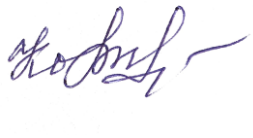
ЧЕРКАСЬКИЙ ДЕРЖАВНИЙ ТЕХНОЛОГІЧНИЙ УНІВЕРСИТЕТ

КОЗЛОВСЬКА Світлана Григорівна



УДК 004.421.5:004.056.55

МЕТОДИ СИНТЕЗУ ГРУП СИМЕТРИЧНИХ ОПЕРАЦІЙ ДЛЯ ПОТОКОВОГО ШИФРУВАННЯ

05.13.05 – комп’ютерні системи і компоненти

Автореферат

дисертації на здобуття наукового ступеня

кандидата технічних наук

Черкаси – 2019

Дисертацією є рукопис.

Роботу виконано в Черкаському державному технологічному університеті Міністерства освіти і науки України.

Науковий керівник: доктор технічних наук, професор
Рудницький Володимир Миколайович,
Черкаський державний технологічний університет,
завідувач кафедри інформаційної безпеки та
комп'ютерної інженерії.

Офіційні опоненти: доктор технічних наук, професор,
Кулик Анатолій Ярославович,
Вінницький національний медичний університет
ім. М. І. Пирогова, завідувач кафедри біофізики,
інформатики та медичної апаратури;

доктор технічних наук, професор
Пархуць Любомир Теодорович,
Національний університет «Львівська політехніка»,
професор кафедри захисту інформації.

Захист відбудеться «27» *червня* 2019 р. о 10^{00} на засіданні спеціалізованої вченої ради К 73.052.04 при Черкаському державному технологічному університеті за адресою: 18006, Черкаси, бульвар Шевченка, 460.

З дисертацією можна ознайомитися в бібліотеці Черкаського державного технологічного університету за адресою: 18006, Черкаси, бульвар Шевченка, 460.

Автореферат розіслано «27» *травня* 2019 р.

Учений секретар
спеціалізованої вченої ради Е. В. Фауре

ЗАГАЛЬНА ХАРАКТЕРИСТИКА РОБОТИ

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

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

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

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

Попри це, задачі синтезу груп симетричних двохоперандних операцій потокового шифрування не було розглянуто. Таким чином, можна стверджувати, що тема дисертаційного дослідження «Методи синтезу груп симетричних операцій для потокового шифрування» є актуальною.

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

Дисертаційна робота виконана відповідно до Постанови Президії НАНУ від 25.02.2009 р. № 55 «Про основні наукові напрями та найважливіші проблеми фундаментальних досліджень у галузі природничих, технічних і гуманітарних наук на 2009 - 2013 рр.» (п. 1.2.7.1. Розробка методів та інформаційних технологій розв’язання задач комп’ютерної криптографії та стеганографії; п. 1.2.7.2. Розробка методів підвищення продуктивності систем асиметричної криптографії), Постанови Президії НАНУ від 20.12.13 №179 «Основні наукові напрями та найважливіші проблеми фундаментальних досліджень у галузі природничих, технічних і гуманітарних наук Національної академії наук України на 2014-2018 рр.», а саме – пп. 1.2.8.1. «Розробка методів та інформаційних технологій розв’язання задач комп’ютерної криптографії та стеганографії», а також Постанови КМУ від 7

вересня 2011 року №942 «Про затвердження переліку пріоритетних тематичних напрямів наукових досліджень і науково-технічних розробок на період до 2020 року», а саме – «Технології та засоби захисту інформації». Результати дисертаційної роботи включені в НДР «Метод синтезу швидкодіючих систем захисту інформації на основі спеціалізованих логічних функцій» (ДР № 0108U000506), «Метод синтезу механізмів захисту інформації в спеціалізованих автоматизованих системах» (ДР № 0108U000508), «Синтез операцій криптографічного перетворення з заданим характеристиками» (ДР № 0116U008714), в яких автор брав участь як виконавець.

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

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

– розробити метод побудови та дослідження двохоперандних операцій криптоперетворення;

– розробити методи синтезу груп симетричних двохрозрядних двохоперандних операцій потокового шифрування;

– удосконалити метод підвищення стійкості й надійності потокового шифрування та оцінити його ефективність.

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

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

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

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

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

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

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

потоковому шифруванні;

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

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

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

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

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

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

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

Особистий внесок здобувача. Усі нові результати дисертаційної роботи автор отримав самостійно. У опублікованих у співавторстві наукових працях з питань, що стосуються цього дослідження, автору належать: проведення аналізу та дослідження властивостей результатів шифрування фрагменту інформації, здійсненого на основі поєднання матричних операцій криптоперетворення [1], проведення побудови удосконалених моделей двохоперандних операцій криптографічного перетворення інформації [2, 6], проведення оцінки результатів застосування операцій потокового шифрування за їхнього випадкового вибору на

основі додаткової гамуючої послідовності [3], виконання узагальнення експериментальних досліджень результатів тестування псевдовипадкових послідовностей за різних алгоритмів і операцій реалізації [5], розгляд можливості підвищення стійкості до лінійного криптоаналізу за рахунок використання результатів попереднього перетворення в якості гамуючої послідовності для вибору операцій під час захисту програм [7], проведення побудови та узагальнення перестановочних схем операцій [12]. Результати, опубліковані в [4, 8-11], отримано одноосібно.

Апробація результатів дисертації. Результати дисертаційної роботи доповідалися й обговорювалися на Першій міжнародній науково-технічній конференції «Проблеми інформатизації» (Черкаси – Київ – Тольятті – Полтава, 2013), Науково-практичній конференції «Теоретико-методологічні і науково-практичні засади інформаційного, фінансового та облікового забезпечення розвитку економіки» (Черкаси, 2013), Міжнародній науково-практичній конференції «Проблеми моделювання структури і процесів економічних систем» (Черкаси, 2014), Науково-практичній конференції «Управління економіко-соціальними системами розвитку суспільства в умовах євроінтеграції» (Черкаси, 2015), Всеукраїнській науково-практичній конференції «Фінансово-економічне та обліково-аналітичне забезпечення підприємницької діяльності» (Черкаси, 2016), Шостій міжнародній науково-технічній конференції «Проблеми інформатизації» (Черкаси – Баку – Бельсько-Бяла – Харків, 2018).

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

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

ОСНОВНИЙ ЗМІСТ РОБОТИ

У **вступі** обґрунтовано актуальність теми, сформульовано мету дослідження та визначено задачі для її реалізації, наведено наукову новизну і практичне значення дисертаційної роботи.

У **першому розділі** розглянуто сучасний стан та перспективи розвитку методів синтезу й аналізу операцій криптографічного перетворення для захисту конфіденційної інформації. Показано, що наразі криптографія залишається основним засобом захисту конфіденційної інформації. Наведено основні терміни й визначення, необхідні для проведення дисертаційного дослідження. Розглянуто класифікації криптографічних методів та проаналізовано шляхи розвитку комп’ютерної криптографії.

Визначено, що одним із перспективних напрямів розвитку систем криптографічного захисту інформації є використання операцій криптографічного перетворення на основі логічних функцій. Розглянуто сучасний стан досліджень операцій криптографічного перетворення інформації з акцентуванням на особливостях застосування в потоковому та блочному шифруваннях.

Наведено результати бібліографічного пошуку та огляду основних результатів досліджень, пов'язаних із синтезом та аналізом операцій криптографічного перетворення інформації. Встановлено, що двохоперандним операціям криптографічного перетворення інформації, спеціалізованих для потокового шифрування, не приділено достатньої уваги. Множину цих операцій необхідно досліджувати й розширювати, розвивати методи їх синтезу, оскільки їхнє використання забезпечує підвищення стійкості й надійності потокових шифрів. Наведено теоретичні передумови та результати проведення обчислювального експерименту, в результаті якого на основі перебору розраховано повну множину таблиць істинності симетричних двохрозрядних двохоперандних операцій крипто перетворення, а також основні відомі й фрагментарні результати дослідження цих операцій. На основі проведеного аналізу сформульовано мету й задачі наукового дослідження.

Другий розділ присвячено математичному моделюванню та дослідженню двохоперандних операцій криптографічного перетворення інформації на основі відомих таблиць істинності.

Для забезпечення ефективності проведення досліджень проаналізовано та класифіковано таблиці істинності симетричних двохрозрядних двохоперандних операцій криптоперетворення. Результати класифікації двохрозрядних двохоперандних операцій криптоперетворення наведено в табл. 1. Кожна з наведених двохоперандних операцій є операцією вибору однієї з чотирьох одноопераднних операцій перетворення першого операнда (x_1, x_2) залежно від значення другого операнда (y_1, y_2), який виконує функцію команд управління $(y_1 = k_1, y_2 = k_2)$. Послідовність одноопераднних операцій для їхнього вибору представлено послідовністю індексів операції. Взаємозв'язок індексів двохоперандної операції з моделями одноопераднних операцій наведено в табл. 2.

На основі унікальності наборів одноопераднних операцій в табл. 1 наведено операції, розбиті на 24 набори двохоперандних операцій (НДО) по чотири операції в кожному наборі. Всім наборам двохоперандних операцій присвоєно порядковий номер. Крім того, всі операції поділено на чотири математичні групи.

Для подальшого дослідження обрано операції першої групи. Як приклад розглянемо та дослідимо одну з операцій першого НДО.

Таблиця 1

Класифікація моделей двохоперандних операцій криптоперетворення інформації, отриманих за результатами експерименту

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

Представимо математичну модель операції $O_{13,19,1,7}$:

$$O_{13,19,1,7}=\begin{cases}F_{13}^{k},\ якщо k_1=0;\ k_2=0\\ F_{19}^{d}, якщо k_1=0;\ k_2=1\\ F_{1}^{k},\ якщо k_1=1;\ k_2=0\\ F_{7}^{d}, якщо k_1=1;\ k_2=1\end{cases}=\begin{cases}\begin{bmatrix}x_1\\x_2\end{bmatrix}\oplus\begin{bmatrix}1\\0\end{bmatrix},\ якщо k_1=0;\ k_2=0\\ \begin{bmatrix}x_1\\x_2\end{bmatrix}\oplus\begin{bmatrix}1\\1\end{bmatrix}, якщо k_1=0;\ k_2=1\\ \begin{bmatrix}x_1\\x_2\end{bmatrix}\oplus\begin{bmatrix}0\\0\end{bmatrix},\ якщо k_1=1;\ k_2=0\\ \begin{bmatrix}x_1\\x_2\end{bmatrix}\oplus\begin{bmatrix}0\\1\end{bmatrix}, якщо k_1=1;\ k_2=1\end{cases}=\begin{cases}\begin{bmatrix}x_1\oplus1\\x_2\end{bmatrix},\ якщо k_1=0;\ k_2=0\\ \begin{bmatrix}x_1\oplus1\\x_2\oplus1\end{bmatrix}, якщо k_1=0;\ k_2=1\\ \begin{bmatrix}x_1\\x_2\end{bmatrix},\ якщо k_1=1;\ k_2=0\\ \begin{bmatrix}x_1\\x_2\oplus1\end{bmatrix}, якщо k_1=1;\ k_2=1\end{cases}$$

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

$$O_{13,19,1,7}=\begin{cases}\begin{bmatrix}x_1\oplus1\\x_2\end{bmatrix}=\begin{bmatrix}x_1\oplus k_1\oplus1\\x_2\oplus k_2\end{bmatrix},\ якщо k_1=0;\ k_2=0\\ \begin{bmatrix}x_1\oplus1\\x_2\oplus1\end{bmatrix}=\begin{bmatrix}x_1\oplus k_1\oplus1\\x_2\oplus k_2\end{bmatrix}, якщо k_1=0;\ k_2=1\\ \begin{bmatrix}x_1\\x_2\end{bmatrix}=\begin{bmatrix}x_1\oplus k_1\oplus1\\x_2\oplus k_2\end{bmatrix},\ якщо k_1=1;\ k_2=0\\ \begin{bmatrix}x_1\\x_2\oplus1\end{bmatrix}=\begin{bmatrix}x_1\oplus k_1\oplus1\\x_2\oplus k_2\end{bmatrix}, якщо k_1=1;\ k_2=1\end{cases}=\begin{bmatrix}x_1\oplus k_1\oplus1\\x_2\oplus k_2\end{bmatrix}=\begin{bmatrix}x_1\oplus y_1\oplus1\\x_2\oplus y_2\end{bmatrix}$$

Таблиця 2

Моделі двохрозрядних одноопераднних операцій криптоперетворення інформації для дослідження двохоперандних операцій

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

Як зрозуміло з отриманого виразу, реалізація операції $O_{13,19,1,7}$ призведе до порозрядного додавання за модулем два першого й другого операндів з додатковим інвертуванням першого біту результату. Під час процесу математичного перетворення отримано модель двохоперандної операції, яка може бути зреалізована як на апаратному, так і на програмному рівнях.

Розглянемо та дослідимо одну з операцій третього НДО, наприклад, $O_{15,21,9,3}$:

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

$$=\begin{bmatrix}x_1\oplus k_1\oplus 1\\ x_1\oplus x_2\oplus k_1\oplus k_2\end{bmatrix}=\begin{bmatrix}x_1\oplus y_1\oplus 1\\ x_1\oplus x_2\oplus y_1\oplus y_2\end{bmatrix}$$

Розглянемо та дослідимо одну з операцій п’ятого НДО, наприклад, $O_{11,17,5,23}$:

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

$$=\begin{bmatrix}x_2\oplus k_2\\ x_1\oplus x_2\oplus k_1\oplus k_2\oplus 1\end{bmatrix}=\begin{bmatrix}x_2\oplus y_2\\ x_1\oplus x_2\oplus y_1\oplus y_2\oplus 1\end{bmatrix}$$

Під час дослідження встановлено, що будь-яку з операцій НДО першої групи можна отримати з довільної операції цього НДО на основі перестановочних схем. На рис. 1 наведено перестановочну схему для побудови операції $O_{15,21,9,3}$ на основі операції $O_{3,9,21,15}$ в НДО 3, а на рис. 2 – перестановочну схему для побудови операції $O_{11,17,5,23}$ з операції $O_{5,23,11,17}$ в НДО 5.

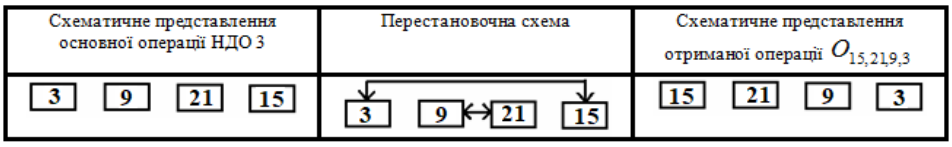


Рис.1. Перестановочна схема побудови операції $O_{15,21,9,3}$ з операції $O_{3,9,21,15}$

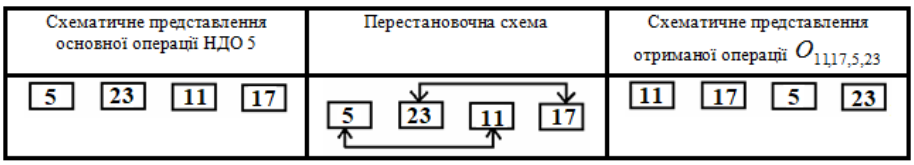


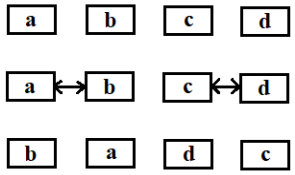
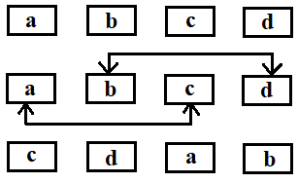
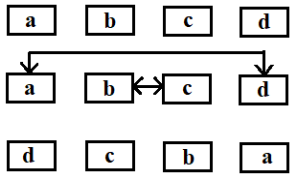
Рис.2. Перестановочна схема побудови операції $O_{11,17,5,23}$ з операції $O_{5,23,11,17}$

В процесі дослідження побудовано математичні моделі для всіх операцій першої математичної групи, а також перестановочні схеми побудови цих

операцій. На основі аналізу отриманих результатів побудовано узагальнені перестановочні схеми для першої математичної групи двохоперандних операцій криптоперетворення, представлені в табл. 3.

Таблиця 3

Узагальнені перестановочні схеми для першої математичної групи двохоперандних операцій криптоперетворення

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

Неодноразово використана послідовність математичних перетворень експериментальних даних, яка забезпечує отримання придатних для застосування двохоперандних операцій криптоперетворення в сукупності з перестановочними схемами візуалізації побудови операцій, є методом побудови та дослідження двохоперандних операцій криптоперетворення на основі результатів обчислювального експерименту.

В процесі дослідження встановлено, що перестановочні схеми побудови таблиць істинності наборів двохоперандних операцій криптоперетворення першої математичної групи не перетинаються. Сукупність наборів таблиць істинності двохоперандних операцій криптоперетворення першої математичної групи створюють повну групу наборів таблиць істинності двохоперандних операцій криптоперетворення.

Застосування цієї групи перестановочних схем забезпечує побудову повної групи операцій криптоперетворення на основі будь-якої з операцій цієї групи, а також забезпечує побудову повної групи таблиць підстановок.

Отримані результати дозволили зробити таке припущення: якщо взяти будь-яку операцію з цієї невідомої групи, то застосування побудованої групи перестановочних схем забезпечить побудову повної групи наборів двохоперандних

операцій криптоперетворення невідомої групи. Для підтвердження цієї гіпотези необхідно провести додаткове дослідження принаймні ще однієї математичної групи операцій.

Третій розділ присвячено дослідженню другої математичної групи двохоперандних операцій криптоперетворення.

Дослідження проведено шляхом застосування методу побудови та дослідження двохоперандних операцій криптоперетворення на основі результатів обчислювального експерименту.

Дослідимо декілька операцій з НДО 12, наприклад $O_{15,24,9,6}$ та $O_{24,9,6,15}$:

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

$$=\begin{bmatrix}x_1\oplus x_2\oplus k_1\oplus k_2\oplus 1\\ x_1\oplus k_1\end{bmatrix}=\begin{bmatrix}x_1\oplus x_2\oplus y_1\oplus y_2\oplus 1\\ x_1\oplus y_1\end{bmatrix}$$

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

$$=\begin{bmatrix}x_1\oplus x_2\cdot \bar{k}_2\oplus k_1\oplus k_2\oplus 1\\ x_1\oplus x_2\cdot k_2\oplus k_1\oplus 1\end{bmatrix}=\begin{bmatrix}x_1\oplus x_2\cdot \bar{y}_2\oplus y_1\oplus y_2\oplus 1\\ x_1\oplus x_2\cdot y_2\oplus y_1\oplus 1\end{bmatrix}$$

Перестановочні схеми побудови цих операцій на основі операції $O_{6,15,24,9}$ наведено на рис. 3 та рис. 4.

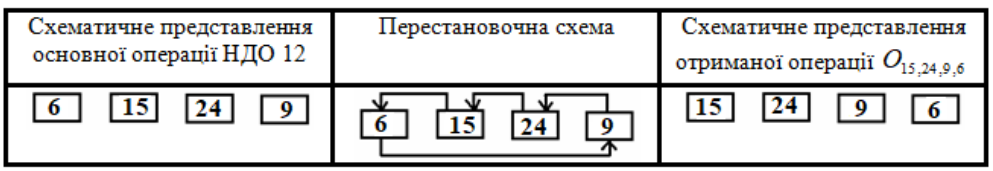


Рис. 3. Перестановочна схема побудови операції $O_{15,24,9,6}$ з операції $O_{6,15,24,9}$

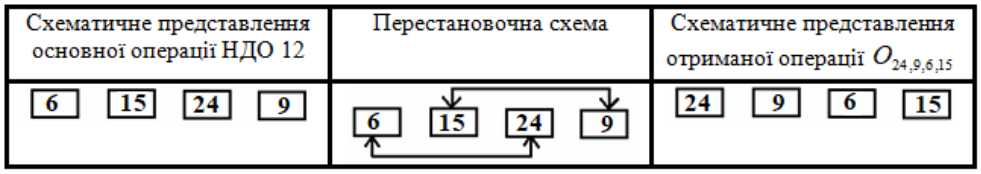


Рис. 4. Перестановочна схема побудови операції $O_{24,9,6,15}$ з операції $O_{6,15,24,9}$

Досліджено всю множину операцій другої групи.

Узагальнені перестановочні схеми побудови операцій цієї групи наведено в табл.4.

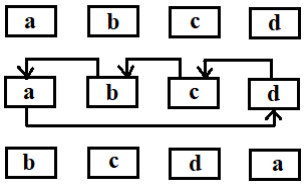
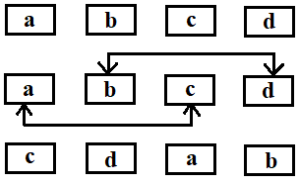
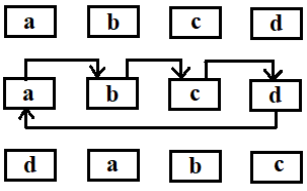
Перестановочні схеми для побудови таблиць істинності різних НДО з різних математичних груп наведено в табл. 5 і табл. 6.

В процесі дослідження перестановочних схем таблиць істинності встановлено:

- сукупність наборів таблиць істинності двохоперандних операцій криптоперетворення другої математичної групи створюють повну групу наборів таблиць істинності двохоперандних операцій криптоперетворення;
- встановлено, що групи перестановочних схем першої та другої математичної групи досліджених операцій криптоперетворення співпадають;
- отримано підтвердження припущення про те, що застосування повної групи перестановочних схем забезпечить побудову повної групи наборів двохоперандних операцій криптоперетворення невідомої групи та їх таблиць підстановки, якщо взяти будь-яку операцію з цієї невідомої групи.

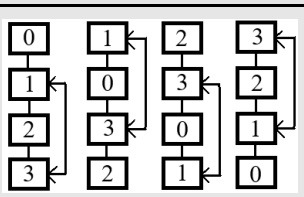
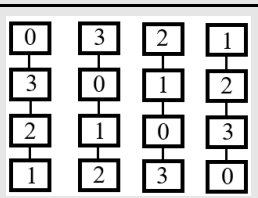
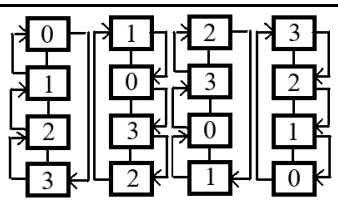
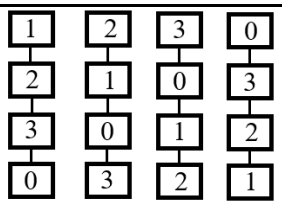
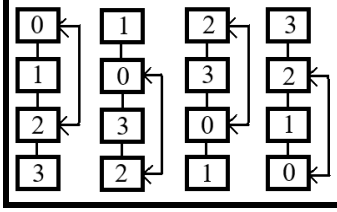
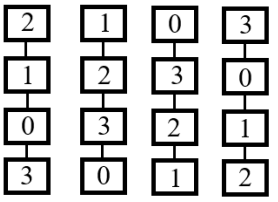
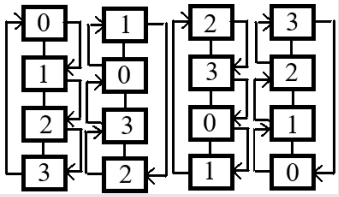
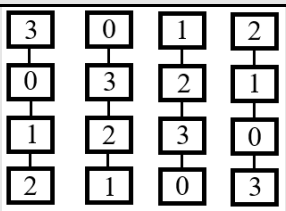
Таблиця 4

Узагальнені перестановочні схеми для першої математичної групи двохоперандних операцій криптоперетворення

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

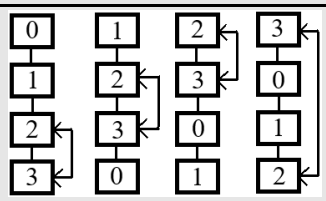
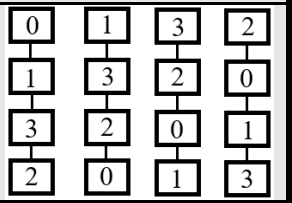
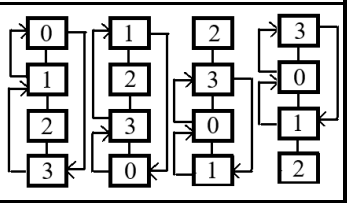
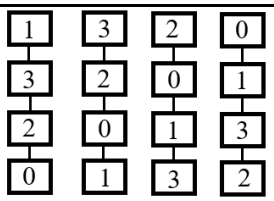
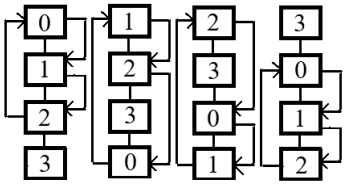
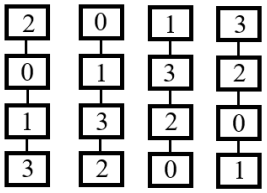
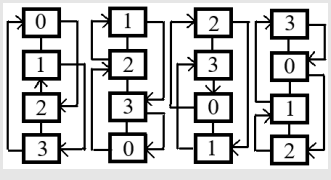
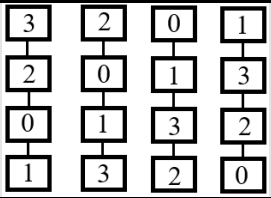
Таблиця 5

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

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

Таблиця 6

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

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

Четвертий розділ присвячено синтезу груп двохоперандних операцій криптоперетворення та оцінюванню ефективності їхнього застосування. Після узагальнення результату дослідження моделей операцій першої групи отримано класифікацію операцій з поділом на базові операції, поєднання базових операцій з операціями перестановки та поєднання базових операцій з операціями перестановки та інверсії. Ця класифікація (наведено в табл. 7) стала основою для розроблення методу синтезу груп двохрозрядних двохоперандних операцій для симетричного потокового шифрування, що полягає в:

- синтезі двохоперандних операцій базової групи на основі додавання за модулем два одноопераднних операцій обробки кожного операнда. Перетворення виконано на основі моделі $F = \begin{bmatrix} k_1 \\ k_2 \end{bmatrix}$. Це наведено в табл. 7;
- виконанні над операціями базової групи операцій перестановок;
- виконанні над операціями базової групи в поєднанні з операціями перестановок операцій інверсії.

Оскільки основною операцією цієї групи є операція додавання за модулем два, то й групу було названо симетричною групою двохоперандних двохрозрядних операцій криптографічного додавання за модулем два.

За аналогією з цим методом розроблено метод синтезу симетричної групи двохоперандних двохрозрядних операцій криптографічного додавання за модулем чотири, оскільки основною операцією другої групи є операція додавання за модулем чотири. Ці методи відрізняються синтезом операцій базової групи. Замість моделі: $F = \begin{bmatrix} k_1 \\ k_2 \end{bmatrix}$ використано модель $F = \begin{bmatrix} k_1 \oplus x_2 \cdot k_2 \\ k_2 \end{bmatrix}$, тобто:

$$O_{1,8,13,20} = F_{3,5}^{1} \oplus F_{nk}^{2.1} = \begin{bmatrix} x_1 \\ x_2 \end{bmatrix} \oplus \begin{bmatrix} k_1 \oplus x_2 \cdot k_2 \\ k_2 \end{bmatrix} = \begin{bmatrix} x_1 \oplus x_2 \cdot k_2 \oplus k_1 \\ x_2 \oplus k_2 \end{bmatrix}$$

$$O_{2,19,14,7} = F_{6,5}^{1} \oplus F_{nk}^{2.2} = \begin{bmatrix} x_1 \oplus x_2 \\ x_2 \end{bmatrix} \oplus \begin{bmatrix} x_2 \cdot k_2 \oplus k_1 \oplus k_2 \\ k_2 \end{bmatrix} = \begin{bmatrix} x_1 \oplus x_2 \oplus x_2 \cdot k_2 \oplus k_1 \oplus k_2 \\ x_2 \oplus k_2 \end{bmatrix} = \begin{bmatrix} x_1 \oplus x_2 \cdot \overline{k_2} \oplus k_1 \oplus k_2 \\ x_2 \oplus k_2 \end{bmatrix}$$

$$O_{3,12,21,18} = F_{3,6}^{1} \oplus F_{nk}^{2.3} = \begin{bmatrix} x_1 \\ x_1 \oplus x_2 \end{bmatrix} \oplus \begin{bmatrix} x_2 \cdot k_2 \oplus k_1 \\ x_2 \cdot k_2 \oplus k_1 \oplus k_2 \end{bmatrix} = \begin{bmatrix} x_1 \oplus x_2 \cdot k_2 \oplus k_1 \\ x_1 \oplus x_2 \oplus x_2 \cdot k_2 \oplus k_1 \oplus k_2 \end{bmatrix} = \begin{bmatrix} x_1 \oplus x_2 \cdot k_2 \oplus k_1 \\ x_1 \oplus x_2 \cdot \overline{k_2} \oplus k_1 \oplus k_2 \end{bmatrix}$$

Результати синтезу цієї групи операцій наведено в табл. 8.

Схемотехнічну реалізацію синтезованих груп операцій наведено на рис. 7.

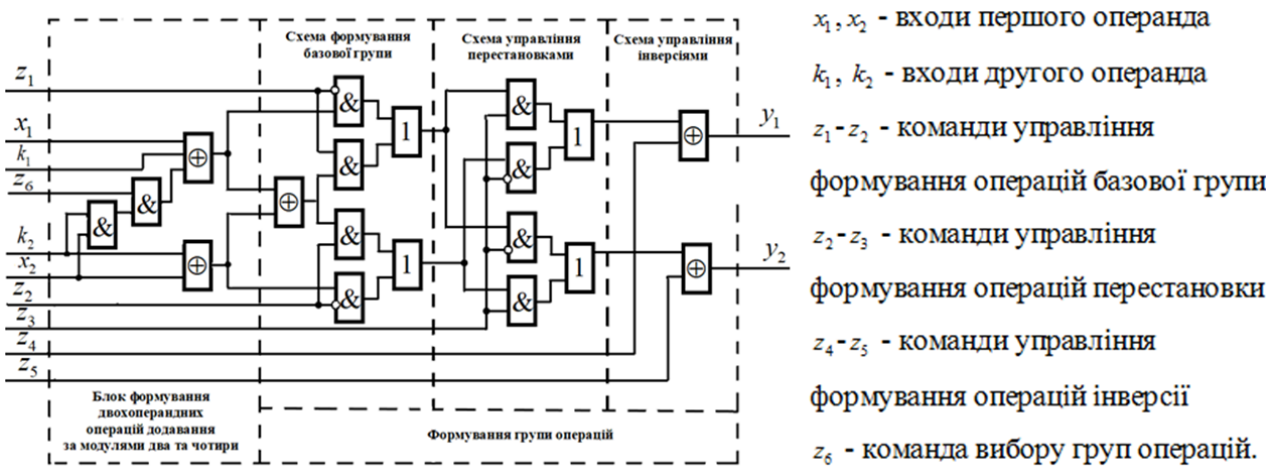


Рис. 7. Функціональна схема пристрою реалізації груп операцій додавання за модулями два та чотири

Під час дослідження встановлено, що побудований пристрій доцільно застосовувати в блоці криптоперетворення під час реалізації методу підвищення стійкості та надійності потокового шифрування (рис. 8). Зведені результати тестування програмної реалізації цього методу наведено в табл. 9.

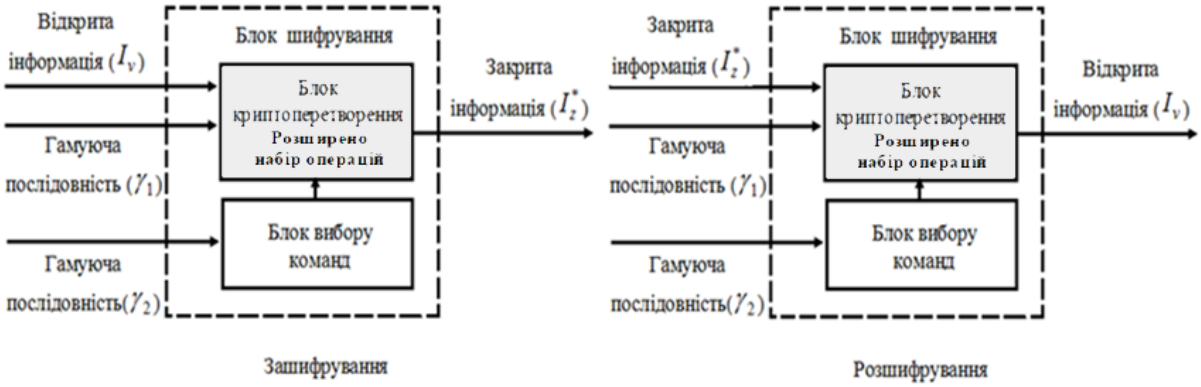


Рис.8. Застосування синтезованих груп операцій в методі підвищення стійкості та надійності потокового шифрування

Таблиця 9

Зведені результати тестування методу підвищення стійкості та надійності потокового шифрування за різних наборів операцій криптоперетворення

Генерація послідовності на основі застосування	Кількість тестів, в яких пройшло тестування	
	99% послід.	96% послід.
Відомої групи з 12-ти операцій криптографічного додавання за модулем два з точністю до перестановки (аналог)	126 (67 %)	188 (100 %)
Першої синтезованої група з 24-ох операцій криптографічного додавання за модулем два	131 (69,7 %)	188 (100 %)
Другої синтезованої група з 24-ох операцій криптографічного додавання за модулем чотири	132(70,2 %)	187 (99,5 %)
Сумісного використання першої та другої синтезованих груп операцій криптографічного додавання (48 операцій)	131 (69,7 %)	188 (100 %)
Сумісного використання наявних операцій криптографічного додавання (60 операцій)	142 (75,5 %)	188 (100 %)

Таблиця 7

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

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

Таблиця 8

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

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

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

У **додатках** наведено акти впровадження результатів дисертаційної роботи, результати обчислювальних експериментів та результати статистичного аналізу на основі тестів NIST_STS.

ВИСНОВКИ

У дисертаційній роботі вирішено важливу науково-технічну задачу підвищення якості систем потокового шифрування конфіденційної інформації за рахунок збільшення стійкості та варіативності перетворення на основі додаткового використання груп двохоперандних двохрозрядних операцій синтезованих на основі додавання за модулями два та чотири. А саме:

1) розроблено метод побудови та дослідження двохоперандних операцій криптоперетворення на основі результатів обчислювального експерименту, шляхом формального опису та класифікації наборів та груп операцій, з подальшим дослідженням виокремлених сукупностей на основі математичного опису та визначеної послідовності математичних перетворень, а також побудови перестановочних схем, що забезпечило виявлення сутності операції на основі встановлення нових взаємозв'язків між операндами й результатами, а також можливість застосування відомих раніше одноопераднних операцій в потоковому шифруванні на апаратному і програмному рівнях;

2) вперше розроблено методи синтезу груп симетричних двохрозрядних двохоперандних операцій потокового шифрування на основі результатів обчислювального експерименту шляхом застосування результатів реалізації методу побудови та дослідження двохоперандних операцій криптоперетворення та табличного представлення класифікації групи одноопераднних двохрозрядних операцій криптографічного перетворення, а також встановлення нових раніше невідомих взаємозв'язків між одноопераднними та двохоперандними операціями, що забезпечило синтез математичних груп симетричних двохоперандних операцій на основі додавання за модулем два та додавання за модулем чотири. Побудова нових математичних груп операцій реалізована шляхом математичних перетворень трьох відомих двохрозрядних одноопераднних операцій базової групи. Побудова групи перестановочних схем таблиці істинності забезпечила можливість побудови невідомої математичної групи операцій на основі однієї операції, яка належить цій групі;

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

4) практична цінність роботи полягає в тому, що отримані наукові

результати доведено здобувачем до конкретних інженерних методик, моделей та варіантів функціональних схем спеціалізованих дискретних пристроїв, які реалізують криптографічне перетворення інформації на основі застосування синтезованих груп операцій потокового шифрування та забезпечують підвищення варіативності й стійкості до лінійного криптоаналізу. На підставі проведених досліджень одержано такі практичні результати: побудовано математичні моделі, алгоритми функціонування та функціональні схеми реалізації груп операцій криптографічного додавання за модулем два та за модулем чотири, що дає можливість підвищувати якість систем потокового й блокового шифрування інформації. У разі застосування синтезованих груп операцій в методі підвищення стійкості та надійності потокового шифрування найкращі результати тестування пакетом тестів NIST_STS отримано під час застосування 12-ти відомих та 48-ми синтезованих операцій криптоперетворення. Крім того, сумісне застосування операцій вп’ятеро підвищує варіативність потокового шифрування.

Результати роботи впроваджено у Центральному конструкторському бюро «Сокіл» Науково-виробничого комплексу «ФОТОПРИЛАД» (м. Черкаси) під час проектування спеціалізованого модуля операційної системи, а також в навчальному процес Черкаського державного технологічного університету.

СПИСОК ОПУБЛІКОВАНИХ ПРАЦЬ ЗА ТЕМОЮ ДИСЕРТАЦІЇ

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

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

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

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

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

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

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

8. Козловська С. Г. Проблеми захисту управлінської інформації. *Теоретико-методологічні і науково-практичні засади інформаційного, фінансового та*

облікового забезпечення розвитку економіки: зб. тез доп. наук.-практ. конф., м. Черкаси, 21-22 лист. 2013 р. Черкаси, 2013. С.50-51.

9. Козловська С. Г. Технічні способи запобігання просочуванню інформації. *Проблеми моделювання структури і процесів економічних систем*: зб. тез доп. міжнар. наук.-практ. конф., м. Черкаси, 17-18 квіт. 2014 р. Черкаси, 2014. С. 93-95.

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

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

12. Лада Н. В., Козловська С. Г. Синтез та аналіз перестановочних схем побудови двохоперандних операцій криптоперетворення. *Проблеми інформатизації*: матеріали Шостої міжнар. наук.-техн. конф.: тези доп., (Черкаси – Баку – Бельсько-Бяла - Харків, 14-16 листоп. 2018 р.). Черкаси: ЧДТУ; Баку: ВА ЗС АР, Бельсько-Бяла: УТіГН, Харків: НТУ «ХПІ», 2018. С. 11.

АНОТАЦІЯ

Козловська С. Г. Методи синтезу груп симетричних операцій для потокового шифрування. – Рукопис.

Дисертація на здобуття наукового ступеня кандидата технічних наук за спеціальністю 05.13.05 – комп'ютерні системи і компоненти. – Черкаський державний технологічний університет, Черкаси, 2019.

Дисертаційну роботу присвячено підвищенню якості систем потокового шифрування конфіденційної інформації за рахунок збільшення стійкості та варіативності перетворення завдяки додатковому використанню груп двохоперандних двохрозрядних операцій синтезованих на основі додавання за модулями два та чотири.

Для цього розроблено метод побудови та дослідження двохоперандних операцій криптоперетворення на основі результатів обчислювального експерименту, шляхом формалізації, класифікації та математичного перетворення. Розроблено методи синтезу груп симетричних двохрозрядних двохоперандних операцій потокового шифрування завдяки результатам обчислювального експерименту шляхом застосування результатів реалізації розробленої технології та табличного представлення класифікації групи одноопераднних двохрозрядних операцій криптографічного перетворення, а також встановлення нових раніше невідомих взаємозв'язків між одноопераднними та двохоперандними операціями. Удосконалено метод підвищення стійкості та надійності потокового шифрування на основі додаткового застосування синтезованих груп симетричних двохоперандних операцій криптографічного перетворення інформації, що забезпечило підвищення стійкості та варіативності потокового шифрування.

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

АННОТАЦИЯ

Козловская С. Г. Методы синтеза групп симметричных операций для потокового шифрования. – Рукопись.

Диссертация на соискание ученой степени кандидата технических наук по специальности 05.13.05 – компьютерные системы и компоненты. – Черкасский государственный технологический университет, Черкассы, 2019.

Диссертационная работа посвящена повышению качества систем потокового шифрования конфиденциальной информации за счет увеличения устойчивости и вариативности преобразования на основе дополнительного использования групп двухоперандных двухразрядных операций синтезированных на основе сложения по модулям два и четыре.

Первый раздел посвящен анализу современного состояния и перспектив развития компьютерной криптографии, на основе которых формулируется цель и задачи научного исследования. Второй раздел посвящен математическому моделированию и исследованию двухоперандных операций криптографического преобразования информации на основе известных таблиц истинности. Третий раздел посвящен исследованию второй математической группы двухоперандных операций криптопреобразования. Четвертый раздел посвящен синтезу групп двухоперандных операций криптопреобразования и оценке эффективности их применения.

В работе впервые разработан метод построения и исследования двухоперандных операций криптопреобразования на основе результатов вычислительного эксперимента, путем формализации, классификации и математического преобразования, что обеспечило установление новых взаимосвязей между операндами и результатами, а также возможность применения одноперандных операций в потоковом шифровании. Впервые разработаны методы синтеза групп симметричных двухразрядных двухоперандных операций потокового шифрования на основе результатов вычислительного эксперимента путем применения результатов реализации разработанного метода построения и исследования двухоперандных операций и табличного представления классификации группы одноперандных двухразрядных операций криптографического преобразования, а также установление новых ранее неизвестных взаимосвязей между одноперандными и двухоперандными операциями, что обеспечило синтез математических групп симметричных двухоперандных операций на основе сложения по модулю два и сложения по модулю четыре. Усовершенствован метод повышения устойчивости и надежности потокового шифрования на основе дополнительного применения синтезированных групп симметричных двухоперандных операций криптографического преобразования информации, что обеспечило повышение устойчивости и вариативности потокового шифрования.

На основании проведенных исследований получены следующие практические результаты: построены математические модели, алгоритмы функционирования и функциональные схемы реализации групп операций криптографического сложения по модулю два и по модулю четыре, что дает возможность повышать качество систем потокового и блочного шифрования информации. Результаты работы внедрены в Центральном конструкторском бюро «Сокол» Научно-

производственного комплекса «ФОТОПРИБОР» (г. Черкассы) при проектировании специализированного модуля операционной системы, а также в учебный процесс Черкасского государственного технологического университета.

Ключевые слова: компьютерная криптография, потоковое шифрование, операции криптографического сложения, синтез групп операций, устойчивость, вариативность.

ABSTRACT

Kozlovska S.H. Methods of synthesis of symmetric operations groups for stream encryption. – Manuscript.

Thesis for scientific degree of candidate of technical sciences, specialty: 05.13.05 – Computer Systems and Components. – Cherkasy State Technological University, Cherkasy, 2019.

The thesis is devoted to the improvement of the confidential information's stream ciphering systems at the expense of increasing the stability and variability of transformation basing on the additional use of two-operand two-bit operations' groups synthesized on the bases of modulo-2 and modulo-4 addition.

For this purpose, a method for constructing and investigating the two-operand operations of cryptographic transformation based on the results of a calculation experiment, through formalization, classification and mathematical transformation has been developed. The synthesizing methods of symmetric two-bit two-operand stream ciphering operations' groups based on the results of a calculation experiment are developed using the implementation results of the developed technology and the table representation of the group's classification of the one-operand two-bit operations of cryptographic transformation, as well as establishing the new previously unknown relationships between one-operand and two-operand operations. The method of increasing the stability and reliability of stream ciphering basing on the additional application of the synthesized groups of symmetric two-operand operations of cryptographic information transformation has been improved, which has provided increased stability and variation of stream ciphering.

Keywords: computer cryptography, stream ciphering, operations of cryptographic addition, synthesizing the operations' groups, stability, variability.

Формат 60х84/16 Гарнітура Таймс. Папір офсет.
Ум. друк. арк. 0,9. Тираж 100 пр.
Зам. №347 від 24.04.2019р.
Друк ПП Сисюк С.В.
Україна, м. Черкаси, вул. Чехова, 53, оф. 01
тел.: (067)947-88-41
e-mail: plotoservise@gmail.com