Голові спеціалізованої вченої ради Д 26.861.05 при Державному університеті інформаційно-телекомунікаційних технологій

03110, м. Київ, Солом'янська, 7

ВІДГУК

офіційного опонента
головного наукового співробітника Державного науково-дослідного інституту випробувань і сертифікації озброєння та військової техніки,
доктора технічних наук, професора Рудницького Володимира Миколайовича
на дисертаційну роботу
Якименка Ігоря Зіновійовича
«Методи та засоби криптографічного захисту інформації на основі системи залишкових класів»,
представлену на здобуття наукового ступеня доктора технічних наук
за спеціальністю 05.13. 21 – Системи захисту інформації

Цей відгук підготовлено за матеріалами дисертації, що містить загальний обсяг – 420 сторінок, основний зміст викладений на 347 сторінках, у тому числі 65 таблицях та 99 рисунках, 7 актів і 1 довідки про впровадження результатів дисертаційного дослідження, автореферату на 41 стор. і копій 61 наукової праці здобувача.

1. Актуальність теми дисертаційної роботи

У сучасних умовах стрімкого розвитку інформаційно-комунікаційних технологій та зростання обсягів передавання, обробки і зберігання даних проблема забезпечення криптографічного захисту інформації набуває особливої ваги. Традиційні криптографічні методи, що ґрунтуються на арифметиці з багаторозрядними числами, дедалі частіше стикаються з обмеженнями щодо продуктивності, енергоефективності та апаратної реалізації, особливо в умовах обмежених ресурсів або необхідності паралельної обробки даних. Крім того, розвиток високопродуктивних обчислень і перспективи появи квантових обчислювальних засобів актуалізують пошук альтернативних математичних підходів до побудови криптографічних перетворень.

Система залишкових класів є перспективним математичним апаратом, який забезпечує природну паралельність обчислень, підвищену швидкодію

арифметичних операцій, завадостійкість та можливість ефективної апаратної реалізації. Використання системи залишкових класів у криптографії відкриває нові можливості для побудови симетричних і асиметричних алгоритмів шифрування, механізмів контролю цілісності та автентифікації, а також схем захисту від побічних каналів витоку інформації.

Крім того, актуальність і практичне значення даної наукової роботи підтверджується включенням її результатів до ряду держбюджетних та госпдоговірних тем (Державні реєстраційні номери 0109U000035, 0115U001607, 0112U008458, 0117U000414, 0121U114705, 0118U003182, 0118U100457 0123U104713), в яких здобувач виступав керівником, відповідальним виконавцем та виконавцем.

Таким чином, усе сказане обумовлює актуальність теми дисертаційної роботи Якименка Ігоря Зіновійовича і наукову новизну поставлених в ній проблемних завдань досліджень.

2. Наукова новизна результатів роботи

У роботі досліджено підвищення рівня стійкості та ефективності криптосистем шляхом створення нових методів, засобів та методології криптографічного захисту інформації в системі залишкових класів.

Виходячи з того, що нові наукові результати – це нові знання в певній галузі фундаментальних чи прикладних наук, можна вважати основними науковими результатами дисертації наступні:

- вперше розроблено симетричний криптоалгоритм у СЗК, який за рахунок розбиття відкритого повідомлення на залишки по відповідних попарно взаємнопростих модулях (ключах) та використання китайської теореми про залишки (КТЗ) дозволяє розпаралелити обчислювальний процес, зменшити розмірність операндів та на основі побудованих аналітичних виразів встановити розрядність та кількість модулів СЗК для забезпечення такої ж стійкості, як і сучасний симетричний криптоалгоритм AES-256;
- вперше розроблено високопродуктивні симетричні та асиметричні криптоалгоритми на основі СЗК та її модифікованої досконалої форми (МДФ), які за рахунок довільної заміни базисних чисел в процесі шифрування на попарно взаємнопрості з відповідними модулями додаткові ключі дозволяють підвищити криптостійкість та забезпечити необхідний рівень захисту інформаційних потоків;
- вперше розроблено криптографічний алгоритм, в якому за рахунок шифрування відкритого тексту у вигляді залишків за допомогою КТЗ і розшифрування на основі операції пошуку залишків за відповідними модулями

забезпечується підвищення швидкості розшифрування інформації без втрати стійкості алгоритму;

• вперше розроблено одно- та двоключові симетричні криптографічні методи в поліноміальній СЗК, які за рахунок заміни в процесі шифрування базисних поліномів на довільно вибрані попарно взаємнопрості з модулями поліноми дозволяють створити додаткову структурну неоднозначність, ускладнити криптоаналіз через необхідність розв'язання NP-повної задачі та збільшити криптографічну стійкість;

• вперше розроблено симетричні методи шифрування/розшифрування інформаційних потоків в ієрархічній цілочисельній та поліноміальній СЗК, які за рахунок представлення зашифрованого тексту наборами залишків за відповідними модулями (ключами) та розпаралелення процесу обчислень дозволяють підвищити стійкість криптоалгоритму та збільшити його швидкодію;

• вперше розроблено методологію криптографічного захисту інформації в СЗК, яка за рахунок застосування векторно-модульних методів модулярного множення та експоненціювання, цілочисельної, модифікованої досконалої форми, поліноміальної та ієрархічної систем залишкових класів, що дозволило забезпечити збільшення стійкості, зменшення часової складності, підвищення швидкодії алгоритмів, спеціалізованого програмного забезпечення та побудувати єдину стратегію криптографічного захисту інформаційних потоків на основі системи залишкових класів;

• отримали подальший розвиток поліноміальний, дво- та тримодульний цілочисельні асиметричні алгоритми шифрування Рабіна, які за рахунок заміни операції множення на операцію додавання та використання векторно-модульного методу модулярного множення дозволяють зменшити часову складність криптографічних перетворень і підвищити швидкодію реалізації алгоритмів.

3. Достовірність наукових результатів

Точність та достовірність основних наукових результатів роботи підтверджується наведеними в розділах 2, 3, 4 і 5 системами формальних методик і перетворень, що не містить принципових помилок, а також рядом наведених прикладів і впровадженням розроблених засобів. Отримані результати теоретичних досліджень збігаються з результатами імітаційного моделювання, і результатами з відомих часткових рішень.

4. Цінність дисертаційної роботи для науки

Цінність дисертації полягає в тому, що в ній запропоновано нове рішення

важливої науково-технічної проблеми в теорії побудови комп'ютерних криптографічних засобів надійного захисту інформації з високою швидкістю шифрування. Змістовний аспект запропонованого рішення, який спрямований на підвищення рівня стійкості та ефективності криптосистем шляхом створення нових методів, засобів та методології криптографічного захисту інформації в системі залишкових класів, не був відомий раніше.

5. Практична корисність роботи

Практична корисність роботи обумовлена тим, що використання запропонованих в ній формальних методів і конкретних рішень дозволяє отримувати більш досконалі, порівняно з відомими, засоби забезпечення підвищення рівня стійкості та ефективності криптографічних систем. Результати роботи впроваджено в Акціонерному товаристві «Тернопільобленерго», ТзОВ НВФ «Інтеграл», ТзОВ завод «Рембутехніка», Управлінні кібербезпеки та цифрового розвитку відділу цифрової трансформації Міністерства енергетики України, у навчальному та науковому процесах, Західноукраїнського національного університету на факультеті комп'ютерних інформаційних технологій.

6. Структура роботи

Дисертаційна робота містить анотацію, вступ, 6 розділів, висновки, список використаних джерел та додатки.

У вступі обґрунтовано актуальність теми досліджень; показано зв'язок роботи з науковими програмами, планами, темами; сформульовано мету та основні задачі досліджень; подано наукову новизну і практичне значення отриманих результатів; визначено особистий внесок здобувача; наведено дані про апробацію, публікації та використання результатів дослідження.

У першому розділі проведено аналіз теоретичних основ симетричних та асиметричних криптоалгоритмів, визначено їх переваги і недоліки. Проаналізовано особливості застосування СЗК в криптографічних методах захисту інформації. Встановлено основні переваги СЗК: можливість виконання операцій над числами, які менші за вибрані модулі, розпаралелення процесу обчислень та відсутність міжрозрядних переносів. Обгрунтовано можливість застосування методів шифрування у СЗК, зокрема у її МДФ. Показано, що поєднання поліноміальної арифметики та СЗК дозволить розпаралелити процес виконання базових операцій в кільці поліномів, що, в свою чергу, призведе до підвищення швидкодії програмної реалізації та зменшення часової складності алгоритму, забезпечивши необхідний рівень захищеності.

У другому розділі запропоновано теоретичні основи визначення простих та взаємно простих чисел на основі властивості періодичності, що дає змогу ефективно вирішувати задачі оптимізації обчислень пошуку такого роду чисел.

Розроблено теоретичні основи та алгоритмічне забезпечення для реалізації двох- та трьохмодульного криптоалгоритму Рабіна за допомогою використання тільки операції додавання. Здійснено аналітичне порівняння часових складностей запропонованого та відомого підходів. Показано, що використання розробленого методу дозволяє зменшити часову складність з кубічної до квадратичної.

Удосконалено реалізацію асиметричного алгоритму шифрування Ель-Гамаля, зокрема базові операції модулярного експоненціювання багаторозрядних чисел, на основі СЗК та векторно-модульного алгоритму модулярного множення.

У третьому розділі Розроблено методи побудови системи модулів МДФ СЗК однакової розрядності, що дозволяє більш раціонально використовувати регістри розрядної сітки. Розглянуто теоретичні основи СЗК та різних її форм, визначено їх переваги та недоліки. Показано, що найбільш поширені на даний час модулі потребують виконання операції пошуку оберненого елемента та множення на нього при використанні КТЗ. МДФ СЗК дозволяє спростити цю процедуру. Розроблено симетричні криптоалгоритми у СЗК та МДФ СЗК. Запропоновано метод симетричного шифрування на основі КТЗ, в якому відновлення відкритого тексту відбувається на основі пошуку залишків шифртексту по відповідних модулях.

Проведено оцінки стійкості запропонованих методів на основі теореми розподілу простих чисел та функції Ейлера та досліджено, при якій розрядності та кількості модулів СЗК, розроблені симетричні системи захисту забезпечують таку ж стійкість, як і ключ найбільшої довжини алгоритму AES. Проведено оцінку часової складності математичної атаки та досліджено її залежність складності від розрядності та кількості модулів.

Вперше запропоновані асиметричні криптоалгоритми на основі СЗК та її МДФ, які забезпечують необхідний рівень захисту даних. Обрані системи модулів виступають таємними ключами, а при відновленні числа за його залишками з використанням КТЗ множення відбувається на довільно вибрані коефіцієнти (відкриті ключі) асиметричного шифрування в СЗК. Отримано аналітичні вирази, які вказують, що високої криптостійкості можна досягнути при збільшенні розрядності вхідних параметрів, кількості модулів (ключів), а також вибором таких модулів, для яких значення функції Ейлера буде максимальним. Встановлено, що криптостійкість запропонованих алгоритмів,

аналогічно криптосистемі RSA, ґрунтується на вирішенні задачі факторизації або повного перебору наборів модулів.

У четвертому розділі вперше запропоновано алгоритм пошуку оберненого полінома в кільці Z[x] на основі методу невизначених коефіцієнтів. Однією з основних переваг є зменшення часової складності в порівнянні з відомим. Вперше запропоновані методи відновлення полінома в кільці Z[x], які за рахунок операцій додавання добутку модулів та добутку залишків модулів дають змогу розпаралелити обчислення та уникнути процедури пошуку мультиплікативного оберненого полінома, що в свою чергу, призводить до збільшення ефективності.

Розроблено симетричні криптографічні алгоритми, які ґрунтуються на поліноміальній СЗК. Дослідження вказують, що криптоаналіз запропонованого алгоритму вимагає комбінаторної складності. Встановлено, що стійкість істотно зростає при збільшенні степеня та розмірності поля Галуа.

У **п'ятому розділі** Вперше запропоновано симетричний криптоалгоритм, який базується на ієрархічній СЗК, яка дозволяє послідовно зменшувати розрядність модулів на кожному рівні та забезпечувати необхідний рівень захищеності в залежності від кількості рівнів, модулів та їх розрядностей. Проведені експериментальні дослідження продемонстрували, що розроблений алгоритм має високу стійкість до атак. Проведено порівняльний аналіз стійкості запропонованого алгоритму та алгоритму AES-256.

Вперше запропоновано симетричний криптоалгоритм, заснований на поліноміальній ієрархічній СЗК. У якості таємних ключів застосовано систему незвідних поліномів, а шифрування реалізується шляхом обчислення залишків вхідного полінома за відповідними модулями.

Вперше розроблено методологію криптографічного захисту інформації в СЗК, яка забезпечує комплексний підхід до розробки, реалізації та оптимізації запропонованих криптосистем.

У шостому розділі Здійснено повну програмну реалізацію криптоалгоритмів, розроблених у попередніх розділах. Створене програмне забезпечення продемонструвало ефективність використання СЗК у задачах криптографії, забезпечивши значне прискорення обчислювальних процедур за рахунок властивостей паралелізму та декомпозиції.

Окремо показано, що розроблене програмне забезпечення забезпечує прозорість криптографічних операцій завдяки виведенню всіх вхідних параметрів, проміжних результатів і кінцевих повідомлень. Узагальнення експериментальних результатів, отриманих у межах розділу, підтвердило, що програмна реалізація розроблених криптоалгоритмів у СЗК є ефективною,

масштабованою та придатною до інтеграції у прикладні інформаційні системи різного призначення.

У **висновках** наведені основні наукові та практичні результати дисертаційної роботи.

У **додатках** містяться акти впровадження результатів дисертаційної роботи та лістинги кодів програмної реалізації.

7. Публікації за темою дисертації

Наукові положення дисертації, що пов'язані з розробкою методів, засобів та методології криптографічного захисту інформації в системі залишкових класів достатньо повно відображені в публікаціях автора і пройшли апробацію на міжнародних науково-технічних конференціях і семінарах. Основні результати дисертації достатньо повно відображені в 61 друкованій праці, з них 5 - у колективних монографіях, 11 статей, які індексуються у наукометричній базі Scopus, 15 статей у фахових виданнях України, 22 тез, які індексуються у наукометричній базі Scopus, 6 тез у вітчизняних конференціях, 2 патенти на корисну модель.

8. Автореферат дисертації

Автореферат дисертації за своїм змістом повністю відповідає дисертаційній роботі.

9. Зауваження щодо змісту дисертаційної роботи та автореферату

1. В першому розділі дисертаційного дослідження автор основну увагу приділив аналізу найбільш поширених симетричних алгоритмів шифрування і асиметричних криптосистем, залишивши неоглянутими системи постквантової криптографії, за рахунок чого дещо звузив рамки використання результатів дослідження по можливості застосування цілочисельних систем залишкових класів.
2. Відсутність в дисертації та авторефераті визначення терміну «теоретичні основи» приводить до неоднозначності сприйняття та трактування результатів дисертаційного дослідження. Наприклад, в підрозділі 2.1 «Теоретичні основи визначення простих і взаємно простих чисел на основі властивості періодичності» розробляється векторно-модульний метод пошуку залишку. Даний метод забезпечує зменшення часової складності пошуку залишків і має суттєве значення для розвитку і практичної реалізації теорії простих чисел. В даному випадку підрозділ 2.1, з врахуванням його наповнення, на мою думку доцільно булу б назвати, або «Розвиток теорії …», або «Метод ….».

3. Дисертаційна робота має деякі недоліки по структурі, а також невагомі неточності. Наприклад: розділ 1 дисертації перевантажений описом загальновідомих криптоалгоритмів, причому деякі з них (1.2.4 Криптографія еліптичних кривих) в подальшому не використовуються. На мою думку було б доцільно скоротити наведені матеріали, обмеживши критичним розглядом їх основних недоліків з виокремленням тих які дозволяє усунути дана робота. В розділах 2-5 надмірна увага приділена аналізу публікацій по відповідних тематиках. Ці матеріали доцільно було б розмістити в першому розділі. В п.3.1 розглянуто методи побудови наборів модулів системи залишкових класів однакової розрядності, при умові, що відомі всі модулі, крім двох. Доцільно було б розглянути даний метод для більшої кількості невідомих модулів. Розділи 4-5 перенасичені викладками математичних розрахунків, які знижують інформативність представленого матеріалу. Деякі з цих розрахунків можна було б винести в додатки. У висновках дисертаційного дослідження немає однозначного твердження про досягнення підвищення рівня стійкості криптографічних систем, а є констатація досягнення підвищення ефективності захисту інформаційних потоків. Відсутність порівняльного аналізу результатів програмної реалізації криптоалгоритмів в системі залишкових класів значно зменшує практичну цінність як 6 розділу, так і дисертації вцілому. Із за технічної помилки за рахунок використання автонумерації списку основних публікацій здобувача в анотації дисертації виникла їх розбіжність з рефератом дисертації, що ускладнило сприйняття особистого внеску здобувача наведеного у вступі. Автору було б доцільно при оформленні особистого внеску здобувача посилатися не на список основних публікацій в анотації, а на список використаних джерел в дисертації, перемістивши власні публікації на його початок. В дисертації та рефераті присутні граматичні та стилістичні помилки.

Вказані зауваження і недоліки не впливають на загальну позитивну оцінку результатів дисертаційного дослідження та не зменшують її наукову новизну та практичну цінність.

1. Загальна оцінка дисертації

Оцінюючи роботу в цілому, вважаю, що в дисертації отримано нове рішення важливої науково-технічної проблеми підвищення рівня стійкості та ефективності криптосистем шляхом розробки методів, засобів та методології криптографічного захисту інформації на основі цілочисельної, модифікованої досконалої форми, поліноміальної та ієрархічної систем залишкових класів.

Дисертація є завершеною науково-дослідною роботою. Вважаю, що за актуальністю вибраної теми, обсягом і рівнем виконаних теоретичних і експериментальних досліджень, достовірністю і обґрунтованістю висновків, новизною досліджень, значенням отриманих результатів для науки і практики, дисертаційна робота задовольняє вимогам «Порядку присудження та позбавлення наукового ступеня доктора наук», затвердженого постановою Кабінету Міністрів України від 17 листопада 2021 року №1197 та вимогами до опублікування результатів дисертацій на здобуття наукових ступенів доктора і кандидата наук, затвердженим Наказом Міністерства освіти і науки України від 23.09.2019 року №1220 «Про опублікування результатів дисертацій на здобуття наукових ступенів доктора і кандидата наук» (зі змінами внесеними Наказом МОН України від 27.05.2022 № 496), а її автор, Якименко Ігор Зіновійович, заслуговує на присудження наукового ступеня доктора технічних наук за спеціальністю 05.13.21 – Системи захисту інформації.

Офіційний опонент

Головний науковий співробітник
Державного науково-дослідного інституту випробувань
і сертифікації озброєння та військової техніки,
доктор технічних наук, професор

Володимир РУДНИЦЬКИЙ

Підпис Рудницького В.М. завіряю.
Заступник начальника Державного науково-дослідного інституту випробувань і сертифікації озброєння та військової техніки з наукової роботи
доктор технічних наук, старший науковий співробітник

Володимир КРИВЦУН

17 02 2026 р.