 \end{bmatrix}$ та виконаємо над другим операндом одноопераднe перетворення $F_{12,6}=\begin{bmatrix} y_1 \oplus 1 \\ y_1 \oplus y_2 \end{bmatrix}$, у якому $(y_1 \oplus 1)$ – це k_1, а $(y_1 \oplus y_2)$ – це k_2.

В результаті даного перетворення отримуємо:

$$F_{12,6}(O_1^k)=\begin{bmatrix} x_1\cdot\overline{(y_1\oplus 1)}\oplus x_2\cdot(y_1\oplus 1) \\ x_1\cdot(y_1\oplus 1)\oplus x_2\cdot\overline{(y_1\oplus 1)}\end{bmatrix}\oplus\begin{bmatrix}(y_1\oplus y_2)\\ \overline{(y_1\oplus y_2)}\end{bmatrix}=O_1^{d_{15}}\ .$$

Тобто в результаті перетворення отримуємо операцію $O_1^{d_{15}}$,що, в свою чергу відповідає $O_{17}^k=\begin{bmatrix} x_1\cdot k_1\oplus x_2\cdot\bar{k}_1 \\ x_1\cdot\bar{k}_1\oplus x_2\cdot k_1\end{bmatrix}\oplus\begin{bmatrix}k_1\oplus k_2\\ \overline{k_1\oplus k_2}\end{bmatrix}$.

В процесі подальшого двохрозрядного одноопераднього перетворення $F_{12,6}=\begin{bmatrix}y_1\oplus 1\\ y_1\oplus y_2\end{bmatrix}$ над $O_1^{d_{15}}=\begin{bmatrix} x_1\cdot\overline{(y_1\oplus 1)}\oplus x_2\cdot(y_1\oplus 1) \\ x_1\cdot(y_1\oplus 1)\oplus x_2\cdot\overline{(y_1\oplus 1)}\end{bmatrix}\oplus\begin{bmatrix}(y_1\oplus y_2)\\ \overline{(y_1\oplus y_2)}\end{bmatrix}$ отримуємо наступне:

$$F_{12,6}(O_1^{d_3})=\begin{bmatrix} x_1\cdot\bar{k}_1\oplus x_2\cdot k_1 \\ x_1\cdot k_1\oplus x_2\cdot\bar{k}_1\end{bmatrix}\oplus\begin{bmatrix}k_2\\ \bar{k}_2\end{bmatrix}=O_1^k\ ,$$

Таким чином в результаті подвійного перетворення $F_{12,6}=\begin{bmatrix}y_1\oplus 1\\ y_1\oplus y_2\end{bmatrix}$ з O_1^k отримуємо $O_1^k=\begin{bmatrix} x_1\cdot\bar{k}_1\oplus x_2\cdot k_1 \\ x_1\cdot k_1\oplus x_2\cdot\bar{k}_1\end{bmatrix}\oplus\begin{bmatrix}k_2\\ \bar{k}_2\end{bmatrix}$.

Візьмемо двохрозрядну двохоперандну операцію строгого стійкого криптографічного перетворення такого представлення $O_1^k=\begin{bmatrix} x_1\cdot\bar{k}_1\oplus x_2\cdot k_1 \\ x_1\cdot k_1\oplus x_2\cdot\bar{k}_1\end{bmatrix}\oplus\begin{bmatrix}k_2\\ \bar{k}_2\end{bmatrix}$ та виконаємо над другим операндом одноопераднe перетворення $F_{10,3}=\begin{bmatrix}y_2\oplus 1\\ y_1\end{bmatrix}$, у якому $(y_2\oplus 1)$ – це k_1, а (y_1) – це k_2.

В результаті даного перетворення отримуємо:

$$F_{10,3}(O_1^k)=\begin{bmatrix} x_1\cdot\overline{(y_2\oplus 1)}\oplus x_2\cdot(y_2\oplus 1) \\ x_1\cdot(y_2\oplus 1)\oplus x_2\cdot\overline{(y_2\oplus 1)}\end{bmatrix}\oplus\begin{bmatrix}y_1\\ \overline{y_1}\end{bmatrix}=O_1^{d_{16}}\ .$$

Тобто в результаті перетворення отримуємо операцію $O_1^{d_{16}}$,що, в свою чергу відповідає $O_{15}^k=\begin{bmatrix} x_1\cdot k_2\oplus x_2\cdot\bar{k}_2 \\ x_1\cdot\bar{k}_2\oplus x_2\cdot k_2\end{bmatrix}\oplus\begin{bmatrix}k_1\\ \bar{k}_1\end{bmatrix}$.

В процесі подальшого двохрозрядного одноопераднього перетворення $F_{10,3}=\begin{bmatrix}y_2\oplus 1\\ y_1\end{bmatrix}$ над $O_1^{d_{16}}=\begin{bmatrix} x_1\cdot\overline{(y_2\oplus 1)}\oplus x_2\cdot(y_2\oplus 1) \\ x_1\cdot(y_2\oplus 1)\oplus x_2\cdot\overline{(y_2\oplus 1)}\end{bmatrix}\oplus\begin{bmatrix}y_1\\ \overline{y_1}\end{bmatrix}$ отримуємо наступне:

$$F_{10,3}(O_1^{d_{16}}) = \begin{bmatrix} x_1 \cdot \bar{k}_1 \oplus x_2 \cdot k_1 \\ x_1 \cdot k_1 \oplus x_2 \cdot \bar{k}_1 \end{bmatrix} \oplus \begin{bmatrix} k_2 \\ \bar{k}_2 \end{bmatrix} = O_1^k ,$$

Таким чином в результаті подвійного перетворення $F_{10,3} = \begin{bmatrix} y_2 \oplus 1 \\ y_1 \end{bmatrix}$ з O_1^k отримуємо $O_1^k = \begin{bmatrix} x_1 \cdot \bar{k}_1 \oplus x_2 \cdot k_1 \\ x_1 \cdot k_1 \oplus x_2 \cdot \bar{k}_1 \end{bmatrix} \oplus \begin{bmatrix} k_2 \\ \bar{k}_2 \end{bmatrix}$.

Візьмемо двохрозрядну двохоперандну операцію строгого стійкого криптографічного перетворення такого представлення $O_1^k = \begin{bmatrix} x_1 \cdot \bar{k}_1 \oplus x_2 \cdot k_1 \\ x_1 \cdot k_1 \oplus x_2 \cdot \bar{k}_1 \end{bmatrix} \oplus \begin{bmatrix} k_2 \\ \bar{k}_2 \end{bmatrix}$ та виконаємо над другим операндом одноопераднe перетворення $F_{10,6} = \begin{bmatrix} y_2 \oplus 1 \\ y_1 \oplus y_2 \end{bmatrix}$, у якому $(y_2 \oplus 1)$ – це k_1, а $(y_1 \oplus y_2)$ – це k_2.

В результаті даного перетворення отримуємо:

$$F_{10,6}(O_1^k) = \begin{bmatrix} x_1 \cdot \overline{(y_2 \oplus 1)} \oplus x_2 \cdot (y_2 \oplus 1) \\ x_1 \cdot (y_2 \oplus 1) \oplus x_2 \cdot \overline{(y_2 \oplus 1)} \end{bmatrix} \oplus \begin{bmatrix} (y_1 \oplus y_2) \\ \overline{(y_1 \oplus y_2)} \end{bmatrix} = O_1^{d_{17}} .$$

Тобто в результаті перетворення отримуємо операцію $O_1^{d_{17}}$,що, в свою чергу відповідає $O_{14}^k = \begin{bmatrix} x_1 \cdot k_2 \oplus x_2 \cdot \bar{k}_2 \\ x_1 \cdot \bar{k}_2 \oplus x_2 \cdot k_2 \end{bmatrix} \oplus \begin{bmatrix} k_2 \\ \bar{k}_2 \end{bmatrix}$.

В процесі подальшого двохрозрядного одноопераднoго перетворення $F_{10,6} = \begin{bmatrix} y_2 \oplus 1 \\ y_1 \oplus y_2 \end{bmatrix}$ над $O_1^{d_{17}} = \begin{bmatrix} x_1 \cdot \overline{(y_2 \oplus 1)} \oplus x_2 \cdot (y_2 \oplus 1) \\ x_1 \cdot (y_2 \oplus 1) \oplus x_2 \cdot \overline{(y_2 \oplus 1)} \end{bmatrix} \oplus \begin{bmatrix} (y_1 \oplus y_2) \\ \overline{(y_1 \oplus y_2)} \end{bmatrix}$ отримуємо наступне:

$$F_{10,6}(O_1^{d_{17}}) = \begin{bmatrix} x_1 \cdot \bar{k}_1 \oplus x_2 \cdot k_1 \\ x_1 \cdot k_1 \oplus x_2 \cdot \bar{k}_1 \end{bmatrix} \oplus \begin{bmatrix} k_2 \\ \bar{k}_2 \end{bmatrix} = O_1^k ,$$

Таким чином в результаті подвійного перетворення $F_{10,6} = \begin{bmatrix} y_2 \oplus 1 \\ y_1 \oplus y_2 \end{bmatrix}$ з O_1^k отримуємо $O_1^k = \begin{bmatrix} x_1 \cdot \bar{k}_1 \oplus x_2 \cdot k_1 \\ x_1 \cdot k_1 \oplus x_2 \cdot \bar{k}_1 \end{bmatrix} \oplus \begin{bmatrix} k_2 \\ \bar{k}_2 \end{bmatrix}$.

Візьмемо двохрозрядну двохоперандну операцію строгого стійкого криптографічного перетворення такого представлення $O_1^k = \begin{bmatrix} x_1 \cdot \bar{k}_1 \oplus x_2 \cdot k_1 \\ x_1 \cdot k_1 \oplus x_2 \cdot \bar{k}_1 \end{bmatrix} \oplus \begin{bmatrix} k_2 \\ \bar{k}_2 \end{bmatrix}$ та

виконаємо над другим операндом одноопераднe перетворення $F_{9,3}=\begin{bmatrix} y_1 \oplus y_2 \oplus 1 \\ y_1 \end{bmatrix}$,

у якому $(y_1 \oplus y_2 \oplus 1)$ – це k_1, а (y_1) – це k_2.

В результаті даного перетворення отримуємо:

$$F_{9,3}(O_1^k)=\begin{bmatrix} x_1 \cdot \overline{(y_1 \oplus y_2 \oplus 1)} \oplus x_2 \cdot (y_1 \oplus y_2 \oplus 1) \\ x_1 \cdot (y_1 \oplus y_2 \oplus 1) \oplus x_2 \cdot \overline{(y_1 \oplus y_2 \oplus 1)} \end{bmatrix} \oplus \begin{bmatrix} y_1 \\ \overline{y_1} \end{bmatrix} = O_1^{d_{18}}.$$

Тобто в результаті перетворення отримуємо операцію $O_1^{d_{18}}$,що, в свою чергу відповідає $O_{16}^k=\begin{bmatrix} x_1 \cdot (k_1 \oplus k_2) \oplus x_2 \cdot \overline{(k_1 \oplus k_2)} \\ x_1 \cdot \overline{(k_1 \oplus k_2)} \oplus x_2 \cdot (k_1 \oplus k_2) \end{bmatrix} \oplus \begin{bmatrix} k_1 \\ \bar{k}_1 \end{bmatrix}$.

В процесі подальшого двохрозрядного одноопераднoго перетворення $F_{9,3}=\begin{bmatrix} y_1 \oplus y_2 \oplus 1 \\ y_1 \end{bmatrix}$ над $O_1^{d_{18}}=\begin{bmatrix} x_1 \cdot \overline{(y_1 \oplus y_2 \oplus 1)} \oplus x_2 \cdot (y_1 \oplus y_2 \oplus 1) \\ x_1 \cdot (y_1 \oplus y_2 \oplus 1) \oplus x_2 \cdot \overline{(y_1 \oplus y_2 \oplus 1)} \end{bmatrix} \oplus \begin{bmatrix} y_1 \\ \overline{y_1} \end{bmatrix}$ отримуємо наступне:

$$F_{9,3}(O_1^{d_{18}})= \begin{bmatrix} x_1 \cdot \bar{k}_1 \oplus x_2 \cdot k_1 \\ x_1 \cdot k_1 \oplus x_2 \cdot \bar{k}_1 \end{bmatrix} \oplus \begin{bmatrix} k_2 \\ \bar{k}_2 \end{bmatrix} = O_1^k,$$

Таким чином в результаті подвійного перетворення $F_{9,3}=\begin{bmatrix} y_1 \oplus y_2 \oplus 1 \\ y_1 \end{bmatrix}$ з O_1^k отримуємо $O_1^k=\begin{bmatrix} x_1 \cdot \bar{k}_1 \oplus x_2 \cdot k_1 \\ x_1 \cdot k_1 \oplus x_2 \cdot \bar{k}_1 \end{bmatrix} \oplus \begin{bmatrix} k_2 \\ \bar{k}_2 \end{bmatrix}$.

Візьмемо двохрозрядну двохоперандну операцію строгого стійкого криптографічного перетворення такого представлення $O_1^k=\begin{bmatrix} x_1 \cdot \bar{k}_1 \oplus x_2 \cdot k_1 \\ x_1 \cdot k_1 \oplus x_2 \cdot \bar{k}_1 \end{bmatrix} \oplus \begin{bmatrix} k_2 \\ \bar{k}_2 \end{bmatrix}$ та виконаємо над другим операндом одноопераднe перетворення $F_{12,10}=\begin{bmatrix} y_1 \oplus 1 \\ y_2 \oplus 1 \end{bmatrix}$,

у якому $(y_1 \oplus 1)$ – це k_1, а $(y_2 \oplus 1)$ – це k_2.

В результаті даного перетворення отримуємо:

$$F_{12,10}(O_1^k)=\begin{bmatrix} x_1 \cdot \overline{(y_1 \oplus 1)} \oplus x_2 \cdot (y_1 \oplus 1) \\ x_1 \cdot (y_1 \oplus 1) \oplus x_2 \cdot \overline{(y_1 \oplus 1)} \end{bmatrix} \oplus \begin{bmatrix} (y_2 \oplus 1) \\ \overline{(y_2 \oplus 1)} \end{bmatrix} = O_1^{d_{19}}.$$

Тобто в результаті перетворення отримуємо операцію $O_1^{d_{19}}$,що, в свою чергу відповідає $O_{22}^k=\begin{bmatrix} x_1 \cdot k_1 \oplus x_2 \cdot \bar{k}_1 \\ x_1 \cdot \bar{k}_1 \oplus x_2 \cdot k_1 \end{bmatrix} \oplus \begin{bmatrix} \bar{k}_2 \\ k_2 \end{bmatrix}$.

В процесі подальшого двохрозрядного одноопераднього перетворення $F_{12,10}=\begin{bmatrix} y_1 \oplus 1 \\ y_2 \oplus 1 \end{bmatrix}$ над $O_1^{d_{19}}=\begin{bmatrix} x_1 \cdot \overline{(y_1 \oplus 1)} \oplus x_2 \cdot (y_1 \oplus 1) \\ x_1 \cdot (y_1 \oplus 1) \oplus x_2 \cdot \overline{(y_1 \oplus 1)} \end{bmatrix} \oplus \begin{bmatrix} (y_2 \oplus 1) \\ \overline{(y_2 \oplus 1)} \end{bmatrix}$ отримуємо наступне:

$$F_{12,10}(O_1^{d_{19}})=\begin{bmatrix} x_1 \cdot \bar{k}_1 \oplus x_2 \cdot k_1 \\ x_1 \cdot k_1 \oplus x_2 \cdot \bar{k}_1 \end{bmatrix} \oplus \begin{bmatrix} k_2 \\ \bar{k}_2 \end{bmatrix} = O_1^k \ ,$$

Таким чином в результаті подвійного перетворення $F_{12,10}=\begin{bmatrix} y_1 \oplus 1 \\ y_2 \oplus 1 \end{bmatrix}$ з O_1^k отримуємо $O_1^k=\begin{bmatrix} x_1 \cdot \bar{k}_1 \oplus x_2 \cdot k_1 \\ x_1 \cdot k_1 \oplus x_2 \cdot \bar{k}_1 \end{bmatrix} \oplus \begin{bmatrix} k_2 \\ \bar{k}_2 \end{bmatrix}$.

Візьмемо двохрозрядну двохоперандну операцію строгого стійкого криптографічного перетворення такого представлення $O_1^k=\begin{bmatrix} x_1 \cdot \bar{k}_1 \oplus x_2 \cdot k_1 \\ x_1 \cdot k_1 \oplus x_2 \cdot \bar{k}_1 \end{bmatrix} \oplus \begin{bmatrix} k_2 \\ \bar{k}_2 \end{bmatrix}$ та виконаємо над другим операндом одноопераднe перетворення $F_{9,10}=\begin{bmatrix} y_1 \oplus y_2 \oplus 1 \\ y_2 \oplus 1 \end{bmatrix}$, у якому $(y_1 \oplus y_2 \oplus 1)$ – це k_1, а $(y_2 \oplus 1)$ – це k_2.

В результаті даного перетворення отримуємо:

$$F_{9,10}(O_1^k)=\begin{bmatrix} x_1 \cdot \overline{(y_1 \oplus y_2 \oplus 1)} \oplus x_2 \cdot (y_1 \oplus y_2 \oplus 1) \\ x_1 \cdot (y_1 \oplus y_2 \oplus 1) \oplus x_2 \cdot \overline{(y_1 \oplus y_2 \oplus 1)} \end{bmatrix} \oplus \begin{bmatrix} (y_2 \oplus 1) \\ \overline{(y_2 \oplus 1)} \end{bmatrix} = O_1^{d_{20}} \ .$$

Тобто в результаті перетворення отримуємо операцію $O_1^{d_{20}}$,що, в свою чергу відповідає $O_{23}^k=\begin{bmatrix} x_1 \cdot (k_1 \oplus k_2) \oplus x_2 \cdot \overline{(k_1 \oplus k_2)} \\ x_1 \cdot \overline{(k_1 \oplus k_2)} \oplus x_2 \cdot (k_1 \oplus k_2) \end{bmatrix} \oplus \begin{bmatrix} \bar{k}_2 \\ k_2 \end{bmatrix}$.

В процесі подальшого двохрозрядного одноопераднього перетворення $F_{9,10}=\begin{bmatrix} y_1 \oplus y_2 \oplus 1 \\ y_2 \oplus 1 \end{bmatrix}$ над $O_1^{d_{20}}=\begin{bmatrix} x_1 \cdot \overline{(y_1 \oplus y_2 \oplus 1)} \oplus x_2 \cdot (y_1 \oplus y_2 \oplus 1) \\ x_1 \cdot (y_1 \oplus y_2 \oplus 1) \oplus x_2 \cdot \overline{(y_1 \oplus y_2 \oplus 1)} \end{bmatrix} \oplus \begin{bmatrix} (y_2 \oplus 1) \\ \overline{(y_2 \oplus 1)} \end{bmatrix}$ отримуємо наступне:

$$F_{9,10}(O_1^{d_{20}})=\begin{bmatrix} x_1 \cdot \bar{k}_1 \oplus x_2 \cdot k_1 \\ x_1 \cdot k_1 \oplus x_2 \cdot \bar{k}_1 \end{bmatrix} \oplus \begin{bmatrix} k_2 \\ \bar{k}_2 \end{bmatrix} = O_1^k \ .$$

Таким чином в результаті подвійного перетворення $F_{9,10}=\begin{bmatrix} y_1 \oplus y_2 \oplus 1 \\ y_2 \oplus 1 \end{bmatrix}$ з O_1^k отримуємо $O_1^k=\begin{bmatrix} x_1 \cdot \bar{k}_1 \oplus x_2 \cdot k_1 \\ x_1 \cdot k_1 \oplus x_2 \cdot \bar{k}_1 \end{bmatrix} \oplus \begin{bmatrix} k_2 \\ \bar{k}_2 \end{bmatrix}$.

Візьмемо двохрозрядну двохоперандну операцію строгого стійкого криптографічного перетворення такого представлення $O_1^k = \begin{bmatrix} x_1 \cdot \bar{k}_1 \oplus x_2 \cdot k_1 \\ x_1 \cdot k_1 \oplus x_2 \cdot \bar{k}_1 \end{bmatrix} \oplus \begin{bmatrix} k_2 \\ \bar{k}_2 \end{bmatrix}$ та виконаємо над другим операндом одноопераднe перетворення $F_{12,9} = \begin{bmatrix} y_1 \oplus 1 \\ y_1 \oplus y_2 \oplus 1 \end{bmatrix}$, у якому $(y_1 \oplus 1)$ – це k_1, а $(y_1 \oplus y_2 \oplus 1)$ – це k_2.

В результаті даного перетворення отримуємо:

$$F_{12,9}(O_1^k) = \begin{bmatrix} x_1 \cdot \overline{(y_1 \oplus 1)} \oplus x_2 \cdot (y_1 \oplus 1) \\ x_1 \cdot (y_1 \oplus 1) \oplus x_2 \cdot \overline{(y_1 \oplus 1)} \end{bmatrix} \oplus \begin{bmatrix} (y_1 \oplus y_2 \oplus 1) \\ \overline{(y_1 \oplus y_2 \oplus 1)} \end{bmatrix} = O_1^{d_{21}}.$$

Тобто в результаті перетворення отримуємо операцію $O_1^{d_3}$,що, в свою чергу відповідає $O_{21}^k = \begin{bmatrix} x_1 \cdot k_1 \oplus x_2 \cdot \bar{k}_1 \\ x_1 \cdot \bar{k}_1 \oplus x_2 \cdot k_1 \end{bmatrix} \oplus \begin{bmatrix} \overline{k_1 \oplus k_2} \\ k_1 \oplus k_2 \end{bmatrix}$.

В процесі подальшого двохрозрядного одноопераднoго перетворення $F_{12,9} = \begin{bmatrix} y_1 \oplus 1 \\ y_1 \oplus y_2 \oplus 1 \end{bmatrix}$ над $O_1^{d_{21}} = \begin{bmatrix} x_1 \cdot \overline{(y_1 \oplus 1)} \oplus x_2 \cdot (y_1 \oplus 1) \\ x_1 \cdot (y_1 \oplus 1) \oplus x_2 \cdot \overline{(y_1 \oplus 1)} \end{bmatrix} \oplus \begin{bmatrix} (y_1 \oplus y_2 \oplus 1) \\ \overline{(y_1 \oplus y_2 \oplus 1)} \end{bmatrix}$ отримуємо наступне:

$$F_{12,9}(O_1^{d_{21}}) = \begin{bmatrix} x_1 \cdot \bar{k}_1 \oplus x_2 \cdot k_1 \\ x_1 \cdot k_1 \oplus x_2 \cdot \bar{k}_1 \end{bmatrix} \oplus \begin{bmatrix} k_2 \\ \bar{k}_2 \end{bmatrix} = O_1^k,$$

Таким чином в результаті подвійного перетворення $F_{12,9} = \begin{bmatrix} y_1 \oplus 1 \\ y_1 \oplus y_2 \oplus 1 \end{bmatrix}$ з O_1^k отримуємо $O_1^k = \begin{bmatrix} x_1 \cdot \bar{k}_1 \oplus x_2 \cdot k_1 \\ x_1 \cdot k_1 \oplus x_2 \cdot \bar{k}_1 \end{bmatrix} \oplus \begin{bmatrix} k_2 \\ \bar{k}_2 \end{bmatrix}$.

Візьмемо двохрозрядну двохоперандну операцію строгого стійкого криптографічного перетворення такого представлення $O_1^k = \begin{bmatrix} x_1 \cdot \bar{k}_1 \oplus x_2 \cdot k_1 \\ x_1 \cdot k_1 \oplus x_2 \cdot \bar{k}_1 \end{bmatrix} \oplus \begin{bmatrix} k_2 \\ \bar{k}_2 \end{bmatrix}$ та виконаємо над другим операндом одноопераднe перетворення $F_{10,12} = \begin{bmatrix} y_2 \oplus 1 \\ y_1 \oplus 1 \end{bmatrix}$, у якому $(y_2 \oplus 1)$ – це k_1, а $(y_1 \oplus 1)$ – це k_2.

В результаті даного перетворення отримуємо:

$$F_{10,12}(O_1^k) = \begin{bmatrix} x_1 \cdot \overline{(y_2 \oplus 1)} \oplus x_2 \cdot (y_2 \oplus 1) \\ x_1 \cdot (y_2 \oplus 1) \oplus x_2 \cdot \overline{(y_2 \oplus 1)} \end{bmatrix} \oplus \begin{bmatrix} (y_1 \oplus 1) \\ \overline{(y_1 \oplus 1)} \end{bmatrix} = O_1^{d_{22}}.$$

Тобто в результаті перетворення отримуємо операцію $O_1^{d_{22}}$,що, в свою чергу відповідає $O_{19}^k = \begin{bmatrix} x_1 \cdot \bar{k}_2 \oplus x_2 \cdot k_2 \\ x_1 \cdot k_2 \oplus x_2 \cdot \bar{k}_2 \end{bmatrix} \oplus \begin{bmatrix} k_1 \\ \bar{k}_1 \end{bmatrix}$.

В процесі подальшого двохрозрядного одноопераднього перетворення $F_{10,12} = \begin{bmatrix} y_2 \oplus 1 \\ y_1 \oplus 1 \end{bmatrix}$ над $O_1^{d_{22}} = \begin{bmatrix} x_1 \cdot \overline{(y_2 \oplus 1)} \oplus x_2 \cdot (y_2 \oplus 1) \\ x_1 \cdot (y_2 \oplus 1) \oplus x_2 \cdot \overline{(y_2 \oplus 1)} \end{bmatrix} \oplus \begin{bmatrix} (y_1 \oplus 1) \\ \overline{(y_1 \oplus 1)} \end{bmatrix}$ отримуємо наступне:

$$F_{10,12}(O_1^{d_{22}}) = \begin{bmatrix} x_1 \cdot \bar{k}_1 \oplus x_2 \cdot k_1 \\ x_1 \cdot k_1 \oplus x_2 \cdot \bar{k}_1 \end{bmatrix} \oplus \begin{bmatrix} k_2 \\ \bar{k}_2 \end{bmatrix} = O_1^k \ ,$$

Таким чином в результаті подвійного перетворення $F_{10,12} = \begin{bmatrix} y_2 \oplus 1 \\ y_1 \oplus 1 \end{bmatrix}$ з O_1^k отримуємо $O_1^k = \begin{bmatrix} x_1 \cdot \bar{k}_1 \oplus x_2 \cdot k_1 \\ x_1 \cdot k_1 \oplus x_2 \cdot \bar{k}_1 \end{bmatrix} \oplus \begin{bmatrix} k_2 \\ \bar{k}_2 \end{bmatrix}$.

Візьмемо двохрозрядну двохоперандну операцію строгого стійкого криптографічного перетворення такого представлення $O_1^k = \begin{bmatrix} x_1 \cdot \bar{k}_1 \oplus x_2 \cdot k_1 \\ x_1 \cdot k_1 \oplus x_2 \cdot \bar{k}_1 \end{bmatrix} \oplus \begin{bmatrix} k_2 \\ \bar{k}_2 \end{bmatrix}$ та виконаємо над другим операндом одноопераднe перетворення $F_{10,9} = \begin{bmatrix} y_2 \oplus 1 \\ y_1 \oplus y_2 \oplus 1 \end{bmatrix}$, у якому $(y_2 \oplus 1)$ – це k_1, а $(y_1 \oplus y_2 \oplus 1)$ – це k_2.

В результаті даного перетворення отримуємо:

$$F_{10,9}(O_1^k) = \begin{bmatrix} x_1 \cdot \overline{(y_2 \oplus 1)} \oplus x_2 \cdot (y_2 \oplus 1) \\ x_1 \cdot (y_2 \oplus 1) \oplus x_2 \cdot \overline{(y_2 \oplus 1)} \end{bmatrix} \oplus \begin{bmatrix} (y_1 \oplus y_2 \oplus 1) \\ \overline{(y_1 \oplus y_2 \oplus 1)} \end{bmatrix} = O_1^{d_{23}} \ .$$

Тобто в результаті перетворення отримуємо операцію $O_1^{d_{23}}$,що, в свою чергу відповідає $O_{24}^k = \begin{bmatrix} x_1 \cdot k_2 \oplus x_2 \cdot \bar{k}_2 \\ x_1 \cdot \bar{k}_2 \oplus x_2 \cdot k_2 \end{bmatrix} \oplus \begin{bmatrix} \overline{k_1 \oplus k_2} \\ k_1 \oplus k_2 \end{bmatrix}$.

В процесі подальшого двохрозрядного одноопераднього перетворення $F_{10,9} = \begin{bmatrix} y_2 \oplus 1 \\ y_1 \oplus y_2 \oplus 1 \end{bmatrix}$ над $O_1^{d_{23}} = \begin{bmatrix} x_1 \cdot \overline{(y_2 \oplus 1)} \oplus x_2 \cdot (y_2 \oplus 1) \\ x_1 \cdot (y_2 \oplus 1) \oplus x_2 \cdot \overline{(y_2 \oplus 1)} \end{bmatrix} \oplus \begin{bmatrix} (y_1 \oplus y_2 \oplus 1) \\ \overline{(y_1 \oplus y_2 \oplus 1)} \end{bmatrix}$ отримуємо наступне:

$$F_{10,9}(O_1^{d_{23}}) = \begin{bmatrix} x_1 \cdot \bar{k}_1 \oplus x_2 \cdot k_1 \\ x_1 \cdot k_1 \oplus x_2 \cdot \bar{k}_1 \end{bmatrix} \oplus \begin{bmatrix} k_2 \\ \bar{k}_2 \end{bmatrix} = O_1^k \ .$$

Таким чином в результаті подвійного перетворення $F_{10,9}=\begin{bmatrix} y_2 \oplus 1 \\ y_1 \oplus y_2 \oplus 1 \end{bmatrix}$ з O_1^k отримуємо $O_1^k=\begin{bmatrix} x_1 \cdot \bar{k}_1 \oplus x_2 \cdot k_1 \\ x_1 \cdot k_1 \oplus x_2 \cdot \bar{k}_1 \end{bmatrix} \oplus \begin{bmatrix} k_2 \\ \bar{k}_2 \end{bmatrix}$.

Візьмемо двохрозрядну двохоперандну операцію строгого стійкого криптографічного перетворення такого представлення $O_1^k=\begin{bmatrix} x_1 \cdot \bar{k}_1 \oplus x_2 \cdot k_1 \\ x_1 \cdot k_1 \oplus x_2 \cdot \bar{k}_1 \end{bmatrix} \oplus \begin{bmatrix} k_2 \\ \bar{k}_2 \end{bmatrix}$ та виконаємо над другим операндом одноопераднe перетворення $F_{9,12}=\begin{bmatrix} y_1 \oplus y_2 \oplus 1 \\ y_1 \oplus 1 \end{bmatrix}$, у якому $(y_1 \oplus y_2 \oplus 1)$ – це k_1, а $(y_1 \oplus 1)$ – це k_2.

В результаті даного перетворення отримуємо:

$$F_{9,12}(O_1^k)=\begin{bmatrix} x_1 \cdot \overline{(y_1 \oplus y_2 \oplus 1)} \oplus x_2 \cdot (y_1 \oplus y_2 \oplus 1) \\ x_1 \cdot (y_1 \oplus y_2 \oplus 1) \oplus x_2 \cdot \overline{(y_1 \oplus y_2 \oplus 1)} \end{bmatrix} \oplus \begin{bmatrix} (y_1 \oplus 1) \\ \overline{(y_1 \oplus 1)} \end{bmatrix} = O_1^{d_{24}}.$$

Тобто в результаті перетворення отримуємо операцію $O_1^{d_{24}}$,що, в свою чергу відповідає $O_{20}^k=\begin{bmatrix} x_1 \cdot (k_1 \oplus k_2) \oplus x_2 \cdot \overline{(k_1 \oplus k_2)} \\ x_1 \cdot \overline{(k_1 \oplus k_2)} \oplus x_2 \cdot (k_1 \oplus k_2) \end{bmatrix} \oplus \begin{bmatrix} \bar{k}_1 \\ k_1 \end{bmatrix}$.

В процесі подальшого двохрозрядного одноопераднoго перетворення $F_{9,12}=\begin{bmatrix} y_1 \oplus y_2 \oplus 1 \\ y_1 \oplus 1 \end{bmatrix}$ над $O_1^{d_{24}}=\begin{bmatrix} x_1 \cdot \overline{(y_1 \oplus y_2 \oplus 1)} \oplus x_2 \cdot (y_1 \oplus y_2 \oplus 1) \\ x_1 \cdot (y_1 \oplus y_2 \oplus 1) \oplus x_2 \cdot \overline{(y_1 \oplus y_2 \oplus 1)} \end{bmatrix} \oplus \begin{bmatrix} (y_1 \oplus 1) \\ \overline{(y_1 \oplus 1)} \end{bmatrix}$ отримуємо наступне:

$$F_{9,12}(O_1^{d_{24}})= \begin{bmatrix} x_1 \cdot \bar{k}_1 \oplus x_2 \cdot k_1 \\ x_1 \cdot k_1 \oplus x_2 \cdot \bar{k}_1 \end{bmatrix} \oplus \begin{bmatrix} k_2 \\ \bar{k}_2 \end{bmatrix} = O_1^k,$$

Таким чином в результаті подвійного перетворення $F_{9,12}=\begin{bmatrix} y_1 \oplus y_2 \oplus 1 \\ y_1 \oplus 1 \end{bmatrix}$ з O_1^k отримуємо $O_1^k=\begin{bmatrix} x_1 \cdot \bar{k}_1 \oplus x_2 \cdot k_1 \\ x_1 \cdot k_1 \oplus x_2 \cdot \bar{k}_1 \end{bmatrix} \oplus \begin{bmatrix} k_2 \\ \bar{k}_2 \end{bmatrix}$.

Таким чином, можна стверджувати, що в результаті отримання оберненої операції до O_1^k при подвійному перетворенні другого операнда за допомогою двохрозрядної одноопераднoї операції, отримуємо початкову операцію, тобто O_1^k.

Взаємозв'язки між прямими і оберненими операціями наведені на рис.4.1.

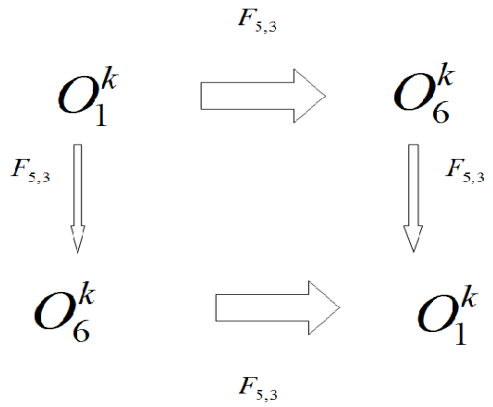


Рис.4.1 Взаємозвязки між прямими і оберненими операціями

Отримані на основі перетворення другого операнда взаємозв’язки між прямими і оберненими операціями дозволяють генерувати обернені операції при випадковій генерації операцій криптоперетворення.

Взаємозвязки між прямими і оберненими операціями при їх випадковій генерації наведені на рис.4.2.

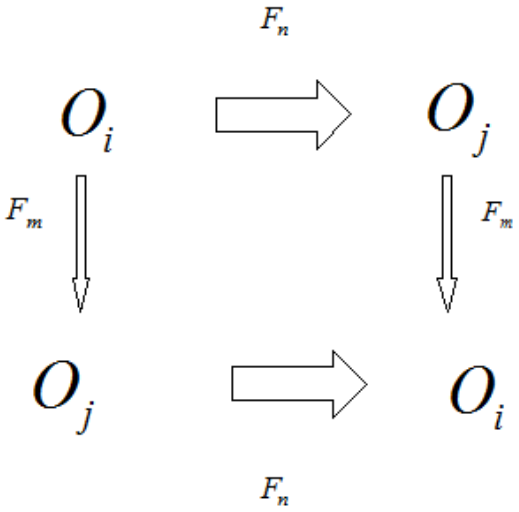


Рис.4.2. Взаємозв’язки між прямими і оберненими операціями при псевдовипадковій генерації операцій.

Таким чином, можна стверджувати, що в результаті перетворення другого операнда отримано всі 24 пари операцій, які забезпечують пряме і обернене перетворення інформації. Отриманий результат забезпечує випадкову генерацію операцій криптоперетворення для систем комп'ютерної криптографії.

Сутність методу полягає в наступному:

1. Визначення заданої двохрозрядної двохоперандної операції ССКК на основі перетворення другого операнда.
2. Випадкова генерація групи одноопераднних двохрозрядних операції ССКК.
3. Синтез групи двохрозрядних двохоперандних операцій строгого стійкого криптографічного перетворення на основі заданої операції, шляхом перетворення другого операнда відомої операції.
4. Модифікація заданої двохрозрядної двохоперандної операції шляхом перетворення другого операнда відомої операції.
5. Синтез оберненої операції до модифікованої операції
6. Синтез групи прямих і обернених двохрозрядних двохоперандних операцій строгого стійкого криптографічного перетворення на основі модифікованої заданої двохрозрядної двохоперандної операції шляхом послідовного перебору та перетворення другого операнда відомої операції шляхом вибору наступної одноопераднної операції.
7. Пункти 4–6 повторюються до завершення синтезу групи модифікованих двохрозрядних двохоперандних операцій строгого стійкого криптографічного перетворення.
8. Пункти 2–7 повторюються до повного завершення криптоперетворення інформації.

Алгоритм реалізації методу генерації псевдовипадкових послідовностей двохрозрядних двохоперандних операцій ССКК на основі перетворення другого операнда наведений на рис.4.3.

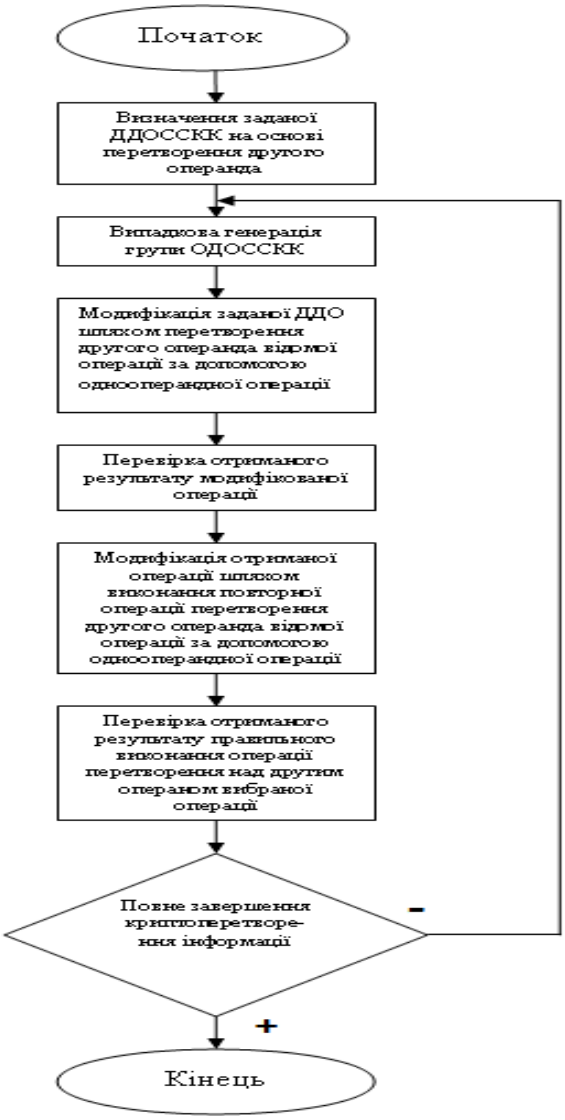


Рисунок 4.3 – Блок-схема методу генерації псевдовипадкових послідовностей двохрозрядних двохоперандних операцій ССКК на основі перетворення другого операнда

Для розробки програмно-апаратних засобів реалізації систем потокового шифрування на основі генерації псевдовипадкових послідовностей операцій криптографічного кодування необхідно розглянути всі варіанти функціонування алгоритму представленому на рис.4.3.

4.3. Практична реалізація запропонованих генераторів взаємопов'язаних псевдовипадкових послідовностей прямих і обернених двохрозрядних двохоперандних операцій строгого стійкого криптографічного кодування на основі перетворення другого операнда

В ході дослідження було встановлено, що генератори взаємопов'язаних псевдовипадкових послідовностей прямих і обернених двохрозрядних двохоперандних операцій ССКК на основі перетворення другого операнда можуть бути застосовані при виборі будь-якої операції криптоперетворення з групи двохрозрядних двохоперандних операцій ССКК.

Розглянемо варіант генерації операцій з використанням груп одно- та двохоперандних операцій на початкововому етапі синтезу без застосування перестановок операцій. Даний варіант генерації операцій наведено на рис. 4.4.

F_1	F_2	F_3	O_1	O_2	O_3
F_4	F_5	F_6	O_4	O_5	O_6
F_7	F_8	F_9	O_7	O_8	O_9
F_{10}	F_{11}	F_{12}	O_{10}	O_{11}	O_{12}
F_{13}	F_{14}	F_{15}	O_{13}	O_{14}	O_{15}
F_{16}	F_{17}	F_{18}	O_{16}	O_{17}	O_{18}
F_{19}	F_{20}	F_{21}	O_{19}	O_{20}	O_{21}
F_{22}	F_{23}	F_{24}	O_{22}	O_{23}	O_{24}

Рис. 4.4 – Генерація операцій з використанням груп одно- та двохоперандних операцій без застосування перестановок операцій

На рис 4.4 використані наступні позначення:

$\mathbf{O_{1\text{-}24}}$ – це двохрозрядні двохоперандні операції ССКК;

$\mathbf{F_{1\text{-}24}}$ – це двохрозрядні одноопераднді операції ССКК.

Розглянемо варіант генерації операцій з використанням перестановок одноопераднді операцій криптоперетворення. Якщо провести перестановку одноопераднді операцій ССКК, а послідовність двохрозрядних операцій ССКК залишити без змін, то ми отримуємо нову групу двохрозрядних двохоперандних операцій строгого стійкого криптоперетворення (рис. 4.5).

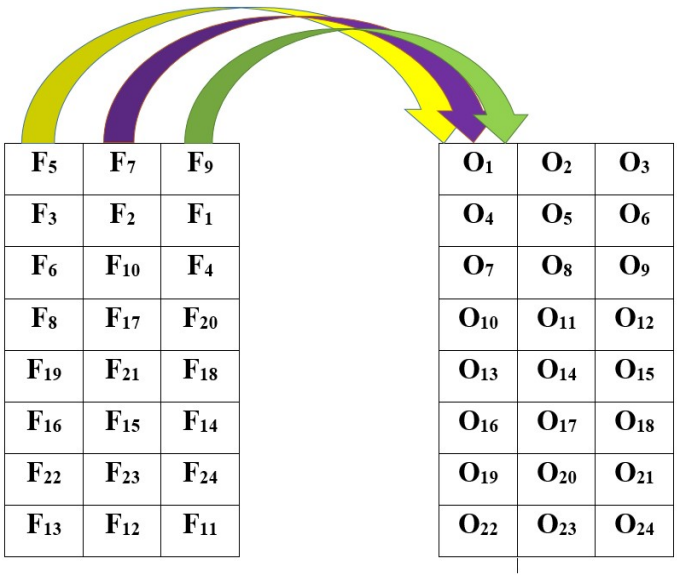
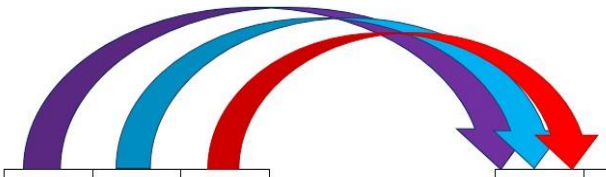


Рис. 4.5 – Генерація операцій з використанням перестановок одноопераднді операцій криптоперетворення

Розглянемо варіант генерації операцій з використанням перестановок двохоперандних операцій криптоперетворення. Якщо виконати перестановку двохоперандних операцій ССКК, а группу одноопераднді операцій залишити без змін, то буде отримано нову групу операцій двохрозрядних двохоперандних операцій строгого стійкого криптографічного перетворення (рис. 4.6).



F_1	F_2	F_3	O_5	O_7	O_9
F_4	F_5	F_6	O_3	O_2	O_1
F_7	F_8	F_9	O_6	O_{10}	O_4
F_{10}	F_{11}	F_{12}	O_8	O_{17}	O_{20}
F_{13}	F_{14}	F_{15}	O_{19}	O_{21}	O_{18}
F_{16}	F_{17}	F_{18}	O_{16}	O_{15}	O_{14}
F_{19}	F_{20}	F_{21}	O_{22}	O_{23}	O_{24}
F_{22}	F_{23}	F_{24}	O_{13}	O_{12}	O_{11}

Рис. 4.6 – Генерація операцій з використанням перестановок двохоперандних операцій криптоперетворення

Розглянемо варіант генерації операцій з використанням перестановок одноопераднних та двохоперандних операцій криптоперетворення. Якщо виконати перестановку двохоперандних та одноопераднних операцій ССКК, то буде отримано нову послідовність операцій двохрозрядних двохоперандних операцій строгого стійкого криптографічного перетворення (рис.4.7).

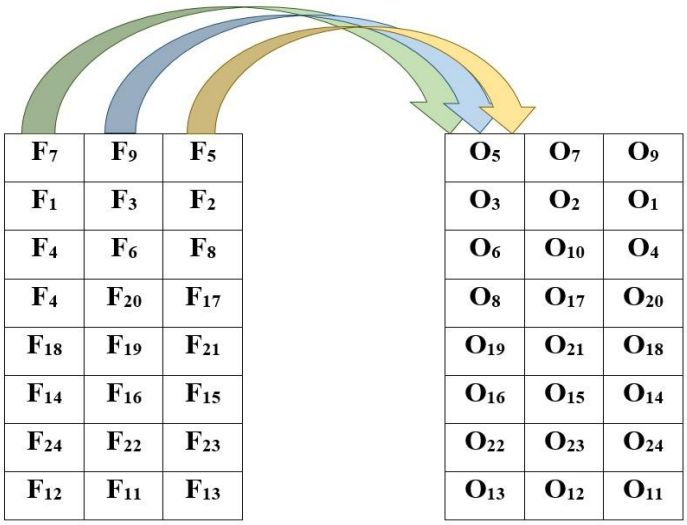


Рисунок 4.7 – Генерація операцій з використанням перестановок одно- та двохоперандних операцій криптоперетворення

З вищевказаного можна зробити висновок, що при кожній з виконаних перестановок, буде отримано нову послідовність двохрозрядних двохоперандних операцій строгого стійкого криптографічного перетворення.

Розглянуті варіанти генерації послідовності операцій, сумісно з алгоритмами синтезу операцій оберненого перетворення (рис.4.4 – 4.7) дозволяють покращити метод підвищення стійкості та надійності потокового шифрування (рис1.1).

Структурна схема удосконаленого методу підвищення стійкості та надійності потокового шифрування шляхом генерації псевдовипадкових послідовностей прямих та обернених операцій криптоперетворення наведено на рис.4.8.

Рисунок 4.8 – Структурна схема удосконаленого методу підвищення стійкості та надійності потокового шифрування шляхом генерації псевдовипадкових послідовностей прямих та обернених операцій криптоперетворення

Запровонована структурна схема удосконаленого методу підвищення стійкості та надійності потокового шифрування шляхом генерації псевдовипадкових послідовностей прямих та обернених операцій криптоперетворення реалізує автоматичну генерацію операцій ССКК. Дана структурна схема забезпечує реалізацію потокового шифрування, створюючи при цьому наступні переваги перед відомими технічними рішеннями:

- розширили варіативність криптографічних перетворень за рахунок збільшення кількості операцій, які застосовуються з 12 до 24 операцій. Підвищення криптостійкості перетворення інформації за рахунок збільшення варівтивності шляхом розширення множини операцій;

- створили можливість застосувати в методі підвищення стійкості та надійності потокового шифрування операцій ССКК, які забезпечують максимальну невизначеність результатів перетворення;
- псевдовипадкові послідовності двохрозрядних двохоперандних операцій строгого стійкого криптографічного кодування генеруються на 15-20% швидше порівняно з табличним методом синтезу операцій;
- забезпечили можливість автоматичної генерації псевдовипадкової послідовності операцій криптоперетворення, період якої визначається наступним чином: якщо T_g - період згенерованої псевдовипадкової послідовності операцій, O_n - кількість двохоперандних операцій криптоперетворення, F_m - кількість одноопераднних операцій криптоперетворення тоді $T_g = O_n ! \cdot F_m !$. При використанні двохрозрядних двохоперандних операцій криптоперетворення період згенерованої послідовності буде рівним $T_g = 24 ! \cdot 24 !$.

Наведені переваги удосконаленого методу підвищення стійкості та надійності потокового шифрування забезпечують доцільність його застосування для захисту потоків конфіденційної інформації в кіберпросторі.

Висновки до 4 розділу

Вперше розроблено метод генерації псевдовипадкових послідовностей двохрозрядних двохоперандних операцій строгого стійкого криптографічного кодування на основі перетворення другого операнда, що дозволяє значно спростити процес дослідження та синтезу групи операцій строгого стійкого криптоперетворення та робить можливим використання його при вдосконаленні методу підвищення криптостійкості і надійності потокового шифрування.

1. Запропоновано технологію розробки методу генерації псевдовипадкових послідовностей двохрозрядних двохоперандних операцій

строгого стійкого криптографічного кодування на основі перетворення другого операнда, що дозволяє значно спростити процес дослідження та синтезу групи операцій строгого стійкого криптоперетворення.

2. Реалізація даного методу забезпечує псевдовипадковий синтез операцій криптоперетворення. Даний метод генерації псевдовипадкових послідовностей двохрозрядних двохоперандних операцій строгого стійкого криптографічного кодування, на основі перетворення другого операнда доцільно використати при вдосконаленні методу підвищення криптостійкості і надійності потокового шифрування.

3. Отримані на основі перетворення другого операнда взаємозв’язки між прямими і оберненими операціями дозволяють генерувати обернені операції при випадковій генерації операцій криптоперетворення.

4. Результати розділу опубліковано [2,5].

ВИСНОВКИ

У дисертаційній роботі вирішено важливу науково-технічну задачу підвищення швидкості потокового шифрування за рахунок генерації псевдовипадкових послідовностей групи двохрозрядних двохоперандних операцій строгого стійкого криптографічного кодування на основі перетворення другого операнда:

1) вперше розроблено метод синтезу обернених двохрозрядних двохоперандних операцій строгого стійкого криптографічного кодування на основі множини двохрозрядних двохоперандних операцій строгого стійкого криптографічного кодування, встановлених взаємозв’язків між прямими та оберненими операціями, шляхом перетворення другого операнда за рахунок реалізації побудованої моделі автомата синтезу другого операнда оберненої операції, що забезпечило можливість практичного застосування даних операцій;

2) вперше розроблено метод синтезу групи двохрозрядних двохоперандних операцій строгого стійкого криптографічного кодування на основі використання відомої двохрозрядної двохоперандної операції строгого стійкого криптографічного кодування та перетвореннями другого операнда шляхом послідовного виконання над даною операцією групи двохрозрядних одноопераднихоперацій, що забезпечило можливість збільшення варіативності криптопримітивів при практичному застосуванні даних операцій;

3) вперше розроблено метод генерації псевдовипадкових послідовностей двохрозрядних двохоперандних операцій строгого стійкого криптографічного кодування на основі використання груп двохрозрядних двохоперандних операцій строгого стійкого криптографічного кодування і двохрозрядних одноопераднихоперацій строгого стійкого криптографічного кодування, шляхом перетворень других операндів прямих

та обернених двохоперандних операцій, що дозволило досягти підвищення швидкості потокового шифрування за рахунок генерації псевдовипадкових послідовностей прямих та обернених двохрозрядних двохоперандних операцій строгого стійкого криптографічного кодування. Отриманий результат забезпечив швидкість реалізації методу підвищення стійкості та надійності потокового шифрування;

4) практична цінність роботи полягає в доведенні здобувачем отриманих наукових результатів до конкретних алгоритмів генерації псевдовипадкових послідовностей двохрозрядних двохоперандних операцій строгого стійкого криптографічного кодування на основі перетворення другого операнда.

Розширено варіативність криптографічних перетворень за рахунок збільшення кількості операцій з 12 до 24. Розроблений генератор псевдовипадкових послідовностей двохрозрядних двохоперандних операцій строгого стійкого криптографічного кодування забезпечує синтез операцій на 15-20% швидше, порівняно з табличним методом синтезу при забезпеченні періоду послідовності $(24!)^2$. Отриманий результат забезпечив швидкість реалізації методу підвищення стійкості та надійності потокового шифрування при максимальній невизначеності результатів перетворення.

Результати дисертації використані та впроваджені у таких організаціях: Черкаський державний технологічний університет, КНП «Черкаська міська консультативно-діагностична поліклініка» Філія №2, «Нова Пошта», ПАТ «Черкасиобленерго».

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Бреус Р.В. Синтез двохрозрядних двохоперандних операцій строгого стійкого криптографічного кодування шляхом перетворення другого операнда. Системи управління, навігації та зв'язку: Полтава: ПНТУ, 2019. – Вип. 5 (57). – С. 29–32.

2. Рудницький В.М., Бреус Р.В., Лада Н.В. Генерація послідовностей операцій криптографічного перетворення. Вісник інженерної авадемії України: Київ, 2019. – Вип. 3. – С.75–80.

3. Rudnitsky V., Berdibayev R., Breus R., Lada N., Pustovit M. Synthesis of reverse two-bit dual-operated strictly straight cryptographic coding on the basis of another operation. Advanced Information Systems. Quarterly scientific and technical journal. Kharkiv: National Technical University "Kharkiv Polytechnic Institute", 2019. Vol 3, No. 4, pp. 109-114.

4. Lada N., Dzyuba V., Breus R., Lada S. Synthesis of sets of non-symmetric two-operand two-bit crypto operations within the permutation accuracy. Technology audit and production reserves № 2/2(52), 2020, pp. 28-31.

5. Лада Н.В., Бреус Р. В., Лада С.В. Генерація моделей прямих і обернених двохрозрядних двохоперандних операцій строгого стійкого криптографічного кодування. Science and Education a New Dimension Natural and Technical science: Budapest, 2020. V. 238, p. 27-30.

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

7. Бреус Р.В. Уніфікація опису операцій криптографічного перетворення. Проблеми інформатизації: матеріали Четвертої міжнар. наук.-техн. конф.: тези доп., (Черкаси – Баку – Бельсько-Бяла – Полтава, 3–4 листоп. 2016 р.). Черкаси: ЧДТУ, 2016. С. 9.

8. Бреус Р.В. Математичні моделі побудови операцій розширеного матричного криптографічного перетворення. Проблеми інформатизації:

матеріали П’ятої міжнар. наук.-техн. конф.: тези доп., (Черкаси – Баку – Бельсько-Бяла – Полтава, 13-15 листоп. 2017 р.). Черкаси: ЧДТУ, 2017. С. 13.

9. Лада Н.В., Бреус Р.В., Рудницька Ю. В., Висоцький С. В. Аналіз групи двоопераднних симетричних криптовалютних операцій. Проблеми інформатизації: матеріали Сьомого Інтернаціоналу, науково-технічна конф.: тези доп., (Черкаси - Харків - Баку - Бельсько-Бяла, 13–15 листопада 2019 р.). Черкаси: ЧДТУ; Баку: ВА ЗС АР, Більсько-Бяла: УТіГН, Харків: НТУ "ХПІ", 2019., Т.1, С. 85.

10. Daniel Jancarczyk, Volodymyr Rudnytskyi, Roksolana Breus, Mykhailo Pustovit, Olga Veselska and Ruslana Ziubina. Two-Operand Operations of Strict Stable Cryptographic Coding With Different Operands’ Bits. The 5-th IEEE International Symposium on Smart and Wireless Systems within the International Conferences on Intelligent Data Acquisition and Advanced Computing Systems, 17-18 September, 2020, Dortmund, Germany.

11. Бабаш А. В. Криптография. Аспекты защиты / А. В. Бабаш, Г. П. Шанкин. – М. : Солон-Р, 2002. – 512 с.

12. Соколов В. Ю. Інформаційні системи і технології: навчальний посібник / В. Ю. Соколов. – К. : Вид-во ДУІКТ, 2010. – 138 с.

13. Горбенко І.Д., Горбенко Ю.І. Прикладна криптологія: Теорія. Практика. Застосування: Підручник для ВНЗ Харків: «Форт», 2013. – 880 с.

14. Закон України «Про захист персональних даних» N 4452-VI 22 вересня 2012 року

15. Хорошко В.А. Методи й засоби захисту інформації / В.А. Хорошко, А. А. Чекатков. – К.: Юніор, 2003. – 504 с.

16. Закон України «Про електронний цифровий підпис» // Відомості Верховної Ради України (ВВР). –2003. –36. –Ст. 276.

17. Рябко Б. Я., Фионов А. Н. Криптографические методы защиты информации. — Москва. — Изд-во Горяч.Линия-Телеком, 2005. 229 с.

18. Запечников С. В.Криптографические протоколы и их применение в финансовой и коммерческой деятельности/ Запечников С. В. –Москва :2007.

19. Сингх С. Книга шифров. Тайная история шифров и их расшифровки. М.: Аст, Астрель, 2006. 447 с.

20. Мао В. Современная криптография. Теория и практика. М.: Вильямс, 2005. 763 с.

21. Актуальні проблеми інформаційної безпеки України. Аналітична доповідь УЦЕПД / /Національна безпека і оборона. — К., 2001. — №1. — С. 2-59.

22. Остапов С.Е. Технології захисту інформації : навчальний посібник /С.Е. Остапов, С. П. Євсеєв, О.Г. Король. –Х.: Вид. ХНЕУ, 2013. –476с. (Укр. мов.).

23. Домарев, В. В. Защита информации и безопасность компьютерных систем / В.В. Домарев. —Київ. : DiaSoft, 1999. —453, [23] с. : ил., табл. — Библиогр.: с. 451-453.

24. Дорошенко А. Н. Информационная безопасность. Методы и средства защиты информации в компьютерных системах : учебн. пособ. / А. Н. Дорошенко, Л. Л. Ткачев. –М. : МГУПИ, 2006. –143 с.

25. Кібербезпека в Україні: правові та організаційні питання:матеріали міжн. наук.практ.конф., м.Одеса, 22листопада 2019р. Одеса : ОДУВС, 2019. 108с.ISBN 678-717-70204.

26. Галатенко В.А. Основы информационной безопасности: курс лекций: учеб. пособ. / под ред.В.Б.Бетелина. Изд. 3-е. М.: ИНТУИТ.РУ «Интернет-университет Информационных Технологий», 2006. 208 с.

27. Бауэр Ф. Расшифрованные секреты. Методы и принципы криптологии. М.: Мир, 2007. 550 с.

28. Шнайер Б. Прикладная криптография. Протоколы, алгоритмы, исходные тексты на языке Си. М.: Триумф, 2003. 806 с.

29. Алферов А.П., Зубов А.Ю., Кузьмин А.С., Черемушкин А. В. Основы криптографии. М.: Гелиос АРВ, 2001. 479 с.

30. Єсімов С.С. Захист персональних даних у контексті розвитку динамічних інформаційних систем. Науковий вісник Львівського державного університету внутрішніх справ. 2013. No 3. С. 198–208.

31. Франчук В.М. Захист інформаційних ресурсів: криптографічні та стеганографічні методи захисту даних. Посібник для викладачів, вчителів та студентів інформатичних спеціальностей. –К.: НПУ імені М.П. Драгоманова, 2012. –120с.

32. Яковлев А.В., Безбогов А.А., Родин В.В., Шамкин В.Н.. Криптографическая защита информации. –Тамбов:Из-воТамб. Гос. Тех.. ун-та, 2006. –140 с.

33. Гатчин Ю.А. Основы криптографических алгоритмов: навчальний посібник/ Гатчин Ю.А., КоробейниковА. Г.–СПб: ГИТМО, 2002.

34. Баранов О.А. Інформаційне право України: стан, проблеми, перспективи. –К.: Видавничий дім"Софт Прес", 2005.–316с.

35. Сапегин Л.Н. Типичные дефекты в криптографических протоколах. Специальная техника средств связи / Сапегин Л.Н.–Пенза:ПНИЭИ, 1996.

36. Скудис, Э. Противостояние хакерам / Эд Скудис. – М.: ДМК Пресс, 2003. – 512 с.

37. Закон України «Про захист інформації в автоматизованих системах» // ВВР, 1994, No 31, ст.. 286

38. Ирвин Дж., ХарльД. Передача данных в сетях: инженерный поход.: Пер. сангл. – СПб.: БХВ– Петербург, 2003 – 448 с.

39. Горбенко І.Д. Захист інформації в інформаційно-телекомунікаційних системах: Навч. Посібник. Ч.1. Криптографічний захист інформації/ І.Д.Горбенко.Т.О.Гріненко. –Харків: ХНУРЕ, 2004. –368 с.

40. Вигерс Карл Разработка требований к программному обеспечению. Пер, с англ. -М.: Издательско-торговый дом «Русская Редакция», 2004. -576с.

41. Петров А. А. Компьютерная безопасность. Криптографические методы защиты/ А. А. Петров. -М.: ДМК, 2000. -448 с.

42. Інформаційна безпека комп'ютерних систем і мереж: Методичні вказівки // Укл. А.Ф. Карачка, М.П. Карпінський, А.В. Кулик, Т.В. Лендюк. – Тернопіль: ТАНГ, 2007. –68 с.

43. Блинов А.М. Информационная безопасность : учеб. пособие. Ч. 1 / А.М. Блинов.–СПб. : СПБГУЭФ, 2010. –96с.

44. Щебланін Ю.М.Математична модель порушника інформаційної безпеки / Ю.М. Щебланін, Д.І.Рабчун// Кібербезпека: освіта, наука, техніка.– 2018. –No 1 (1). –С. 63–72.

45. Основні параметри для ідентифікації порушника інформаційної безпеки / А.І. Гізун, В.В. Волянська, В.О.Риндюк, С.О. Гнатюк// Захист інформації.–2013.–Вип. 15 (1).–С. 66–74.

46. Погребняк А.В. Технології комп'ютерної безпеки. Монографія. МЕГУ, Рівне, 2011.-117с.Pogrebnyak A.V. Technologiesofcomputersafety. Monograph. IEGU, Rivne, 2011.-117p.

47. Баранов В М. и др. Защита информации в системах и средствах информатизации и связи. Учебное пособие. –СПб.: 1996. –111 с

48. Заплотинський Б. А. Основи інформаційної безпеки. Конспект лекцій. – КІІВіП НУ "ОЮА", кафедра інформаційно-аналітичної та інноваційної діяльності, 2017. –128с.

49. Бурячок В.Л. Інфомаційна та кібербезпека / В.Л.Бурячок, В.Б. Толубко, В.О. Хорошко, С.В. Толюпа. –К.: ДУТ, 2015. –288 с.

50. Голубєв В. О. Інформаційна безпека: проблеми боротьби зі злочинами у сфері використання комп'ютерних технологій / В.О.Голубєв, В.Д.Гавловський, В.С.Цимбалюк ; за заг. ред. Р.А.Калюжного. – Запоріжжя : Просвіта, 2001. – 252с.

51. Сороківська О. А. Інформаційна безпека підприємства : нові загрози та перспективи / О.А.Сороківська, В.Л.Гевко // Вісник Хмельницького національного університету. – 2010. – No2, т.2. – С.32—35.

52. Марущак А. І. Інформаційно-правові напрями дослідження проблем інформаційної безпеки / А.І.Марущак // Державна безпека України. – 2011. – No21. – С.92–95.

53. Технології розвитку і захисту національного інформаційного простору / [О.С Онищенко (керівник проекту), вступ –Горовий В.М; Розділ 1. -Онищенко О.С. , Горовий В.М.; Розділ 2 -Половинчак Ю.М.; Розділ 3. – Горова С.В.; Розділ 4 : 4.1 –Костенко Л.Й., 4.2.-Матвійчук А.В.; Розділ 5 – Чуприна Л.А.; Розділ 6.-Попик В.І.; Розділ 7: 7.1. –Дубровіна Л.А.,Індиченко Г.В.,7.2.-Дубровіна Л.А. за уч . Індиченко Г.В., 7.3-Дубровіна Л.А.; Висновки –Онищенко О.С., Горовий В.М.]; НАН України, Нац. б-ка України ім. В. І. Вернадського. –К.: НБУВ, 2015. –343 с

54. Національний інформаційний комплекс і його роль у глобальному інформаційному просторі / [О. С. Онищенко, В. М. Горовий, В. І. Попик та ін.]; НАН України, Нац. б-ка України ім. В. І. Вернадського. –К.: НБУВ, 2014. –264 с.

55. Богуш В. М. Інформаційна безпека держави /В. М. Богуш, О. К.Юдін. –К.: «МК-Прес», 2005. –432 с

56. Андреєв В.І. Основи інформаційної безпеки / В. І. Андреєв, В. О. Хорошко, В.С.Чередниченко, М. Є. Шелест. –К. : Вид. ДУІКТ, 2009. –292 с.

57. Закон України «Про Концепцію Національної програми інформатизації» від 4 лютого 1998 року № 75/98-ВР.

58. Варенко В.М. Інформаційно-аналітична діяльність: Навч. посіб. / В.М. Варенко. –К.: Університет «Україна», 2014. –417с.

59. Кулицький С.П. Основи організації інформаційної діяльності у сфері управління: Навч. посіб./ С.П. Кулицький –К.: МАУП. 2002. –224с

60. Законодавчі та нормативні документи України у сфері інформації, 3-19 видавничої та бібліотечної справи: Темат. добірка. У 2 ч. / Уклад. Т. Ю. Жигун. — 3-тє вид., допов. — К.: Кн. палата України, 2007. Ч. 1: Правове регулювання у сфері інформації. — 176 с.

61. Інформаційні технології — Методи убезпечення — Критерії оцінення безпеки ІТ — Частина 2: Функ-ціональні компоненти безпеки: ISO / IEC 15408-2 2008 — ISO / IEC. — Перше редагування. 2008-08-19; Остання зміна. 2014-12-01. — Міжнародна організація по стандартизації, 2008 — III. — 218 с. (Міжнародний стандарт).

62. Інформаційні технології — Методи убезпечення — Критерії оцінення безпеки ІТ — Частина 3: Ком-поненти убезпечення: ISO / IEC 15408-2 2008 — ISO / IEC. — Перше редагування. 2008-08-19; Остання зміна. 2014-12-01. — Міжнародна ор-ганізація по стандартизації, 2008 — III. — 174 с. (Міжнародний стандарт).

63. Защита компьютерной информации. Эффективные методы и средства / Шаньгин В. Ф. - М.: ДМК Пресс, 2008. - 544 с.: ил.

64. Дубов Д.В. Стратегічні аспекти кібербезпеки України [Текст] / Дубов Дмитро Володимирович // Стратегічні пріоритети : [наук.-аналіт. щокварт. зб.] / Нац. ін-т стратег. дослідж. –Київ : НІСД, 2013. –2013. No 4(29). –С. 119-126. –Бібліогр. : с. 125-126

65. Барабаш О.В. Построение функционально устойчивых распределенных информационных систем: монография. К.: НАОУ, 2004. 224 с.

66. Джарратано Дж., Райли Г. Экспертные системы: принципы разработки и программирования, 4-е издание.: Пер. с анг. – М.: ООО «И. Д. Вильямс», 2007. – 1152 с.

67. Зима В. М., Молдовян А. А., Молдовян Н. А. Безопасность глобальных сетевых технологий. – 2-е изд. СПб.: БХВ-Петербург, 2003. – 368 с.: ил.

68. ДСТУ ISO/IEC 27032:2016 Інформаційні технології. Методи захисту. Настанови щодо кібербезпеки (ISO/IEC 27032:2012, IDT).

69. David Kushner, «The Real Story of Stuxnet». IEEE Spectrum, March 2013.

70. Stuxnet. Under the Microscope: Aleksandr Matrosov, Eugene Rodionov, David Harley–SanDiego(USA), ESET, 2010. –72 с.

71. Михайлов А.В. Компьютерные вирусы и борьба с ними/А. В. Михайлов.—М. : Диалог-МИФИ, 2011.—104 с.

72. Алексеев П. П. Антивирусы / П.П. Алексеев, А. П. Корш, Р. Г. Прокди.—М. :Наука и техника, 2010.—80 с.

73. Дубов Д. В. Кіберпростір як новий вимір геополітичного суперництва : моно-графія / Д. В. Дубов. – К. : НІСД, 2014. – 328 с.

74. Скудис Эд. Противостояние хакерам. Пошаговое руководство по компьютерным атакам и эффективной защите: Пер. с англ.: ил. (Серия «Защита и администрирование»).

75. Толюпа С.В. Методика оцінки комплексної системи захисту інформації на об’єкті інформаційної діяльності / С.В. Толюпа, І.В. Борисов // Науково-технічний журнал “Сучасний захист інформації”. – 2013. - №2. – С. 43-49.

76. Принципы и порядок разработки комплексных сис-тем защиты информации в информационно-телекомму-никационных системах/ Ю.В. Землянко, А.А Замула, А.А. Ткач, Н.И. Литвинова, Я.А. Пересечанская // Прикладная радиоэлектроника: науч.-техн. журнал. – 2010. Том 9. No 3. – С. 460–469.

77. Дубов Д.В. Кібербезпека : світові тенденції та виклики для України / Д.В. Дубов, М.А. Ожеван. - К. : НІСД, 2011. - 30 с.

78. Коутинхо, С. Введение в теорию чисел. Алгоритм RSA / С. Коутинхо. – М.: Постмаркет, 2001. – 328 с.

79. МихайловА.С. Архитектура сетевого программного комплекса для анализа криптографических протоколов / МихайловА.С.,ПершиковА.Г., Тарасов И.Л.// Научная сессия МИФИ-2001–Москва :МИФИ,2001.

80. Рудницький В.М. Визначення множини логічних функцій для синтезу цифрових пристроїв систем захисту інформації / В.М. Рудницький,

Н.М. Пантелєєва, В.Г. Бабенко // Системи управління, навігації та зв’язку: Зб. наук. пр. – Київ. - 2008. – Вип. 4(8). – С. 155-157.

81. Рудницький В.М. Моделювання логічного пристрою для систем захисту інформації / В.М. Рудницький, Н.М. Пантелєєва, В.Г. Бабенко // Проблеми і перспективи розвитку банківської системи України: Зб. наук. пр. - Суми. – 2006. - Т. 18. – С. 185-190.

82. Бабенко В.Г. Технологія визначення спеціальних логічних функцій для систем захисту інформації / В.Г. Бабенко, В.М. Рудницький, Т.В. Дахно // Вісник інженерної академії України. – 2007. – Вип. 3-4. – С.64-67.

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

84. Рудницький В. М., Миронець І. В., Бабенко В. Г. Систематизація повної множини логічних функцій для криптографічного перетворення інформації. Системи обробки інформації: зб. наук. пр. Харків: ХУПС ім. І. Кожедуба. 2011. Вип. 8 (98). С. 184–188.

85. Бабенко В. Г., Миронець І. В., Рудницький С. В. Декодування інформації в групі дворозрядних операцій криптографічного перетворення. Системи управління, навігації та зв'язку: зб. наук. пр. Київ: Центр. наук.-досл. ін-т навігації і управл., 2011. Вип. 4 (20). С. 208–212.

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

87. Рудницький В.М. Модель уніфікованого пристрою криптографічного перетворення інформації / В.М. Рудницький, В.Г. Бабенко // Системи обробки інформації: Зб. наук. пр. – Харків. – 2009. – Випуск . – С. 173-177.

88. Рудницький В. М., Миронець І. В., Бабенко В. Г. Обґрунтування можливості розширення набору функцій перекодування інформації для захисту конфіденційних інформаційних ресурсів. Системи управління,

навігації та зв’язку: зб. наук. пр. Київ: Центр. наук.-досл. ін-т навігації і управл., 2010. Вип. 2 (14). С.118–122.

89. Рудницький В. М., Миронець І. В., Бабенко В. Г. Методологія підвищення оперативності доступу до конфіденційних інформаційних ресурсів. Системи обробки інформації: зб. наук. пр. Харків: ХУПС ім. І. Кожедуба, 2010. Вип. 5 (86). С.15–19.

90. Рудницький В. М., Миронець І. В., Бабенко В. Г. Реалізація методу підвищення оперативності доступу до конфіденційних інформаційних ресурсів. Вісник Черкаського державного технологічного університету. Серія: Технічні науки. 2010. Вип. №3. С. 60–65.

91. Рудницький В. М., Миронець І. В., Бабенко В. Г. Технологія побудови пристрою реалізації методу підвищення оперативності доступу до конфіденційних інформаційних ресурсів. Зб. наук. пр. Харківського університету Повітряних Сил. Харків: ХУПС ім. І. Кожедуба. 2011. Вип. 3 (29). С. 145–150.

92. Рудницький В. М., Бабенко В. Г., Рудницький С. В. Метод синтезу матричних моделей операцій криптографічного кодування та декодування інформації. Зб. наук. пр. Харків. ун-ту Повітряних Сил. Харків: ХУПС ім. І. Кожедуба, 2012. Вип. 4 (33). С. 198–200.

93. Рудницький В. М., Бабенко В. Г., Рудницький С. В. Метод синтезу матричних моделей операцій криптографічного перекодування інформації. Захист інформації : наук.-практ. журн. 2012. № 3 (56). С. 50–56.

94. Голуб С. В., Бабенко В. Г., Рудницький С. В. Метод синтезу операцій криптографічного перетворення на основі додавання за модулем два Системи обробки інформації: зб. наук. пр. Харків: ХУПС ім. І. Кожедуба, 2012. Вип. 3 (101), т. 1. С. 119–122.

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

96. Голуб С. В., Бабенко В. Г., Рудницький С. В., Мельник Р. П. Вдосконалення методу синтезу операцій криптографічного перетворення на основі дискретно-алгебраїчного представлення операцій. Системи управління, навігації та зв'язку : зб. наук. праць. Київ: Центр. наук.-досл. ін-т навігації і управл., 2012. Вип. 2 (22). С. 163–168.

97. Бабенко В. Г., Рудницький С. В. Реалізація методу захисту інформації на основі матричних операцій криптографічного перетворення. Системи обробки інформації: зб. наук. пр. Харків: ХУПС ім. І. Кожедуба, 2012. № 9 (107). С. 130–139.

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

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

100. Бабенко В. Г., Пивнева С. В., Мельник О. Г., Мельник Р. П. Параллельная реализация нелинейного расширенного матричного криптографического преобразования. Вектор науки Тольяттинского государственного. Тольятти: ТГУ, 2014. №3 (29). С. 17–19.

101. Рудницкий В. Н., Пивнева С. В., Бабенко В. Г., Стабецкая Т. А., Король К. В. Синтез модели обратной нелинейной операции расширенного матричного криптографического преобразования. Вектор науки Тольяттинского государственного университета. Тольятти: ТГУ, 2014. №4 (30). С. 18–21.

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

103. Рудницький В. М., Бабенко В. Г., Стабецька Т. А. Узагальнений метод синтезу обернених нелінійних операцій розширеного матричного криптографічного перетворення. Системи обробки інформації: зб. наук. пр. Харків: ХУПС ім. І. Кожедуба, 2014. Вип. 6 (122). С. 118–121.

104. Рудницький В.М. Операції криптографічного перетворення інформації в двійково-четвірковій системі числення / В.М. Рудницький, І.В. Миронець, В.В. Веретельник // Системи обробки інформації: зб. наук. праць – Вип. 3(101) – Х. : Харк. ун-т повітряних сил ім. Івана. Кожедуба, 2012. - С. 169-173.

105. Рудницький В.М. Метод криптографічного кодування інформації з введенням інформаційної надмірності на основі двохрозрядних логічних функцій / В.М. Рудницький, І.В. Миронець, В.В. Веретельник // Системи обробки інформації: зб. наук. праць – Вип. 4(102) – Х. : Харк. ун-т повітряних сил ім. Івана. Кожедуба, 2012. - С. 175-177.

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

107. Синтез елементарних функцій перестановок, керованих інформацією / В. М. Рудницький, Т. В. Миронюк, О. Г. Мельник, В. П. Щербина // Безпека інформації. – Т. 20, № 3. – Київ : НАУ, 2014. – С. 242–247.

108. Миронюк Т. В. Визначення елементарних операцій базової групи перестановок, керованих інформацією / Т. В. Миронюк // Вісник Черкаського державного технологічного університету. – 2016. – № 2. - С. 100–105.

109. Миронюк Т. В. Дискретна модель базових груп операцій перестановок, керованих інформацією, для криптоперетворення / Т. В. Миронюк, Є. В. Ланських // Smart and Young : щомісячний наук. журн. – Вип. 11-12. – Київ, 2016. – С. 58–65.

110. Миронюк Т. В. Апаратна реалізація операцій перестановки, керованих інформацією, для комп’ютерних криптографічних систем /

Т. В. Миронюк, І. В. Миронець // The scientific potential of the present : proceedings of the International Scientific Conference (St. Andrews, Scotland, UK, December 1, 2016) / ed. N. P. Kazmyna // NGO «European Scientifi Platform»/ - Vinnytsia : PE Rogalska I. O., 2016/ - P. 112–115.

111. Бабенко В. Г., Рудницький С. В., Мельник Р. П. Визначення множини трирозрядних елементарних операцій криптографічного перетворення. Вісник Інженерної академії України. Київ: Інтерсервіс, 2012. Вип. 3 (4). С. 77–79.

112. Бабенко В. Г., Мельник Р. П., Рудницький С. В. Дослідження способів запису трьохрозрядних криптографічних операцій. Системи управління, навігації та зв'язку: зб. наук. пр. Київ: Центр. наук.-досл. ін-т навігації і управл., 2012. Вип. 1 (21), т. 2. С. 170–173.

113. V. Rudnytskyi, I. Opirskyy, O. Melnyk, M. Pustovit The implementation of strict stable cryptographic coding operations Сучасні інформаційні системи Щоквартальний науково-технічнийй журнал – Х.: НТУ «ХПІ» 2019, Т 3, №4 С. 109-114.

114. Бабенко В. Г., Лада Н. В. Синтез і аналіз операцій криптографічного додавання за модулем два. Системи обробки інформації: зб. наук. пр. Харків: ХУПС ім. І. Кожедуба, 2014. Вип. 2 (118). С. 116–118.

115. Бабенко В. Г., Лада Н. В. Аналіз результатів виконання модифікованих операцій додавання за модулем два з точністю до перестановки. The scientific potential of the present: proceedings of the Internat. sci. conf., (St. Andrews, Scotland, UK, December, 1, 2016) / ed. N. P. Kazmyna. NGO «European Scientific Platform». Vinnytsia: PE Rogalska I. O., 2016. С. 108–111. (Шотландия, Логос)

116. Бабенко В. Г., Лада Н. В. Технологія дослідження операцій за модулем два. Smart and Young: щомісячний наук. журн. 2016. № 11–12. Ч. 1. С. 49–54.

117. Рудницкий В.Н., Фауре Э.В., Щерба А.И. Метод и критерий оценивания качества последовательностей случайных чисел. Кибернетика и

системный анализ. 2016. Том 52, № 2. С. 116-124. (переклад англ.: E.V. Faure, A.I. Shcherba, and V.M. Rudnytskyi. 2016. The Method and Criterion for Quality Assessment of Random Number Sequences. Cybernetics and Systems Analysis Volume 52, Issue 2 (March 2016), pp 277-284.) DOI: 10.1007/s10559-016-9824-3.

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

119. Лада Н. В., Козловська С. Г., Рудницький С. В. Побудова математичної групи симетричних операцій на основі додавання за модулем два. Сучасна спеціальна техніка: науково-практичний журнал. Київ, 2019. № 4 (59). С. 33-41.

120. Лада Н. В., Рудницький С. В., Зажома В. М., Рудницька Ю. В. Дослідження і синтез групи симетричних модифікованих операцій правостороннього додавання за модулем чотири. Системи управління, навігації та зв'язку. Збірник наукових праць. Полтава: ПНТУ, 2020. № 1 (59). С. 93-96. - doi:https://doi.org/ 10.26906/SUNZ.2020.1.093

121. Fedotova-Piven I.M. The inversion method of four-bit boolean sac cryptotransforms / I.M. Fedotova-Piven, V.M. Rudnitskiy, O.B. Piven, T.V. Mironyuk // Radio Electronics, Computer Science, Control.- NU «Zaporizhzhia Polytechnic». - 2019. - № 4(51). – P. 199-210. DOI10.15588/1607-3274-2019-4-19 p-ISSN 2313-688X.

122. Лада Н. В., Козловська С. Г. Застосування операцій криптографічного додавання за модулем два з точністю до перестановки в потокових шифрах. Системи управління, навігації та зв'язку: зб. наук. праць. Полтава: ПНТУ, 2018. Т. 1 (47). С. 127-130. - doi:https://doi.org/10.26906/SUNZ.2018.1.127

123. Конхейм А. Г. Основы криптографии/ Конхейм А. Г. –М.: Радио и связь, 1987. –412 с.

124. Коркішко Т., Мельник А. Алгоримти та процесори симметричного блокового шифрування. – Львів, БаК, 2003.-163 с.

125. Рудницький В. М., Лада Н. В., Федотова-Півень І. М., Пустовіт М. О., Нестеренко О.Б. Побудова двохрозрядних двохоперандних операцій строгого стійкого криптографічного кодування. Системи управління, навігації та зв'язку. Збірник наукових праць. – Полтава: ПНТУ, 2018. – Т. 6 (52). – С. 113-115. - doi:https://doi.org/10.26906/SUNZ.2018.6.113.

126. Шнайер Б. Прикладная криптография. Протоколы, алгоритмы, исходные тексты на языке Си. М.: Триумф, 2003. 806 с.

127. Рудницький В.М., Опірський І.Р., Мельник О.Г., Пустовіт М.О. Синтез групи операцій строгого стійкого криптографічного кодування для побудови потокових шифрів. Ukrainian Scientific Journal of Information Security, 2018, vol.24, issue3, pp.195-200.

ДОДАТОК А

Список публікацій здобувача за темою дисертації

1. Бреус Р. В. Синтез двохрозрядних двохоперандних операцій строгого стійкого криптографічного кодування шляхом перетворення другого операнда. *Системи управління, навігації та зв'язку*. Полтава: ПНТУ, 2019. Вип. 5 (57). С 29–32.

2. Рудницький В. М., Бреус Р. В., Лада Н. В. Генерація послідовностей операцій криптографічного перетворення. *Вісник Інженерної академії України.* Київ, 2019. Вип. 3. С.75–80.

3. Rudnitsky V., Berdibayev R., Breus R., Lada N., Pustovit M. Synthesis of reverse two-bit dual-operated strictly straight cryptographic coding on the basis of another operation. *Advanced Information Systems:* Quarterly scientific and technical journal. Kharkiv: National Technical University «Kharkiv Polytechnic Institute», 2019. Vol. 3, No. 4, pp. 109–114.

4. Lada N., Dzyuba V., Breus R., Lada S. Synthesis of sets of non-symmetric two-operand two-bit crypto operations within the permutation accuracy. *Technology audit and production reserves.* № 2/2(52), 2020, pp. 28–31.

5. Лада Н. В., Бреус Р. В., Лада С. В. Генерація моделей прямих і обернених двохрозрядних двохоперандних операцій строгого стійкого криптографічного кодування. *Science and Education a New Dimension Natural and Technical Science.* Budapest, 2020. V. 238, p. 27–30.

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

7. Бреус Р. В. Уніфікація опису операцій криптографічного перетворення. *Проблеми інформатизації: матеріали Четвертої міжнар. наук.-техн. конф.*: тези доп., (Черкаси – Баку – Бельсько-Бяла – Полтава, 3–4 листоп. 2016 р.). Черкаси: ЧДТУ, 2016. С. 9.

8. Бреус Р.В. Математичні моделі побудови операцій розширеного матричного криптографічного перетворення. *Проблеми інформатизації: матеріали П'ятої міжнар. наук.-техн. конф.*: тези доп., (Черкаси – Баку – Бельсько-Бяла – Полтава, 13-15 листоп. 2017 р.). Черкаси: ЧДТУ, 2017. С. 13.

9. Лада Н. В., Бреус Р. В., Рудницька Ю. В., Висоцький С. В. Аналіз групи двоопераднних симетричних криптовалютних операцій. *Проблеми інформатизації: матеріали Сьомої міжнар. наук.-техн. конф*.: тези доп., (Черкаси – Харків – Баку – Бельсько-Бяла, 13–15 листопада 2019 р.). Черкаси: ЧДТУ; Баку: ВА ЗС АР, Бельсько-Бяла: УТіГН, Харків: НТУ «ХПІ», 2019., Т.1, С. 85.

10. Jancarczyk D., Rudnytskyi V., Breus R., Pustovit M., Veselska O. and Ziubina R. Two-Operand Operations of Strict Stable Cryptographic Coding With Different Operands' Bits. *The 5-th IEEE International Symposium on Smart and Wireless Systems within the International Conferences on Intelligent Data Acquisition and Advanced Computing Systems*, 2020, Dortmund, Germany.

Відомості про апробацію результатів дисертації

1. Бреус Р. В. Уніфікація опису операцій криптографічного перетворення. *Проблеми інформатизації: матеріали Четвертої міжнар. наук.-техн. конф.*: тези доп., (Черкаси – Баку – Бельсько-Бяла – Полтава, 3–4 листоп. 2016 р.). Черкаси: ЧДТУ, 2016. С. 9.

2. Бреус Р.В. Математичні моделі побудови операцій розширеного матричного криптографічного перетворення. *Проблеми інформатизації: матеріали П'ятої міжнар. наук.-техн. конф.*: тези доп., (Черкаси – Баку – Бельсько-Бяла – Полтава, 13-15 листоп. 2017 р.). Черкаси: ЧДТУ, 2017. С. 13.

3. Лада Н. В., Бреус Р. В., Рудницька Ю. В., Висоцький С. В. Аналіз групи двоопераднних симетричних криптовалютних операцій. *Проблеми інформатизації: матеріали Сьомої міжнар. наук.-техн. конф.*: тези доп., (Черкаси – Харків – Баку – Бельсько-Бяла, 13–15 листопада 2019 р.). Черкаси: ЧДТУ; Баку: ВА ЗС АР, Бельсько-Бяла: УТіГН, Харків: НТУ «ХПІ», 2019., Т.1, С. 85.

4. Jancarczyk D., Rudnytskyi V., Breus R., Pustovit M., Veselska O. and Ziubina R. Two-Operand Operations of Strict Stable Cryptographic Coding With Different Operands' Bits. *The 5-th IEEE International Symposium on Smart and Wireless Systems within the International Conferences on Intelligent Data Acquisition and Advanced Computing Systems*, 2020, Dortmund, Germany.

ДОДАТОК Б

«ЗАТВЕРДЖУЮ»
Ректор Черкаського
державного технологічного
університету

_____ О.О. Григор

«10» 03 2019р

АКТ
впровадження результатів дисертаційної роботи
Бреус Роксолани Василівни в навчальний процес
Черкаського державного технологічного університету

Комісія у складі: завідувача кафедри інформаційної безпеки та комп'ютерної інженерії д.т.н., професора Рудницького В.М., доцента кафедри інформаційної безпеки та комп'ютерної інженерії к.т.н., доцента Хрульова М.В. старшого викладача кафедри інформаційної безпеки та комп'ютерної інженерії к.т.н., Лади Н.В., проаналізувавши дисертаційне дослідження Бреус Роксолани Василівни, встановила наступне:

1. При підготовці бакалаврів за напрямом 125 «Кібербезпека» в курсі лекцій з дисциплін «Комплексні системи захисту інформації» та «Програмний захист інформації в інформаційно-комунікаційних системах» використовуються результати дисертаційного дослідження:

- метод синтезу обернених двохрозрядних двохоперандних операцій строгого стійкого криптографічного кодування на основі перетворення другого операнда шляхом реалізації моделі автомата побудови другого операнда оберненої операції;
- синтез групи двохрозрядних двохоперандних операцій строгого стійкого криптографічного кодування на основі перетворення другого операнда відомої операції шляхом виконання над ним двохрозрядної одноопераднодної операції.

2. При виконанні дипломних та курсових робіт використовуються запропоновані методи синтезу прямих та обернених двохрозрядних двохоперандних операцій строгого стійкого криптографічного кодування на основі перетворення другого операнда.

Завідувач кафедри ІБ та КІ, д.т.н., проф. Рудницького В.М.
Доцент кафедри ІБ та КІ, к.т.н., доц. Хрульов М.В.
Старший викладач кафедри ІБ та КІ, к.т.н. Лада Н.В.

«ЗАТВЕРДЖУЮ»
Керівник відділення № 6
ТОВ «Нова пошта» м. Черкаси
_____ І.В. Пахар
«15» 12 2021 р

АКТ

впровадження результатів дисертаційної роботи

Бреус Роксолани Василівни

на ТОВ «Нова пошта»

Для підвищення захисту особистих даних працівників та клієнтів пошти, а також захисту оплати послуг були використані наступні результати дисертаційного дослідження, отримані Бреус Роксоланою Василівною:

- метод синтезу групи двохрозрядних двохоперандних операцій строгого стійкого криптографічного кодування на основі перетворення другого операнда відомої операції шляхом виконання над ним двохрозрядної одноопераднної операції;

- метод синтезу обернених двохрозрядних двохоперандних операцій строгого стійкого криптографічного кодування на основі перетворення другого операнда у вигляді реалізації моделі автомата побудови другого операнда оберненої операції.

Керівник відділення № 6
ТОВ «Нова пошта» м. Черкаси І.В. Пахар

«ЗАТВЕРДЖУЮ»
Головний лікар
КНП «Черкаська міська
консультативно-діагностична
поліклініка» (філія №2)

_____ В.В.Шевченко

«10» 06 2020р

АКТ

впровадження результатів дисертаційної роботи

Бреус Роксолани Василівни

в КНП «Черкаська міська консультативно-діагностична поліклініка»

(філія №2)

Для забезпечення захисту персональних даних персоналу та пацієнтів в організації були використані наступні наукові результати, отримані. Бреус Роксоланою Василівною, зокрема:

- метод синтезу групи ДДО ССКК на основі перетворення другого операнда відомої операції;

- метод синтезу обернених двохрозрядних двохоперандних операцій строгого стійкого криптографічного кодування на основі перетворення другого операнда шляхом реалізації моделі автомата побудови другого операнда оберненої операції.

Головний лікар
КНП «ЧМКДП»
(філія №2) В.В. Шевченко

«ЗАТВЕРДЖУЮ»
Голова правління
ПАТ «Черкасиобленерго»

_____ О.Г.Самчук

«30» 12 2019 р

АКТ

впровадження результатів дисертаційної роботи

Бреус Роксолани Василівни

на ПАТ «Черкасиобленерго»

Для підвищення захисту персональних даних працівників підприємства та клієнтів, були використані такі наукові результати, одержані Бреус Роксоланою Василівною:

- метод синтезу групи двохрозрядних двохоперандних операцій строгого стійкого криптографічного кодування на основі перетворення другого операнда відомої операції шляхом виконання над ним двохрозрядної одноопераднної операції;

- метод генерації псевдовипадкових послідовностей ДДО ССКК на основі перетворення другого операнда.

Голова правління
ПАТ «Черкасиобленерго» О.Г. Самчук