МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ЧЕРКАСЬКИЙ ДЕРЖАВНИЙ ТЕХНОЛОГІЧНИЙ УНІВЕРСИТЕТ

БАБЕНКО ВІРА ГРИГОРІВНА

УДК 004.056.55:004.312.2

МЕТОДОЛОГІЯ СИНТЕЗУ ОПЕРАЦІЙ ПЕРЕТВОРЕННЯ ІНФОРМАЦІЇ ДЛЯ КОМП'ЮТЕРНОЇ КРИПТОГРАФІЇ

спеціальність 05.13.05 – комп'ютерні системи та компоненти

Автореферат
дисертації на здобуття наукового ступеня
доктора технічних наук

Черкаси 2020

Дисертацією є рукопис.

Робота виконана на кафедрі інформаційної безпеки та комп'ютерної інженерії Черкаського державного технологічного університету Міністерства освіти і науки України

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

Офіційні опоненти:

доктор технічних наук, професор **Семенов Сергій Геннадійович,** Національний технічний університет «Харківський політехнічний інститут», завідувач кафедри обчислювальної техніки та програмування;

Лауреат Державної премії України, доктор технічних наук, професор **Корченко Олександр Григорович,** Національний авіаційний університет, завідувач кафедри безпеки інформаційних технологій;

доктор технічних наук, професор **Можаєв Олександр Олександрович,** Харківський національний університет внутрішніх справ Міністерства внутрішніх справ України, професор кафедри інформаційних технологій та кібербезпеки.

Захист відбудеться 18.09.2020 р. о 11.00 годині на засіданні спеціалізованої вченої ради Д 73.052.04 при Черкаському державному технологічному університеті, за адресою 18006, м. Черкаси, бульв. Шевченка, 460, корп. 1.

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

Автореферат розісланий « 18 » серпня 2020 року.

Учений секретар
спеціалізованої вченої ради
Д 73.052.04
к.т.н., доцент — Ю. Ю. Бондаренко

ЗАГАЛЬНА ХАРАКТЕРИСТИКА РОБОТИ

Актуальність теми. Глобалізація інформаційних процесів й автоматизація їх обробки в усіх сферах людської діяльності зумовлені тенденцією постійного збільшення обсягів інформації, що циркулює в мережах та системах. Ці процеси не лише характеризуються позитивними наслідками, але водночас спричиняють появу нових негативних інформаційних впливів, зокрема – сприяють стрімкому розвитку кіберзлочинності. У зв'язку з цим зростає потреба захисту інформації, яка має відповідну цінність як для держави, так і для окремих користувачів, а також набувають особливої актуальності для сьогодення проблеми інформаційної безпеки та захисту інформаційних ресурсів.

Криптографічний захист інформації залишається одним із найважливіших способів забезпечення безпеки інформації в комп'ютерних мережах і системах.

Вагомий внесок у розвиток криптографічних методів захисту інформації зробили такі науковці, як А. А. Молдовян, І. Д. Горбенко, К. Є. Шеннон, Брюс Шнайєр, Р. А. Хаді, W. Diffie, M. E. Hellman, R. L. Rivest, A. Shamir, В. В. Ященко, О. А. Логачов, С. О. Шестаков, А. Н. Фіонов, Б. Я. Рябко, Дж. Л. Мессі, Чарльз Г. Беннет, Ж. Брассар, B. Chor, U. M. Maurer, N. Koblitz та ін.

Традиційні криптографічні алгоритми поділяють на високошвидкісні потокові та блокові шифри, які володіють високою стійкістю і складністю. На сьогоднішній день стандартизовані криптографічні алгоритми демонструють високу стійкість зашифрованої інформації, однак створення перших квантових комп'ютерів ставить під питання їх стійкість до постквантового криптографічного аналізу. Подальше збільшення стійкості за рахунок ускладнення криптографічних алгоритмів зумовлює складнощі щодо їх застосування в системах реального часу.

Основним критерієм при виборі криптосистем є стійкість, проте для деяких задач, наприклад, для шифрування великого об'єму даних, захисту онлайнових платіжних систем та ін. ключову роль відіграє швидкість криптографічної обробки даних. Незважаючи на різноманітність сучасних криптографічних методів та систем, далеко не всі володіють необхідним рівнем ефективності (швидкодії та стійкості) для забезпечення захисту інформаційних ресурсів. Крім того, стрімкий розвиток обчислювальних засобів та їх одночасне здешевлення формулюють нові вимоги як до стійкості, так і до швидкодії систем криптографічного захисту, тому зростання криптостійкості має бути не меншим за ріст швидкодії. Отже, завжди існуватиме потреба підвищення стійкості та швидкодії криптографічних методів захисту інформації.

У багатьох наукових роботах було показано, що один із найперспективніших напрямків розвитку криптографії – у поєднанні криптології та комп'ютерної інженерії; він полягає в розширенні спектра операцій криптографічного перетворення, забезпечуючи на їх основі вдосконалення існуючих та побудову нових криптографічних алгоритмів.

Сутність процесу криптографічного перетворення зводиться до перетворення блоку інформації за допомогою випадково вибраних таблиць підстановок, реалізованих на основі дискретних моделей кодування. Основна задача даного криптографічного перетворення полягає у випадковій генерації моделей таблиць підстановок, які відповідають заданим вимогам щодо якості криптоперетворень блоку даних. Основні переваги: велика варіативність при виборі таблиць підстановок (для одного байта існує 256! таблиць підстановок); висока швидкість генерації моделей таблиць підстановок; висока швидкість реалізації дискретних моделей пристроїв кодування. Саме таке криптографічне перетворення об'єднує сильні сторони потокового й блочного шифрування і забезпечує протидію постквантовому криптоаналізу за рахунок збільшення варіативності криптографічних алгоритмів.

Переваги криптографічного кодування безпосередньо пов'язані з проблемами, які виникають при їх реалізації. Основна проблема полягає в тому, що через величезну кількість таблиць підстановок відсутні як загальні підходи, так і алгоритми для побудови множин груп дискретних моделей. Відсутні методи синтезу груп дискретних моделей операцій криптографічного кодування із заданими властивостями. Рішення даної проблеми стане підґрунтям для створення теоретичної бази побудови високоефективних систем комп'ютерної криптографії. Виходячи з цього можна стверджувати що тема дисертаційного дослідження є актуальною.

Зв'язок роботи з науковими програмами, планами, темами. Результати дисертаційної роботи включені до звітів НДР: «Методи та засоби захисту інформації МНС України на основі операцій криптографічного кодування» (ДР № 0112U003579), «Криптографічне кодування: методи та засоби реалізації (частина 2)» (ДР № 0113U001475), «Ефективність систем інформаційної безпеки», шифр НДР «Безпека» (ДРН 0113U004731), «Ефективність систем інформаційної безпеки» (Шифр «Перетворення»), «Синтез операцій криптографічного перетворення з заданим характеристиками» (ДР № 0116U008714), «Розробка методів та засобів оцінки ефективності соціоінжинірингу» (ДР № 0116U008715), при виконанні держбюджетної теми № 36Б115 «Розробка методів синтезу тестових моделей поведінки програмних об'єктів, підвищення оперативності передачі та захисту інформації у телекомунікаційних системах» (ДР № 0115U003103) (Кіровоградський національний технічний університет), в яких автор брав участь як виконавець.

Мета і задачі дослідження. Основною метою дисертаційної роботи є рішення науково-технічної проблеми підвищення ефективності функціонування систем комп'ютерної криптографії шляхом створення методології синтезу операцій перетворення інформації та побудови криптографічних примітивів на їх основі.

Рішення даної наукової проблеми передбачає удосконалення теорії, спрямованої на подолання суперечностей і труднощів при проектуванні систем комп'ютерної криптографії. Тому в роботі поставлені та вирішені наступні проблемні задачі:

1. Розробити основні положення методології синтезу операцій перетворення інформації для систем комп'ютерної криптографії.

2. На основі застосування запропонованої методології розробити та вдосконалити методи синтезу й аналізу групи нелінійних операцій криптографічного перетворення інформації.

3. Вдосконалити існуючі примітиви комп'ютерної криптографії на основі застосування синтезованих операцій криптографічного перетворення інформації та оцінити їх ефективність.

4. Розробити технологію синтезу операцій для мультиопераційних матричних криптографічних примітивів.

5. Удосконалити методи застосування операцій криптографічного перетворення інформації та оцінити їх ефективність.

Об'єктом дослідження є процеси синтезу операцій перетворення інформації.

Предмет дослідження – методи та засоби синтезу операцій перетворення інформації для комп'ютерної криптографії.

Методи дослідження. Розробка принципів, методів і алгоритмів синтезу операцій криптографічного перетворення згідно з запропонованою методологією базується на положеннях теорії інформації, теорії множин, систем числення, криптографії, методів дискретної математики та комп'ютерного моделювання. Оцінка ефективності криптографічних примітивів базується на основі теорії алгоритмів, математичної статистики, лінійного та нелінійного криптоаналізу.

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

1. Вперше запропонована методологія синтезу операцій криптографічного перетворення інформації на основі існуючих та розроблених методів синтезу операцій прямого, оберненого та взаємного криптографічного перетворення шляхом їх класифікації та узагальнення, що забезпечило можливість розширення бази операцій, використання яких дозволяє вдосконалювати існуючі та синтезувати нові криптоалгоритми і криптопримітиви.

2. Вперше розроблено технологію синтезу операцій для мультиопераційних матричних криптографічних примітивів на основі побудови нових груп операцій з точністю до перестановки шляхом використання запропонованої табличної моделі операції криптоперетворення, що дозволило за рахунок варіативності операцій підвищити криптостійкість існуючих криптопримітивів.

3. Удосконалено методи побудови криптографічних примітивів на прикладі примітивів ковзного шифрування на основі матричних операцій криптографічного перетворення та отриманих узагальнених рекурентних послідовностей для побудови моделей шляхом їх паралельної реалізації, що забезпечило підвищення швидкості шифрування (до двох разів) та стійкості до лінійного криптоаналізу.

4. Удосконалено методи синтезу та аналізу криптографічних алгоритмів на основі узагальненої моделі криптоалгоритму, шляхом послідовно-паралельної реалізації операцій криптографічного перетворення інформації на макро- та мікрорівнях, що забезпечило можливість вирішення протиріч між криптостійкістю, складністю та швидкістю для досягнення заданої ефективності, виходячи з задач проектування.

5. Отримали подальший розвиток математичні моделі та методи синтезу елементарних функцій та операцій криптоперетворення на основі запропонованої методології та вибраної групи нелінійних елементарних функцій шляхом вдосконалення математичного апарату для синтезу прямих та обернених матричних моделей не афінних дискретних перетворень, що в сукупності забезпечило можливість синтезу операцій нелінійних криптографічних перетворень.

Практичне значення одержаних результатів. Практична цінність роботи полягає в доведенні здобувачем отриманих наукових результатів до конкретних інженерних методик, алгоритмів, моделей та варіантів побудови криптографічних алгоритмів.

На підставі проведених досліджень одержано такі практичні результати: розроблено методологію синтезу операцій криптографічного перетворення інформації в рамках запропонованої концепції побудови алгоритмів захисту інформації на їх основі з можливістю підбору оптимальних показників криптостійкості та швидкодії, що дає змогу покращити ефективність функціонування системи криптографічного захисту в цілому; розроблено технологію побудови та використання криптопримітивів на основі синтезованих операцій криптографічного перетворення інформації з можливістю їх паралельного виконання, що дає виграш у швидкості та часі здійснення перетворення безпосередньо інформації; запропоновано варіанти реалізації на програмному та апаратному рівнях нових груп криптографічних операцій заданої розрядності, що володіють властивостями афінності та нелінійності, зокрема матричного та розширеного матричного перетворення. Застосування синтезованих операцій криптографічного перетворення на основі запропонованих варіантів комбінації використання матричного та розширеного матричного перетворення при конструюванні алгоритмів дає можливість збільшити криптостійкість (від 2^{166} до 2^{8157} разів) пропорційно відносно потокового шифрування при зменшенні часу шифрування (від 1,3 до 8 разів).

Практична цінність роботи підтверджена актами впровадження на підприємствах і організаціях: НВК «Фотоприлад», «Науково-дослідний інститут «Акорд» та ПП «Сенсорна електроніка» (м. Черкаси), ТОВ «Люменс-груп» (м. Кіровоград) та в освітній процес у навчальних закладах: Черкаському державному технологічному університеті, Черкаському національному університеті імені Б. Хмельницького, Національному аерокосмічному університеті імені М. Є. Жуковського «ХАІ», Кіровоградському національному технічному університеті.

Особистий внесок здобувача. Усі нові результати дисертаційної роботи отримано автором самостійно. Роботи [1-5, 57, 58, 73] виконані без співавторів. У наукових працях, опублікованих у співавторстві, з питань, що стосуються даного дослідження, автору належать: розробка принципів та методів синтезу наборів функцій для криптографічного перетворення [6-8, 41, 44, 52, 59-61]; перевірка методу підвищення оперативності доступу до конфіденційних інформаційних ресурсів [9-11, 52, 64]; розробка методики формування груп операцій та реалізація побудови моделі процесу декодування або перекодування інформації [12, 13, 18, 52, 53, 61]; опис процесу реалізації методів синтезу матричних моделей операцій криптографічного кодування [14, 15, 53, 62]; основні підходи щодо розробки та реалізації методу синтезу базових операцій криптографічного перетворення, формулювання методу синтезу операцій криптографічного перетворення на основі додавання за модулем два, узагальнення та аналіз одержаних результатів [16-19, 45 ,53, 63, 74-76]; розробка методу захисту інформаційних ресурсів на основі матричних операцій криптографічного перетворення та алгоритмів їх застосування, оцінка статистичних властивостей результатів криптографічного перетворення [20-22, 24, 26, 34, 35, 50, 54-56, 82,83]; формулювання теореми про побудову оберненої матриці розширеного матричного криптографічного перетворення [23, 34, 50, 54]; модель синтезу нелінійної операції розширеного матричного криптографічного перетворення та розробка правил побудови оберненої операції [25, 35, 54]; перевірка результатів застосування методу захисту конфіденційної інформації [27, 28, 54]; аналіз синтезованих та пошук базових операцій криптографічного перетворення [29, 39, 42, 54, 65, 81]; узагальнення методу синтезу обернених операцій нелінійного розширеного матричного криптографічного перетворення [30, 31, 51, 54]; аналіз властивостей результатів перетворення матричними операціями криптографічного перетворення та розробка технології їх використання [32, 84, 85]; способи застосування матричних операцій криптографічного перетворення для LSB методу [33]; опис особливостей застосування ключових елементів для здійснення процесу вбудовування повідомлення великої довжини з використанням декількох контейнерів [38, 68-71]; спосіб застосування матричних операцій криптографічного перетворення в примітивах ковзного шифрування [36, 37]; опис способів застосування операцій криптографічного перетворення для синтезу алгоритмів захисту [43, 55, 56, 67, 72, 86]; синтез моделей надлишкових позиційних систем числення [40, 46, 47]; аналіз сучасного стану мереж передачі даних [48, 49] та способів захисту систем моніторингу веб-ресурсів [77]; побудова матричних операцій декодування інформації за допомогою логічних визначників [66, 79, 80]; опис варіантів реалізації правил синтезу операцій криптографічного перетворення [78-80]; розробка математичних моделей пристроїв [87-90].

Із робіт, що опубліковані у співавторстві, у дисертаційній роботі використовуються результати, одержані особисто здобувачем.

Апробація результатів дисертації. Основні положення дисертаційної роботи доповідалися та обговорювалися більш ніж на 10 міжнародних та

всеукраїнських наукових семінарах та конференціях, серед яких: міжнародна науково-практична конференція «Інтегровані інтелектуальні робототехнічні комплекси» (Київ, 2009, 2014); всеукраїнські науково-технічна та науково-практична конференції: «Інтегровані комп'ютерні технології в машинобудуванні ІКТМ-2011» (Харків, 2011), «Інформаційна безпека держави, суспільства та особистості» (Кіровоград, 2015), восьма наукова конференція ХУПС ім. І. Кожедуба «Новітні технології – для захисту повітряного простору» (Харків, 2012); п'ятнадцята міжнародна науково-технічна конференція «Моделирование, идентификация, синтез систем управления (МИССУ-2012)» (Канака, Крим, 2012), перша міжнародна заочна науково-практична конференція «Информационные системы и технологии: управление и безопасность» (Тольятті-Русе, 2012), міжнародні науково-практичні конференції: «Методи та засоби кодування, захисту й ущільнення інформації» (Вінниця, 2013, 2016) та «Інформаційні технології та комп'ютерна інженерія» (ІТКІ-2014) (Вінниця, 2014); міжнародні науково-практичні конференції: «Проблеми інформатизації» (Черкаси, 2009, 2013, 2016-2019) та «Інформаційні технології в освіті, науці і техніці» (Черкаси, 2014, 2016); п'ята міжнародна науково-технічна конференція «Сучасні напрями розвитку інформаційно-комунікаційних технологій та засобів управління» (Харків, 2015); міжнародні науково-практичні конференції: «Проблеми науково-технічного та правового забезпечення кібербезпеки у сучасному світі «ПНПЗК-2016»» (Харків, 2016), «Наукова думка інформаційного століття» (Дніпро, 2017), «Інноваційні тенденції сьогодення у сфері природничих, гуманітарних та точних наук» (Івано-Франківськ, 2017), «Наука у контексті сучасних глобалізаційних процесів» (Полтава, 2017), «Науковий і інноваційний потенціал сьогодення» (Ополе, Польща, 2018), Second International Workshop on Computer Modeling and Intelligent Systems (CMIS-2019) (Запоріжжя, 2019).

Публікації. Основні результати дисертаційної роботи викладено в 90 друкованих працях, а саме: 49 наукових статтях у журналах, з них 40 – у фахових виданнях України, 6 статтях у наукових фахових виданнях за кордоном, 7 монографіях, з яких 2 видані за кордоном, 4 деклараційних патенти на корисну модель та 30 тезах доповідей на міжнародних та всеукраїнських наукових конференціях і семінарах.

Структура й обсяг дисертації. Дисертація складається зі вступу, шести розділів, висновків, списку використаних джерел з 258 найменувань на 30 сторінках та додатків на 76 сторінках. Загальний обсяг дисертації становить 474 сторінок, в тому числі 336 сторінок основної частини, 65 рисунків, 55 таблиць.

ОСНОВНИЙ ЗМІСТ РОБОТИ

Вступ містить обґрунтування актуальності теми роботи, мету, об'єкт, предмет та задачі дослідження, визначення наукової новизни та практичної значущості отриманих результатів, відомості про їх апробацію та реалізацію, а також характеристику публікацій.

Перший розділ присвячений аналітичному огляду систем криптографічного захисту (зокрема – їх типам за Шенноном), стандартних вимог до криптографічних систем (розглядаються загальноприйняті вимоги та

вимоги згідно з Керкгоффсом). Для здійснення аналізу розглянуто принципи побудови й схеми криптологічних систем. Особливу увагу приділено дослідженню основних властивостей функцій криптографічного перетворення для побудови стійких шифрів. Проведений аналіз сучасних криптосистем та виокремлені основні характеристики ефективності функціонування системи криптографічного захисту, а саме: криптостійкість (*K*), складність реалізації криптографічного перетворення (*C*), швидкість виконання криптографічного перетворення (*V*), статистичні властивості результатів криптографічного перетворення (*H*).

На основі вибраних комплексних показників якості та ефективності функціонування криптосистеми пропонується проводити порівняльний аналіз методів та принципів, покладених в основу архітектури ефективних криптоалгоритмів для систем захисту інформаційних ресурсів.

Взаємозалежності ефективних криптосистем визначаються на основі описаних показників та можуть бути досягнуті за наступних умов:

1. Криптостійкість $K \to max$, якщо $\begin{cases} C \to max \\ V \to min \end{cases}$;
2. Складність $C \to min$, якщо $\begin{cases} V \to max \\ K \to min \end{cases}$;
3. Швидкість $V \to max$, якщо $\begin{cases} C \to min \\ K \to min \end{cases}$;
4. Статистичні характеристики $H \to max$, якщо $\begin{cases} C \to max \\ V \to min \\ K \to max \end{cases}$.

Оскільки швидкість та складність виконання криптографічного алгоритму напряму залежать від швидкості та складності виконання операцій перетворення інформації, які складають основу алгоритму $V_{ALG} \to V(F_i)$ і $C_{ALG} \to C(F_i)$, тоді швидкість виконання алгоритму напряму залежить від складності $V(F_i) \to C(F_i)$ і $V_{ALG} \to C_{ALG}$. Звідси, якщо зростає складність, то знижується швидкість $\uparrow C_{ALG} \Rightarrow \downarrow V_{ALG}$ і навпаки.

Отже, виникає протиріччя між складністю, криптостійкістю та швидкістю: складність алгоритму повинна бути мінімальною, показники швидкості, криптостійкості та статистичні властивості – максимальними

$$\begin{cases} C \to min \\ V \to max \\ K \to max \\ H \to max \end{cases}.$$

Для вирішення зазначених протиріч сформульовані мета та задачі дисертаційного дослідження. Структурно-логічна схема проведення наукового дослідження представлена на рис. 1. Етапи наукового дослідження виявляють взаємозв'язки між задачами та результатами дослідження, а також їх внесок у вирішення сформульованої наукової проблеми.

Рис. 1. Структурно-логічна схема проведення наукового дослідження

Другий розділ присвячений розробці та узагальненню методів синтезу операцій криптографічного перетворення, а також побудові та формалізації методології синтезу логічних операцій для криптографічного перетворення інформації.

Елементарна функція – це функція криптографічного перетворення множини вхідних значень в одне вихідне значення.

Наприклад: $f_m^{(N)}(x_1,x_2,...,x_N)$, де N – кількість розрядів інформації, m – це номер функції перетворення, який визначається десятковим значенням двохрозрядного коду результату перетворення; $x_1,x_2,...,x_N$ – значення розрядів інформації відповідно. Оскільки $x_1,x_2,...,x_N \in \{0;1\}$, тоді значення елементарних функцій $f_1^{(1)}, f_2^{(2)},...,f_m^{(N)} \in \{0;1\}$.

Отримані елементарні функції для криптографічного перетворення інформації мають одну спільну особливість – однакову кількість нулів та одиниць. Тому кількість елементарних функцій для криптографічного перетворення визначається як $K_{eo} = C_{2^N}^{2^{N-1}}$, де N – розрядність елементарних функцій для криптографічного перетворення.

Під композицією двох логічних операцій будемо розуміти їх послідовне виконання.

Криптографічна операція – це понумерований набір елементарних функцій, які в сукупності забезпечують виконання криптографічного перетворення. Отже, криптографічна операція – це композиція відповідних елементарних функцій перетворення $F_{1,2,...m} = (f_1^{(1)}, f_2^{(2)},..., f_m^{(N)})$.

В роботі доведено, що криптографічні операції утворюють групу. Виходячи з цього, як для криптографічних операцій, так і для елементарних функцій виконується властивість суперпозиції: серед множини елементарних функцій існують відповідні набори пар функцій – таких, що $F_i\ (F_j\ (f_1(x_1,x_2,...,x_N), f_2(x_1,x_2,...,x_N),...,f_m(x_1,x_2,...,x_N))) = (x_1,x_2,...,x_N)$.

Тобто множину основних елементарних функцій, з яких формуються криптографічні операції, можливо використовувати як для перетворення, так і для оберненого перетворення відповідно.

При проведенні досліджень операцій криптографічного перетворення було встановлено, що загальна кількість даних операцій утворюється поєднанням базових операцій, операцій перестановки та операцій інверсії: $N = N_б \cdot N_n \cdot N_i$, де $N_б$ – кількість базових операцій, N_n – кількість операцій перестановки, N_i – кількість операцій інверсії.

Множина двохрозрядних криптографічних операцій утворює групу відносно операції композиції. Ця група ізоморфна групі S^4. А це означає, що будь-яке поєднання базових операцій, операцій перестановок та операцій інверсії теж утворюватиме групу.

Виходячи з наведеного вище, можна визначити залежність кількості операцій криптографічного перетворення від їх розрядності $K_{on} = 2^N!$.

Множина *N*-розрядних криптографічних операцій утворює групу відносно операції композиції. Ця група ізоморфна групі S^{2^N}.

Подальші дослідження були пов'язані з елементарними функціями, що будуються на основі додавання за модулем два. Синтезовані на їх основі операції криптографічного перетворення були названі операціями матричного криптографічного перетворення. В узагальненому вигляді матричні операції криптографічного перетворення, синтезовані на основі додавання за модулем два, можна представити як

$$\vec{F}_k = \begin{pmatrix} a_{11}x_1 \oplus a_{12}x_2 \oplus \ldots \oplus a_{1n}x_n \oplus b_1 \\ a_{21}x_1 \oplus a_{22}x_2 \oplus \ldots \oplus a_{2n}x_n \oplus b_2 \\ \ldots \\ a_{n1}x_1 \oplus a_{n2}x_2 \oplus \ldots \oplus a_{nn}x_n \oplus b_n \end{pmatrix},$$

де $a_{ij} \in [0,1]; b_i \in [0,1]$; $x_1 \ldots x_n$ – операнди; $\oplus$ – операція «сума за mod 2».

У другому розділі удосконалено існуючі та розроблено нові методи синтезу операцій прямого, оберненого та взаємного матричного криптографічного перетворення.

Оскільки операції криптографічного перетворення утворюють групу, то існує операція криптографічного перетворення $y = F_*^k(x)$, яка забезпечує перетворення результату виконання однієї операції в результат виконання іншої операції без етапу виконання оберненої операції. Ці операції будемо називати операціями взаємного криптографічного перетворення.

Метод синтезу операцій матричного криптографічного взаємного перетворення полягає в наступному. Якщо справедливі операції криптографічного перетворення: $y = F_1^k(x)$, $y = F_2^k(x)$, такі що $F_1^k(F_2^k(x)) = y$, а також справедливими є операції криптографічного перетворення: $y = F_3^k(x)$, $y = F_4^k(x)$, такі що $F_3^k(F_4^k(x)) = y$, то існує функція $y = F_*^k(x)$, яка забезпечує перетворення інформації: $y = F_*^k(F_1^k(x)) = F_3^k(x)$.

Узагальнивши отримані результати, ми встановили, що для побудови матричних операцій взаємного криптографічного перетворення необхідно вирішити наступну систему рівнянь:

$$\vec{F}_p = \begin{pmatrix} d_{11}(a_{11}x_1 \oplus a_{12}x_2 \oplus \ldots \oplus a_{1n}x_n) \oplus \\ \oplus d_{12}(a_{21}x_1 \oplus a_{22}x_2 \oplus \ldots \oplus a_{2n}x_n) \oplus \ldots \oplus \\ \oplus d_{1n}(a_{n1}x_1 \oplus a_{n2}x_2 \oplus \ldots \oplus a_{nn}x_n) \\ d_{21}(a_{11}x_1 \oplus a_{12}x_2 \oplus \ldots \oplus a_{1n}x_n) \oplus \\ \oplus d_{22}(a_{21}x_1 \oplus a_{22}x_2 \oplus \ldots \oplus a_{2n}x_n) \oplus \ldots \oplus \\ \oplus d_{2n}(a_{n1}x_1 \oplus a_{n2}x_2 \oplus \ldots \oplus a_{nn}x_n) \\ \ldots \\ d_{n1}(a_{11}x_1 \oplus a_{12}x_2 \oplus \ldots \oplus a_{1n}x_n) \oplus \\ \oplus d_{n2}(a_{21}x_1 \oplus a_{22}x_2 \oplus \ldots \oplus a_{2n}x_n) \oplus \ldots \oplus \\ \oplus d_{nn}(a_{n1}x_1 \oplus a_{n2}x_2 \oplus \ldots \oplus a_{nn}x_n) \end{pmatrix} = \begin{pmatrix} c_{11}x_1 \oplus c_{12}x_2 \oplus \ldots \oplus \\ \oplus c_{1n}x_n \\ c_{21}x_1 \oplus c_{22}x_2 \oplus \ldots \oplus \\ \oplus c_{2n}x_n \\ \ldots \\ c_{n1}x_1 \oplus c_{n2}x_2 \oplus \ldots \oplus \\ \oplus c_{nn}x_n \end{pmatrix},$$

де $a_{ij}, c_{ij}, d_{ij} \in [0,1]$; $x_1 \ldots x_n$ – операнди-розряди відповідно.

Запропоновано технологію підвищення швидкості доступу до конфіденційних інформаційних ресурсів на основі застосування операцій взаємного криптографічного перетворення.

Побудова операції оберненого криптографічного перетворення є частковим випадком побудови операції взаємного криптографічного перетворення, і вона реалізується на основі вирішення системи рівнянь заданого виду:

$$\vec{F}_d = \begin{pmatrix} b_{11}(a_{11}x_1 \oplus a_{12}x_2 \oplus ... \oplus a_{1n}x_n) \oplus \\ \oplus b_{12}(a_{21}x_1 \oplus a_{22}x_2 \oplus ... \oplus a_{2n}x_n) \oplus ... \oplus \\ \oplus b_{1n}(a_{n1}x_1 \oplus a_{n2}x_2 \oplus ... \oplus a_{nn}x_n) \\ b_{21}(a_{11}x_1 \oplus a_{12}x_2 \oplus ... \oplus a_{1n}x_n) \oplus \\ \oplus b_{22}(a_{21}x_1 \oplus a_{22}x_2 \oplus ... \oplus a_{2n}x_n) \oplus ... \oplus \\ \oplus b_{2n}(a_{n1}x_1 \oplus a_{n2}x_2 \oplus ... \oplus a_{nn}x_n) \\ . \quad . \quad . \quad . \quad . \quad . \quad . \quad . \quad . \quad . \quad . \quad . \\ b_{n1}(a_{11}x_1 \oplus a_{12}x_2 \oplus ... \oplus a_{1n}x_n) \oplus \\ \oplus b_{n2}(a_{21}x_1 \oplus a_{22}x_2 \oplus ... \oplus a_{2n}x_n) \oplus ... \oplus \\ \oplus b_{nn}(a_{n1}x_1 \oplus a_{n2}x_2 \oplus ... \oplus a_{nn}x_n) \end{pmatrix} = \begin{pmatrix} a_{11}x_1 & & & \\ & a_{22}x_2 & & \\ . & . & . & . \\ & & & a_{nn}x_n \end{pmatrix}.$$

де $a_{ij}, b_{ij} \in [0,1]$; $x_1 .. x_n$ – операнди-розряди відповідно.

Були сформульовані вимоги до існування операцій прямого, оберненого та взаємного матричного криптографічного перетворення.

На основі отриманих результатів запропоновано концепцію побудови методології синтезу операцій криптографічного перетворення інформації, основна суть якої полягає в класифікації операцій криптографічного перетворення та їх невід'ємної складової – елементарних функцій на групи, що дозволяє проводити паралельно дослідження кожної з груп окремо. Крім того, – класифікувати операції криптоперетворення на базові операції, операції перестановки та операції інверсії, а елементарні функції класифікувати на прямі та обернені, що забезпечить необхідність та можливість синтезу і дослідження лише базових операцій криптографічного перетворення.

Розглянемо кількісні характеристики для моделювання n-розрядних операцій криптографічного перетворення операцій.

Якщо $M_f = \{f_1, f_2, f_3, ... f_m\}$ множина елементарних функцій, тоді $m = 2^{2^n}$.

Якщо $M_f = \{f_1, f_2, f_3, ... f_p\}$ множина елементарних функцій для безнадлишкового криптографічного перетворення, тоді $p = C_{2^n}^{2^{n-1}}$.

Якщо відібрана на основі класифікації підмножина елементарних функцій криптографічного перетворення складає, для прикладу, k-у частину від загальної кількості елементарних функцій для криптографічного перетворення, тоді на попередньому етапі дослідження аналізується підмножина $M_f^* = \{f_1, f_2, f_3, ... f_v\}$ де $v = \frac{1}{k} C_{2^n}^{2^{n-1}}$, а в процесі моделювання

буде використано $g = \frac{1}{2k} C_{2^n}^{2^{n-1}}$ елементарних функцій.

Якщо $M_F = \{F_1, F_2, F_3, \ldots F_p\}$ множина n-розрядних операцій криптографічного перетворення, тоді $p = 2^n!$. Тому в процесі моделювання необхідно побудувати лише множину базових операцій, яка складає $M_F^* = \{F_1, F_2, F_3, \ldots F_v\}$, де $v = \frac{2^n!}{2^n \cdot n!}$.

Виходячи з наведеного, можна стверджувати, що при проведенні моделювання і дослідження кількість елементарних функцій для криптографічного перетворення зменшується в $2k$ рази, а кількість операцій криптографічного перетворення зменшується в $2^n \times n!$ разів.

Якщо підмножина елементарних функцій для криптографічного перетворення M_f^* вибрана і поділена на прямі та обернені операції правильно, тоді отримана в процесі моделювання на її основі підмножина M_F^* забезпечує реалізацію прямого, оберненого та взаємного криптографічного перетворення.

Наведені вирази для кількісних характеристик показують, що при значеннях n 3, 4 та 5 дані множини операцій криптоперетворення можуть бути отримані на основі обчислювального експерименту як таблиці підстановок.

Проте таблична реалізація операцій криптоперетворення як за швидкістю реалізації, так і за об'ємом необхідної пам'яті значно поступається аналітичній реалізації на основі моделей операцій прямого, оберненого та взаємного криптоперетворення.

Для практичної реалізації операцій криптографічного перетворення необхідно:

1. Класифікувати елементарні функції заданої розрядності на групи, виходячи із складності мінімальних диз'юнктивно нормальних форм представлення. Складність операції будемо оцінювати кількістю операцій в її представленні.

2. Визначити групу елементарних функцій, яка не досліджувалася раніше.

3. На основі різних форм представлення спростити сприйняття процесу реалізації функції, встановити логічні взаємозв'язки та основну логічну змінну, на основі якої побудована елементарна функція.

4. Побудувати модель елементарної функції, на основі якої розробити методи синтезу груп прямих та обернених елементарних функцій, а також повної групи вибраних елементарних функцій. Для кожної групи елементарних функцій вдосконалюються існуючі або розробляються нові методи синтезу для забезпечення простоти та швидкості їх реалізації.

5. На основі синтезованої групи прямих елементарних функцій записуються отримані за результатами моделювання базові операції

криптографічного перетворення в аналітичному представленні. Розробляється новий або вдосконалюється існуючий метод синтезу базових операцій криптографічного перетворення для даної групи операцій.

6. З урахуванням особливостей побудованої групи операцій будується узагальнена аналітична модель операції даної групи, на основі якої розробляється метод синтезу операцій криптографічного перетворення, придатний для практичної реалізації.

7. В синтезованій групі операцій встановлюються взаємозв'язки між операціями для забезпечення оберненого та взаємного перетворення. Розробляються методи синтезу операцій оберненого та взаємного криптографічного перетворення.

8. Проводиться аналіз можливості використання розроблених моделей та методів для синтезу аналогічних груп операцій (побудованих на основі аналогічних елементарних функцій за своїм фізичним чи математичним змістом) більшої розрядності. При позитивних результатах аналізу проводиться вдосконалення розроблених методів для синтезу груп операцій криптографічного перетворення заданої розрядності.

Синтезувавши нові елементарні функції та побудовані на їх основі операції криптоперетворення, отримаємо нові можливості для вдосконалення криптопримітивів. Адже розуміння фізичного змісту цих елементарних функцій та операцій криптоперетворення дозволить встановити нові підходи до побудови та вдосконалення криптографічних примітивів.

У **третьому розділі** проведена класифікація трирозрядних елементарних функцій для криптографічного перетворення інформації за складністю та функціональними особливостями перетворення.

Синтез повної множини прямих та обернених елементарних функцій базується на виразі: $f = \hat{x}_i \cdot \hat{x}_j \vee \hat{x}_i \cdot \hat{x}_l \vee \bar{\hat{x}}_i \cdot \bar{\hat{x}}_j \cdot \bar{\hat{x}}_l$, де $\hat{x}$ – будь-яке значення аргументу; $\bar{\hat{x}}$ – інверсне до будь-якого значення аргументу, за умови: $i, j, l \in [1,2,3]$; $i \neq j \neq l$.

Метод синтезу трьохрозрядних розширених матричних елементарних функцій в дискретному представленні, сутність якого полягає в наступному:

1. Виходячи із задач проектування, визначити, які формалізовані правила необхідно використати та на основі перебору значень i, j, l, де $i, j, l \in [1,2,3]$ за умови $i \neq j \neq l$; $j < l$ отримати три основні трьохрозрядні розширені матричні елементарні функції, які будуть використовуватися, а саме:

- при синтезі множини прямих трьохрозрядних розширених матричних елементарних функцій необхідно використати $f = x_i \cdot \hat{x}_j \vee x_i \cdot \hat{x}_l \vee \bar{x}_i \cdot \bar{\hat{x}}_j \cdot \bar{\hat{x}}_l$; $f = x_j \cdot \hat{x}_i \vee x_j \cdot \hat{x}_l \vee \bar{x}_j \cdot \bar{\hat{x}}_i \cdot \bar{\hat{x}}_l$; $f = x_l \cdot \hat{x}_j \vee x_l \cdot \hat{x}_i \vee \bar{x}_l \cdot \bar{\hat{x}}_j \cdot \bar{\hat{x}}_i$;
- при синтезі множини обернених трьохрозрядних розширених матричних елементарних функцій необхідно використати $f = \bar{x}_i \cdot \hat{x}_j \vee \bar{x}_i \cdot \hat{x}_l \vee x_i \cdot \bar{\hat{x}}_j \cdot \bar{\hat{x}}_l$; $f = \bar{x}_j \cdot \hat{x}_i \vee \bar{x}_j \cdot \hat{x}_l \vee x_j \cdot \bar{\hat{x}}_i \cdot \bar{\hat{x}}_l$;

$f = \bar{x}_l \cdot \hat{x}_j \vee \bar{x}_l \cdot \hat{x}_i \vee x_l \cdot \bar{\bar{x}}_j \cdot \bar{\bar{x}}_i$;

- при синтезі повної множини трьохрозрядних розширених матричних елементарних функцій необхідно використати

$f = \hat{x}_i \cdot \hat{x}_j \vee \vec{x}_i \cdot \hat{x}_l \vee \hat{\bar{x}}_i \cdot \bar{\bar{x}}_j \cdot \bar{\bar{x}}_l$; $f = \hat{x}_j \cdot \hat{x}_i \vee \hat{x}_j \cdot \hat{x}_l \vee \hat{\bar{x}}_j \cdot \bar{\bar{x}}_i \cdot \bar{\bar{x}}_l$;

$f = \hat{x}_l \cdot \hat{x}_j \vee \hat{x}_l \cdot \hat{x}_i \vee \hat{\bar{x}}_l \cdot \bar{\bar{x}}_j \cdot \bar{\bar{x}}_i$.

2. На основі перебору значень інверсії $\hat{x}_i$, $\hat{x}_j$, $\hat{x}_l$, де $\hat{x}_i \in [x_i, \bar{x}_i]$, $\hat{x}_j \in [x_j, \bar{x}_j]$, $\hat{x}_l \in [x_l, \bar{x}_l]$, підставивши отримані набори в три основні трьохрозрядні розширені матричні елементарні функції, отримати повну множину трьохрозрядних розширених матричних елементарних функцій відповідно до задачі синтезу.

Узагальнені правила синтезу прямих трьохрозрядних розширених матричних елементарних функцій будуть описані виразом:

$$f = x_i \oplus (\hat{x}_j \cdot \hat{x}_l), \quad (1)$$

де x – пряме значення аргументу; $\bar{x}$ – інверсне значення аргументу; $\hat{x}$ – будь-яке значення аргументу; $\bar{\bar{x}}$ – інверсне до будь-якого значення аргументу, $i, j, l \in [1,2,3]$ за умови $i \neq j \neq l$.

Узагальнені правила синтезу обернених трьохрозрядних розширених матричних елементарних функцій будуть описані виразом:

$$f = x_i \oplus (\hat{x}_j \cdot \hat{x}_l) \oplus 1. \quad (2)$$

Вирази (1), (2) дають змогу розробити метод синтезу трьохрозрядних розширених матричних елементарних функцій в модульно-дискретному представленні.

Сутність розробленого методу синтезу елементарних функцій в дискретно-алгебраїчному представленні полягає в наступному:

1) на основі виразу (1) шляхом перебору значень i, j, l, де $i, j, l \in [1,2,3]$ за умови $i \neq j \neq l$; $j < l$ отримано три основні трьохрозрядні розширені матричні елементарні функції;
2) на основі перебору значень інверсії $\hat{x}_j$, $\hat{x}_l$, де $\hat{x}_j \in [x_j, \bar{x}_j]$, $\hat{x}_l \in [x_l, \bar{x}_l]$ підставивши отримані набори в три основні трьохрозрядні розширені матричні елементарні функції, отримати повну множину із 12 прямих трьохрозрядних розширених матричних елементарних функцій;
3) на основі виразу (2), інвертуванням множини прямих трьохрозрядних розширених матричних елементарних функцій, шляхом додавання по модулю два, отримана множина обернених розширених матричних елементарних функцій;
4) об'єднанням множини прямих і обернених елементарних функцій отримана повна множина із 24 трьохрозрядних розширених матричних елементарних функцій.

Метод синтезу m-розрядних розширених матричних елементарних функцій полягає в наступному:

1. На основі виразу $f = x_i \oplus (\hat{x}_j \cdot \hat{x}_l \cdot \ldots \cdot \hat{x}_q)$ шляхом перебору значень i, j, l, …, q, де $i,j,l \in [1,2,\ldots,n]$, …, $q \in [1,2,\ldots,n]$ за умови $i \neq j \neq l \neq \ldots \neq q$; $j < l < \ldots < q$ отримати основні n-розрядні розширені матричні елементарні функції.

2. На основі перебору значень інверсії $\hat{x}_j$, $\hat{x}_l$, … , $\hat{x}_q$ де, $\hat{x}_j \in [x_j, \bar{x}_j]$, $\hat{x}_l \in [x_l, \bar{x}_l]$, …, $\hat{x}_q \in [x_q, \bar{x}_q]$ підставивши отримані набори в основні трьохрозрядні розширені матричні елементарні функції, отримати повну множину прямих трьохрозрядних розширених матричних елементарних функцій.

3. На основі виразу $f = x_i \oplus (\hat{x}_j \cdot \hat{x}_l \cdot \ldots \cdot \hat{x}_q) \oplus 1$ інвертувавши множину прямих трьохрозрядних розширених матричних елементарних функцій, шляхом додавання по модулю два, отримати множину обернених розширених матричних елементарних функцій.

4. Об’єднавши множини прямих і обернених елементарних функцій, отримати повну множину трьохрозрядних розширених матричних елементарних функцій.

Можливо синтезувати модель прямої m-розрядної елементарної функції розширеного матричного перетворення в дискретному представленні: $f = x_i \cdot \hat{x}_j \vee x_i \cdot \hat{x}_l \vee \ldots \vee x_i \cdot \hat{x}_q \vee (\bar{x}_i \cdot \bar{\hat{x}}_j \cdot \bar{\hat{x}}_l \cdot \ldots \cdot \bar{\hat{x}}_q)$, де $i,j,l \in [1,2,\ldots,n]$, …, $q \in [1,2,\ldots,n]$ за умов $i \neq j \neq l \neq \ldots \neq q$ та $j < l < \ldots < q$.

Можливо синтезувати модель оберненої m-розрядної елементарної функції розширеного матричного перетворення в дискретному представленні:

$$f = \bar{x}_i \cdot \hat{x}_j \vee \bar{x}_i \cdot \hat{x}_l \vee \ldots \vee \bar{x}_i \cdot \hat{x}_q \vee (x_i \cdot \bar{\hat{x}}_j \cdot \bar{\hat{x}}_l \cdot \ldots \cdot \bar{\hat{x}}_q).$$

Кількість прямих m-розрядних елементарних функцій розширеного матричного перетворення визначається:

$$K_{П} = K_{O} = 2^{m-1} \cdot m \cdot C_n^m = \frac{2^{m-1} \cdot m \cdot n!}{m!(n-m)!}.$$

Загальна кількість m-розрядних елементарних функцій розширеного матричного перетворення (прямих та обернених) визначається:

$$K_{\Sigma} = K_{П} + K_{O} = 2 \cdot 2^{m-1} \cdot m \cdot C_n^m = \frac{2^m \cdot m \cdot n!}{m!(n-m)!}.$$

Для криптографічного перетворення n-розрядної інформації можуть бути використані елементарні функції розрядності від 3 до n.

Кількість n-розрядних елементарних функцій розширеного матричного перетворення можна отримати

$$K_{\Sigma} = \Sigma_{m=3}^{n} \frac{2^m \cdot m \cdot n!}{m!(n-m)!}.$$

В узагальненому вигляді операції розширеного матричного криптографічного перетворення, синтезовані на основі за модулем два, можна

представити як

$$\vec{F}_k = \begin{bmatrix} x_l \oplus d_1(\hat{x}_i \cdot \hat{x}_j) \\ x_i \oplus d_2(\hat{x}_l \cdot \hat{x}_j) \\ x_j \oplus d_3(\hat{x}_i \cdot \hat{x}_l) \end{bmatrix} \oplus \begin{bmatrix} b_1^d \\ b_2^d \\ b_n^d \end{bmatrix},$$

де $l,i,j \in \{1...3\}$, $b_i^d \in \{0,1\}$.

Дана операція може бути використана для криптоперетворення у таких випадках:

1. Якщо в операції криптоперетворення елементарна функція має в розширенні логічний добуток двох аргументів без інверсії, тоді в даній операції будуть присутні елементарна функція, яка матиме в розширенні логічний добуток двох аргументів з інверсіями, та елементарна функція, яка матиме в розширенні логічний добуток двох аргументів, один з яких з інверсією, а інший – без інверсії;

2. Якщо в операції криптоперетворення елементарна функція має в розширенні логічний добуток двох аргументів з інверсіями, тоді в даній операції будуть присутні елементарна функція, яка матиме в розширенні логічний добуток двох аргументів без інверсій, та елементарна функція, яка матиме в розширенні логічний добуток двох аргументів, один з яких з інверсією, а інший – без інверсії;

3. Якщо в операції криптоперетворення елементарна функція має в розширенні логічний добуток двох аргументів, один з яких із інверсією, а інший без інверсії, тоді в даній операції будуть присутні елементарні функції, які матимуть в розширенні логічний добуток двох аргументів з інверсіями та без інверсій, або елементарні функції, які матимуть в розширенні логічний добуток двох аргументів, один з яких буде з інверсією, а інший – без інверсії.

Формалізуємо правила побудови операції криптографічного перетворення. Для $F\begin{pmatrix} a_i \\ a_j \\ a_l \end{pmatrix} = \begin{pmatrix} b_i \oplus b_j \cdot b_l \\ c_j \oplus c_i \cdot c_l \\ d_l \oplus d_i \cdot d_j \end{pmatrix}$, заданої множиною f другого степеня $f = a_i \oplus (a_j \cdot a_l)$ змінних $a_i,\ a_j,\ a_l$, $i,j,l \in \{1,2,3\}$, $i \neq j \neq l$, $a_i, b_i, c_i, d_i \in \{x_i, \bar{x}_i\}$, існує $F^{-1}\begin{pmatrix} a_i \\ a_j \\ a_l \end{pmatrix}$ лише тоді:

1. Якщо $b_j = x_j$, $b_l = x_l$, то або $\begin{cases} c_i = \bar{x}_i,\ c_l = \bar{x}_l, \\ \left[\begin{array}{l} d_i = \bar{x}_i, d_l = x_l, \\ d_i = x_i, d_j = \bar{x}_j, \end{array}\right. \end{cases}$ або $\begin{cases} \left[\begin{array}{l} c_i = \bar{x}_i, c_l = x_l, \\ c_i = x_i, c_l = \bar{x}_l, \end{array}\right. \\ d_i = \bar{x}_i,\ d_j = \bar{x}_j. \end{cases}$

2. Якщо $b_j = \bar{x}_j$, $b_l = \bar{x}_l$, то або $\begin{cases} c_i = x_i,\ c_l = x_l, \\ \left[\begin{array}{l} d_i = \bar{x}_i, d_l = x_l, \\ d_i = x_i, d_j = \bar{x}_j, \end{array}\right. \end{cases}$ або $\begin{cases} \left[\begin{array}{l} c_i = \bar{x}_i, c_l = x_l, \\ c_i = x_i, c_l = \bar{x}_l, \end{array}\right. \\ d_i = x_i,\ d_j = x_j. \end{cases}$

3. Якщо $\begin{bmatrix} b_i = \bar{x}_j, b_l = x_l, \\ b_i = x_j, b_l = \bar{x}_l, \end{bmatrix}$ то або $\begin{cases} c_i = \bar{x}_i,\ c_l = \bar{x}_l, \\ d_i = x_i, d_j = x_j \end{cases}$ або $\begin{cases} c_i = x_i, c_l = x_l \\ d_i = \bar{x}_i,\ d_j = \bar{x}_j, \end{cases}$ або

$$\begin{cases} \begin{bmatrix} c_i = \bar{x}_i, c_l = x_l, \\ c_i = x_i, c_l = \bar{x}_l, \end{bmatrix} \\ \begin{bmatrix} d_i = \bar{x}_i, d_l = x_l, \\ d_i = x_i, d_j = \bar{x}_j. \end{bmatrix} \end{cases}$$

Таким чином, операція $F^{-1}\begin{pmatrix} a_i \\ a_j \\ a_l \end{pmatrix}$ існує лише тоді, якщо $\begin{bmatrix} \begin{cases} b_i \oplus c_i \oplus d_i = 1 \\ b_i \vee c_i \vee d_i = 1 \end{cases} \\ \begin{cases} b_j \oplus c_j \oplus d_j = 1 \\ b_j \vee c_j \vee d_j = 1 \end{cases} \\ \begin{cases} b_l \oplus c_l \oplus d_l = 1 \\ b_l \vee c_l \vee d_l = 1 \end{cases} \end{bmatrix}$.

Ці правила дозволяють синтезувати операцію розширеного матричного криптографічного перетворення на основі випадкового вибору трьох значень булевих змінних b_j, b_l, c_i.

Формалізуємо правила синтезу оберненої операції криптоперетворення.

Нехай заданій множині f другого степеня $f = a_1 \oplus (a_2 \cdot a_3)$ змінних a_1, a_2, a_3 існує обернена і, причому, єдина f^{-1} того ж класу, а саме: $f^{-1} = A_1 \oplus (A_2 \cdot A_3)$, при цьому:

1. Якщо змінна $a_i \in \{a_1;\ a_2;\ a_3\}$, то $A_i \in \{a_1;\ a_2;\ a_3\}$ для $i = 1,2,3$;

2. Якщо змінна $a_i \in \{\bar{a}_1;\ \bar{a}_2;\ \bar{a}_3\}$, то $A_i \in \{\bar{a}_1;\ \bar{a}_2;\ \bar{a}_3\}$ для $i = 1,2,3$;

3. Якщо $\begin{cases} a_2 \in \{\bar{a}_1;\ \bar{a}_2;\ \bar{a}_3\} \\ a_3 \in \{a_1;\ a_2;\ a_3\} \end{cases}$ і $\begin{cases} a_2 \in \{a_1;\ a_2;\ a_3\} \\ a_3 \in \{\bar{a}_1;\ \bar{a}_2;\ \bar{a}_3\} \end{cases}$, то або $\begin{cases} A_2 \in \{\bar{a}_1;\ \bar{a}_2;\ \bar{a}_3\} \\ A_3 \in \{a_1;\ a_2;\ a_3\} \end{cases}$, або $\begin{cases} A_2 \in \{a_1;\ a_2;\ a_3\} \\ A_3 \in \{\bar{a}_1;\ \bar{a}_2;\ \bar{a}_3\} \end{cases}$.

4. Якщо заданій множині f першого степеня $f = a_1$ змінних a_1, a_2, a_3 існує обернена і, причому, єдина f^{-1} того ж класу, а саме: $f^{-1} = A_1$, при цьому: якщо змінна $a_i \in \{a_1;\ a_2;\ a_3\}$,то $A_i \in \{a_1;\ a_2;\ a_3\}$ для $i = 1,2,3$.

Алгоритмічний метод синтезу операції оберненого розширеного матричного криптографічного перетворення полягає в наступному.

Якщо операція прямого криптоперетворення $F^k\begin{pmatrix} a_i \\ a_j \\ a_l \end{pmatrix} = \begin{pmatrix} a_{pi} \oplus a_{pj} \cdot a_{pl} \\ a_{rj} \oplus a_{ri} \cdot a_{rl} \\ a_{tl} \oplus a_{ti} \cdot a_{tj} \end{pmatrix}$, тоді операція оберненого криптоперетворення

$$F^d\begin{pmatrix} A_i \\ A_j \\ A_l \end{pmatrix} = \begin{pmatrix} A_{ir} \oplus A_{it} \cdot A_{ip} \\ A_{jt} \oplus A_{jp} \cdot A_{jr} \\ A_{lp} \oplus A_{lt} \cdot A_{lr} \end{pmatrix}, \quad \text{де} \quad i,j,l,p,r,t \in \{1,2,3\}, \quad i \neq j \neq l; \quad p \neq r \neq t;$$

$A_{ji} \in \{y_i, \bar{y}_i\}$.

За умови: якщо $\begin{cases} a_{ir} = \bar{x}_i, \ a_{lr} = \bar{x}_l, \\ a_{it} = x_i, a_{jt} = x_j \end{cases}$ або, $\begin{cases} a_{ri} = x_i, a_{rl} = x_l, \\ a_{ti} = \bar{x}_i, \ a_{tl} = \bar{x}_l \end{cases}$, отримаємо

$\begin{cases} A_{lt} = \bar{y}_t, \ A_{lr} = \bar{y}_r, \\ A_{lt} = y_t, \ A_{lr} = y_r \end{cases}$ або $\begin{cases} A_{lt} = y_t, \ A_{lr} = y_r, \\ A_{lt} = \bar{y}_t, \ A_{lr} = \bar{y}_r. \end{cases}$ Якщо $\begin{bmatrix} a_{pj} = \bar{x}_j, a_{pl} = x_l, \\ a_{pj} = x_j, a_{pl} = \bar{x}_l \end{bmatrix}$, отримаємо

$$\begin{cases} \begin{bmatrix} A_{jp} = y_p \\ A_{jr} = \bar{y}_r \end{bmatrix}, \text{ якщо } A_{ip} = \bar{y}_p; \\ \begin{bmatrix} A_{jp} = \bar{y}_p \\ A_{jr} = y_r \end{bmatrix}, \text{ якщо } A_{ip} = y_p; \end{cases} \text{ або } \begin{cases} \begin{bmatrix} A_{jp} = y_p \\ A_{jr} = \bar{y}_r \end{bmatrix}, \text{ якщо } A_{ir} = y_r; \\ \begin{bmatrix} A_{jp} = \bar{y}_p \\ A_{jr} = y_r \end{bmatrix}, \text{ якщо } A_{ir} = \bar{y}_r. \end{cases}$$

Даний метод деталізується на побудову обернених операцій при наявності однієї чи двох замін, а також на більшу кількість змінних.

Метод синтезу операції оберненого розширеного матричного криптографічного перетворення на основі індексації рядків полягає в наступному.

Для того, щоб побудувати для операції розширеного матричного криптографічного перетворення з двома доповненнями операцію оберненого перетворення, потрібно:

1) побудувати лінійну операцію оберненого перетворення у матричному представленні;

2) побудувати відповідні два доповнення, враховуючи, що прямі доповнення переходять у прямі, інверсні – у інверсні, а у змішаних доповненнях порядок інвертування зберігається, якщо послідовність індексів доповнення співпадає з послідовністю індексів відповідних рядків матричної моделі для операції перетворення, і змінюється – у протилежному випадку.

Четвертий розділ присвячений реалізації криптопримітивів ковзного шифрування на основі матричних операцій криптографічного перетворення.

Шестиразове спрощене ковзне шифрування перетворює послідовність p_k у q_k.

$$\begin{aligned} q_1 &= x_1; \\ q_2 &= x_2; \\ q_3 &= x_1 \oplus x_3; \\ q_4 &= x_2 \oplus x_4; \\ q_5 &= x_3 \oplus x_5; \\ q_6 &= x_4 \oplus x_6; \\ q_7 &= x_5 \oplus x_7; \\ q_8 &= x_6 \oplus x_8; \\ q_9 &= x_1 \oplus x_7 \oplus x_9; \\ q_{10} &= x_2 \oplus x_8 \oplus x_{10}; \\ q_{11} &= x_1 \oplus x_3 \oplus x_9 \oplus x_{11}; \\ q_{12} &= x_2 \oplus x_4 \oplus x_{10} \oplus x_{12}; \\ q_{13} &= x_3 \oplus x_5 \oplus x_{11} \oplus x_{13}; \\ q_{14} &= x_4 \oplus x_6 \oplus x_{12} \oplus x_{14}; \\ &\ldots\ldots\ldots \end{aligned}$$

Функція перетворення одного елемента шестиразового спрощеного ковзного шифрування може бути описана рекурентною послідовністю

$$q_n = q_{n-8} \oplus x_{n-2} \oplus x_n.$$

На основі викладеного вище можна стверджувати, що функції перетворення елементів ковзного шифрування представляються рекурентними послідовностями і є окремими випадками з усієї множини рекурентних послідовностей, які можуть бути застосовані для синтезу матричних операцій криптографічного перетворення.

Примітив шестиразового ковзного шифрування побудований на основі отриманої рекурентної послідовності і може бути представлений у вигляді матричної моделі

$$F(x) = \begin{bmatrix} x_1 \\ x_2 \\ x_1 \oplus x_3 \\ x_2 \oplus x_4 \\ x_3 \oplus x_5 \\ x_4 \oplus x_6 \\ x_5 \oplus x_7 \\ x_6 \oplus x_8 \\ x_1 \oplus x_7 \oplus x_9 \\ x_2 \oplus x_8 \oplus x_{10} \\ x_1 \oplus x_3 \oplus x_9 \oplus x_{11} \\ x_2 \oplus x_4 \oplus x_{10} \oplus x_{12} \\ x_3 \oplus x_5 \oplus x_{11} \oplus x_{13} \\ x_4 \oplus x_6 \oplus x_{12} \oplus x_{14} \\ . \ . \ . \ . \ . \ . \ . \ . \ . \ . \end{bmatrix} \oplus \begin{bmatrix} m_1 \oplus m_2 \oplus m_3 \oplus m_4 \oplus m_5 \oplus m_6 \\ m_2 \oplus m_3 \oplus m_5 \\ m_1 \oplus m_2 \oplus m_3 \oplus m_6 \\ m_2 \oplus m_3 \\ m_4 \oplus m_5 \oplus m_6 \\ m_5 \\ m_6 \\ 0 \\ m_1 \oplus m_2 \oplus m_3 \oplus m_4 \oplus m_5 \oplus m_6 \\ m_2 \oplus m_3 \oplus m_5 \\ m_1 \oplus m_2 \oplus m_3 \oplus m_6 \\ m_2 \oplus m_3 \\ m_4 \oplus m_5 \oplus m_6 \\ m_5 \\ . \ . \ . \ . \ . \ . \ . \ . \ . \ . \end{bmatrix}$$

Рекурентна послідовність, яка описує блок обробки раундового ключа, представляється як $m_n = m_{n-8}$.

Оскільки $m_1 \oplus m_2 \oplus .....\oplus m_n = m_k$, і випадкові елементи раундового ключа формуються на основі одного й того ж алгоритму, отже, враховуючи теорему Шеннона, можна стверджувати, що повторне застосування елементів раундового ключа не підвищує криптостійкості.

Виходячи з цього, з'явилася можливість оптимізувати операцію криптографічного перетворення блоку обробки раундового ключа без зменшення криптостійкості наступною моделлю:

$$F(x) = \begin{bmatrix} x_1 \\ x_1 \oplus x_{21} \\ x_1 \oplus x_2 \oplus x_3 \\ x_1 \oplus x_2 \oplus x_3 \oplus x_4 \\ x_1 \oplus x_2 \oplus x_3 \oplus x_4 \oplus x_5 \\ . \ . \ . \ . \ . \ . \ . \ . \ . \\ x_1 \oplus x_2 \oplus x_3 \oplus .....\oplus x_n \end{bmatrix} \oplus \begin{bmatrix} m_1 \\ m_2 \\ m_3 \\ m_4 \\ m_5 \\ m_6 \\ m_6 \\ ..... \\ m_L \end{bmatrix}, \text{ де } L - \text{кількість раундів.}$$

Таким чином оптимізована операція дозволяє збільшити швидкість обробки раундового ключа для моделі примітиву ковзного шифрування до п’яти разів, а швидкість виконання операцій криптографічного перетворення підвищити до двох разів відносно реалізації матричної операції.

Така оптимізація дає змогу зменшити апаратну складність реалізації примітиву ковзного шифрування за рахунок скорочення кількості операцій додавання за модулем два.

Використання матричних операцій криптографічного перетворення дає можливість розпаралелити процес реалізації примітиву ковзного шифрування.

Застосування матричних операцій для багаторазового спрощеного ковзного шифрування дозволяє скоротити кількість операцій в порівнянні з одноразовим спрощеним ковзним шифруванням, що дає виграш як у часі, так і спрощенні складності реалізації примітивів.

Отримано узагальнений вираз рекурентної послідовності для опису виконання багаторазового прямого примітиву ковзного шифрування (ПКШ): $y_i^k = y_{i-1}^k \oplus y_i^{k-1}$, де $y_0^k = y_d^{k-1}$ та $i \in \{1,\dots,d\}$, де, в свою чергу, k – кількість раундів ковзного перетворення, а d – розрядність перетворення.

П’ятий розділ присвячений моделюванню операцій для мультиопераційних матричних криптографічних примітивів.

Отримані узагальнені матричні моделі операції додавання за модулем два та за модулем чотири будуть представлені відповідно: $F_{\mathrm{mod}2} = \begin{bmatrix} x_1 \\ x_2 \end{bmatrix} \oplus \begin{bmatrix} k_1 \\ k_2 \end{bmatrix}$, $F_{\mathrm{mod}4} = \begin{bmatrix} x_1 \oplus k_2 \cdot x_2 \\ x_2 \end{bmatrix} \oplus \begin{bmatrix} k_1 \\ k_2 \end{bmatrix}$.

Проведемо моделювання двохоперандних операцій, які відповідають властивостям A@B=C; B@A=C; A@C=B; C@A=B; B@C=A; C@B=A, де @ – позначення операції, та які можуть використовуватися для розробки криптоалгоритмів.

Для того, щоб операція володіла вказаними властивостями, необхідне виконання наступних умов: у кожному стовпці матриці перетворення не повинно бути повтору команди (значення операнда); у кожному рядку матриці перетворення не повинно бути повтору значення операнда (команди); матриця повинна бути симетрична відносно головної діагоналі, тобто має виконуватися рівність $A[i,j] = A[j,i]$.

Для пошуку таких операцій використаємо табличне представлення операцій (табл.1).

У результаті експерименту були отримані двохоперандні операції криптографічного перетворення (табл. 2).

Таблиця 1

Табличне представлення операцій

Значення операнда 1	**Значення операнда 2**				**Значення операнда 2**				**Значення операнда 2**			
	0	**1**	**2**	**3**	**0**	**1**	**2**	**3**	**0**	**1**	**2**	**3**
0	0	1	2	3	0	1	2	3	0	1	2	3
1	1	0	3	2	1	3	0	2	1	0	3	2
2	2	3	1	0	2	0	3	1	2	3	0	1
3	3	2	0	1	3	2	1	0	3	2	1	0

Таблиця 2

Результати моделювання операцій над двома операндами

Набори матричних операцій			
<1, 7, 13, 19> <7, 1, 19, 13> <13, 19, 1, 7> <19, 13, 7, 1>	<1, 7, 15, 21> <7, 1, 21, 15> <15, 21, 7, 1> <21, 15, 1, 7>	<1, 8, 13, 20> <8, 13, 20, 1> <13, 20, 1, 8> <20, 1, 8, 13>	<1, 10, 16, 19> <10, 19, 1, 16> <16, 1, 19, 10> <19, 16, 10, 1>
<2, 19, 14, 7> <7, 2, 19, 14> <14, 7, 2, 19> <19, 14, 7, 2>	<2, 20, 14, 8> <8, 14, 20, 2> <14, 8, 2, 20> <20, 2, 8, 14>	<2, 20, 17, 11> <11, 17, 2, 20> <17, 11, 20, 2> <20, 2, 11, 17>	<2, 24, 18, 8> <8, 18, 24, 2> <18, 2, 8, 24> <24, 8, 2, 18>
<3, 9, 19, 13> <9, 3, 13, 19> <13, 19, 3, 9> <19, 13, 9, 3>	<3, 9, 21, 15> <9, 3, 15, 21> <15, 21, 9, 3> <21, 15, 3, 9>	<3, 11, 23, 15> <11, 15, 3, 23> <15, 23, 11, 3> <23, 3, 15, 11>	<3, 12, 21, 18> <12, 21, 18, 3> <18, 3, 12, 21> <21, 18, 3, 12>
<4, 13, 7, 22> <7, 4, 22, 13> <13, 22, 4, 7> <22, 7, 13, 4>	<4, 16, 10, 22> <10, 22, 4, 16> <16, 4, 22, 10> <22, 10, 16, 4>	<4, 16, 12, 24> <12, 24, 16, 4> <16, 4, 24, 12> <24, 12, 4, 16>	<4, 17, 10, 23> <10, 23, 4, 17> <17, 10, 23, 4> <23, 4, 17, 10>
<5, 21, 9, 17> <9, 5, 17, 21> <17, 9, 21, 5> <21, 17, 5, 9>	<5, 22, 11, 16> <11, 16, 5, 22> <16, 5, 22, 11> <22, 11, 16, 5>	<5, 23, 8, 14> <8, 14, 23, 5> <14, 8, 5, 23> <23, 5, 14, 8>	<5, 23, 11, 17> <11, 17, 5, 23> <17, 11, 23, 5> <23, 5, 17, 11>
<6, 14, 20, 12> <12, 20, 14, 6> <14, 12, 6, 20> <20, 6, 12, 14>	<6, 15, 24, 9> <9, 6, 15, 24> <15, 24, 9, 6> <24, 9, 6, 15>	<6, 18, 22, 10> <10, 22, 6, 18> <18, 6, 10, 22> <22, 10, 18, 6>	<6, 18, 24, 12> <12, 24, 18, 6> <18, 6, 12, 24> <24, 12, 6, 18>

У таблиці 2 позначення <6, 14, 20, 12> – скорочений запис моделі двохоперандної операції, де числами представлено номери одноопераднних операцій, що поєднуються (табл. 3).

Результати моделювання операцій показали, що дані множини операцій є математичними групами з точністю до перестановки.

Таблиця 3

Вхідні дані для моделювання двохоперандних операцій
(група дворозрядних одноопераднних операцій криптографічного перетворення)

Номер операції	**Модель операції**	**Номер операції**	**Модель операції**	**Номер операції**	**Модель операції**
1	$F_1 = \begin{bmatrix} x_1 \\ x_2 \end{bmatrix} \oplus \begin{bmatrix} 0 \\ 0 \end{bmatrix}$	**9**	$F_9 = \begin{bmatrix} x_1 \\ x_1 \oplus x_2 \end{bmatrix} \oplus \begin{bmatrix} 0 \\ 1 \end{bmatrix}$	**17**	$F_{17} = \begin{bmatrix} x_2 \\ x_1 \oplus x_2 \end{bmatrix} \oplus \begin{bmatrix} 1 \\ 0 \end{bmatrix}$
2	$F_2 = \begin{bmatrix} x_1 \oplus x_2 \\ x_2 \end{bmatrix} \oplus \begin{bmatrix} 0 \\ 0 \end{bmatrix}$	**10**	$F_{10} = \begin{bmatrix} x_2 \\ x_1 \end{bmatrix} \oplus \begin{bmatrix} 0 \\ 1 \end{bmatrix}$	**18**	$F_{18} = \begin{bmatrix} x_1 \oplus x_2 \\ x_1 \end{bmatrix} \oplus \begin{bmatrix} 1 \\ 0 \end{bmatrix}$
3	$F_3 = \begin{bmatrix} x_1 \\ x_1 \oplus x_2 \end{bmatrix} \oplus \begin{bmatrix} 0 \\ 0 \end{bmatrix}$	**11**	$F_{11} = \begin{bmatrix} x_2 \\ x_1 \oplus x_2 \end{bmatrix} \oplus \begin{bmatrix} 0 \\ 1 \end{bmatrix}$	**19**	$F_{19} = \begin{bmatrix} x_1 \\ x_2 \end{bmatrix} \oplus \begin{bmatrix} 1 \\ 1 \end{bmatrix}$
4	$F_4 = \begin{bmatrix} x_2 \\ x_1 \end{bmatrix} \oplus \begin{bmatrix} 0 \\ 0 \end{bmatrix}$	**12**	$F_{12} = \begin{bmatrix} x_1 \oplus x_2 \\ x_1 \end{bmatrix} \oplus \begin{bmatrix} 0 \\ 1 \end{bmatrix}$	**20**	$F_{20} = \begin{bmatrix} x_1 \oplus x_2 \\ x_2 \end{bmatrix} \oplus \begin{bmatrix} 1 \\ 1 \end{bmatrix}$
5	$F_5 = \begin{bmatrix} x_2 \\ x_1 \oplus x_2 \end{bmatrix} \oplus \begin{bmatrix} 0 \\ 0 \end{bmatrix}$	**13**	$F_{13} = \begin{bmatrix} x_1 \\ x_2 \end{bmatrix} \oplus \begin{bmatrix} 1 \\ 0 \end{bmatrix}$	**21**	$F_{21} = \begin{bmatrix} x_1 \\ x_1 \oplus x_2 \end{bmatrix} \oplus \begin{bmatrix} 1 \\ 1 \end{bmatrix}$
6	$F_6 = \begin{bmatrix} x_1 \oplus x_2 \\ x_1 \end{bmatrix} \oplus \begin{bmatrix} 0 \\ 0 \end{bmatrix}$	**14**	$F_{14} = \begin{bmatrix} x_1 \oplus x_2 \\ x_2 \end{bmatrix} \oplus \begin{bmatrix} 1 \\ 0 \end{bmatrix}$	**22**	$F_{22} = \begin{bmatrix} x_2 \\ x_1 \end{bmatrix} \oplus \begin{bmatrix} 1 \\ 1 \end{bmatrix}$
7	$F_7 = \begin{bmatrix} x_1 \\ x_2 \end{bmatrix} \oplus \begin{bmatrix} 0 \\ 1 \end{bmatrix}$	**15**	$F_{15} = \begin{bmatrix} x_1 \\ x_1 \oplus x_2 \end{bmatrix} \oplus \begin{bmatrix} 1 \\ 0 \end{bmatrix}$	**23**	$F_{23} = \begin{bmatrix} x_2 \\ x_1 \oplus x_2 \end{bmatrix} \oplus \begin{bmatrix} 1 \\ 1 \end{bmatrix}$
8	$F_8 = \begin{bmatrix} x_1 \oplus x_2 \\ x_2 \end{bmatrix} \oplus \begin{bmatrix} 0 \\ 1 \end{bmatrix}$	**16**	$F_{16} = \begin{bmatrix} x_2 \\ x_1 \end{bmatrix} \oplus \begin{bmatrix} 1 \\ 0 \end{bmatrix}$	**24**	$F_{24} = \begin{bmatrix} x_1 \oplus x_2 \\ x_1 \end{bmatrix} \oplus \begin{bmatrix} 1 \\ 1 \end{bmatrix}$

Таблиця 4

Узагальнені моделі груп операцій

Номер групи		**0**	**1**	**2**	**3**	Моделі операцій	
						Позначення	Модель
1	**0**	a	b	d	c	**<1,7,13,19>**	$O_{1,7,13,19}=\begin{cases}\begin{bmatrix}x_1\\x_2\end{bmatrix}, \text{якщо } k_1=0; k_2=0\\ \begin{bmatrix}x_1\\x_2\oplus 1\end{bmatrix}, \text{якщо } k_1=0; k_2=1\\ \begin{bmatrix}x_1\oplus 1\\x_2\end{bmatrix}, \text{якщо } k_1=1; k_2=0\\ \begin{bmatrix}x_1\oplus 1\\x_2\oplus 1\end{bmatrix}, \text{якщо } k_1=1; k_2=1\end{cases}$
	1	b	a	c	d		
	2	d	c	a	b		
	3	c	d	b	a		
2	**0**	a	c	d	b	**<2,19,14,7>**	$O_{2,19,14,7}=\begin{cases}\begin{bmatrix}x_1\oplus x_2\\x_2\end{bmatrix}, \text{якщо } k_1=0; k_2=0\\ \begin{bmatrix}x_1\oplus 1\\x_2\oplus 1\end{bmatrix}, \text{якщо } k_1=0; k_2=1\\ \begin{bmatrix}x_1\oplus x_2\oplus 1\\x_2\end{bmatrix}, \text{якщо } k_1=1; k_2=0\\ \begin{bmatrix}x_1\\x_2\oplus 1\end{bmatrix}, \text{якщо } k_1=1; k_2=1\end{cases}$
	1	c	d	b	a		
	2	d	b	a	c		
	3	b	a	c	d		
3	**0**	a	b	c	d	**<3,9,19,13>**	$O_{3,9,19,13}=\begin{cases}\begin{bmatrix}x_1\\x_1\oplus x_2\end{bmatrix}, \text{якщо } k_1=0; k_2=0\\ \begin{bmatrix}x_1\\x_1\oplus x_2\oplus 1\end{bmatrix}, \text{якщо } k_1=0; k_2=1\\ \begin{bmatrix}x_1\oplus 1\\x_2\oplus 1\end{bmatrix}, \text{якщо } k_1=1; k_2=0\\ \begin{bmatrix}x_1\oplus 1\\x_2\end{bmatrix}, \text{якщо } k_1=1; k_2=1\end{cases}$
	1	b	a	d	c		
	2	c	d	b	a		
	3	d	c	a	b		
4	**0**	a	d	b	c	**<4,13,7,22>**	$O_{4,13,7,22}=\begin{cases}\begin{bmatrix}x_2\\x_1\end{bmatrix}, \text{якщо } k_1=0; k_2=0\\ \begin{bmatrix}x_1\oplus 1\\x_2\end{bmatrix}, \text{якщо } k_1=0; k_2=1\\ \begin{bmatrix}x_1\\x_2\oplus 1\end{bmatrix}, \text{якщо } k_1=1; k_2=0\\ \begin{bmatrix}x_2\oplus 1\\x_1\oplus 1\end{bmatrix}, \text{якщо } k_1=1; k_2=1\end{cases}$
	1	d	c	a	b		
	2	b	a	c	d		
	3	c	b	d	a		

Розглянуті операції можуть бути використані, наприклад, при реалізації багаторазових ПКШ. Так, при синтезі прямого ПКШ замість додавання за

модулем два можуть бути використані й інші синтезовані операції. Тоді узагальнену модель рекурентної послідовності можливо записати як: $y_i^k = y_{i-1}^k(\nabla) y_i^{k-1}$, де $y_0^k = y_d^{k-1}$ $i \in \{1,\ldots,d\}$, де, в свою чергу, k – кількість раундів ковзного шифрування, d – розрядність перетворення, а (∇) – двохоперандна криптографічна операція.

Операція, яка використовується для реалізації багаторазового криптопримітиву ковзного шифрування, може змінюватися на будь-якому раунді зашифрування. Узагальнену модель рекурентної послідовності багаторазового криптопримітиву ковзного шифрування зі змінною раундовою операцією запишемо як $y_i^k = y_{i-1}^k(\nabla k) y_i^{k-1}$, де $y_0^k = y_d^{k-1}$ $i \in \{1,\ldots,d\}$, де, в свою чергу, k – кількість раундів ковзного шифрування, d – розрядність перетворення, (∇k) – двохоперандна криптографічна операція для k-го раунду.

Крім того, операція, яка використовується для реалізації багаторазового криптопримітиву ковзного шифрування, може змінюватися деяку кількість разів у самому раунді зашифрування. Максимальна кількість змінних операцій раунду визначається кількістю елементів примітиву ковзного шифрування. Тому узагальнену модель рекурентної послідовності багаторазового криптопримітиву ковзного шифрування зі змінними операціями в раунді можна представити як

$$y_i^k = y_{i-1}^k(\nabla k_i) y_i^{k-1}, \qquad (3)$$

де $y_0^{k_i} = y_d^{k_i-1}$ $i \in \{1,\ldots,d\}$, де, в свою чергу, k – кількість раундів ковзного шифрування, d – розрядність перетворення, (∇k_i) – двохоперандна криптографічна операція для перетворення i-того елемента для k-го раунду.

Шостий розділ присвячено синтезу криптоалгоритмів на основі операцій криптографічного перетворення інформації.

Для забезпечення максимальної криптостійкості повинна виконуватися основна вимога до вибору операцій, а саме: будь-які вибрані операції, що виконуються послідовно, не належать одній групі.

Складність реалізації будь-якої операції $F_{i.j}$ однакова, тому складність операції криптографічного перетворення дорівнює складності виконуваної операції: $C(F_i) = C(F_{i.j}),\ j = 1..k$. Звідси, складність криптографічного алгоритму $C_{ALG} = \sum_{i=1}^{n} C(F_i) = \sum_{i=1}^{n} C(F_{i.j}) = C(F_{1.j}) + C(F_{2.j}) + \ldots + C(F_{n.j})$, де $j = 1..k$, n – кількість операцій перетворення, що реалізують алгоритм криптографічного перетворення ($F_i, i = 1..n$); k – кількість операцій групи, що реалізує операцію перетворення.

Час виконання криптографічного алгоритму розраховується як сума часу виконання операцій в алгоритмі криптографічного перетворення, тому що операції виконуються послідовно:

$$Time_{ALG} = \sum_{i=1}^{n} Time(F_i) = \sum_{i=1}^{n} Time(F_{i.j}) = Time(F_{1.j}) + Time(F_{2.j}) + \ldots + Time(F_{n.j}),$$

де $j = 1..k$, n – кількість операцій перетворення, що реалізують алгоритм криптографічного перетворення ($F_i, i = 1..n$); k – кількість операцій групи, що реалізує операцію перетворення.

Швидкість реалізації алгоритму визначається як

$$V_{ALG} = \frac{1}{Time_{ALG}} = \frac{1}{Time(F_{1.j}) + Time(F_{2.j}) + \ldots + Time(F_{n.j})} = \frac{1}{\sum_{i=1}^{n} Time(F_{i.j})}.$$

Час реалізації криптоалгоритму, виходячи із його складності:

$$Time_{ALG} = \sum_{i=1}^{n} k_i \cdot C(F_{i.j}) = k_1 \cdot C(F_{1.j}) + k_2 \cdot C(F_{2.j}) + \ldots + k_n \cdot C(F_{n.j}).$$

Враховуючи зазначене вище, швидкість виконання криптоалгоритму визначатиметься як

$$V_{ALG} = \frac{1}{\sum_{i=1}^{n} k_i \cdot C(F_{i.j})} = \frac{1}{k_1 \cdot C(F_{1.j}) + k_2 \cdot C(F_{2.j}) + \ldots + k_n \cdot C(F_{n.j})}.$$

Криптостійкість операції F_i визначається як добуток значень криптостійкості операцій:

$$K_{ALG} = \prod_{i=1}^{n} K(F_i) = \prod_{i=1}^{n} K(F_{i.j}) = K(F_{1.j}) \cdot K(F_{2.j}) \cdot \ldots \cdot K(F_{n.j}).$$

Крім цього, криптографічний алгоритм може здійснюватися послідовністю перетворень, кожне з яких побудоване на основі різних операцій, при цьому послідовне виконання операцій над однаковою кількістю операндів за умови використання операцій з різних математичних груп забезпечує підвищення криптостійкості.

Застосування операцій криптографічного перетворення можливо в якості макро- та мікрооперацій. Наприклад, модель багаторазового криптопримітиву ковзного шифрування (3) описує макрооперацію y_i^k, яка містить в собі мікрооперацію ∇k_i.

Здійснено аналіз результатів тестування алгоритмів синтезованих на основі операцій криптографічного перетворення інформації на основі тестів NIST STS (рис.3, 4).

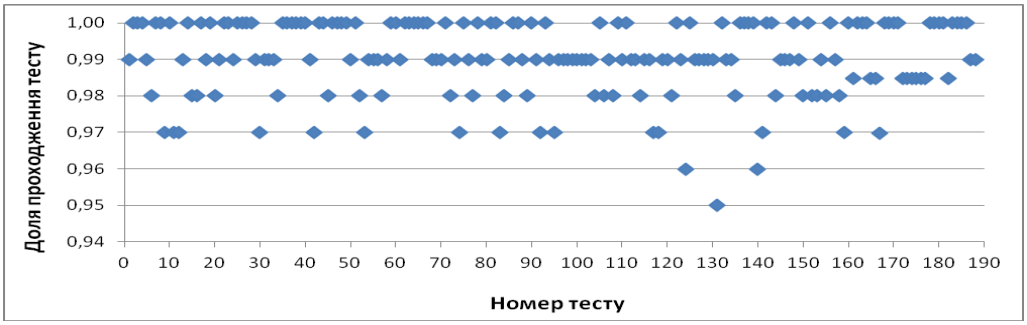

Рис. 3. Статистичний портрет програмної реалізації алгоритму на основі матричних операцій

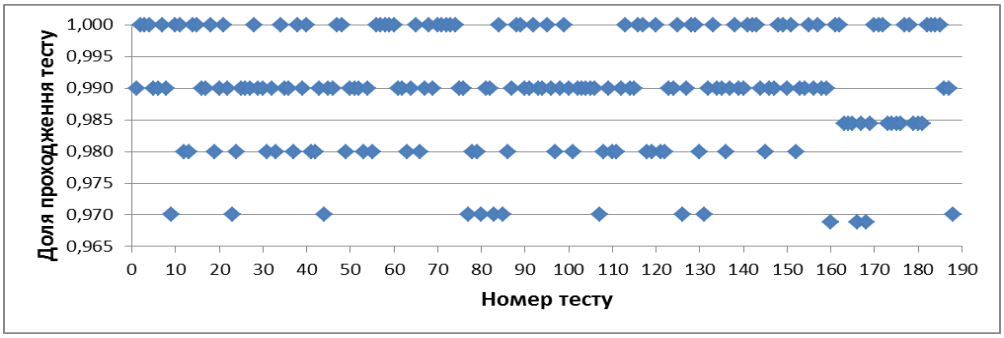

Рис. 4. Статистичний портрет програмної реалізації алгоритму на основі комбінації матричних та розширених матричних операцій

На рис 5 та рис. 6 відображені результати розрахунку довжини ключової послідовності при використанні комбінації матричних та розширених матричних перетворень.

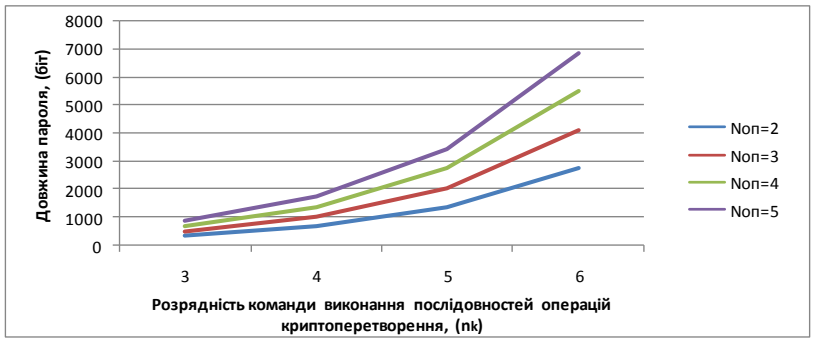

Рис. 5. Результати розрахунку довжини ключової послідовності при використанні комбінації матричних та розширених матричних перетворень

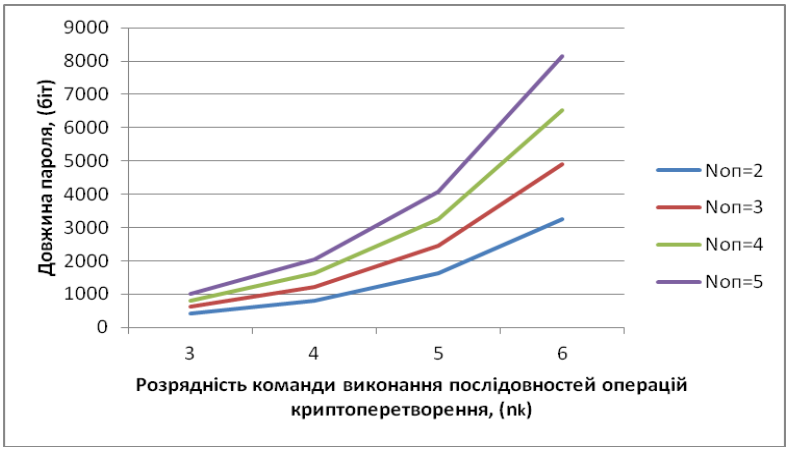

Рис. 6. Результати розрахунку довжини ключової послідовності при використанні комбінації матричних та розширених матричних перетворень

Зведені результати розрахунку коефіцієнта швидкодії при використанні матричних перетворень зображені на рис 7.

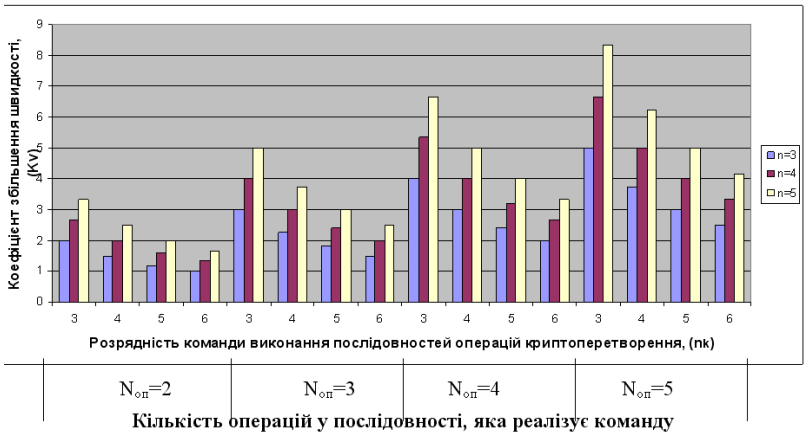

Рис. 7. Результати розрахунку коефіцієнта швидкодії при використанні матричних перетворень

Практична криптостійкість залежить від розрядності пароля, тоді для комбінації операцій матричного та розширеного матричного криптографічного перетворення довжина пароля визначається як $R_{П} = R_{П}^{M} + R_{П}^{PM} = (2^{n_k} \cdot N_{on}) log_2(N_{мо}(n)) + (2^{n_k} \cdot N_{on}) log_2(N_{рмо}(n)) =$ $= П_0 log_2(N_{мо}(n)) + П_0 log_2(N_{рмо}(n))$ і буде пропорційною величині $K_{on} = 2^{R_П} = 2^{(R_П^M + R_П^{PM})}$.

Таким чином, застосування операцій розширеного матричного перетворення залежно від параметрів n_k і N_{on} дає змогу збільшити криптостійкість від 10^{32} до 10^{150} разів пропорційно відносно потокового шифрування при зменшенні часу шифрування від 1,5 до 6 разів, а застосування синтезованих операцій криптографічного перетворення на основі запропонованих варіантів комбінації використання матричного та розширеного матричного перетворення при конструюванні алгоритмів дає можливість збільшити криптостійкість від 2^{166} до 2^{8157} разів пропорційно відносно потокового шифрування при зменшенні часу шифрування від 1,3 до 8 разів.

ВИСНОВКИ

У дисертаційній роботі розв’язана актуальна науково-технічна проблема підвищення ефективності функціонування систем комп’ютерної криптографії шляхом створення методології синтезу операцій перетворення інформації та побудови криптографічних примітивів на їх основі.

Основні наукові та практичні результати полягають у наступному:

1. Здійснено побудову та формалізацію методології синтезу і аналізу логічних операцій перетворення інформації для систем комп’ютерної криптографії шляхом розробки й узагальнення методів синтезу елементарних функцій та операцій на основі них. Основні положення методології дозволили розробити технологію побудови методів синтезу операцій прямого, оберненого та взаємного криптографічного перетворення інформації. Одержані результати

забезпечують розробників криптографічних алгоритмів новими можливостями вдосконалення як криптопримітивів, так і криптосистем в цілому, зокрема розширенням бази операцій, що використовуються для їх побудови. Удосконалено технологію організації доступу до інформаційних ресурсів шляхом реалізації методу підвищення оперативності доступу до конфіденційних інформаційних ресурсів на основі одержаних математичних моделей синтезу операцій взаємного криптографічного перетворення, застосування яких дозволить створювати програмно-апаратні засоби, які забезпечать підвищення швидкості доступу до конфіденційних інформаційних ресурсів.

2. Отримали подальший розвиток математичні моделі й методи синтезу елементарних функцій і операцій криптоперетворення на основі запропонованої методології та вибраної із класифікації групи нелінійних елементарних функцій розширеного матричного криптоперетворення шляхом вдосконалення математичного апарату для синтезу прямих та обернених матричних моделей не афінних дискретних перетворень, що в сукупності забезпечили можливість синтезу операцій нелінійних криптографічних перетворень. Удосконалено математичний апарат для синтезу моделей не афінних дискретних перетворень, застосування якого забезпечить можливість побудови нелінійних матричних операцій криптографічного перетворення. Розроблені методи, моделі та вдосконалений математичний апарат в сукупності підтверджують коректність основних положень запропонованої методології синтезу операцій криптографічного перетворення інформації.

3. На прикладі примітивів ковзного шифрування удосконалено методи побудови криптографічних примітивів шляхом застосування матричних операцій криптографічного перетворення, що дало змогу побудувати узагальнені моделі операцій, які реалізують багаторазове ковзне шифрування. Одержано узагальнені рекурентні послідовності, що описують функції перетворення інформації при здійсненні багаторазового ковзного шифрування, що дало змогу побудувати алгоритми паралельної реалізації криптопримітивів багаторазового ковзного шифрування заданої кількості ітерацій. Ці результати забезпечили підвищення швидкості шифрування до двох разів та стійкість до лінійного криптоаналізу при реалізації багаторазового ковзного шифрування.

4. Розроблено технологію синтезу операцій для мультиопераційних матричних криптографічних примітивів на основі побудови нових груп операцій з точністю до перестановки як вхідних операндів, так і результатів виконання операції, шляхом використання запропонованої табличної моделі операції криптоперетворення. Застосування отриманих результатів забезпечило варіативність операцій при вдосконаленні мультиопераційних криптопримітивів та підвищення стійкості криптоалгоритмів, побудованих на їх основі.

5. Удосконалено методи синтезу та аналізу криптографічних алгоритмів на основі узагальненої моделі криптоалгоритму шляхом послідовно-паралельної реалізації операцій криптографічного перетворення інформації на мікро- та макрорівнях. Отримані результати забезпечили можливість вирішення протиріч

між криптостійкістю, складністю та швидкістю в процесі проектування криптоалгоритмів. Отримана можливість забезпечення гнучкого керування даними параметрами в процесі синтезу криптоалгоритмів для досягнення заданої ефективності, виходячи з задач проектування.

6. На підставі проведених досліджень одержано такі практичні результати: розроблено методологію синтезу операцій криптографічного перетворення інформації в рамках запропонованої концепції побудови алгоритмів захисту інформації в комп'ютерних системах та мережах на їх основі з можливістю підбору оптимальних показників криптостійкості та швидкодії, що дає змогу покращити ефективність функціонування системи комп'ютерної криптографії; технологію побудови та використання криптопримітивів на основі синтезованих операцій криптографічного перетворення інформації з можливістю їх паралельного виконання, що дає виграш у швидкості та часі здійснення перетворення безпосередньо інформації, варіанти реалізації на програмному та апаратному рівнях нових груп криптографічних операцій заданої розрядності, що володіють властивостями афінності та нелінійності, зокрема матричного та розширеного матричного перетворення. Застосування синтезованих операцій криптографічного перетворення на основі запропонованих варіантів комбінації використання матричного та розширеного матричного перетворення при конструюванні алгоритмів дає можливість збільшити криптостійкість (від 2^{166} до 2^{8157} разів) пропорційно відносно потокового шифрування при зменшенні часу шифрування (від 1,3 до 8 разів).

Практична цінність роботи підтверджена актами впровадження на підприємствах та організаціях: НВК «Фотоприлад», «Науково-дослідний інститут «Акорд» та ПП «Сенсорна електроніка» (м. Черкаси), ТОВ «Люменс-груп» (м. Кіровоград) та в освітній процес у навчальних закладах: Черкаському державному технологічному університеті, Черкаському національному університеті імені Б. Хмельницького, Національному аерокосмічному університеті імені М. Є. Жуковського «ХАІ», Кіровоградському національному технічному університеті.

СПИСОК ОПУБЛІКОВАНИХ ПРАЦЬ ЗА ТЕМОЮ ДИСЕРТАЦІЇ

1. Бабенко В. Г. Дослідження матричних операцій криптографічного перетворення на основі арифметичних операцій за модулем. *Системи управління, навігації та зв'язку*. 2012. Вип. 4 (24). С. 85–88.

2. Бабенко В. Г. Дослідження матричних операцій криптографічного перетворення на основі арифметичних операцій за модулем. *Системи управління, навігації та зв'язку*. 2012. Вип. 4 (24). С. 85–88.

3. Бабенко В. Г. Параллельная реализация скользящего шифрования. *Системи обробки інформації*. 2013. Вип. 9 (116). С. 131–134.

4. Бабенко В. Г. Оптимизация матричных операций скользящего шифрования. *Системи озброєння і військова техніка*. 2013. № 4 (36). С. 132–135.

5. Бабенко В. Г. Складності та особливості побудови ефективних криптоалгоритмів. *Вісник Черкаського державного технологічного університету*. 2014. № 3. С. 87–91.

6. Бабенко В. Г. Застосування операцій криптографічного перетворення для синтезу криптоалгоритмів. *Сучасна спеціальна техніка*. 2014. № 3 (38). С. 49–55.

7. 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*. 2010. Вип. 2 (14). С. 118–122.

8. Рудницький В. М., Миронець І. В., Бабенко В. Г. Методологія підвищення оперативності доступу до конфіденційних інформаційних ресурсів. *Системи обробки інформації*. 2010. Вип. 5 (86). С. 15–19.

9. Рудницький В. М., Миронець І. В., Бабенко В. Г. Реалізація методу підвищення оперативності доступу до конфіденційних інформаційних ресурсів. *Вісник Черкаського державного технологічного університету*. 2010. № 3. С. 60–65.

10. Рудницький В. М., Бабенко В. Г., Жиляєв Д. А. Алгебраїчна структура множини логічних операцій кодування. *Наука і техніка Повітряних Сил Збройних Сил України*. 2011. Вип. 2 (6). С. 112–114.

11. Рудницький В. М., Миронець І. В., Бабенко В. Г. Систематизація повної множини логічних функцій для криптографічного перетворення інформації. *Системи обробки інформації*. 2011. Вип. 8 (98). С. 184–188.

12. Рудницький В. М., Миронець І. В., Бабенко В. Г. Технологія побудови пристрою реалізації методу підвищення оперативності доступу до конфіденційних інформаційних ресурсів. *Збірник наукових праць Харківського університету Повітряних Сил*. 2011. Вип. 3 (29). С. 145–150.

13. Бабенко В. Г., Миронець І. В., Рудницький С. В. Декодування інформації в групі дворозрядних операцій криптографічного перетворення. *Системи управління, навігації та зв'язку*. 2011. Вип. 4 (20). С. 208–212.

14. Бабенко В. Г., Рудницький С. В., Мельник Р. П. Визначення множини трирозрядних елементарних операцій криптографічного перетворення. *Вісник інженерної академії України*. 2012. Вип. 3 (4). С. 77–79.

15. Рудницький В. М., Бабенко В. Г., Рудницький С. В. Метод синтезу матричних моделей операцій криптографічного кодування та декодування інформації. *Збірник наукових праць Харківського університету Повітряних Сил*. 2012. Вип. 4 (33). С. 198–200.

16. Рудницький В. М., Бабенко В. Г., Рудницький С. В. Метод синтезу матричних моделей операцій криптографічного перекодування інформації. *Захист інформації*. 2012. № 3 (56). С. 50–56.

17. Голуб С. В., Бабенко В. Г., Рудницький С. В. Метод синтезу операцій криптографічного перетворення на основі додавання за модулем два. *Системи обробки інформації*. 2012. Вип. 3 (101). Т. 1. С. 119–122.

18. Бабенко В. Г., Мельник Р. П., Рудницький С. В. Дослідження способів запису трьохрозрядних криптографічних операцій. *Системи управління, навігації та зв'язку.* 2012. Вип. 1 (21). Т. 2. С. 170–173.

19. Бабенко В. Г., Рудницький С. В. Синтез функцій перекодування для групи трьохрозрядних криптографічних операцій. *Системи озброєння і військова техніка*. 2012. Вип. 1 (29). С. 84–87.

20. Вдосконалення методу синтезу операцій криптографічного перетворення на основі дискретно-алгебраїчного представлення операцій / С. В. Голуб, В. Г. Бабенко, С. В. Рудницький, Р. П. Мельник. *Системи управління, навігації та зв'язку.* 2012. Вип. 2 (22). С. 163–168.

21. Бабенко В. Г., Рудницький С. В. Реалізація методу захисту інформації на основі матричних операцій криптографічного перетворення. *Системи обробки інформації*. 2012. № 9 (107). С. 130–139.

22. 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 науч.-практ. конф. Тольятти: ПВГУС, 2012. С. 67–77.

23. Бабенко В., Мельник О., Мельник Р. Класифікація трирозрядних елементарних функцій для криптографічного перетворення інформації. *Безпека інформації*. 2013. Т. 19. № 1. С. 56–59.

24. Бабенко В. Г., Стабецька Т. А. Побудова моделі оберненої нелінійної операції матричного криптографічного перетворення. *Системи управління, навігації та зв'язку*. 2013. Вип. 3 (27). С. 117–119.

25. Параллельная реализация нелинейного расширенного матричного криптографического преобразования / В. Г. Бабенко, С. В. Пивнева, О. Г. Мельник, Р. П. Мельник. *Вектор науки Тольяттинского государственного университета*. 2014. № 3 (29). С. 17–19.

26. Синтез модели обратной нелинейной операции расширенного матричного криптографического преобразования / В. Н. Рудницкий, С. В. Пивнева, В. Г. Бабенко и др. *Вектор науки Тольяттинского государственного университета*. 2014. № 4 (30). С. 18–21.

27. Бабенко В. Г., Мельник Р. П., Гончар С. В. Оцінка ефективності використання операцій криптографічного перетворення. *Вісник Інженерної академії України*. 2014. Вип. 2. С. 39–41.

28. Метод захисту конфіденційної інформації як складова управління інформаційною безпекою ДСНС України / Р. П. Мельник, О. Г. Мельник, С. В. Гончар, В. Г. Бабенко. *Системи обробки інформації*. 2014. Вип. 4 (120). С. 145–148.

29. Рудницкий В. Н., Козлов Е. В., Бабенко В. Г. Способ параллельной реализации операций матричного криптографического преобразования. *Вектор науки Тольяттинского государственного университета*. 2014. № 2 (28). С. 11–15.

30. Бабенко В. Г., Лада Н. В. Синтез і аналіз операцій криптографічного додавання за модулем два. *Системи обробки інформації*. 2014. Вип. 2 (118). С. 116–118.

31. Бабенко В. Г., Мельник О. Г., Стабецька Т. А. Синтез нелінійних операцій криптографічного перетворення. *Безпека інформації*. 2014. Т. 20. № 2. С. 143–147.

32. Рудницький В. М., Бабенко В. Г., Стабецька Т. А. Узагальнений метод синтезу обернених нелінійних операцій розширеного матричного криптографічного перетворення. *Системи обробки інформації*. 2014. Вип. 6 (122). С. 118–121.

33. Бабенко В. Г., Козловська С. Г. Особливості використання матричних операцій криптографічного перетворення інформації. *Системи обробки інформації*. 2015. Вип. 3 (128). С. 84–87.

34. Бабенко В. Г., Ланських Є. В., Зажома В. М. Вбудовування даних в стеганоконтейнер на основі надлишкових позиційних систем числення. *Вісник Черкаського державного технологічного університету*. 2015. № 1. С. 111–115.

35. Бабенко В. Г., Мельник Р. П., Гончар С. В. Розробка методів синтезу трирозрядних розширених матричних елементарних функцій. *Наука і техніка Повітряних Сил Збройних Сил України*. 2015. Вип. 1 (18). С. 154–156.

36. Мельник Р. П., Бабенко В. Г., Гончар С. В. Удосконалений метод синтезу розширених матричних елементарних функцій для криптоперетворення даних. *Системи озброєння і військова техніка*. 2015. Вип. 1 (41). С. 132–134.

37. Бабенко В. Г., Мельник О. Г., Нестеренко О. Б. Моделювання примітивів ковзного шифрування на основі рекурентних послідовностей. *Наука і техніка Повітряних Сил Збройних Сил України*. 2015. Вип. 3 (20). С. 129–133.

38. Бабенко В. Г., Мельник О. Г., Мельник Р. П. Мультиопераційне багаторазове ковзне шифрування. *Системи озброєння і військова техніка*. 2015. Вип. 3 (43). С. 70–72.

39. Бабенко В. Г., Зажома В. М., Нестеренко О. Б. Метод вбудовування стегоповідомлення на основі ключового елементу. *Автоматизированные системы управления и приборы автоматики.* Харьков. 2014. Вып. 168. С. 53–58.

40. Бабенко В. Г., Лада Н. В., Лада С. В. Дослідження взаємозв'язків між операціями в матричних моделях криптографічного перетворення. *Вісник Черкаського державного технологічного університету.* 2016. № 1. С. 5–11.

41. Эффективное совмещенное мультиоперандное сложение в избыточной линейной рекуррентной системе счисления третьего порядка / И. Н. Федотова-Пивень, В. Г. Бабенко, О. Б. Пивень, С. Ю. Куницкая. *Wschodnioeuropejskie Czasopismo Naukowe:* East European sci. journ. 2016. No. 11 (15). Part 2. P. 19–24. (Варшава, Польща).

42. Реалізація вершинної мінімізації булевих функцій для моделювання процесів, що не формалізуються / В. М. Рудницький, І. В. Миронець, В. Г. Бабенко та ін. *Science and Education a New Dimension. Natural and Ttechnical Science:* міжнар. наук. журн. 2017. Vol. 14. Iss. 132. P. 85–88. (BUDAPEST) (Будапешт, Угорщина).

43. Особенности применения операций перестановок, управляемых информацией, для криптографического преобразования / Т. В. Миронюк, И. В. Миронец, В. Г. Бабенко, С. В. Сысоенко. *Wschodnioeuropejskie Czasopismo Naukowe:* East European sci. journ. 2017. No. 11 (27). Part 1. P. 85–93. (Варшава, Польща).

44. Сисоєнко С. В., Миронець І. В., Бабенко В. Г. Побудова узагальненої математичної моделі групового матричного криптографічного перетворення. *Сучасна спеціальна техніка*. 2018. № 4. С. 96–103.

45. Миронець І. В., Бабенко В. Г., Сисоєнко С. В. Метод мінімізації булевих функцій з великою кількістю змінних на основі направленого перебору. *Щомісячний науковий журнал «Smart and Young»*. 2016. № 7. С. 63–71.

46. Бабенко В. Г., Лада Н. В. Технологія дослідження операцій за модулем два. *Щомісячний науковий журнал «Smart and Young»*. 2016. № 11–12. Ч. 1. С. 49–54.

47. Бабенко В. Г., Кучеренко С. Ю., Зажома В. М. Моделирование позиционных избыточных систем счисления. *Системи управління, навігації та зв'язку.* 2010. Вип. 4 (16). С. 51–54.

48. Бабенко В. Г., Кучеренко С. Ю., Зажома В. М. Синтез правил выполнения операций сложения на основе моделей позиционных систем счисления. *Системи обробки інформації*. 2010. Вип. 9 (90). С. 179–182.

49. Бабенко В. Г., Шадхін В. Ю., Шевченко О. О. Дослідження принципів організації передачі даних в TCP/IP-мережах. *Вісник Черкаського державного технологічного університету.* 2010. № 2. С. 3–6.

50. Бабенко В. Г., Шадхін В. Ю., Компанієць В. О. Оперативний розподіл навантаження на мережі передачі даних. *Вісник Хмельницького національного університету*. 2010. Вип. 3. С. 217–220.

51. Эвристические алгоритмы и распределённые вычисления в прикладных задачах (вып. 2): кол. монограф. / под ред. Б. Ф. Мельникова. Ульяновск, 2013. 202 с.

52. Наукоемкие технологии в инфокоммуникациях: обработка и защита информации: кол. монограф. / под ред. В. М. Безрука, В. В. Баранника. Харьков: Компания СМИТ, 2013. 398 с.

53. Криптографическое кодирование: методы и средства реализации: монография / В. Н. Рудницкий, С. В. Пивнева, В. Г. Бабенко и др.; Тольят. гос. ун-т. Тольятти, 2013. 196 с.

54. Криптографическое кодирование: методы и средства реализации (часть 2): монография / В. Н. Рудницкий, В. Я. Мильчевич, В. Г. Бабенко и др. Харьков: Щедрая усадьба плюс, 2014. 224 с.

55. Криптографическое кодирование: кол. монограф. / под ред. В. Н. Рудницкого, В. Я. Мильчевича. Харьков: Щедрая усадьба плюс, 2014. 240 с.

56. Рудницький В. М., Лада Н. В., Бабенко В. Г. Криптографічне кодування: синтез операцій потокового шифрування з точністю до перестановки: монографія. Харків: ДІСА ПЛЮС, 2018. 184 с.

57. Криптографічне кодування: обробка та захист інформації: кол. монографія / Бабенко В. Г., Лада Н. В. та ін.; під. ред. В. М. Рудницького. Харків: ДІСА ПЛЮС, 2018. 139 с.

58. Бабенко В. Г. Етапи реалізації технології підвищення швидкодії систем захисту інформації. *Методи та засоби кодування, захисту й ущільнення інформації:* тези доп. Третьої міжнар. наук.-практ. конф., (20–22 квіт. 2011 р.). Вінниця: ВНТУ, 2011. С. 80–81.

59. Бабенко В. Г. Використання матричних операцій криптографічного перетворення для ковзного шифрування. *Проблеми інформатизації:* тези доп. Першої міжнар. наук.-техн. конф., (19–20 груд. 2013 р.). Черкаси: ЧДТУ; Київ: ДУТ; Тольятті: ТДУ; Полтава: ПНТУ, 2013. С. 22.

60. Миронець І. В., Бабенко В. Г. Методика синтезу функцій декодування на основі спеціалізованих логічних функцій. *Проблеми інформатизації:* зб. тез доп. наук.-техн. семінару, (15–16 квіт. 2009 р.). Черкаси: ЧДТУ, 2009. Вип. 1 (3). С. 18–19.

61. Миронець І. В., Бабенко В. Г. Вдосконалена методика синтезу функцій декодування на основі спеціалізованих логічних функцій. *Інтегровані інтелектуальні робототехнічні комплекси:* зб. тез Другої міжнар. наук.-практ. конф., (25–28 трав. 2009 р.). Київ: НАУ, 2009. С. 228–229.

62. Бабенко В. Г., Рудницький С. В. Дослідження двохрозрядних операцій криптографічного перетворення. *Інтегровані комп'ютерні технології в машинобудуванні ІКТМ-2011:* тези доп. Всеукр. наук.-техн. конф. Харків: НАУ «ХАІ», 2011. Т. 3. С. 218.

63. Бабенко В. Г., Рудницький С. В. Синтез функцій декодування інформації в групі трьохрозрядних криптографічних операцій перетворення. *Моделювання, ідентифікація, синтез систем керування:* зб. тез П'ятнадцятої міжнар. наук.-техн. конф., (9–16 верес. 2012 р.). Донецьк: Вид-во Ін-ту прикл. математики і механіки НАН України, 2012. С. 190–191.

64. Бабенко В. Г., Рудницький С. В. Моделювання логічних функцій для систем захисту інформації. *Методи та засоби кодування, захисту й ущільнення інформації:* тези доп. Третьої міжнар. наук.-практ. конф. Вінниця: ВНТУ, 2011. С. 82–83.

65. Бабенко В. Г., Рудницький С. В. Дослідження групи трьохрозрядних

криптографічних операцій. *Новітні технології – для захисту повітряного простору:* тези доп. Восьмої наук. конф. Харків. ун-ту Повітр. Сил ім. І. Кожедуба, (18–19 квіт. 2012 р.). Харків: ХУПС ім. І. Кожедуба, 2012. С. 218.

66. Бабенко В. Г., Лада Н. В. Дослідження множини операцій криптографічного додавання. *Інформаційні технології в освіті, науці і техніці (ІТОНТ-2014):* тези доп. ІІ Міжнар. наук.-практ. конф., (м. Черкаси, Україна, 24–26 квіт. 2014 р.). Черкаси: ЧДТУ, 2014. Т. 1. С. 135–136.

67. Бабенко В. Г., Стабецька Т. А. Операції матричного криптографічного декодування на основі логічних визначників. *Методи та засоби кодування, захисту й ущільнення інформації:* тези доп. Четвертої міжнар. наук.-практ. конф., (м. Вінниця, Україна, 23–25 квіт. 2013 р.). Вінниця: ТД Едельвейс і К, 2013. С. 135–137.

68. Бабенко В. Г., Лада Н. В. Синтез і аналіз мікрооперацій для криптографічного перетворення. *Проблеми інформатизації:* тези доп. Другої міжнар. наук.-техн. конф., (м. Черкаси, Україна – м. Тольятті, Росія, 25–26 листоп. 2014 р.). Черкаси: ЧДТУ; Тольятті: ТДУ, 2014. С. 9–10.

69. Ланських Є. В., Бабенко В. Г., Зажома В. М. Алгоритми вбудовування повідомлення для LSB методу. *Інформаційні технології в освіті, науці і техніці (ІТОНТ-2014):* тези доп. ІІ Міжнар. наук.-практ. конф., (м. Черкаси, Україна, 24–26 квіт. 2014 р.). Черкаси: ЧДТУ, 2014. Т. 1. С. 141–142.

70. Ланських Є. В., Бабенко В. Г., Зажома В. М. Технологія застосування ключового елементу стеганоконтейнера для LSB методу. *Інтегровані інтелектуальні робототехнічні комплекси (ІІРТК-2014):* тези доп. Сьомої міжнар. наук.-практ. конф., (19–20 трав. 2014 р.). Київ: НАУ, 2014. С. 312–313.

71. Ланських Є. В., Бабенко В. Г., Зажома В. М. Використання надлишковості систем числення в стеганографічних системах. *Інформаційні технології та комп'ютерна інженерія (ІТКІ-2014):* тези доп. Четвертої міжнар. наук.-практ. конф., (м. Вінниця, Україна, 27–30 трав. 2014 р.). Вінниця: ВНТУ, 2014. С. 161–162.

72. Гресько Є. І., Бабенко В. Г. Огляд стеганографічних методів приховування інформації. *Інформаційна безпека держави, суспільства та особистості:* зб. тез доп. Всеукр. наук.-практ. конф., (16 квіт. 2015 р.). Кіровоград: КНТУ, 2015. С. 87–89.

73. Бабенко В. Г., Рудницький С. В. Способи синтезу алгоритмів на основі операцій криптографічного перетворення інформації. *Проблеми інформатизації:* тези доп. Другої міжнар. наук.-техн. конф. (м. Черкаси, Україна – м. Тольятті, Росія, 25–26 листоп. 2014 р.). Черкаси: ЧДТУ; Тольятті: ТДУ, 2014. С. 10.

74. Бабенко В. Г. Синтез моделей реалізації багаторазового примітиву ковзного шифрування. *Сучасні напрями розвитку інформаційно-комунікаційних технологій та засобів управління:* матеріали П'ятої міжнар. наук.-техн. конф.,

(23–24 квіт. 2015 р.). Полтава: ПНТУ; Баку: ВА ЗС АР; Кіровоград: КЛА НАУ; Харків: ХНДІ ТМ, 2015. С. 59.

75. 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:* зб. наук. праць «ЛОГОΣ». 2016. С. 108–111.

76. Бабенко В. Г., Лада Н. В., Лада С. В. Взаємозв'язки між операціями в матричних моделях криптографічного перетворення. *Проблеми науково-технічного та правового забезпечення кібербезпеки у сучасному світі «ПНПЗК-2016»:* тези доп. Першої міжнар. наук.-практ. конф., (30 берез.–1 квіт. 2016 р.). Харків: Нац. техн. ун-т «ХПІ», 2016. С. 17.

77. Бабенко В. Г., Лада Н. В., Лада С. В. Аналіз множини операцій, синтезованих на основі додавання за модулем два. *Методи та засоби кодування, захисту й ущільнення інформації:* тези доп. П'ятої міжнар. наук.-практ. конф., (19–21 квіт. 2016 р.). Вінниця: ВНТУ, 2016. С. 54–57.

78. Бабенко В. Г., Висоцький С. В. Забезпечення захисту інформації для системи моніторингу та статистики web-ресурсів. *Інформаційні технології в освіті, науці й техніці (ІТОНТ-2016):* тези доп. Третьої міжнар. наук.-практ. конф., (12–14 трав. 2016 р.). Черкаси: ЧДТУ, 2016. С. 85–86.

79. Бабенко В. Г., Ланських Є. В. Дослідження заміни операції для реалізації матричного криптографічного перетворення. *Інтегровані інтелектуальні робототехнічні комплекси (ІІРТК-2016):* тези доп. Дев'ятої міжнар. наук.-практ. конф., (17–18 трав. 2016 р.). Київ: НАУ, 2016. С. 246–248.

80. Бабенко В. Г., Стабецька Т. А. Синтез обернених операцій розширеного матричного криптографічного перетворення. *Проблеми інформатизації:* тези доп. Четвертої міжнар. наук.-техн. конф., (м. Черкаси, Україна, 3–4 листоп. 2016 р.). Черкаси: ЧДТУ; Баку: ВА ЗС АР; Бельсько-Бяла: УТіГН; Полтава: ПНТУ, 2016. С. 9.

81. Стабецька Т. А., Бабенко В. Г. Алгоритми побудови та застосування операцій розширеного матричного криптографічного перетворення. *Наукова думка інформаційного століття:* матеріали Міжнар. наук.-практ. конф., (м. Дніпропетровськ, Україна, 19 черв. 2017 р.). Одеса: Друкарня «Друкарик», 2017. Т. 6. С. 86–94.

82. Миронюк Т. В., Бабенко В. Г. Аналіз статистичних властивостей результатів криптографічного перетворення на основі операцій перестановок, керованих інформацією. *Інноваційні тенденції сьогодення у сфері природничих, гуманітарних та точних наук:* матеріали Міжнар. наук.-практ. конф., (м. Івано-Франківськ, Україна, 17 жовт. 2017 р.). Одеса: Друкарня «Друкарик», 2017. Т. 2. С. 41–47.

83. Бабенко В. Г., Лада Н. В. Потокові шифри з використанням групи модифікованих операцій криптографічного додавання за модулем два з точністю до перестановки. *Проблеми інформатизації:* тези доп. П'ятої міжнар.

наук.-техн. конф., (м. Черкаси, Україна, 13–15 листоп. 2017 р.). Черкаси: ЧДТУ; Баку: ВА ЗС АР; Бельсько-Бяла: УТіГН; Полтава: ПНТУ, 2017. С. 12.

84. Стабецька Т. А., Бабенко В. Г. Порівняльна оцінка основних параметрів методу захисту інформації на основі операцій розширеного матричного криптографічного перетворення. *Наука у контексті сучасних глобалізаційних процесів: зб. наук. праць* «*ΛΌГОΣ*» з *матеріалами Міжнар. наук.-практ. конф.*, (м. Полтава, Україна, 19 листоп. 2017 р.) / відп. за вип. М. А. Голденблат; ГО «Європейська наукова платформа». Одеса: Друкарня «Друкарик», 2017. Т. 10. С. 81–84.

85. Бабенко В. Г., Нестеренко О. Б., Пустовіт М. О. Дослідження результатів багатораундового шифрування, реалізованого на основі операцій строгого стійкого кодування. *Проблеми інформатизації:* тези доп. Шостої міжнар. наук.-техн. конф., (м. Черкаси, Україна, 14–16 листоп. 2018 р.). Черкаси: ЧДТУ; Баку: ВА ЗС АР; Бельсько-Бяла: УТіГН; Полтава: ПНТУ, 2018. С. 9–10.

86. Сисоєнко С. В., Бабенко В. Г. Аналіз складності реалізації моделей операцій групового матричного криптографічного перетворення. *Naukowy i innowacyjny potencjał prezentacji:* kolekcja prac naukowych «ΛΌГОΣ» z materiałami Międzynar. nauk.-prakt. konf., (Opole, 18 listopada 2018 r.). Równe: Volynsky Oberegi, 2018. T. 7. S. 5–53.

87. Sysoienko S., Myronets I., Babenko V. Practical implementation effectiveness of the speed increasing method of group matrix cryptographic transformation. *Second International Workshop on Computer Modeling and Proceedings of the Second International Workshop on Computer Modeling and Intelligent Systems (CMIS-2019),* (Zaporizhzhia, Ukraine, April 15–19, 2019). P. 402–412. URL: http://ceur-ws.org/Vol-2353/paper32.pdf

88. Пристрій для виконання логічних операцій криптографічного перетворення: деклараc. пат. на корисну модель 45916 Україна, МПК H03M 13/00 / Рудницький В. М., Паціра Є. В., Миронець І. В., Бабенко В. Г. № u200907997; заявл. 29.07.2009; опубл. 25.11.2009, Бюл. № 22. 3 с.

89. Пристрій для виконання логічних операцій криптографічного перетворення: деклараc. пат. на корисну модель 45917 Україна, МПК H03M 13/00 / Рудницький В. М., Паціра Є. В., Миронець І. В., Бабенко В. Г. № u200907998; заявл. 29.07.2009; опубл. 25.11.2009, Бюл. № 22. 3 с.

90. Пристрій для виконання логічних операцій криптографічного перетворення: деклара. пат. на корисну модель 46617 Україна, МПК H03M 13/00 / Рудницький В. М., Паціра Є. В., Миронець І. В., Бабенко В. Г. № u200908000; заявл. 29.07.2009; опубл. 25.12.2009, Бюл. № 24. 3 с.

91. Пристрій для виконання логічних операцій криптографічного перетворення: деклараc. пат. на корисну модель 46618 Україна, МПК H03M 13/00 / Рудницький В. М., Паціра Є. В., Миронець І. В., Бабенко В. Г. № u200908001; заявл. 29.07.2009; опубл. 25.12.2009, Бюл. № 24. 3 с.

АНОТАЦІЯ

Бабенко В. Г. Методологія синтезу операцій перетворення інформації для комп'ютерної криптографії. – На правах рукопису.

Дисертація на здобуття наукового ступеня доктора технічних наук за спеціальністю 05.13.05 – комп'ютерні системи та компоненти. – Черкаси: Черкаський державний технологічний університет.

Дисертаційна робота присвячена вирішенню проблеми підвищення ефективності функціонування криптосистем на основі використання створеної методології синтезу операцій криптографічного перетворення інформації. Застосування технології побудови та використання криптопримітивів на основі синтезованих операцій криптоперетворення, що мають властивості афінності та нелінійності, забезпечило можливість збільшення стійкості за рахунок варіативності операцій та швидкості перетворення внаслідок паралельної реалізації. Розроблено технологію синтезу операцій для мультиопераційних матричних криптографічних примітивів підвищеної стійкості. Удосконалено методи синтезу та аналізу криптографічних алгоритмів на основі узагальненої моделі криптографічного алгоритму. Отримано можливість забезпечення гнучкого керування параметрами криптографічних алгоритмів у процесі їх синтезу, виходячи з задач проектування.

Результати роботи впроваджено на чотирьох підприємствах та в чотирьох вищих навчальних закладах.

Ключові слова: комп'ютерна криптографія, операції криптографічного перетворення, нелінійність, варіативність, паралельна реалізація, узагальнена модель, криптостійкість, швидкість перетворення.

АННОТАЦИЯ

Бабенко В. Г. Методология синтеза операций преобразования информации для компьютерной криптографии. – На правах рукописи.

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

Диссертация посвящена решению проблемы повышения эффективности функционирования криптосистем на основе использования созданной методологии синтеза операций криптографического преобразования информации. Применение технологии построения и использования криптопримитивов на основе синтезированных операций криптопреобразования, обладающих свойствами аффинности и нелинейности, обеспечило возможность увеличения стойкости за счет вариативности операций и скорости преобразования вследствие параллельной реализации. Разработана технология синтеза операций для мультиоперационных матричных криптографических примитивов повышенной стойкости. Усовершенствованы

методы синтеза и анализа криптографических алгоритмов на основе обобщенной модели криптографического алгоритма. Получена возможность обеспечения гибкого управления параметрами криптографических алгоритмов в процессе их синтеза, исходя из задач проектирования.

Результаты работы внедрены на четырех предприятиях и в четырех высших учебных заведениях.

Ключевые слова: компьютерная криптография, операции криптографического преобразования, нелинейность, вариативность, параллельная реализация, обобщенная модель, криптостойкость, скорость преобразования.

ABSTRACT

Babenko V. G. The methodology for the synthesis of information transformation operations for computer cryptography. – As a manuscript.

Thesis for the degree of doctor of technical sciences, specialty 05.13.05 – computer systems and components. – Cherkasy: Cherkasy State Technological University.

The dissertation is devoted to solving the problem of increasing the efficiency of the use of cryptosystems based on created methodology for the synthesis of operations of cryptographic transformation of information and the construction of cryptographic primitives based on them.

The object of the research is the processes of synthesis of information transformation operations.

The subject of research is methods and means of synthesizing information transformation operations for computer cryptography.

A methodology for the synthesis of operations of cryptographic transformation of information is proposed on the basis of existing and developed methods of the synthesis of operations of direct, reverse and mutual cryptographic transformation by their classification and generalization, which has made it possible to expand the base of operations, the use of which allows to improve existing cryptoalgorithms and crypto primitives and synthesize new ones.

The use of the technology for the construction and use of crypto primitives based on synthesized cryptographic transformation operations with affinity and nonlinearity properties has provided the possibility to increase the security due to the variability of operations and the conversion speed due to parallel implementation.

A technology for synthesizing operations for multioperational matrix cryptographic primitives of increased security has been developed. This technology has been developed for the synthesis of operations for multioperational matrix cryptographic primitives based on the construction of new groups of operations accurate to permutation by using the proposed tabular model of the cryptographic

transformation operation, which has made it possible, due to the variability of operations, to increase the cryptographic security of existing cryptographic primitives.

Methods for constructing cryptographic primitives have been improved on the example of sliding encryption primitives based on matrix operations of cryptographic transformation and the obtained generalized recurrent sequences for building models by their parallel implementation, which has provided an increase in encryption speed up to 2 times and security to linear cryptanalysis.

The methods of synthesis and analysis of cryptographic algorithms based on a generalized model of the cryptographic algorithm by sequentially-parallel implementation of operations of cryptographic transformation of information at macro and micro levels have been improved, which has made it possible to resolve contradictions between cryptographic security, complexity and speed in order to achieve a given efficiency, based on design tasks.

Mathematical models and methods of the synthesis of elementary functions and operations of cryptographic transformations have been further developed on the basis of the group of elementary functions of the extended matrix cryptographic transformation selected from the classification, by improving the mathematical apparatus for synthesizing direct and inverse matrix models of non-affine discrete transformations. Together they have provided the possibility of synthesizing operations of nonlinear cryptographic transformations and confirmed the correctness of the main provisions of the proposed methodology.

Variants of implementation at the software and hardware levels of new groups of cryptographic operations of a given bit width with the properties of affinity and nonlinearity, in particular, matrix and extended matrix transformations are proposed.

The use of synthesized operations of cryptographic transformation based on the proposed options for combining the use of matrix and extended matrix transformations in the design of algorithms allows to increase the cryptographic security from 2^{166} to 2^{8157} times in proportion to stream encryption while reducing the encryption time from 1.3 to 8 times.

The ability to provide flexible control of the parameters of cryptographic algorithms in the process of their synthesis, based on design problems, has been obtained.

The results of the work have been implemented at four enterprises and at four higher educational institutions.

Keywords: computer cryptography, cryptographic transformation operations, nonlinearity, variability, parallel implementation, generalized model, cryptographic resistance, transformation speed.