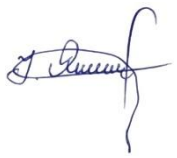
МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ДЕРЖАВНИЙ УНІВЕРСИТЕТ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ

ЯКИМЕНКО ІГОР ЗІНОВІЙОВИЧ



УДК 004.056.53

МЕТОДИ ТА ЗАСОБИ КРИПТОГРАФІЧНОГО ЗАХИСТУ ІНФОРМАЦІЇ НА ОСНОВІ СИСТЕМИ ЗАЛИШКОВИХ КЛАСІВ

05.13.21 – Системи захисту інформації

Реферат
дисертації на здобуття наукового ступеня
доктора технічних наук

Київ – 2026

Дисертацією є рукопис.

Робота виконана у Західноукраїнському національному університеті Міністерства освіти і науки України.

Офіційні опоненти: доктор технічних наук, професор
Євсеєв Сергій Петрович,
Національний технічний
університет «Харківський політехнічний інститут»,
завідувач кафедри кібербезпеки;

доктор технічних наук, професор
Рудницький Володимир Миколайович,
Державний науково-дослідний
інститут випробувань і сертифікації
озброєння та військової техніки,
головний науковий співробітник;

доктор технічних наук, професор
Смірнов Олексій Анатолійович,
Центральноукраїнський національний
технічний університет,
завідувач кафедри кібербезпеки
та програмного забезпечення.

Захист відбудеться «05» березня 2026 р. о 14 годині на засіданні спеціалізованої вченої ради Д 26.861.05 при Державному університеті інформаційно-комунікаційних технологій за адресою: 03110, Україна, м. Київ, вул. Солом'янська, 7, конференц-зал.

З дисертацією можна ознайомитись у бібліотеці Державного університету інформаційно-комунікаційних технологій за адресою: 03110, Україна, м. Київ, вул. Солом'янська, 7.

Реферат розісланий «03» лютого 2026 р.

Учений секретар
спеціалізованої вченої ради Д 26.861.05,
канд. пед. наук, доцент Вікторія КОРЕЦЬКА

ЗАГАЛЬНА ХАРАКТЕРИСТИКА РОБОТИ

Актуальність теми. Розв’язання переважної більшості сучасних задач науки і техніки безумовно пов’язані з опрацюванням та захищеною передачею інформаційних потоків. Традиційні технології забезпечення захисту інформації зазвичай передбачають застосування симетричних та/або асиметричних криптоалгоритмів. Значний вклад у їх розвиток внесли такі вітчизняні та зарубіжні вчені: В.К. Задірака, І.Д. Горбенко, О.Г. Корченко, А.А. Хорошко, О.П. Скринник, О.В. Потій, М. Є. Шелест, О.О. Кузнецов, М.П. Карпінський, В. П. Сіденко, Ю.О. Дрейс, С.О. Гнатюк, В.М. Кінзерявий, Н. Фергюссон, М. Рабін, Т. Ель-Гамаль, Н. Кобліц, В. Діффі, М. Хелман та інші.

Слід зазначити, що вимоги, які ставляться до сучасних систем захисту інформації, як правило, досить строгі та, як наслідок, громіздкі в реалізації та затратні в експлуатації. Крім того, для підвищення стійкості криптоалгоритмів потрібно збільшувати довжину ключів і, відповідно, значення операндів математичних перетворень. Це приводить до зменшення швидкодії криптоалгоритмів. Найперспективнішим шляхом її підвищення є розпаралелення процесу обчислень. Цією властивістю володіє непозиційна система залишкових класів (СЗК).

Значний теоретичний та прикладний внесок у розвиток СЗК та її застосування зробили такі вчені: М. Валах (M. Valach), А. Свобода (A. Svoboda), І. Акушський, Д. Юдицький, В. Амербаєв, В. Торгашев, В. Краснобаєв, Я. Николайчук, В. Яцків, М. Касянчук, А. Омонді (A. Omondi), Б. Премкумар (B. Premkumar), А. Молахоссеіні (A. Molahosseini), А.Мохан (A.Mohan) та інші.

До інших основних переваг СЗК можна віднести можливість виконання операцій над малорозрядними операндами та відсутність міжрозрядних переносів. Такі властивості дозволяють ефективно використовувати СЗК, зокрема, її модифіковану досконалу форму (МДФ), в криптографії.

Крім того, при значних зростаннях обчислювальних можливостей, сучасні симетричні та асиметричні криптосистеми стають надзвичайно вразливими. Це означає, що їх криптоаналіз може здійснюватися за прийнятний для зловмисника час. Тому для забезпечення цілісності, конфіденційності та доступності інформації виникає потреба в розробці нових криптографічних алгоритмів, які будуть стійкішими до криптоаналітичних атак. В цьому напрямку поліноміальні криптоалгоритми відкривають нові перспективи. Аналогічно до цілочисельних застосувань, у кільці поліномів $Z[x]$ можливі базові операції додавання, множення, піднесення до степеня, ділення з остачею тощо. Поліноми успішно можна використовувати у вигляді відкритого і зашифрованого тексту, відкритого і таємного ключів при застосуванні в криптографічних алгоритмах.

Слід ще відзначити, що поєднання поліноміальної арифметики та СЗК дає змогу використати переваги останньої, зокрема, розпаралелення процесу обчислень. Це призводить до зменшення часової складності та спрощення процесу обчислень при шифруванні/розшифровуванні. А використання двох різнотипних ключів забезпечить підвищення стійкості запропонованої системи до криптоаналізу.

У цьому контексті особливий інтерес викликає використання цілочисельних та поліноміальних багаторівневих або ієрархічних СЗК (ІСЗК). Такий підхід дає змогу оптимізувати арифметичні операції та зменшити обсяг необхідних обчислень, забезпечуючи при цьому високий рівень безпеки даних. Завдяки своїм унікальним властивостям та високому потенціалу оптимізації ІСЗК відкриває нові перспективи у сфері криптографічного захисту даних.

Отже, розробка нових методів шифрування в СЗК та дослідження їх стійкості до криптоаналізу на даний час є надзвичайно актуальною задачею.

Враховуючи викладене, актуальною науково-прикладною проблемою є розробка методів, засобів та методології криптографічного захисту інформації на основі цілочисельної, модифікованої досконалої форми, поліноміальної та ієрархічної систем залишкових класів, яка виникає в результаті об'єктивного *протиріччя* між потребою забезпечення високої криптографічної стійкості та передавання великих обсягів конфіденційної інформації, з одного боку, та забезпечення підвищення швидкодії процесу шифрування/розшифрування.

Наукова концепція дисертації полягає у побудові та обґрунтуванні єдиної стратегії криптографічного захисту інформаційних потоків, в якій криптографічні перетворення виконуються в системі залишкових класів (СЗК) та її похідних формах (цілочисельній, модифікованій досконалій, поліноміальній та ієрархічній), а обчислювально затратні операції множення/піднесення до степеня реалізуються через операції додавання із застосуванням векторно-модульних алгоритмів модулярного множення та експоненціювання.

Зв'язок роботи з науковими програмами, планами і темами. Дисертаційна робота виконувалася у рамках таких науково-дослідних держбюджетних та госпдоговірних робіт кафедр комп'ютерної інженерії, спеціалізованих комп'ютерних систем та кібербезпеки Західноукраїнського національного університету: «Паралельні методи та засоби реалізації алгоритмів захисту інформації в комп'ютерних мережах з використанням математичного апарату еліптичних кривих» (Державний реєстраційний номер 0109U000035), «Опрацювання багаторозрядних чисел в системі залишкових класів» (Державний реєстраційний номер 0115U001607), «Розробка теоретичних засад методів формування та цифрового опрацювання даних у розподілених спеціалізованих комп'ютерних системах» (Державний реєстраційний номер 0112U008458), «Теоретичні основи та апаратні засоби підвищення продуктивності роботи безпровідних сенсорних мереж» (Державний реєстраційний номер 0117U000414), «Виконання завдань Перспективного плану розвитку наукового напряму "Технічні науки" Західноукраїнського національного університету. Розробка методів та алгоритмів захищеного зберігання даних» (Державний реєстраційний номер 0121U114705), «Методи, алгоритми та засоби надійного захищеного зберігання даних на основі модулярних коригуючих кодів» (Державний реєстраційний номер 0118U003182), «Розробка алгоритмів надійного розподіленого зберігання даних на основі модулярних коригуючих кодів» (Державний реєстраційний номер 0118U100457), «Стійкі до криптоаналізу методи та засоби шифрування в поліноміальних системах» (Державний реєстраційний номер 0123U104713).

Мета і завдання дослідження. Метою дисертаційної роботи є підвищення рівня стійкості та ефективності криптосистем шляхом створення нових методів, засобів та методології криптографічного захисту інформації в системі залишкових класів.

Для досягнення поставленої мети у дисертаційній роботі необхідно розв'язати низку взаємопов'язаних задач:

1) проаналізувати сучасні методи, алгоритми та засоби захисту інформаційних потоків з метою визначення перспектив підвищення їх стійкості на основі використання різних форм СЗК та поліноміальних систем числення;

2) удосконалити та підвищити ефективність алгоритмічного забезпечення для реалізації асиметричних криптосистем Рабіна та Ель-Гамаля на основі операції додавання та векторно-модульного алгоритму модулярного множення та експоненціювання;

3) удосконалити та підвищити ефективність методів пошуку оберненого полінома за модулем та відновлення полінома за його залишками на основі методу невизначених коефіцієнтів;

4) розробити симетричний та асиметричний криптографічні алгоритми в СЗК та дослідити їх стійкість до криптоаналітичних атак;

5) розробити криптографічний одноключовий та двоключовий алгоритми в поліноміальній СЗК та дослідити їх стійкість;

6) розробити ієрархічний цілочисельний та поліноміальний криптографічні алгоритми на основі СЗК та дослідити їх стійкість;

7) розробити алгоритмічне та програмне забезпечення запропонованих методів шифрування;

8) розробити методологію криптографічного захисту інформації на основі заміни в алгоритмах шифрування операції множення операцією додавання, з використанням цілочисельної, модифікованої досконалої форми, поліноміальної та ієрархічної систем залишкових класів для розробки нових криптографічних алгоритмів.

Об'єкт дослідження – процеси шифрування інформаційних потоків на основі системи залишкових класів.

Предмет дослідження – методи та засоби криптографічного захисту інформації на основі цілочисельної та поліноміальної систем залишкових класів.

Методи дослідження. Проведені дослідження ґрунтуються на застосуванні математичних основ алгебри і теорії чисел (для розробки методів пошуку оберненого полінома, відновлення полінома за його залишками, реалізації китайської теореми про залишки (КТЗ)), теорії алгоритмів (для оцінки стійкості відомих та розроблених методів), методах криптографії (для розробки тримодульної криптосистеми Рабіна, векторно-модульної криптосистеми Ель-Гамаля), програмуванні (для реалізації симетричних, асиметричних цілочисельних криптоалгоритмів в СЗК та симетричних криптоалгоритмів в поліноміальній СЗК), теорії множин (для побудови методології захисту інформаційних потоків на основі цілочисельної та поліноміальної СЗК), статистиці (для обробки експериментальних результатів).

Наукова новизна отриманих результатів полягає в наступному:

1) вперше розроблено симетричний криптоалгоритм у системі залишкових класів, який за рахунок розбиття відкритого повідомлення на залишки по відповідних попарно взаємнопростих модулях (ключах) та використання китайської теореми про залишки дозволяє розпаралелити обчислювальний процес, зменшити розмірність операндів та на основі побудованих аналітичних виразів встановити розрядність та кількість модулів системи залишкових класів для забезпечення такої ж стійкості, як і сучасний симетричний криптоалгоритм AES-256;

2) вперше розроблено високопродуктивні симетричні та асиметричні криптоалгоритми на основі системи залишкових класів та її модифікованої досконалої форми, 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;

3) вперше розроблено криптографічний метод, в якому за рахунок шифрування відкритого тексту у вигляді залишків за допомогою китайської теореми про залишки і розшифрування на основі операції пошуку залишків за відповідними модулями забезпечується підвищення швидкості розшифрування інформації без втрати стійкості алгоритму;

4) отримав подальший розвиток метод пошуку оберненого полінома в кільці Z[x] на основі методу невизначених коефіцієнтів, який за рахунок усунення операції пошуку найбільшого спільного дільника двох поліномів дозволив зменшити часову складність та підвищити швидкодію алгоритму при його використанні в поліноміальних криптосистемах;

5) удосконалено методи відновлення полінома за його залишками в кільці Z[x], які за рахунок використання операції додавання добутку модулів або їх залишків за відповідними модулями дозволяють уникнути обчислювально громіздкої процедури пошуку мультиплікативного оберненого полінома, що, в свою чергу, призводить до збільшення швидкодії та зменшення часової складності поліноміальних алгоритмів шифрування;

6) вперше розроблено одно- та двоключові симетричні криптографічні методи в поліноміальній системі залишкових класів, 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;

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

8) отримали подальший розвиток поліноміальний, дво- та тримодульний цілочисельні асиметричні криптосистеми 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;

9) вперше розроблено методологію криптографічного захисту інформації в системі залишкових класів, яка за рахунок застосування векторно-модульних методів модулярного множення та експоненціювання, цілочисельної, модифікованої досконалої форми, поліноміальної та ієрархічної систем залишкових класів дає змогу 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.

Практичне значення одержаних результатів:

1) розроблено алгоритмічне забезпечення для дво- та тримодульної криптосистеми Рабіна та криптосистеми Ель-Гамаля на основі СЗК, а також з використанням векторно-модульного методу модулярного множення та експоненціювання, що дозволило значно зменшити часову складність криптографічних перетворень у порівнянні з традиційними підходами;

2) здійснено програмну реалізацію симетричних та асиметричних криптоалгоритмів у СЗК, завдяки чому емпірично підтверджено переваги запропонованих методів, що є підґрунтям для впровадження розроблених алгоритмів у сучасні інформаційні системи;

3) розроблено програмне забезпечення для реалізації ієрархічного симетричного криптоалгоритму в СЗК, яке завдяки розпаралеленню процесу обчислення забезпечує високу швидкодію процесів шифрування/дешифрування, що надає переваг при застосуванні у багаторівневих системах захисту даних;

4) розроблено програмне забезпечення симетричного шифрування в поліноміальній СЗК, яке забезпечує зручність використання та дозволяє адаптивно налаштовувати параметри відповідно до задач користувача, а також спрощує пояснення складних процесів шифрування.

Результати досліджень впроваджені або плануються до впровадження (підтверджено відповідними актами) в Акціонерному товаристві «Тернопільобленерго» (№5291/24 від 17.12.2025 р.), ТзОВ НВФ «Інтеграл» (№03-07/2025 від 07.03.2025 р.), ТзОВ завод «Рембутехніка» (№ЦКБ/04-25 від 10.02.2025 р.), Управлінні кібербезпеки та цифрового розвитку відділу цифрової трансформації Міністерства енергетики України, Департаменті Бюро економічної безпеки України (від 12.01.2025 р.), використані при виконанні п’яти науково-дослідних робіт у Західноукраїнському національному університеті (ЗУНУ) (від 05.12.2025 р.), у навчальному та науковому процесах факультету комп’ютерних інформаційних технологій ЗУНУ (від 5.09.2025 р.).

Особистий внесок здобувача. Наукові положення, які містяться в дисертації, отримані здобувачем особисто. У друкованих працях, опублікованих у співавторстві, автору належить: [1, 32] – запропоновано симетричний криптоалгоритм в ІПСЗК та проведено дослідження криптостійкості, [2] – запропоновано симетричний криптоалгоритм в ПСЗК, [3] – запропоновано асиметричний криптоалгоритм в СЗК, [4] – удосконалено метод пошуку

оберненого поліному в кільці Z[x] на основі методу невизначених коефіцієнтів, [5] – запропоновано симетричні криптоалгоритми у СЗК, [6, 11, 17, 30, 31, 38, 57] – розроблена метод побудови МДФ СЗК та МДФ СЗК для модулів однакової розрядності, [7, 28] – представлено теоретичні основи аналітичного обчислення коефіцієнтів базисних чисел перетворення Крестенсона, [9] – представлено метод пониження складності виконання основних операцій криптосистеми Рабіна, [10] – запропоновано метод множення багаторозрядних чисел у системі залишкових класів для асиметричних криптосистем, [12] – удосконалено метод відновлення полінома по його залишках на основі операції додавання, [13, 19, 31, 40, 41, 52] – розроблено алгоритмічне забезпечення криптосистеми Рабіна з використанням операції додавання та на основі МДФ СЗК, [14, 43] – удосконалено реалізацію криптоалгоритму Ель-Гамаля на основі векторно-модульного методу модулярного множення, експоненціювання та на основі СЗК, [19] – запропоновано модифікований метод шифрування Рабіна з використанням різних форм СЗК, [21] – удосконалено алгоритм пошуку символів Якобі, [22] – представлено аналітичний пошук модулів досконалої форми системи залишкових класів та їх застосування в китайській теоремі про залишки, [26] – запропоновано теоретичні основи виконання модулярних операцій множення та експоненціювання в теоретико–числовому базисі Крестенсона–Радемахера, [33] – запропоновано симетричний криптографічний алгоритм в ІСЗК, [34] – проведено аналіз тенденцій досліджень та майбутні виклики алгоритмів шифрування з використанням СЗК, [36] – удосконалено реалізацію поліноміального криптоалгоритму Рабіна на основі операції додавання, [39] удосконалено реалізацію трьохмодульного криптоалгоритму Рабіна на основі операції додавання, [42] представлено метод визначення простих та взаємно простих чисел типу 2^n+k на основі властивості періодичності, [44] – запропоновано метод відновлення десяткового числа з його залишків на основі додавання модулів добутку, [53] – розроблено методологію криптографічного захисту інформації на основі цілочисельної, модифікованої досконалої та поліноміальної систем залишкових класів, [58] – Розроблено фундаментальні основи теорії дискретного логарифму у базисі Радемахера-Крестенсона; [59] – розроблено векторно-модульний метод модулярного множення.

Апробація результатів дисертації. Основні результати дисертаційної роботи доповідались і обговорювались на таких міжнародних та вітчизняних конференціях, школах, семінарах, як: International Conference on Advanced Computer Information Technologies (2025, 2024, 2023, 2022, 2021, 2020, 2018 роки), Intelligent Information Technologies and Systems of Information Security (2021 рік), International Conference on Computer Sciences and Information Technologies (CSIT) (2020 рік), Conference on Computer Science and Information Technologies (2020 рік), International Conference on Advanced Trends in Radioelectronics, Telecommunications and Computer Engineering (2020, 2018, 2016 роки), IEEE International Conference on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications (IDAACS) (2019, 2017, 2015, 2012 роки), VI Всеукраїнська школа-семінар молодих вчених і студентів «Сучасні комп’ютерні інформаційні технології» (ACIT) (2018 рік), Науково-

технічна конференція «Інформаційні моделі, системи та технології» (2018 рік), Міжнародна науково-технічна конференція молодих учених та студентів «Актуальні задачі сучасних технологій» (2018 рік), International Conference The Experience of Designing and Application of CAD Systems in Microelectronics (CADSM) (2017, 2015 роки), Міжнародна науково-технічна конференція ITSec-2025 Безпека інформаційних технологій (2025, 2024 роки), International Conference on Control, Automation and Systems (ICCAS–2016) (2016 рік), Міжнародна науково-практична конференція «Сучасні інформаційні та електронні технології» (2014 рік).

Публікації. За результатами досліджень, які викладені в дисертації, опубліковано 61 наукову працю, серед яких 5 колективних монографій, 26 публікацій у наукових фахових виданнях України та закордонних виданнях, в тому числі 11 статей включено в наукометричні бази Scopus та/або Web of Science (з них, відповідно до класифікації SCImago Journal and Country Rank або Journal Citation Reports, три статті віднесено до квартилю Q2, чотири – до квартилю Q3 та одна – до квартилю Q4) та 28 публікацій у матеріалах міжнародних та всеукраїнських конференцій (з них 22 публікацій включено в наукометричні бази Scopus та/або Web of Science), 2 патенти на корисну модель. Одна стаття, розділ монографії і одні тези написані автором одноосібно.

Обсяг і структура дисертації. Дисертація складається з анотації, змісту, вступу, шістьох розділів, загальних висновків, списку використаних джерел і додатків. Основний текст роботи викладено на 347 сторінках. Список використаних джерел нараховує 331 найменувань на 38 сторінках. Робота містить 65 таблиць та 99 рисунків (з них 10 таблиць і 6 рисунків займають повну сторінку), 2 додатків на 35 сторінках. Загальний обсяг роботи 420 сторінок.

ОСНОВНИЙ ЗМІСТ РОБОТИ

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** проаналізовано сучасний стан криптографічних методів захисту інформації з акцентом на симетричні та асиметричні алгоритми, встановлено їх ключові переваги та обмеження, а також досліджено перспективи застосування СЗК та поліноміальної арифметики для підвищення ефективності криптографічного захисту.

Проведений аналіз теоретичних основ симетричних криптоалгоритмів засвідчив, що серед існуючих рішень алгоритм AES демонструє найкращі показники з точки зору криптографічної стійкості, швидкодії та пропускної здатності. Принципово новий підхід до симетричного шифрування забезпечується використанням СЗК, де замість єдиного монолітного ключа використовується розподілена система модулів. Це кардинально змінює парадигму криптоаналізу - замість атаки на один ключ зловмисник повинен одночасно компрометувати всі модулі системи, що комбінаторно збільшує

складність зламу. Результати порівняльного аналізу симетричних криптоалгоритмів подано в таблиці 1.

Таблиця 1

Порівняльна характеристика симетричних криптоалгоритмів

Параметр порівняння	AES-256	DES	3DES	Криптосистеми			
				СЗК	МДФ СЗК	СЗК зі зміною базисних чисел	КТЗ
				k – кількість модулів, l – їх розмірність			
Довжина ключа	256 біт	56 біт	168 біт	$k \times l$ біт	$k \times l$ біт	$2k \times l$ біт	$k \times l$ біт
Розмір блоку	128 біт	64 біт	64 біт	Змінний ($N < P$)	Змінний ($N < P$)	Змінний ($N < P$)	Підблоки < p_i
Криптостійкість	2^{255}	2^{55}	2^{112}	$\left(\left(\frac{2^{l+1}}{l}\right)^k l^2\right)$	$\left(\left(\frac{2^{l+1}}{l}\right)^k l^2\right)$	$O\left(\begin{matrix}log_2(k-1)) \\ \cdot k \cdot l^6\end{matrix}\right)$	$O\left(\left(\frac{2^{l+1}}{l}\right)^k (l \cdot \log 2l)^2\right)$
Паралелізація	Обмежена	Ні	Ні	Повна	Повна	Повна	Часткова
Швидкість шифрування	Висока	Середня	Низька	Висока	Найвища	Висока	Середня
Швидкість розшифрування	Висока	Середня	Низька	Низька	Висока	Низька	Висока
Математична основа	Підстановки/перестановки	Feistel мережа	Triple DES	КТЗ	МДФ + КТЗ	Модифікована КТЗ	КТЗ для підблоків
Стійкість до квантових атак	Підвищена	Вразливий	Вразливий	Підвищена	Підвищена	Найвища	Підвищена

Проведений комплексний аналіз найбільш поширених асиметричних криптосистем, зокрема системи Рабіна, Ель-Гамаля, RSA та криптографії на основі математичного апарату еліптичних кривих, виявив їх критичну залежність від складних арифметичних операцій. Встановлено, що основними операціями в цих системах є модулярне множення, модулярне експоненціювання та пошук оберненого елемента за модулем, які характеризуються значною часовою складністю.

Порівняльні характеристики асиметричних криптосистем наведено в таблиці 2.

Розроблені методи не просто покращують існуючі алгоритми, а створюють новий підхід до криптографічних рішень, здатних адаптуватися до майбутніх викликів інформаційної безпеки, включаючи квантові загрози та вимоги IoT-середовищ. Особливе значення має гібридний СЗК-алгоритм, який формує новий клас криптосистем з подвійним рівнем захисту та унікальною комбінацією симетричних і асиметричних елементів.

Таблиця 2

Порівняльна характеристика асиметричних криптосистем

Криптосистема	Математична основа	Розмір ключа (біт)	Стійкість до квантових атак	Часова складність, k-кількість модулів, l – їх розрядність	Переваги
1	2	3	4	5	6
RSA	Факторизація великих чисел	2048–4096	Низька	O(l^3)	Стандартизований, надійний
Рабіна	Квадратичні лишки	1024–2048	Низька	O(l^3)	Простота реалізації
Ель-Гамаля	Дискретний логарифм	2048–4096	Низька	O($l^2(log_2\ log_2 l)^2$)	Семантична безпека
ECC	Еліптичні криві	256–512	Низька	O(l^3)	Короткі ключі
Асиметричний у СЗК	СЗК + гібридна архітектура	$k\times(l+1)$	Висока	$O(k^2 \cdot l^{k+7})$	Подвійний захист, паралелізація
Удосконалений Рабіна (СЗК)	Квадратичні лишки + СЗК	1024–2048	Підвищена	$O(l^2\left(\frac{k^2+k}{2}\right) + \frac{l}{2}log_2\ l)$	Паралелізація, зниження складності
Удосконалений Ель-Гамаля (СЗК)	Дискретний логарифм + СЗК	2048–4096	Підвищена	$O\left(l^2 + \frac{3}{2}llog_2 l\right)$	8-кратне прискорення при l=256
Поліноміальний алгоритм Рабіна	Квадратичні лишки в Z[x]	Змінний	Висока	$O\left(5l\ log_2\ l + l^{\frac{3}{2}} + l\right)$	Квантова стійкість
Двомодульний Рабіна (СЗК)	Квадратичні лишки	1024	Підвищена	$O(l^2\left(\frac{k^2+k}{2}\right) + \frac{l}{2}log_2\ l)$	Простота, швидкість
Тримодульний Рабіна (СЗК)	Квадратичні лишки	1536	Підвищена	$O(l^2/3)$	Оптимальний компроміс

Проаналізовано особливості застосування СЗК у криптографічних методах захисту інформації та встановлено її унікальні переваги. Виділено основні переваги СЗК: можливість виконання операцій над числами меншої розрядності порівняно з вибраними модулями, природне розпаралелення процесу обчислень, як найбільш перспективний шлях підвищення швидкодії обчислювальних систем, та повну відсутність міжрозрядних переносів.

Досліджено різні форми СЗК та встановлено їх порівняльні характеристики щодо відновлення десяткового числа та обчислювальної складності. Обґрунтовано можливість ефективного застосування методів шифрування у СЗК.

Проведений аналіз літературних джерел підтвердив актуальність та критичну важливість поліноміальних алгоритмів у сучасних системах захисту інформаційних потоків. Встановлено, що поліноміальна арифметика в кільці поліномів Z[x] дозволяє здійснювати базові операції додавання, множення, ділення з остачею та використовувати поліноми як відкриті/зашифровані тексти і ключі в криптографічних алгоритмах.

Досліджено методи пошуку оберненого полінома за модулем та відновлення полінома за його залишками, виявлено їх обмеження у вигляді строго послідовної структури та необхідності виконання операцій над поліномами вищих порядків.

Проаналізовано особливості ІСЗК, яка сприяє оптимізації обчислень і одночасно підвищує рівень криптографічної безпеки.

Досліджено сучасні тенденції розвитку криптографічних систем та встановлено, що традиційні підходи стають дедалі більш вразливими до криптоаналітичних атак через зростання обчислювальних можливостей. Проведений аналіз засвідчив необхідність створення нових криптоалгоритмів із підвищеним рівнем стійкості, що актуалізує потребу в розробці методів, які ефективно поєднують переваги різних математичних підходів.

У другому розділі запропоновано удосконалення реалізації асиметричних криптосистем Рабіна та Ель-Гамаля на основі операції додавання та з використанням СЗК.

Для зменшення часової складності при шифруванні за допомогою тримодульної криптосистеми Рабіна пропонується використовувати векторно-модульний метод модулярного множення. На першому етапі вибираються три великих простих числа *p, q i r* та обчислюється значення $t= p \cdot q \cdot r$, де число t - відкритий ключ, а p, q і r – таємний.

Шифрування відкритого повідомлення M відбувається за допомогою відкритого ключа *t* за формулою (1).

З використанням векторно-модульного методу модулярного множення значення $M \cdot M \bmod t$ шукаються таким чином. Відкритий блок M представляється у двійковій формі: $M = \sum_{i=0}^{l-1} a_i \cdot 2^i$, де $a_i = 0, 1$, l–розрядність модуля. Далі будуються два вектор-рядки, в першому з яких записуються елементи a_i, в другому - $m_0 = 2^0 M \bmod t$, $m_i = 2 \cdot h_{i-1} \bmod t$.

Результат модулярного множення $M \cdot M \bmod t$ знаходиться згідно формули:

$$C = M^2 \bmod t = \left(\sum_{i=0}^{l-1} a_i \cdot m_i\right) \bmod t, \quad (1)$$

В результаті операція модулярного множення замінюється операцією додавання тих m_i, для яких відповідні a_i рівні 1. Даний метод характеризується меншою часовою складністю порівняно з класичними.

При розшифруванні криптограми *C*, вводяться додаткові допоміжні величини s, w і u:

$$s = C \bmod p;\ w = C \bmod q;\ u = C \bmod r. \quad (2)$$

Значення x, y і z шукаються з таких порівнянь:

$$x^2 \equiv s(\bmod p),\ y^2 \equiv w(\bmod q),\ z^2 \equiv u(\bmod r). \quad (3)$$

Для знаходження *x, y* і *z* необхідно обчислити значення кореня квадратного за модулем. Класичні підходи з використання символів Якобі або Лежандра є трудомісткими. Тому доцільно використати метод, який вимагає тільки операції додавання та перевірки, чи є число повним квадратом. Така процедура дозволяє суттєво зменшити обчислювальну складову методу Рабіна. Отже, для пошуку значення $\sqrt{s} \bmod t$ необхідно виконати наступну послідовність дій: $s + t$, $s + 2t$, …, $s + i \cdot t$, де i - значення, при якому $s + i \cdot t$ буде повним квадратом.

Аналогічно шукається $y^2 \equiv w(mod\, q)$, $z^2 \equiv u(mod\, r)$. Оскільки розв'язками порівнянь (4) буде шість значень, то для розшифрування потрібно розв'язати вісім систем порівнянь, що утворюються як комбінації усіх можливих варіантів пошуку відкритого повідомлення (i=1…8):

$$\begin{cases} M_i \equiv \pm x(mod\, p); \\ M_i \equiv \pm y(mod\, q); \\ M_i \equiv \pm z(mod\, r). \end{cases} \quad (4)$$

Шуканим повідомленням M буде один із розв'язків систем порівнянь (4). Для їх вирішення доцільно використати метод на основі додавання добутку модулів, який характеризується меншою обчислювальною складністю в порівнянні з класичними: використання КТЗ та алгоритму Гарнера.

Для прикладу розглянемо одну із систем порівнянь (4), в якій параметри x, y, z додатні. Оскільки будь-яку конгруенцію x mod p =M_1 можна представити у вигляді $x = \gamma p + M_1$, де γ = 0, 1, 2, …, то до залишку $M_1^{(1)} = x$ потрібно додавати модуль p стільки разів, поки не буде виконуватись конгруенція $M_1^{(2)} \equiv y(mod\, q)$, де $M_1^{(2)} = \mathrm{M}_1^{(1)} + \gamma_1 p$. Далі необхідно додавати добуток pq, поки не буде виконуватись конгруенція $M_1^{(3)} \equiv z(mod\, r)$, де $M_1^{(3)} = M_1^{(2)} + \gamma_2 pq = M_1$. Аналогічним чином шукаються розв'язки інших систем порівнянь (4).

Здійснено аналітичне порівняння часових складностей запропонованого та відомого підходів.

Встановлено, що удосконалення реалізації тримодульної криптосистеми Рабіна суттєво оптимізує обчислювальний процес, замінюючи в процесі шифрування операцію множення операцією додавання з використанням векторно-модульного методу, а при розшифруванні використовується метод додавання добутку модулів. Це дало змогу зменшити часову складність з $O(2kl^3 + 2l^2k+lk)$ до $01\left(\mathrm{l}^2\left(\frac{\mathrm{k}^2+\mathrm{k}}{2}\right)+\frac{\mathrm{l}}{2}\log_2 \mathrm{l}\right)$ (рисунок 1).

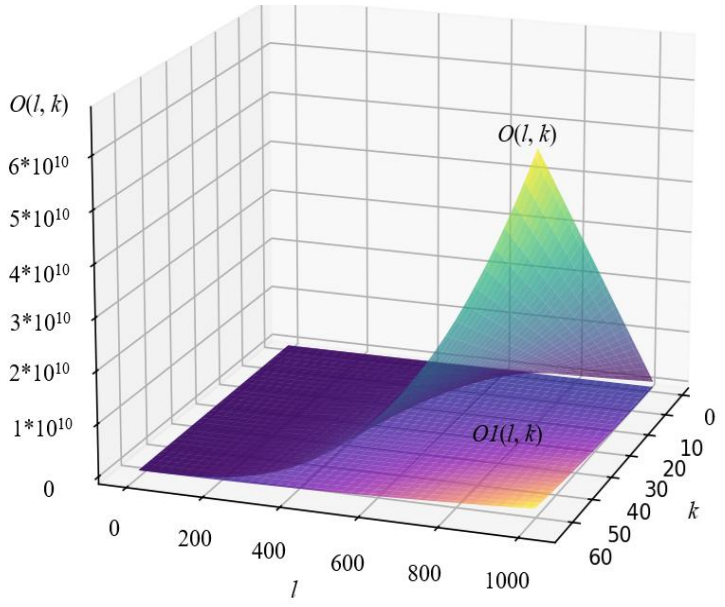


Рис. 1. Графічна залежність часової складності запропонованого методу від кількості модулів та їх розрядності

Ефективність запропонованого удосконалення реалізації криптосистеми Рабіна визначається як співвідношення часових складностей:

$$\mathrm{E}(l,k) = \frac{(2l^3 + 4l^2 + 2l + l^{1{,}465})}{l^2\left(\frac{k^2+k}{2}\right) + \frac{l\, log_2\, l}{2}} = \frac{4l^2 + 8l + 2l^{0{,}465} + 4}{l(k^2+k) + log_2\, l}. \quad (5)$$

Результати проведених досліджень свідчать, що впровадження розробленого алгоритмічного забезпечення для тримодульного криптоалгоритму Рабіна, заснованого на операції додавання, дозволяє значно знизити часову складність базових операцій. Зокрема, при параметрах k=3 та l=256 складність зменшується у 128 разів, переходячи з кубічної до квадратичної.

Запропонований підхід для удосконалення реалізації криптоалгоритму Ель-Гамаля базується на принципово новій концепції сумісного застосування СЗК з векторно-модульним алгоритмом модулярного експоненціювання, що забезпечує суттєве зниження обчислювальної складності.

У процесі генерування ключів для криптосистеми Ель-Гамаля обчислення здійснюються згідно формули $y = q^x \, mod \, p = (\left(\sum_{i=0}^{l-1} b_i B_i q_i\right) mod P \,) mod \, p$, де y, p і q – відкритий ключ, x- таємний ключ, $q_i = (q \, mod \, p_i)^x \, mod \, p_i$, $P = \prod_{i=1}^{k} p_i$, $B_i = \frac{p}{p_i}$, $b_i = B_i^{-1} \, mod \, p_i$, k – кількість модулів та потоків. Пошук значення q_i здійснюється на основі використання векторно-модульного методу модулярного експоненціювання, представивши $x = \sum_{j=0}^{l-1} x_j \cdot 2^j$, де $x_j = 0{,}1$. Тоді $\mathrm{q_i} = (\mathrm{q \bmod p_i})^{\sum_{j=0}^{l-1} x_j \cdot 2^j} \bmod \mathrm{p_i} = \prod_{j=0}^{l-1} (\mathrm{q \bmod p_i})^{x_j \cdot 2^j} = \prod_{j=0}^{l-1} \mathrm{s_j} \bmod \mathrm{p_i}$, де $s_j = (q \, mod \, p_i)^{2^i} \, mod \, p_i = \left(s_{j-1}\right)^2 \, mod \, p_i$. Ключова перевага цього підходу полягає у заміні складних операцій множення багаторозрядних чисел простими операціями додавання та табличного пошуку, що кардинально знижує обчислювальну та часову складності.

Етап шифрування включає обчислення значень $b = y^v \cdot M \, mod \, p$, $a = q^v \, mod \, p$, де M – відкритий текст, на основі використання векторно-модульного методу модулярного експоненціювання.

Процедура розшифрування $M = b \cdot (a^x)^{-1} \, mod \, p$ включає операції піднесення до степеня за допомогою векторно-модульного методу та пошуку оберненого елемента за модулем на основі додавання залишку. В загальному для знаходження $\eta = \varepsilon^{-1} \, mod \, p$ спочатку обчислюється $\eta_0 = p \, mod \, \varepsilon \neq 0$, після чого послідовно виконується операція додавання: $\eta_1 = (\eta_0 + 1) \, mod \, \varepsilon$, $\eta_2 = (\eta_1 + \eta_0) \, mod \, \varepsilon = (2\eta_0 + 1) \, mod \, \varepsilon$,…, $\eta_i = (\eta_{i-1} + \eta_0) \, mod \, \varepsilon = (i\eta_0 + 1) \, mod \, \varepsilon$. Описана процедура продовжується до тих пір, поки деяке число η_i не стане рівним нулю. Тоді обернений елемент визначається за формулою $\eta = \varepsilon^{-1} \, mod \, p = \frac{i \cdot p + 1}{\varepsilon}$.

Побудовано аналітичні вирази оцінки часових складностей класичної $O(l^3 + 4l^2 \, (\, loglogl)^2 + 2l \, log \, logl)$ та удосконаленої реалізації криптосистеми Ель-Гамаля $O\left(l^2 \, (\, log_2 l)^2 + log_2 l * log_2 \left(\frac{l}{2}\right) + \frac{3}{2} l log_2 l\right)$. Результати проведених досліджень свідчать, що використання векторно-модульних методів модулярного множення та експоненціювання, дозволяє значно знизити часову складність базових операцій. Зокрема, для розрядностей модулів l=256 біт складність зменшується у 8 разів, що дає змогу спростити апаратну реалізацію та знизити структурну складність під час схемотехнічного проєктування криптосистеми Ель-Гамаля.

У третьому розділі розроблено симетричні криптоалгоритми СЗК, метод симетричного шифрування на основі КТЗ, асиметричні криптоалгоритми на основі СЗК та її МДФ**.**

Вперше розроблено симетричний криптоалгоритм у СЗК, в якому шифротекстом виступає набір залишків по відповідних модулях (ключах). Відкрите повідомлення в числовій формі (найпоширенішим класичним методом є заміна букви на її номер в алфавіті, причому нумерація починається з 0) розбивається на блоки N, для кожного з яких повинна виконуватись умова $N<P$.

Шифротекстом виступає набір залишків b_i, які отримуються з формули:

$$b_i=N \bmod p_i. \quad (6)$$

Розшифрування або відновлення десяткового числа за його залишками відбувається згідно виразу:

$$N = \left(\sum_{i=1}^{k} b_i M_i m_i\right) mod\, P, \quad (7)$$

де $P = \prod_{i=1}^{k} p_i$, $M_i = \frac{P}{p_i}$, m_i шукається з виразу $m_i = M_i^{-1}\, mod\, p_i = 1$, k – кількість модулів. При цьому повинна виконуватися нерівність $N<P$.

Спростити відновлення десяткового числа за його залишками дозволяє використання МДФ СЗК, в якій модулі підібрані таким чином, що $m_i=\pm 1$.

Здійснено оцінку криптостійкості на основі закону асимптотичного розподілу простих чисел, згідно якого кількість простих чисел на інтервалі від 0 до деякого q наближено визначається за формулою $\pi(q) = \frac{q}{ln\, q}$. З врахуванням часової складності КТЗ загальна часова складність для криптоаналізу запропонованого криптоалгоритму становить $O\left(\left(\frac{2^{l+1}}{l}\right)^k l^2\right)$, де l-розрядність модулів, k – їх кількість. На рис. 2 зображена поверхня, яка характеризує залежність складності $\ln(O(l,k))$ від розрядності l та кількості модулів k. Видно, що із збільшенням вказаних параметрів складність криптоаналізу зростає.

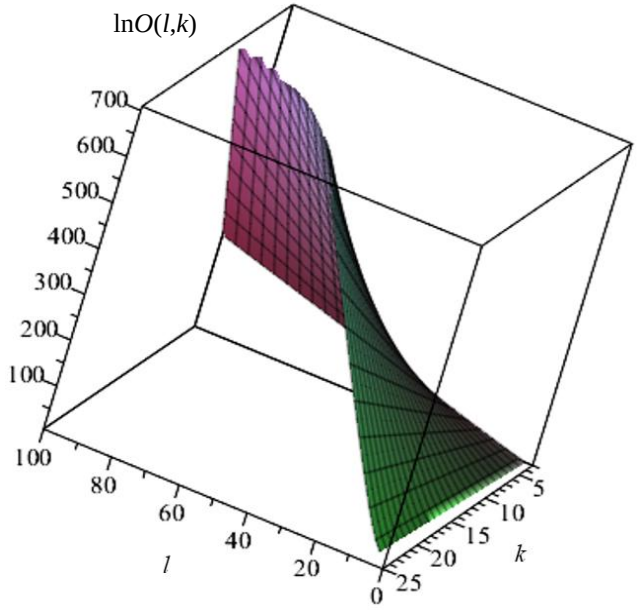


Рис. 2. Залежність складності $\ln(O(l,k))$ від розрядності l та кількості модулів k

Для криптоаналізу сучасного симетричного шифру AES-256 необхідно 2^{255} бітових операцій.

З рівності $\left(\frac{2^{l+1}}{l}\right)^k l^2 = 2^{255}$ можна знайти розрядності та кількість модулів СЗК, які забезпечують таку ж стійкість, як і ключ найбільшої довжини алгоритму AES-256 (таблиця 4). Встановлено, що при кількості модулів l=5, 6, 7, 8 з розрядностями k=139, 115, 98, 85 біт відповідно криптостійкість підвищується у 2 рази. Таблиця 3 демонструє, що із збільшенням кількості модулів їх розрядність зменшується.

Таблиця 3

Розрядності та кількість модулів СЗК, які забезпечують таку ж стійкість, як і ключ найбільшої довжини алгоритму AES-256

К-сть модулів	3	4	5	6	7	8	9	10	11	12	13	14	15
Розрядність	87	66	54	46	40	35	32	29	27	25	23	21	20

У випадку, коли потрібне швидке розшифровування, доцільно використати інший симетричний криптоалгоритм. Однак при його використанні усі модулі СЗК мають перевищувати максимальне числове значення відповідного блоку відкритого тексту b_i. На рис. 3 представлена загальна схема шифрування запропонованим методом.

Шифротекст отримується згідно виразу (7). Слід відмітити, що криптостійкість даного методу буде менша порівняно з попереднім, оскільки складність пошуку залишків $O(l\cdot\log_2 l)$ менша, ніж для множення – $O(l^2)$ і оцінюватиметься згідно виразу $O\left(\left(\frac{2^{l+1}}{l}\right)^k (l\cdot log_2 2l)^2\right)$. Встановлено, що при кількості модулів k=5 та їх розрядності l=150 біт стійкість в 3 рази перевищує стійкість AES-256.

Використання МДФ СЗК (m_i=±1) приводить до зменшення кількості арифметичних операцій (зокрема, уникнення пошуку оберненого елемента та множення на нього в (7), спрощення процедури пошуку залишку за модулем P), які виконуються над операндами, що мають меншу розрядність в порівнянні із звичайною цілочисельною формою СЗК. В свою чергу, це зумовлює підвищення швидкодії процесу розшифрування інформації. Представлений алгоритм шифрування доцільно використовувати тоді, коли під час обміну інформацією необхідно швидко зашифрувати повідомленнями, а розшифрування може тривати більше часу.

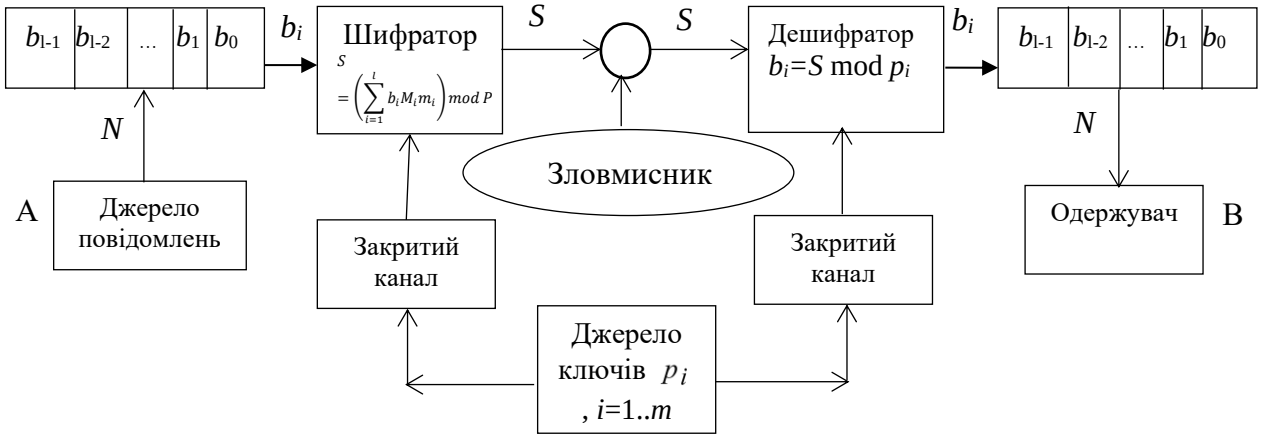


Рис. 3. Загальна схема симетричного шифрування на основі КТЗ

Вперше розроблено симетричні методи шифрування в СЗК та МДФ СЗК на основі зміни базисних чисел. Суть одного з методів симетричного шифрування в СЗК полягає в тому, що при відновленні числа в позиційну систему числення за його залишками у сумі (7) множення відбувається не на параметри $m_i = M_i^{-1}\, mod\, p_i$, а на довільно вибрані коефіцієнти k_i для яких виконуються

умови $1<k_i<p_i$ та НСД $(k_i, p_i)=1$.

Спочатку вибирається блок відкритого тексту $N<P$, який потім записується в СЗК згідно виразу (6). Шифрування відбувається при відновленні числа в позиційну систему числення згідно виразу: $N' = \left(\sum_{i=1}^{k} b_i M_i k_i\right) mod\, P$.

Знайдене число є шифротекстом, яке передається від одного абонента до іншого. При розшифруванні спочатку обчислюються такі величини: $q_i = \left(m_i(k_i^{-1}\, mod\, p_i)\right) mod\, p_i$; $b_i' = N' mod\, p_i$. Для отримання істинних залишків b_i необхідно виконати перетворення згідно співвідношення: $b_i = \left(b_i' q_i\right) mod\, p_i = \left(b_i' m_i k_i^{-1}\right) mod\, p_i$.

Відповідно, відновлення числа N, яке є відкритим текстом, здійснюється за формулою (7) або можна використати вираз, який з неї випливає:

$$N = \left(\sum_{i=1}^{k} M_i m_i \left(\left(b_i' m_i k_i^{-1}\right) mod\, p_i\right)\right) mod\, P = \left(\sum_{i=1}^{k} M_i m_i \left(\left(b_i' q_i\right) mod\, p_i\right)\right) mod\, P. \quad (8)$$

За допомогою функції Ейлера $\phi(p_i)$, здійснено оцінку криптостійкості запропонованого симетричного методу шифрування у СЗК, яка ґрунтується на пошуку всіх можливих варіантів параметрів k_i та модулів криптоперетворень p_i. Набори модулів криптоперетворення у запропонованому методі можна отримати такою кількістю способів: $\prod_{i=1}^{k-1} \phi(p_i)$.

Отримано аналітичний вираз оцінки складності математичної атаки з врахуванням часової складності КТЗ $O\left(k \cdot l^2 \cdot \left(\prod_{i=1}^{k-1} \phi(p_i)\right)^2\right)$. Збільшення криптостійкості можна досягнути завдяки збільшенню кількості модулів p_i і, відповідно, параметрів k_i (ключів), їх розрядності, а також вибором таких модулів, для яких значення $\phi(p_i)$ буде максимальним. Якщо вважати, що всі модулі мають розрядність n, то загальна стійкість оцінюватиметься виразом $O(log_2(k-1) \cdot k \cdot l^6)$.

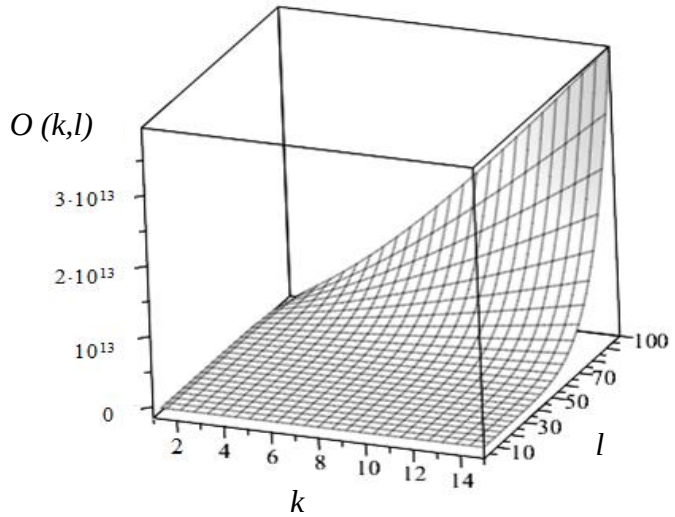


Рис. 4. Залежність криптостійкості алгоритму від розрядності модулів та їх кількості

Графік залежності стійкості від розрядності l та кількості модулів k представлено на рис. 4. Видно, що із збільшенням цих парамет-рів криптостійкість алгоритму різко зростає. Оптимізація параметрів дозволяє досягти балансу між криптографічною безпекою і обмеженими ресурсами, наприклад в IoT-пристроях.

Вперше розроблено асиметричний криптоалгоритм у СЗК, в якому при генерації ключів обидва абоненти повинні вибрати відомі тільки їм обом системи модулів p_i. Звідси випливає симетричність запропонованої криптосистеми. Далі

кожен абонент довільно вибирає цілі числа w_i, які виступають відкритими ключами і для яких виконуються умови $1 \le |w_i| \le p_i$ та НСД ($|w_i|$, p_i)=1. Наявність відкритих ключів свідчить про асиметричність даної криптосистеми.

При шифруванні блок відкритого тексту $S<P$ спочатку записується в СЗК у вигляді залишків згідно виразу (6). Слід зазначити, що конкатенація залишків b_i відразу ж може виступати шифротекстом. Однак зловмисник, перехопивши декілька повідомлень, може зробити висновки про порядок параметрів p_i, що значно спростить криптоаналіз перехопленого тексту. Для усунення даного недоліку процес шифрування полягає в тому, що при відновленні десяткового числа із його залишків згідно формули $S = \left(\sum_{i=1}^{k} b_i P_i f_i\right) mod\, P$, де $P = \prod_{i=1}^{k} p_i > S$, $P_i = \frac{P}{p_i}$, f_i шукається з виразу $f_i P_i \, mod\, p_i = 1$, k – кількість модулів, множення відбувається не на коефіцієнти f_i, а на вибрані отримувачем відкриті ключі w_i, тобто: $S' = \left(\sum_{i=1}^{k} b_i P_i w_i\right) mod\, P$. Знайдене число S' є шифротекстом. В свою чергу, отримувач при розшифруванні обчислює величини $r_i = \left(f_i(w_i^{-1} \, mod\, p_i)\right) mod\, p_i$ та визначає зашифровані залишки $b_i' = S' mod\, p_i$.

Для отримання справжніх залишків b_i виконуються такі операції: $b_i = \left(b_i' r_i\right) mod\, p_i = \left(b_i' f_i w_i^{-1}\right) mod\, p_i$.

Тоді відновлення десяткового числа S, яке є відкритим текстом, відбувається згідно КТЗ. Крім того, можна використати формулу, яка з нього випливає:

$$S = \left(\sum_{i=1}^{k} P_i f_i \left(\left(b_i' f_i w_i^{-1}\right) mod\, p_i\right)\right) mod\, P = \left(\sum_{i=1}^{k} P_i f_i \left(\left(b_i' r_i\right) mod\, p_i\right)\right) mod\, P. \quad (9)$$

Для спрощення розрахунків і, відповідно, зменшення часу при розшифруванні доцільно використовувати МДФ СЗК. Проведено оцінку криптостійкості розробленого асиметричного криптоалгоритму з використанням СЗК, cпійкість якого грунтується на повному переборі усіх можливих варіантів взаємно простих модулів криптоперетворень p_i або розв'язку задачі факторизації (аналогічно криптосистемі RSA). Знаючи зазначені параметри і перехопивши у каналі зв'язку S' та w_i, зловмисник зможе знайти відкритий текст S. Тому оцінка криптостійкості зводиться до визначення часових складностей пошуку p_i, P_i, b_i і становитиме $O(k^2 \cdot l^{k+7})$. Графік її залежності від розрядності модулів та їх кількості представлено на рис. 5.

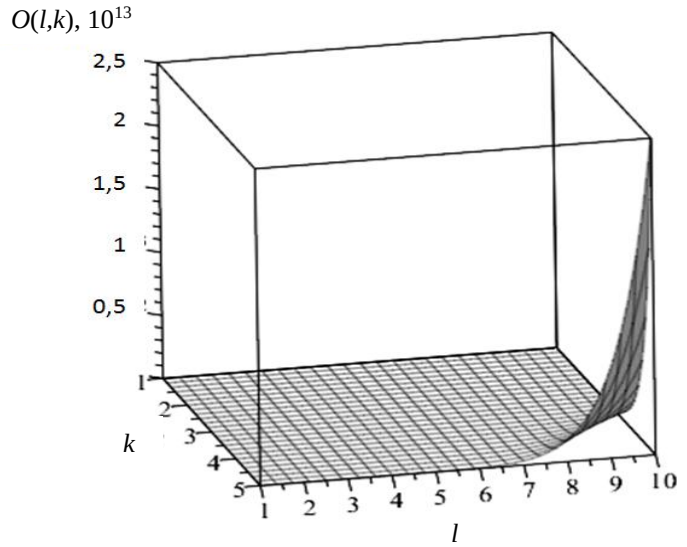


Рис. 5. Залежність криптостійкості запропонованого криптоалгоритму від l та k

Як видно з аналітичної оцінки часової складності та її графічної залежності, збільшення криптостійкості можна досягнути завдяки збільшенню

кількості модулів p_i, їх розрядності, а також вибором таких модулів, для яких значення $\phi(p_i)$ буде максимальним і при кількості модулів k=5 та їх розрядності l=74 біти вона підвищується у 2 рази.

У четвертому розділі розроблені теоретичні основи симетричних криптографічних алгоритмів у поліноміальній СЗК (ПСЗК), удосконалено реалізації методів пошуку оберненого полінома в кільці полінома та відновлення полінома за його залишками, поліноміальну криптосистему Рабіна.

Вдосконалено існуючі методи обчислення мультиплікативного оберненого полінома за модулем $m(x) = r^{-1}(x)\, mod\ g\,(x)$ в кільці поліномів $Z(x)$, де $r(x)$ і $g(x)$ – взаємно прості поліноми (НСД$\big(r(x), g(x)\big) = w, w \in Z$), і $deg\, r\,(x) = n, deg\, g\,(x) = u$ на основі методу невизначених коефіцієнтів, для якого виконується рівність:$r(x) \cdot m(x) \equiv w\, mod\, g\,(x)$. Розроблений алгоритм включає послідовне обчислення добутку поліномів, знаходження залишків через систему перетворень та розв'язування системи рівнянь для невизначених коефіцієнтів. Схема запропонованого удосконалення представлена на рис. 6.

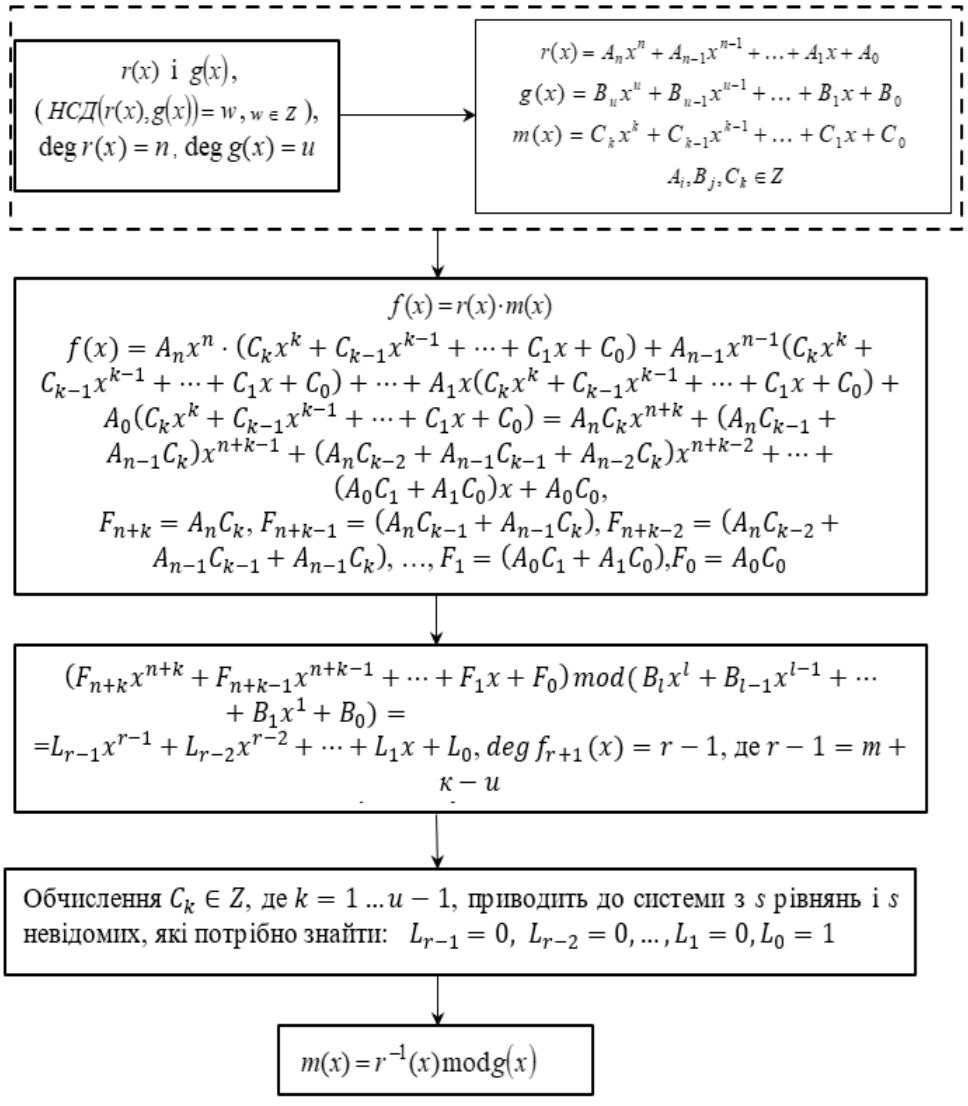


Рис. 6. Схема методу пошуку оберненого полінома в кільці поліномів

Побудовано аналітичні вирази часових складностей запропонованого та класичного методу пошуку оберненого елемента в кільці поліномів. Теоретично доведено, що часова складність запропонованого методу складає $O1(2n\, log_2 n)$ у порівнянні з класичним підходом $O\big(nlog_2 n \cdot (1 + log_2 n)\big)$. Ефективність методу визначається співвідношенням $E(n) = (1 + log_2\, n)/2$. Експериментально встановлено, що при $n = 256$ розроблений метод у 4,5 рази переважає відомі підходи.

Розроблено принципово нові методи відновлення полінома за його залишками у кільці Z[x], які забезпечують можливість розпаралелення обчислень та уникають складної процедури пошуку мультиплікативного оберненого елемента. Метод базується на послідовному додаванні добутку модулів:

$$N_1(x) = b_1(x);\ N_2(x) = N_1(x) + \gamma_1(x)p_1(x);\ N_2(x)\ mod\ p_2\ (x) \equiv b_2(x);$$

$$N_i(x) = N_{i-1}(x) + \gamma_{i-1}(x)p_1(x)p_2(x)\ldots p_{i-1}(x);\ N_i(x)\ mod\ p_i\ (x) \equiv b_i(x);$$

$$\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \quad (10)$$

$$\mathrm{N_k(x) = N_{k\text{-}1}(x) + \gamma_{k\text{-}1}(x)p_1(x)p_2(x)\ldots p_{k\text{-}1}(x);}\ N_k(x)\ mod\ p_k\ (x) \equiv r_k(x).$$

де $\gamma_i(x)$ знаходяться методом невизначених коефіцієнтів.

Для спрощення обчислень, які використовуються у запропонованому методі, можна додавати не добуток поліномів-модулів, а залишок цього добутку від ділення на відповідний поліном. Математичний запис даного методу виглядає таким чином:

$$N_1(x) = b_1(x);\ p_{11}(x) = p_1(x)\ mod\ p_2\ (x);(N_1(x) + \gamma_1(x)p_{11}(x))\ mod\ p_2\ (x) = b_2(x);$$

$$N_2(x) = N_1(x) + \gamma_1(x)p_1(x);\ p_{12}(x) = p_1(x)p_2(x)\ mod\ p_3\ (x);$$

$$(N_2(x) + \gamma_2(x)p_{12}(x))\ mod\ p_3\ (x) = b_3(x);$$

$$\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \quad (11)$$

$$N_i(x) = N_{i-1}(x) + \gamma_{i-1}(x)p_1(x)p_2(x)p_3(x)\ldots p_{i-1}(x);\ p_{1i}(x) =$$

$$p_1(x)p_2(x)\ldots p_i(x)\ mod\ p_{i+1}\ (x);$$

$$N(x) = N_k(x) = N_{k-1}(x) + \gamma_{k-1}(x)p_1(x)p_2(x)p_3(x)\ldots p_{k-1}(x).$$

Аналітично отримано, що часова складність розробленого алгоритму становить $O_1\left((k^2+k)n\ log_2\ n\right)$ на відміну від алгоритму Гарнера, складність якого $\mathrm{O_2\left((k^2+k)(n\log_2 n) + kn\log_2{}^2 n\ loglog\ n\right)}$.

Доведено ефективність методу через співвідношення $E(n,k) = \frac{O_2(k,n)}{O_1(k,n)} = 1 + \frac{\log_2 n \log_2\log_2 n}{k+1}$. Чисельні експерименти показали, що при k=10, n=256 ефективність зростає у 641 раз.

Отримала подальший розвиток криптосистема Рабіна в кільці поліномів з принципово новим підходом до обчислення квадратичних лишків. У запропонованій системі таємні ключі складаються з двох незвідних поліномів $p(x)$ та $q(x)$, відкритий ключ $n(x) = p(x) \cdot q(x)$. Відкритий текст m також потрібно представити у вигляді полінома:

$$m(x) = m_c x^c + m_{c-1}x^{c-1} + \ldots + m_1 x + m_0, \quad (12)$$

де c – степінь полінома $m(x)$.

Блок відкритого тексту $m(x)$ повинен бути максимальним, але не перевищувати $n(x)$. Шифрування відбувається за допомогою піднесення $m(x)$ до квадрату та пошуку його залишку за модулем, який є відкритим ключем:

$$d(x) = m(x)^2\ mod\ n\ (x) = d_e x^e + d_{e-1}x^{e-1} + \ldots + d_1 x + d_0. \quad (13)$$

Для розшифрування необхідно знайти залишки від ділення шифротексту на значення таємного ключа:

$$y(x) = d(x)\, mod\, p\,(x) = x^g + z_{g-1}x^{g-1} + \ldots + z_1 x + z_0. \quad (14)$$

Після цього від знайдених поліномів $y(x)$ та $z(x)$ шукаються квадратні корені за відповідними модулями $p(x)$ та $q(x)$, які є таємним ключем:

$$\eta(x) = \sqrt{y(x)}\, mod\, p\,(x) = \eta_r x^r + \eta_{r-1}x^{r-1} + \cdots + \eta_1 x + \eta_0,$$

$$\lambda(x) = \sqrt{z(x)}\, mod\, q\,(x) = \lambda_s x^s + \lambda_{s-1}x^{s-1} + \ldots + \lambda_1 x + \lambda_0. \quad (15)$$

Розроблено новий метод знаходження квадратних коренів через послідовне додавання модуля допоки не буде повний квадрат $(y(x) + i \cdot p(x)) = \eta(x)^2$, максимальна кількість кроків становитиме $\zeta = \sqrt{(max(deg(y(x)), deg(p(x))))}$.

З отриманих двох пар $(\eta(x);\ -\eta(x) = p(x) - \eta(x))$ та $(\lambda(x);\ -\lambda(x) = q(x) - \lambda(x))$ формується чотири можливих пари систем з двох конгруенцій:

$$\begin{cases} m_1(x)\, mod\, p\,(x) = \eta(x); \\ m_1(x)\, mod\, q\,(x) = \lambda(x); \end{cases} \quad \begin{cases} m_2(x)\, mod\, p\,(x) = p(x) - \eta(x); \\ m_2(x)\, mod\, q\,(x) = \lambda(x); \end{cases} \quad (16)$$

$$\begin{cases} m_3(x)\, mod\, p\,(x) = \eta(x); \\ m_3(x)\, mod\, q\,(x) = q(x) - \lambda(x); \end{cases} \quad \begin{cases} m_4(x)\, mod\, p\,(x) = p(x) - \eta(x); \\ m_4(x)\, mod\, q\,(x) = q(x) - \lambda(x); \end{cases}$$

Розв'язок однієї із систем (21) і буде шуканим відкритим текстом.

Теоретично обґрунтовано зменшення часової складності запропонованого удосконалення поліноміальної криптосистеми Рабіна з $O(n^2 k\, log_2 n \cdot +2n\, log_2\, 2\, n)$ до $O1\left(5n\, log_2 n + n^{\frac{3}{2}} + n\, log_2 n + n\, log_2{}^2 n + n + 2n\, log_2\, 2\, n\right)$.

Вперше розроблено симетричний криптографічний метод в поліноміальній СЗК. Відомо, що довільний поліном $N(x)$ в СЗК представляється у вигляді залишків $b_i(x)$ від ділення $N(x)$ на кожен із системи попарно взаємно простих модулів-поліномів $p_i(x)$:

$$b_i(x) = N(x) \mod p_i(x). \quad (17)$$

Відновлення поліному $N(x)$ відбувається, як правило, на основі китайської теореми про залишки (КТЗ) в кільці поліномів $Z[x]$:

$$N(x) = \left(\sum_{i=1}^{s} b_i(x) M_i(x) m_i(x)\right) mod\, P\,(x), \quad (18)$$

де $P(x) = \prod_{i=1}^{s} p_i(x)$, $M_i(x) = \frac{P(x)}{p_i(x)}$, $m_i(x)$ шукається з виразу $m_i(x) = M_i^{-1}(x)\, mod\, p_i\,(x)$, s – кількість модулів. При цьому для степенів поліномів повинна виконуватися нерівність $\deg N(x) < \deg P(x)$.

Суть одного з методів поліноміального симетричного шифрування в СЗК полягає в тому, що при відновленні полінома за його залишками у сумі (18) множення відбувається не на параметри $m_i(x) = M_i^{-1}(x)\, mod\, p_i\,(x)$, а на довільно вибрані поліноми $k_i(x)$, взаємно прості з $p_i(x)$.

Отже, для генерування ключів обидва абоненти повинні вибрати відомі тільки їм обом системи модулів $p_i(x)$ та відповідні поліноми $k_i(x)$, для яких виконуються такі умови: $1 < deg\, k_i\,(x) < deg\, p_i\,(x)$ та НСД $(k_i(x), p_i(x)) = 1$. Якщо $p_i(x)$ є незвідним поліномом, то друга умова виконується завжди. Відповідно, і відправнику, і отримувачу відомі параметри $M_i(x)$ та $m_i(x)$.

Для шифрування буквенну інформацію необхідно записати у числовій формі. Після цього її необхідно представити у вигляді поліному з коефіцієнтами, які відображають відкритий текст $N(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_0 x^o$, де a_i - послідовність цифрового представлення букв, $i = \overline{0 \dots n}$, (n+1) – довжина повідомлення. Далі блок відкритого тексту $N(x)$ записується в ПСЗК згідно виразу (17). Шифрування відбувається при відновленні числа в позиційну систему числення згідно такого виразу:

$$N'(x) = \left(\sum_{i=1}^{s} b_i(x) M_i(x) k_i(x)\right) mod\, P(x). \quad (19)$$

Знайдений поліном є шифротекстом, який передається по відкритому каналу зв'язку від одного абонента до іншого.

При розшифруванні спочатку обчислюються такі значення:

$$q_i(x) = \left(m_i(x)\left(k_i^{-1}(x)\, mod\, p_i(x)\right)\right) mod\, p_i(x);\ b_i'(x) = N'(x)\, mod\, p_i(x). \quad (20)$$

Для отримання істинних залишків $b_i(x)$ необхідно виконати перетворення згідно співвідношення:

$$b_i(x) = \left(b_i'(x) q_i(x)\right) mod\, p_i(x) = \left(b_i'(x) m_i(x) k_i^{-1}(x)\right) mod\, p_i(x). \quad (21)$$

Відповідно, відновлення полінома $N(x)$, який є відкритим текстом, здійснюється згідно формули (18) або можна використати вираз, який з неї випливає:

$$N(x) = \left(\sum_{i=1}^{s} M_i(x) m_i(x)\left(\left(b_i'(x) m_i(x) k_i^{-1}(x)\right) mod\, p_i(x)\right)\right) mod\, P(x) =$$

$$\left(\sum_{i=1}^{s} M_i(x) m_i(x)\left(\left(b_i'(x) q_i(x)\right) mod\, p_i(x)\right)\right) mod\, P(x). \quad (22)$$

Вперше розроблено новий поліноміальний метод симетричного шифрування на основі КТЗ, основною перевагою якого є те, що відкритий текст $N(x)$ розбивається на блоки – поліноми $N_i(x)$ меншого порядку, ніж вибрані поліноміальні модулі. Ці блоки виступатимуть залишками $b_i(x)$ по вибраних модулях, причому, якщо $deg\, p_i(x) = n$, то $deg\, N_i(x) \le n-1$, тобто $N_i(x) = a_{n-1}x^{n-1} + a_{n-2}x^{n-2} + \cdots + a_0 x^o$. Після вибору параметрів $k_i(x)$ шифрування відбувається згідно з виразом (24). Шифротекстом буде значення $N'(x)$.

Розшифрування відбувається за формулами (21), (22), згідно яких шукаються параметри $q_i(x)$, $b_i(x) = N_i(x)\, mod\, p_i(x) = N_i(x)$, та $b'_i(x)$. Конкатенація коефіцієнтів a_{n-1} поліномів $N_i(x)$ утворює відкритий текст. Слід зазначити, що у випадку, коли потрібне швидке розшифрування, шифротекстом можуть виступати також параметри $b'_i(x)$.

На рис. 7 представлено схему поліноміального симетричного методу шифрування на основі КТЗ. Проведено дослідження криптографічної стійкості запропонованих поліноміальних симетричних криптосистем у СЗК, яка ґрунтується на складності пошуку всіх можливих варіантів параметрів та модулів криптоперетворень. Для криптоаналізу необхідно здійснити повний перебір всіх взаємнопростих поліномів в кільці $Z[x]$ над простим полем Галуа $GF(p)$, де p - просте число. Найбільша складність буде у випадку, якщо поліном $f(x) = a_n x^n + a_{n-1}x^{n-1} + a_{n-2}x^{n-2} + \cdots + a_0 x^0$ є незвідним. Кількість $S_p(n)$

незвідних поліномів $f(x)$ степеня n можна обчислити за формулою: $S_p(n) = \frac{1}{n}\sum_{n|d}\mu(d)p^{n/d}$, де $\mu(d)$ - функція Мебіуса. Вона дорівнює 1, якщо d – дільник степеня n з парною кількістю простих множників; -1, якщо d - дільник степеня n з непарною кількістю простих множників; 0, якщо d містить квадрат простого множника. Відповідно, кількість модулів l не може перевищувати $S_p(n)$.

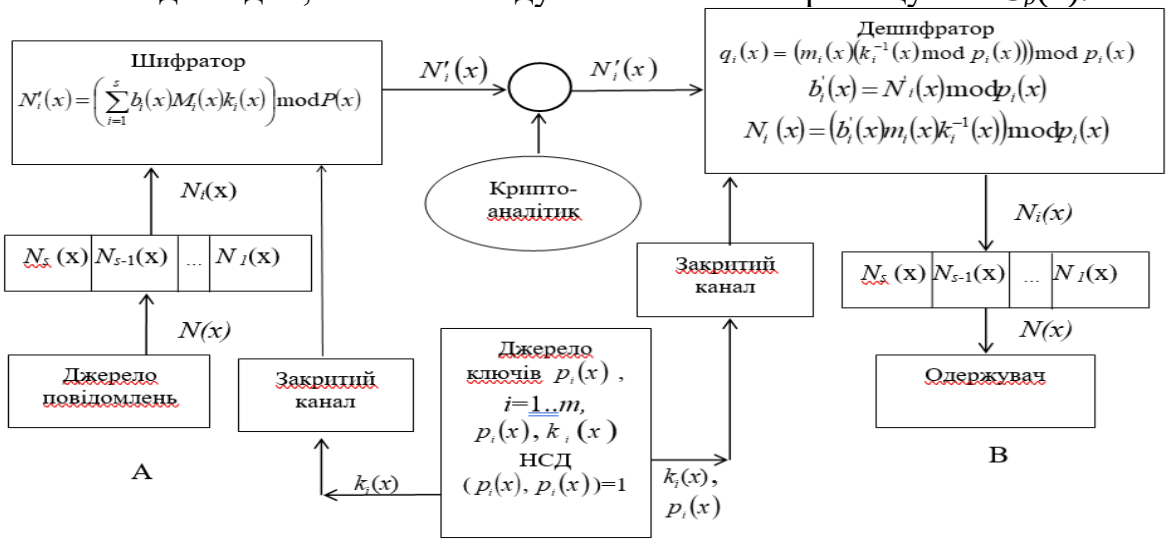


Рис. 7. Поліноміальний симетричний метод шифрування на основі КТЗ

В загальному випадку стійкість запропонованої криптосистеми з l модулів буде визначатися як сумарний час повного перебору всіх незвідних поліномів та складності виконання з кожним обчислень згідно формули:

$$O(n,l) = C^{l}_{S_p(n)} \cdot n^2 \log_2 l = \frac{(S_p(n))!\cdot n^2\cdot\log_2 l}{(S_p(n)-l)!\cdot l!}. \quad (23)$$

На рис. 8 в логарифмічній шкалі з основою 10 представлені графіки залежностей стійкості $O(n,l)$ запропонованого симетричного поліноміального алгоритму шифрування у СЗК від кількості модулів l для степенів полінома n=4, 8 і параметра p=2, p=3, p=5, p=7. З рисунка 8 видно, що усі графіки носять однаковий дзвоноподібний характер. Стійкість істотно зростає при збільшенні степеня та розмірності поля Галуа p і досягає свого максимуму при $l = \frac{S_p(n)}{2}$. Це означає, що криптоаналіз запропонованого алгоритму вимагає комбінаторної складності, яка приводить до NP-повної задачі.

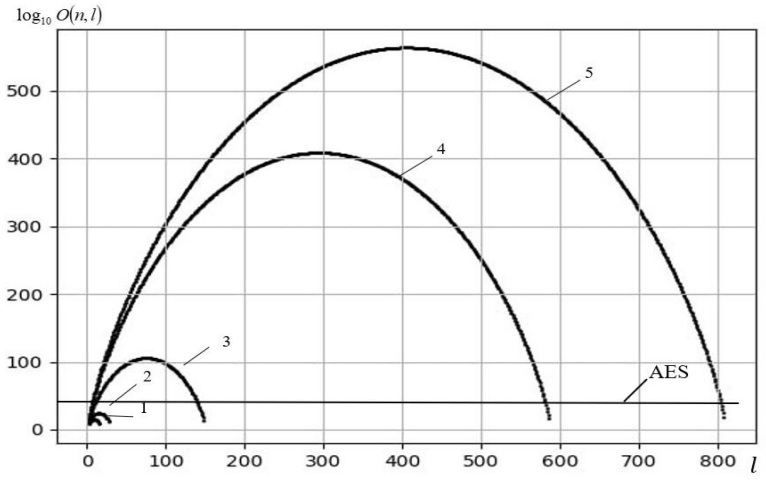


Рис. 8. Графіки залежностей стійкості $O(n,l)$ від кількості модулів l_i степенів полінома n (лінія 1 - p=2, n=4, лінія 2 – p=2, n=8, лінія 3 – p=5, n=4, лінія 4 – p=7, n=4, лінія 5 – p=3, n=8)

Вперше розроблено двоключовий поліноміальний симетричний криптоалгоритм в ПСЗК. Будь-яке повідомлення M запишеться як вектор-рядок

$M = a_1 a_2 \dots a_n$, де a_i - послідовність цифрового представлення букв, $i = \overline{1 \dots n}$, n – кількість літер або довжина повідомлення. Далі вибирається довільний поліном $V(x) = \alpha_r x^r + \alpha_{r-1} x^{r-1} + \dots + \alpha_0$ порядку r в кільці $Z_p[x]$ такий, що в певній точці $x=c$, $c \in Z$, значення $V(\mathrm{c}) = M$. Отже, параметр x, крім полінома $s_i(x)$, виступає в якості ще одного таємного ключа. Слід зауважити, що значення α_0 шукається з виразу $\alpha_0 = M - \alpha_r x^r + \alpha_{r-1} x^{r-1} + \dots + \alpha_1 x$. Для генерації поліноміальних ключів абоненти вибирають відомі тільки їм обом системи модулів $m_i(x)$ та відповідні їм поліноми $s_i(x)$, для яких виконуються такі умови: $1<deg\, s_i\,(x)<deg\, m_i\,(x)$ та НСД($s_i(x)$,$m_i(x)$)=1. Друга умова виконується завжди, коли $m_i(x)$ є незвідним поліномом. Відповідно, і відправнику, і отримувачу відомі параметри $B_i(x)$, $b_i(x)$ і $x=c$. Далі блок відкритого тексту $V(x)$ записується в СЗК згідно виразу:

$$L(x) = \left(\sum_{i=1}^{w} l_i(x) B_i(x) b_i(x)\right) mod\, M\,(x), \qquad (24)$$

де $M(x) = \prod_{i=1}^{w} m_i(x)$, $B_i(x) = \frac{M(x)}{m_i(x)}$, $b_i(x)$ шукається з виразу $b_i(x) = B_i^{-1}(x)\, mod\, m_i\,(x)$, w – кількість модулів. Шифрування відбувається при відновленні числа в позиційну систему числення згідно такого виразу:

$$V'(x) = \left(\sum_{i=1}^{s} l_i(x) B_i(x) s_i\,(x)\right) mod\, M\,(x). \qquad (25)$$

Знайдений поліном є шифротекстом, який передається по відкритому каналі зв'язку від одного абонента до іншого.

При розшифруванні спочатку обчислюються такі параметри:

$$q_i(x) = \left(b_i(x)\left(s_i^{-1}(x)\, mod\, m_i\,(x)\right)\right) mod\, m_i\,(x);\ l_i'(x) = V'(x)\, mod\, m_i\,(x). \qquad (26)$$

Для отримання істинних залишків $l_i(x)$ необхідно виконати перетворення згідно співвідношення:

$$l_i(x) = \left(l_i'(x) q_i(x)\right) mod\, m_i\,(x) = \left(l_i'(x) b_i(x) s_i^{-1}(x)\right) mod\, m_i\,(x). \qquad (27)$$

Відповідно, відновлення полінома $V(x)$, який є відкритим текстом, здійснюється згідно формули (24). Крім цього, можна використати вираз, який з неї випливає:

$$V(x) = \left(\sum_{i=1}^{s} B_i(x) b_i\,(x)\left(\left(l_i'(x) b_i(x) s_i^{-1}(x)\right) mod\, m_i\,(x)\right)\right) mod\, M\,(x) =$$

$$= \left(\sum_{i=1}^{s} B_i(x) b_i(x)\left(\left(l_i'(x) q_i(x)\right) mod\, m_i\,(x)\right)\right) mod\, M\,(x). \qquad (28)$$

Для отримання вхідного повідомлення потрібно знайти значення $V(\mathrm{c})=M$.

Побудовано аналітичний вираз криптографічної стійкості запропонованого симетричного алгоритму шифрування з l модулів, який враховує сумарний час повного перебору всіх незвідних поліномів та визначення коренів рівняння з врахуванням складності виконання кожної операції :

$$O(n,l) = C_{S_p(n)}^{l} \cdot n^4\, log_2\, l = \frac{\left(S_p(n)\right)! \cdot n^4 \cdot log_2 l}{(S_p(n)-l)! \cdot l!}. \qquad (29)$$

На рис. 9, в логарифмічній шкалі з основою 10, представлені криві, які

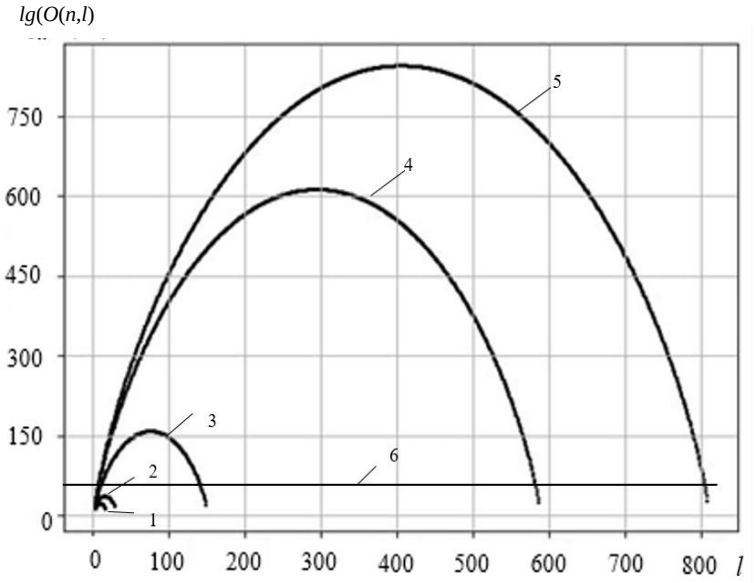


Рис. 9. Графіки залежностей стійкості $O(n,l)$ від кількості модулів l_i степенів полінома n (лінія 1 - p=2, n=4, лінія 2 – p=2, n=8, лінія 3 – p=5, n=4, лінія 4 – p=7, n=4, лінія 5 – p=3, n=8, лінія 6 – стійкість алгоритму шифрування AES

представлені криві, які відображають залежності стійкості запропонованого симетричного поліноміального методу шифрування у скінченних полях від кількості модулів для різних степенів полінома (n=4, 8) та параметрів (p=2, p=3, p=5, p=7). З аналізу рисунка 9 випливає, що стійкість запропонованого симетричного поліноміального алгоритму шифрування значно збільшується при зростанні як степеня полінома n, так і розмірності поля Галуа p.

При певних значеннях n і p, тобто при $l = \frac{S_p(n)}{2}$ спостерігається максимальна стійкість. Це свідчить про те, що атаки на цей алгоритм вимагають значної обчислювальної складності і часто можуть бути формалізовані як NP-повні задачі.

Такий дзвоноподібний характер кривих стійкості може бути пов'язаний з властивостями математичних конструкцій, що лежать в основі алгоритму, і відображає взаємозв'язок між параметрами системи та її стійкістю до атак.

У п’ятому розділі розроблені теоретичні основи симетричного шифрування у цілочисельній та поліноміальній ІСЗК та методологію криптографічного захисту інформації на основі цілочисельної, модифікованої досконалої та поліноміальної СЗК.

Вперше розроблено алгоритм симетричного шифрування у цілочисельній ієрархічній СЗК, основна ідея якого полягає в тому, що на першому рівні вибирається система модулів $p_1, p_2, \ldots, p_l$, які розміщені в порядку зростання. Це забезпечує можливість шифрування блоків відкритого тексту N в діапазоні $[0, P)$, де $P = \prod_{i=1}^{l} p_i$. За формулою (6) обчислюються залишки b_i. Далі для кожного модуля p_i першого рівня вибирається нова система модулів другого рівня: $q_{i1}, q_{i2}, \ldots, q_{il}$, вважаючи для спрощення, що кількість модулів у кожній системі на будь-якому рівні однакова і дорівнює l. Відповідно, обчислюються залишки $b_{ij}=b_i \bmod q_{ij}$.

Далі, в свою чергу, залишки другого рівня з дотриманням відповідних вимог записуються аналогічно в системі модулів третього рівня. Така процедура триває до останнього, k-го рівня.

Отже, кожному залишку r-ого рівня відповідає l систем з l^{r-1} залишками. Таким чином, на $r+1$ рівень передається l^r залишків ($l>1$, $r=1, 2,\ldots, k-1$) і шифротекст складається із l^k чисел, які є залишками останнього рівня ІСЗК. Якщо кількість рівнів дорівнює 1, то має місце звичайне симетричне шифрування у СЗК. Набори модулів відомі для відправника і отримувача.

Як правило, кількість рівнів, визначається умовами конкретної задачі. Такий процес переходу до менших модулів помітно спрощує реалізацію елементарного арифметичного пристрою і скорочує час виконання арифметичних операцій. Слід зазначити, що для задач криптографії кількості модулів на різних рівнях доцільно вибирати різними. Це значно підвищить складність криптоаналізу такої системи шифрування, хоча і ускладнить апаратну реалізацію.

Розшифрування в ІСЗК відбувається в зворотному порядку. Весь шифротекст розбивається на блоки, кількість яких становить l^k. Далі, застосовуючи один із методів відновлення числа із його залишків, наприклад, КТЗ (7), отримуються залишки вищого рівня. На кожному з рівнів в процесі розшифрування кількість залишків зменшується в l разів.

Проведено дослідження криптостійкості розробленого алгоритму з використанням ІСЗК, в якому враховано кількість рівнів k та зміну розрядності модулів на кожному з них. Загальна часова складність криптоаналізу по всіх рівнях обчислюється згідно формули:

$$O(n,k,l)=\prod_k\left(\frac{2^{n-k+1}}{n-k+1}\right)^{l^k}(n-k+1)^2 \qquad (30)$$

На рис. 10 представлений графік, який відображає логарифмічну залежність складності криптоаналізу від розрядності n, кількості модулів $l=3$ та рівнів k.

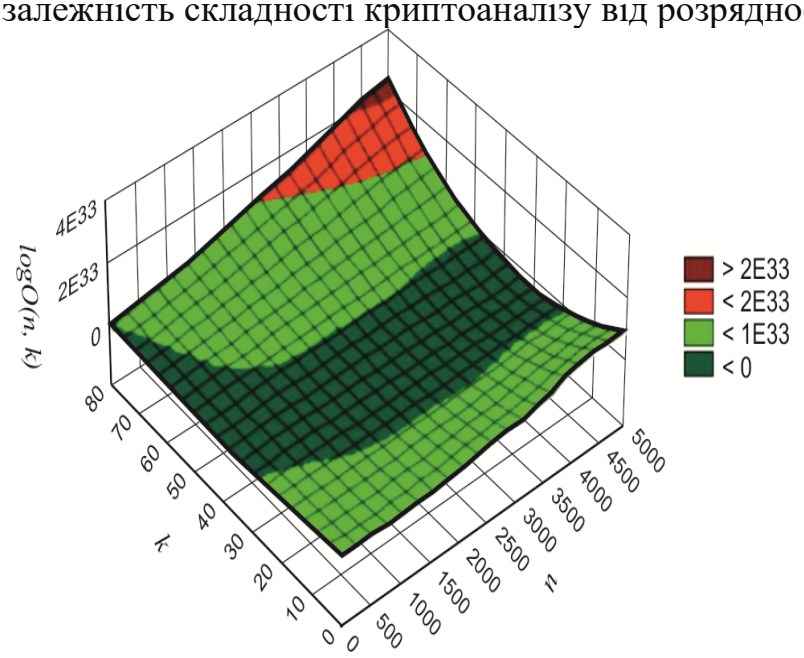


Рис. 10. Залежність логарифму складності криптоаналізу від розрядності n, кількості модулів l та рівнів k

Здійснено порівняння криптостійкості запропонованого криптоалгоритму з AES-256. Рівність $\prod_k\left(\frac{2^{n-k+1}}{n-k+1}\right)^{l^k}(n-k+1)^2=2^{255}$ дає змогу знайти розрядності, кількості рівнів та кількості модулів СЗК, які забезпечують таку ж стійкість, як і алгоритм AES-256. Після логарифмування за основою 2 та виконання елементарних арифметичних перетворень, можна одержати:

$$\sum_k(l^k(n-k+1)+(2-l^k)log_2(n-k+1))=255. \qquad (31)$$

Спостерігається, що зі зростанням цих параметрів складність криптоаналізу збільшується.

Результати експериментальних досліджень вказують, що стійкість запропонованої симетричної криптосистеми, яка базується на використанні ІСЗК зростає із збільшенням кількості рівнів та розрядності вхідних параметрів.

Розв'язок рівняння (31) відносно n для різних значень l та k, одержимо можливі значення n. Зокрема, для 8-бітних модулів при l=2 потрібно 6 рівнів, щоб перевищити стійкість AES-256. Збільшення кількості модулів приводить до зменшення рівнів шифрування (якщо l=3, то k=4; якщо l=4-6, то k=3).

Для 12-бітних модулів при l=2 стійкість запропонованого криптоалгоритму перевищує стійкість AES-256 на п'ятому рівні. При збільшенні кількості модулів (l=3-5) умова перевищення стійкості AES-256 виконується на третьому рівні, а при l=6 – на другому. Таким чином, варіація розрядності модулів, їх кількості та рівнів ієрархії дозволяє досягнути відповідної криптографічної стійкості залежно від конкретної задачі. Встановлено, що при n=8, l=5, k =4 і при n=12, l=4, k =4 спостерігається підвищення криптостійкості приблизно в 9 разів.

Вперше розроблено симетричний криптоалгоритм в ієрархічній поліноміальній системі залишкових класів (ІПСЗК), в якому на кожному із k рівнів ($k \geq 1$), кількість яких обумовлюється обома абонентами, знаходять залишки по відповідній системі модулів, які передають на наступний рівень. Кожному залишку r-ого рівня відповідає l систем з l^{r-1} залишками. Таким чином на r + 1 рівень передається l^r залишків (l >1, r = 1, 2,…, k – 1). Отже, шифротекст складається із l^k поліномів, які є залишками останнього рівня ІПСЗК. Набори модулів відомі для відправника і отримувача.

Для шифрування буквенна інформація записується у відкритого тексту $N(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_0 x^o$, де a_i - послідовність цифрового представлення букв, $i = \overline{0 \ldots n}$, ($n$+1) – довжина повідомлення. Далі блок відкритого тексту $N(x)$ записується в СЗК згідно виразу (23). Шифротекстом у розробленому ІПСЗК є набір залишків останнього рівня кожного блоку $N(x)$. Відновлення вхідного повідомлення (поліному) відбувається у зворотньому порядку, починаючи з k-го рівня до першого на основі формули (12). В результаті проведених обчислень k-го рівня отримуються значення, які є залишками (поліномами) k-1 рівня. На кожному з рівнів в процесі розшифрування кількість залишків поліномів зменшується в l разів.

Побудовано аналітичні вирази стійкості запропонованої криптосистеми з l модулів та k рівнів, яка визначається як добуток часу повного перебору всіх незвідних поліномів та складності виконання з кожним обчислень згідно формули:

$$O(n,l) = \prod_{k=1}^{n-k+1} C_{S_p(n-k+1)}^{l^k} \cdot (n-k+1)^2 log_2 l^k = \prod_{k=1}^{n-k+1} \frac{\left(S_p(n-k+1)\right)! \cdot (n-k+1)^2 \cdot (k)\, log_2 l}{\left(S_p(n-k+1)-l^k\right)! \cdot l^k!} \quad (32)$$

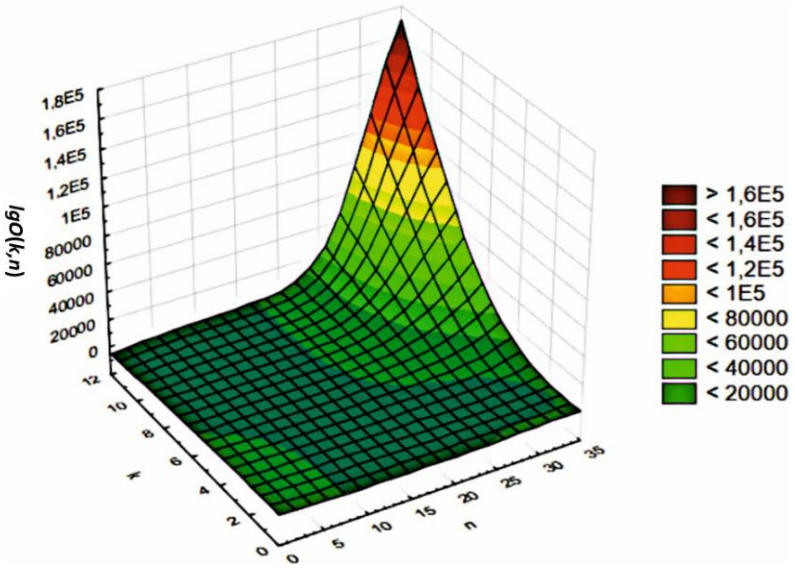


Рис. 11. Стійкість криптосистеми в ІПСЗК в залежності від порядку полінома n і кількості модулів l

На рис. 11 представ-лено залежність стійкості до криптоаналітичних атак від кількості ієрархічних рівнів k та ступеня полінома n при l=3.

З аналізу поверхні можна зробити висновок, що стійкість криптосистеми в ІПСЗК значною мірою залежить від вибору параметрів n і l. Збільшення порядку полінома та кількості модулів сприяє зростанню криптографічної безпеки, і для забезпечення максимальної захищеності системи слід обирати великі значення обох параметрів. Результати чисельного експерименту показують, що збільшення кількості модулів на один при вхідних поліномах степеня n = 32 призводить до зростання стійкості запропонованого симетричного ієрархічного поліноміального криптографічного алгоритму в $4{,}97066*10^{156}$ разів, а при степенях поліномів n = 32, p = 2, l=3 на третьому ієрархічному рівні спостерігається підвищення стійкості криптоалгоритму в 3,34 рази в порівнянні з AES-256.

Вперше розроблена методологія криптографічного захисту інформаційних потоків на основі використання симетричних та асиметричних криптосистем в цілочисельній, модифікованій досконалій та поліноміальній СЗК (її структурно-аналітичне відображення представлено на рис. 12 складається з восьми етапів: 1) процес формування множини блоків відкритого тексту (N, $N(x)$) для цілочисельних і поліноміальних криптографічних систем; 2) Встановлення вимог щодо основних параметрів цілочисельних та поліноміальних симетричних та асиметричних криптографічних систем та захищеності інформації; 3) вибір запропонованих цілочисельних та поліноміальних криптосистем; 4) створення множини базових операцій; 5) формування набору методів виконання операцій; 6) вибір цілочисельної та поліноміальної форм СЗК; 7) програмна реалізація цілочисельних та поліноміальних симетричних та асиметричних криптосистем; 8) програмна реалізація цілочисельних та поліноміальних криптосистем.

Ця методологія забезпечує комплексний підхід до розробки, реалізації та оптимізації запропонованих симетричних та асиметричних цілочисельних, поліноміальних криптосистем на основі використання СЗК, векторно-модульних методів пошуку залишків, модулярного множення та експоненціювання, методу невизначених коефіцієнтів для пошуку оберненого полінома в поліноміальній системі числення, методів відновлення полінома за його залишками на основі додавання добутку модулів, що дає змогу досягти високого рівня захисту інформації при мінімальних витратах на обчислення.

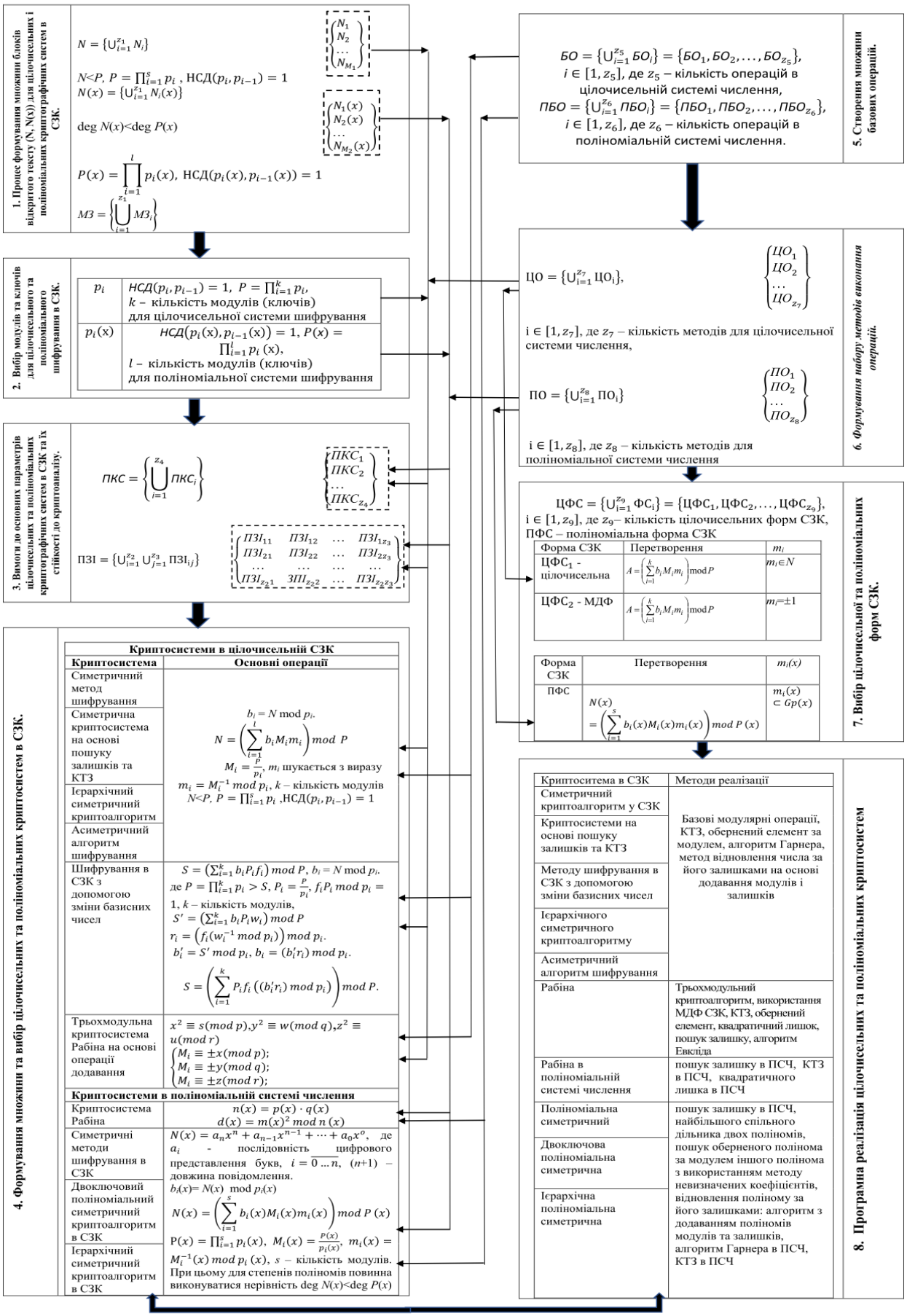


Рис. 12. Структурно-аналітичне представлення методології криптографічного захисту інформації на основі цілочисельної, модифікованої досконалої та ПСЗК

У шостому розділі наведена реалізація запропонованих симетричних та асиметричних цілочисельних, поліноміальних криптосистем на основі використання СЗК.

На рис. 13 представлено діаграму компонентів розробленої програмної системи реалізації криптоалгоритмів в СЗК із врахуванням її практичної імплементації в прикладні інформаційно-комунікаційні системи.

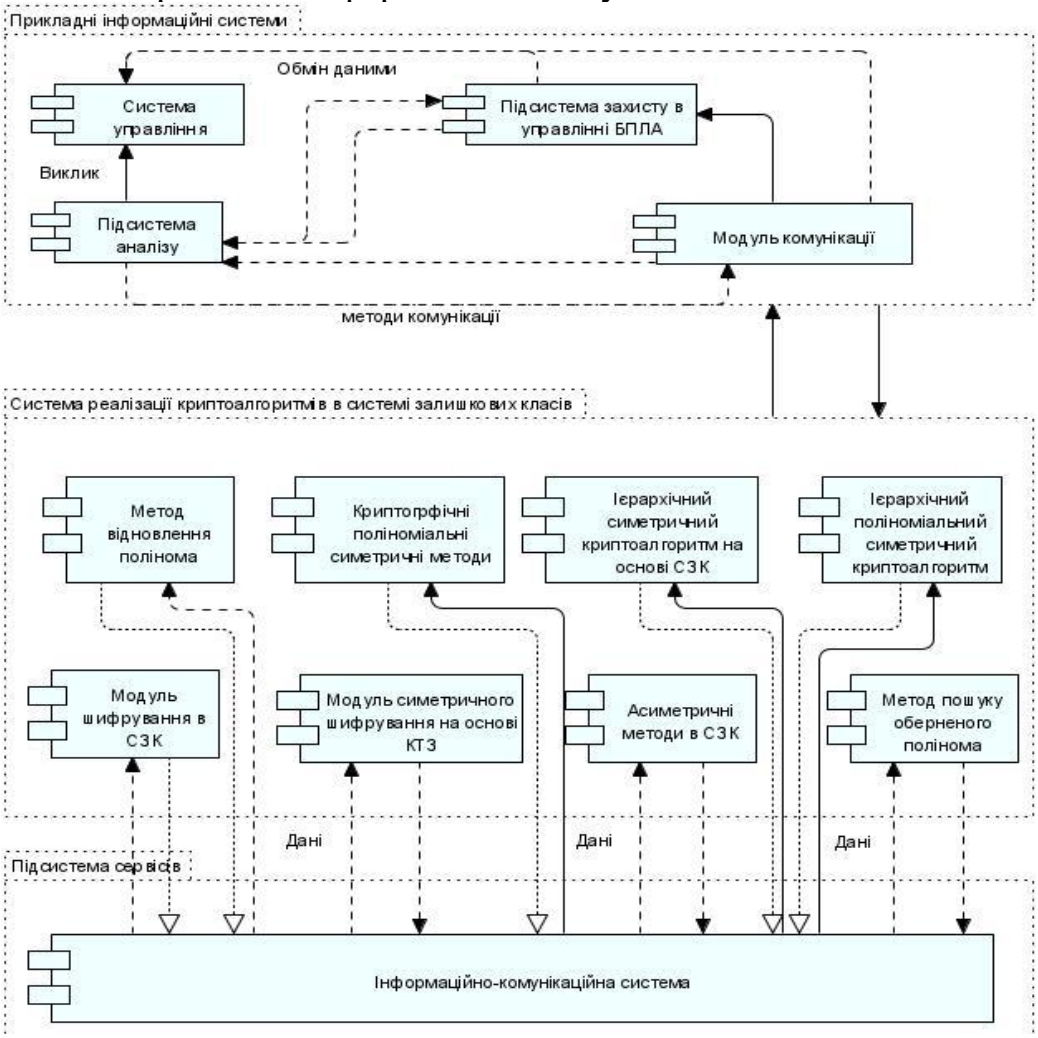


Рис. 13. Діаграма компонентів програмної системи реалізації криптоалгоритмів в СЗК

Програма реалізована за допомогою мови програмування Python. Програма використовує додаткові модулі (рис. 14), а саме: pycrypto, для порівняння швидкодії з AES; tkinter, для побудови GUI інтерфейсу; xlsxwriter, для збереження результатів порівняння швидкодії в таблиці Microsoft Office Excel.

У процесі реалізації програмної системи були створені два основних інтерфейси для взаємодії з користувачем: графічний (GUI) та командний (CLI). Такий підхід забезпечує гнучкість у використанні програмного забезпечення, дозволяючи користувачам обирати найбільш зручний спосіб взаємодії залежно від конкретних завдань та умов експлуатації.

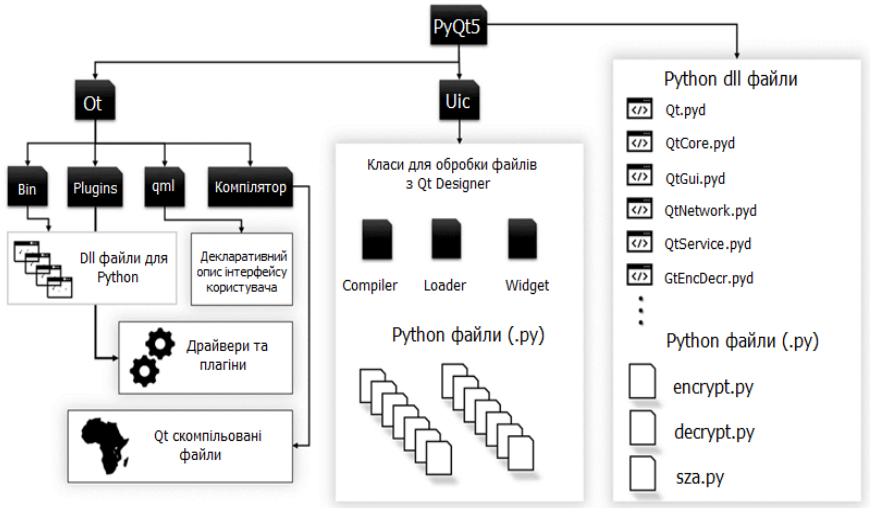


Рис. 14. Структура засобів програмної реалізації з використанням PyQt

З точки зору криптографічних алгоритмів, програмна система підтримує як симетричні, так і асиметричні методи шифрування.

Структурна організація програмного коду представлена у вигляді об'єктно-орієнтованої моделі, де основні компоненти реалізовані у формі класів.

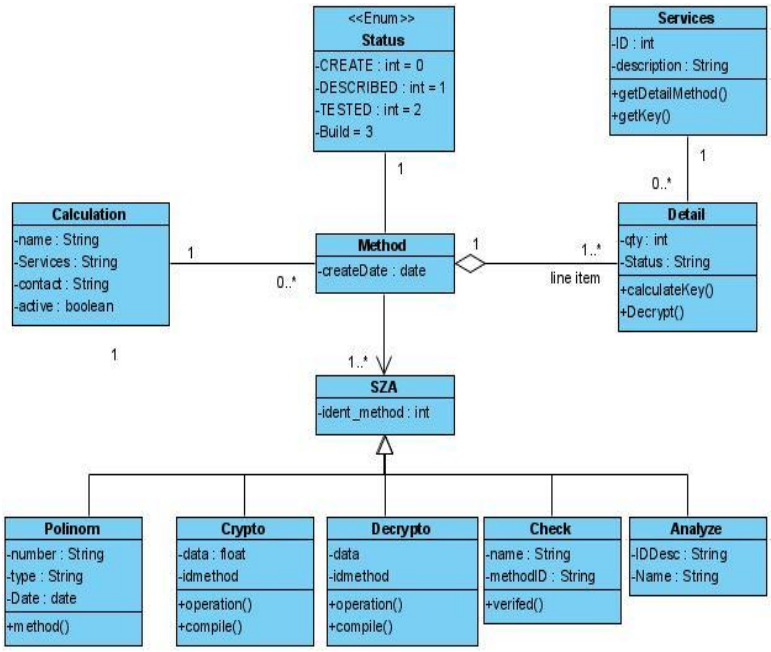


Рис. 15. Діаграма класів системи

Взаємозв'язки між цими класами, їхні функціональні можливості та принципи взаємодії між собою зображені на діаграмі основних реалізованих класів (рис. 15). Така структурна схема наочно демонструє логіку побудови програмної системи та сприяє подальшому вдосконаленню її функціональності. Діаграма комунікації системи демонструє взаємодію основних компонентів під час виконання криптографічних операцій (рис. 16).Вона складається з кількох рівнів: системного, представлення, управління та моделі.

Системний рівень представлений зовнішньою інформаційною системою, яка ініціює запити на виконання криптографічних операцій. Взаємодія розпочинається з ініціалізації методу, що відбувається через інтерфейс користувача (System UI), який приймає запит та передає його до керуючого модуля (Control). Контролер, у свою чергу, викликає відповідні методи криптографічного алгоритму, що відповідає за виконання операцій шифрування або розшифрування.

Для успішного виконання операцій відбувається збір та підготовка необхідних даних. Інтерфейс користувача передає попередню інформацію до контролера, де вона перевіряється на коректність та узгоджується з вимогами системи. Контролер здійснює обробку вхідних даних та передає їх до моделі, яка

включає кілька модулів: профіль користувача, документацію, вимоги, базу даних, математичний опис алгоритмів та фінальне криптографічне рішення. На цьому етапі інформація перевіряється, компілюється та формується у вигляді відповідного математичного представлення.

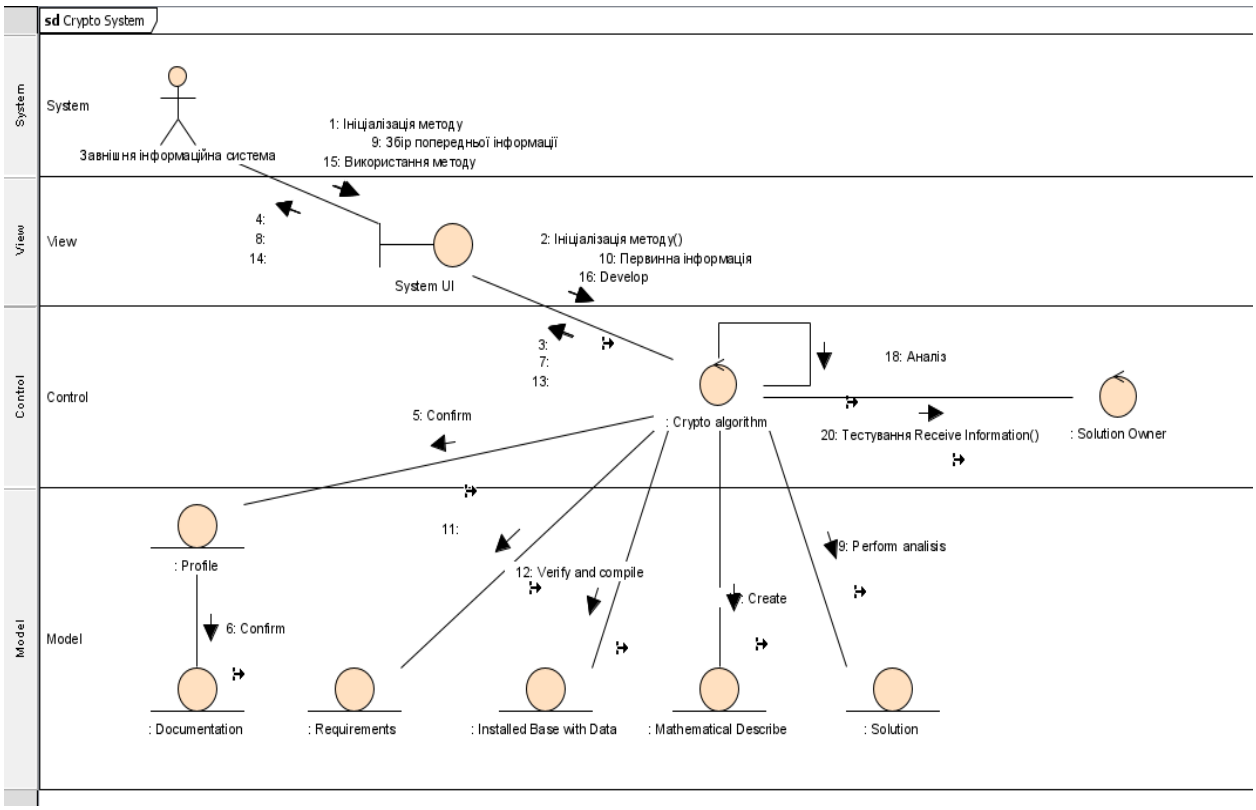


Рис. 16. Діаграма комунікації системи

Після цього здійснюється безпосередня криптографічна обробка, де контролер координує взаємодію між математичним модулем та модулем рішення. Відбувається розрахунок криптографічного алгоритму, створення математичної моделі та її верифікація. Система аналізує отримані результати, проводить їх тестування та перевірку правильності виконання.

На завершальному етапі остаточне криптографічне рішення передається зовнішній інформаційній системі або користувачеві через інтерфейс для подальшого використання. Завдяки чіткій структурі взаємодії між компонентами, система забезпечує модульність, ефективну обробку запитів та високу продуктивність криптографічних алгоритмів.

У додатках наведено лістинг програмних модулів для реалізації розглянутих методів та алгоритмів. Подані документи про використання результатів дисертаційної роботи.

ВИСНОВКИ

У дисертаційній роботі вирішено актуальну науково-прикладну проблему, яка полягає у підвищенні ефективності захисту інформаційних потоків на основі заміни в алгоритмах шифрування операції множення операцією додавання, використання цілочисельної, МДФ, поліноміальної та ієрархічної СЗК для

розробки нових криптографічних алгоритмів. При цьому отримано такі основні теоретичні й практичні результати та наукові висновки:

1. Проведено аналіз існуючих симетричних та асиметричних криптосистем, результати якого засвідчили їх обмеження щодо швидкодії, масштабованості та стійкості до криптоаналітичних атак, включно з квантовими. Обґрунтовано доцільність використання цілочисельної та поліноміальної систем залишкових класів, а також їх модифікацій для підвищення швидкодії, криптостійкості та потенціалу криптоалгоритмів. Результати проведеного аналізу дали можливість визначити завдання дисертаційного дослідження щодо розробки методів та засобів криптографічного захисту інформації на основі системи залишкових класів.

2. Розроблено та вдосконалено алгоритмічне забезпечення для асиметричних криптосистем Ель-Гамаля та Рабіна шляхом використання векторно-модульного методу модулярного множення та експоненціювання у системі залишкових класів, замінюючи операцію множення операцією додавання. Запропоновані підходи забезпечили зменшення часової складності криптографічних перетворень відповідно у 8 та 128 разів при розрядності вхідних параметрів 256 біт без зниження рівня криптостійкості.

3. Вперше розроблено симетричний криптоалгоритм у СЗК та МДФ СЗК, в якому шифрування реалізується шляхом представлення повідомлення у вигляді системи залишків. Розшифровування виконується на основі КТЗ. Встановлено умови (розрядність, кількість модулів), за яких алгоритм забезпечує вищий рівень стійкості в порівнянні з AES-256. Зокрема, при кількості модулів l=5, 6, 7, 8 з відповідними розрядностями k=139, 115, 98, 85 біт стійкість підвищується вдвічі.

4. Розроблено метод симетричного шифрування на основі КТЗ, в якому блок відкритого тексту розбито на підблоки (залишки), що менші за відповідні модулі. Відновлене із залишків десяткове число виступає шифротекстом. Розшифрування відбувається на основі пошуку залишків шифротексту за відповідними модулями. Це дозволило підвищити криптографічну стійкість до криптоаналітичних атак у 3 рази при кількості модулів k=5 та їх розрядності l=150 біт в порівнянні з AES-256 і пришвидшити процес розшифрування.

5. Розроблено метод пошуку оберненого полінома в кільці Z[x] на основі методу невизначених коефіцієнтів, що дозволило уникнути обчислення НСД двох поліномів і забезпечити підвищення швидкодії до 4,5 разів для степеня полінома 256 у порівнянні з класичним алгоритмом Евкліда.

6. Удосконалено метод відновлення полінома за його залишками в кільці Z[x], який не вимагає пошуку оберненого полінома та дозволяє повне розпаралелення процесу обчислень. Встановлено, що для кількості модулів 10 та степеня поліному 256 запропонований підхід підвищує швидкодію у 641 раз в порівнянні з алгоритмом Гарнера.

7. Вперше розроблено високопродуктивні симетричні та асиметричні криптоалгоритми на основі СЗК та МДФ СЗК шляхом довільної заміни базисних чисел в процесі шифрування на попарно взаємнопрості з відповідними модулями додаткові ключі, які дозволяють підвищити рівень стійкості до

криптоаналітичних атак в 2 рази при кількості модулів k=5 та їх розрядності l=74 біти.

8. Вперше розроблено симетричний криптоалгоритм на основі поліноміальної СЗК, стійкість якого базується на комбінаційній складності криптоаналізу, що призводить до NP-повної задачі. Побудовано залежність криптостійкості від розмірності поля Галуа, степеня полінома та кількості модулів.

9. Вперше розроблено симетричний криптоалгоритм на основі ієрархічної СЗК, який має ступінчасту структуру з розподілом модулів по рівнях. Показано, що така архітектура підвищує гнучкість алгоритму та забезпечує співставний або вищий криптозахист в порівнянні з AES-256. Встановлено, що при n=8, l=5, k=4 і при n=12, l=4, k=4 спостерігається підвищення криптостійкості до криптоаналітичних атак приблизно в 9 разів.

10. Вперше розроблено симетричний криптоалгоритм на основі ІПСЗК, який поєднує властивості ПСЗК та багаторівневої структури. Це дає змогу адаптивно керувати параметрами шифрування для досягнення заданих рівнів захисту та підвищити стійкість криптоалгоритму в 3,34 рази при степенях поліномів n = 32, p = 2, l=3 на третьому ієрархічному рівні в порівнянні з AES-256 та збільшити його швидкодію.

11. Вперше розроблено методологію криптографічного захисту інформації в системі залишкових класів, яка забезпечує комплексний підхід до розробки, реалізації та оптимізації запропонованих симетричних та асиметричних цілочисельних криптосистем, криптосистем на основі використання ПСЗК, векторно-модульних методів пошуку залишків, модулярного множення та експоненціювання, методу невизначених коефіцієнтів, методів відновлення поліному за його залишками на основі додавання добутку модулів або їх залишків, 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

12. Здійснена програмна реалізація запропонованих симетричних та асиметричних цілочисельних і поліноміальних криптосистем на основі використання СЗК, яка емпірично підтвердила переваги запропонованих методів і може бути підґрунтям для їх впровадження у сучасні кіберфізичні системи.

ОСНОВНІ ПУБЛІКАЦІЇ ЗДОБУВАЧА ЗА ТЕМОЮ ДИСЕРТАЦІЇ

Статті:

1. Yakymenko I., Kasianchuk M., Martyniuk O., Martyniuk S. A Symmetric Cryptoalgorithm Based on a Hierarchical Residue Number System. *International Journal of Computing,* 2025. 24(1), pp. 92-101. https://doi.org/10.47839/ijc.24.1.3880 (Scopus)

2. Yakymenko I., Karpinski M., Shevchuk R., Kasianchuk M. Symmetric Encryption Algorithms in a Polynomial Residue Number System. *Journal of Applied Mathematics*., 2024, pp. 1-12. DOI:10.1155/2024/4894415 (Scopus).

3. Nykolaychuk Ya., Yakymenko I., Vozna N., Kasianchuk M. Residue Number System Asymmetric Cryptoalgorithms. *Cybernetics and Systems Analysis*. 2022, Vol. 58, No. 4, P.611-618. http://jnas.nbuv.gov.ua/article/UJRN-0001335526. https://doi.org/10.1007/s10559-022-00494-7. (Scopus).

4. Shevchuk R., Yakymenko I., Karpinski M., Shylinska I., Kasianchuk M. Finding the inverse of a polynomial modulo in the ring Z[x] based on the method of undetermined coefficients. *Computer Science*. vol. 25. no. 2. 2024. pp.1-14. DOI:10.7494/csci.2024.25.2.5740 (Scopus).

5. M. M. Kasianchuk, I. Z. Yakymenko, Ya. M. Nykolaychuk Symmetric Cryptoalgorithms in the Residue Number System. *Cybernetics and Systems Analysis*, 2021, Vol 57, Issue 2, p.184-189. https://doi.org/10.1007/s10559-021-00358-6

6. Nykolaychuk Ya., Kasianchuk M., Yakymenko I. Theoretical Foundations of the Modified Perfect form of Residue Number System. *Cybernetics and Systems Analysis*. 2016. Vol. 52, №2. pp. 219-223 (Scopus). DOI: 10.1007/s10559-016-9817-2

7. Nykolaychuk Ya., Kasianchuk M., Yakymenko I. Theoretical Foundations for the Analytical Computation of Coefficients of Basic Numbers of Krestenson's Transformation. *Cybernetics and Systems Analysis*. 2014. Vol. 50, № 5. pp. 649-654 (Scopus). DOI: 10.1007/s10559-014-9654-0

8. Iakymenko I., Kasianchuk M., Kinakh I., Karpinski M. Construction of distributed thermal or piezoelectric sensor based on residue systems. Przeglad Elektrotechniczny. 2017. №1. pp. 290-294 (Scopus). DOI: 10.15199/48.2017.01.69

9. Kasianchuk M., Yakymenko I., Yatskiv S., Gomotiuk O., Bilovus L. The Method of Joint Execution of the Basic Operations of the Rabin Cryptosystem. *CEUR Workshop Proceedings*, 2023, 3373, pp. 425–436. https://ceur-ws.org/Vol-3373/paper28.pdf (Scopus).

10. Kasianchuk M., Yakymenko I., Yatskiv V., Karpinski M., Yatskiv S. Method of Multi-Bit Numbers Multiplication in Residue Number System for Asymmetric Cryptosystems. *CEUR Workshop Proceedings*, 2022, 3156, pp. 365–377. https://ceur-ws.org/Vol-3156/paper27.pdf . (Scopus).

11. Stanislaw Zawislak, Mykhailo Kasianchuk, Igor Iakymenko, Daniel Jancarczyk Methods of Crypto-stable Symmetric Encryption in the Residual Number System. *Procedia Computer Science*. Volume 207, 2022, pp. 128-137. DOI:10.1016/j.procs.2022.09.045 (Scopus)

12. Yakymenko I., Kasianchuk M., Shylinska I. A Method for Polynomial Recovery from its Resudues Based on Addition in Z[x] Ring. *Informatics and Mathematical Methods in Simulation* Vol.14 (2024), No. 4, pp. 305-313. DOI:10.15276/imms.v14.no4.305.

13. Якименко І. З., Касянчук М. М., Івасьєв С. В. Криптосистема Рабіна на основі операції додавання. *Математичне та комп'ютерне моделювання*. Серія: Технічні науки № 19, 2019. 145–150 с. DOI: https://doi.org/10.32626/2308-5916.2019-19.145-150

14. Якименко І. З. Удосконалення реалізації криптоалгоритму Ель-Гамаля на основі системи залишкових класів. *Інформатика та математичні методи в моделюванні*, 2018, 8, № 1. С. 69-77. DOI: 10.15276/imms.v8.no1.69

15. Касянчук М.М., Якименко І.З., Івасьєв С.В., Мандебура Н.М., Неміш В.М. Дослідження часових характеристик апаратної реалізації методів пошуку оберненого елемента за модулем. *Вісник Хмельницького національного університету. Технічні науки*. 2017. №6 (255). С. 191-197.

16. Касянчук М.М., Якименко І.З., Івасьєв С.В., Момотюк О.В. Експериментальне дослідження програмної реалізації методів пошуку оберненого елемента за модулем. *Інформатика та математичні методи в моделюванні*. 2017. Т.7, №3. С. 178–186.

17. Касянчук М.М., Якименко І.З., Івасьєв С.В., Маслияк Б.О. Метод розширення набору модулів модифікованої досконалої форми системи залишкових класів. *Математичне та комп'ютерне моделювання: Технічні науки.* 2017. В.15. С.73-78.

18. Касянчук М.М., Якименко І.З., Паздрій І.Р., Івасьєв С.В. Експериментальне дослідження програмної реалізації сумісного виконання алгоритму Евкліда та множення. *Інформатика та математичні методи в моделюванні.* 2017. Т.7, №1-2. С. 29–36.

19. Касянчук М.М., Якименко І.З., Дубчак Л.О., Рендзеняк Н.А., Мандебура Н.М. Модифікований метод шифрування Рабіна з використанням різних форм системи залишкових класів. *Вісник Хмельницького національного університету. Технічні науки.* 2017. №1(245). С. 127-131.

20. Касянчук М.М., Якименко І.З., Долинюк Т.М., Рендзеняк Н.А. Експериментальне дослідження програмної реалізації методів модулярного експоненціювання. *Інформатика та математичні методи в моделюванні*. 2015. Т.5, №4. С. 376–382.

21. Івасьєв С.В., Якименко І.З., Касянчук М.М. Вдосконалений алгоритм пошуку символів Якобі. *Оптико-електронні інформаційно-енергетичні технології*. 2015. Том 29, № 1. С. 45-50.

22. Касянчук М.М., Якименко І.З., Паздрій І.Р., Николайчук Я.М. Аналітичний пошук модулів досконалої форми системи залишкових класів та їх застосування в китайській теоремі про залишки. *Вісник Хмельницького національного університету. Технічні науки*. 2015. №1(221). С. 170-176.

23. Николайчук Я. М., Касянчук М.М., Якименко І.З., Івасьєв С.В. Ефективний метод модулярного множення в теоретико-числовому базисі Рademахера–Крестенсона. *Вісник Національного університету «Львівська політехніка». Комп'ютерні системи та мережі*. 2014. № 806. С. 195-199.

24. Якименко І.З., Касянчук М.М., Тимошенко Л.М., Гребень Н.Є. Алгоритми опрацювання інформаційних потоків в комп'ютерних системах. *Інформатика та математичні методи в моделюванні*. 2013. Т.3, №3. С. 266–274.

25. Якименко І.З., Касянчук М.М., Кімак В.Л. Теоретичні основи зменшення часової та апаратної складності систем захисту інформаційних потоків на основі еліптичних кривих з використанням теоретико-числового базису Рademахера-Крестенсона. *Вісник Національного університету «Львівська політехніка» «Комп'ютерні системи та мережі».* 2012. №745. С. 190–197.

26. Николайчук Я.М., Касянчук М.М., Якименко І.З., Долинюк Т.М. Теоретичні основи виконання модулярних операцій множення та експоненціювання в теоретико–числовому базисі Крестенсона–Рademахера. *Інформатика та математичні методи в моделюванні*. 2011. №2. С. 123–130.

27. Zadiraka V., Yakymenko I., Kasianchuk M., Ivasiev S. Theoretical and numerical Krestenson's basis and its application to problems of cryptographic protection and factorization of multidigit numbers, *Computer technologies in information security: collective monograph*, By edited V.Zadiraka, Ya.Nykolaichuk, Ternopil: Kart-blansh, 2015. P. 216-260. Ch. 5.

28. Yakymenko I., Kasyanchuk M., Volynskyi O. Fundamental application-oriented tasks in Krestenson base, *Methods of effective protection of information flows: collective monograph*, By edited V.Zadiraka, Ya.Nykolaichuk, Ternopil: Terno-graf, 2014. P. 149-185. Ch.6.

29. Kasianchuk M., Yakymenko I., Ivasiev S. High-Productivity Methods of Finding Residues Multidigital Numbers By Modulo, in *Inżynier XXI Wieku: VI Międzynarodowa Konferencja studentow oraz doktorantow, 02.12.2016: monografia*, 1st ed., Bielsko – Biała (Poland): Akademia Techniczno-Humanistyczna w Bielsku-Białej. 2016. pp. 123-130. Chapter in monograph.

30. Якименко І. Алгоритми побудови модифікованої досконалої форми системи залишкових класів. *Спеціалізовані комп'ютерні технології в інформатиці: Колективна монографія*. Під ред. В.Задіраки, Я.Николайчука. Тернопіль: Бескиди, 2017. С. 580-604.

31. Kasianchuk M., Yakymenko I., Ivasiev S. Theoretical foundations for creating five modular modified perfect form of the system of residual classes, in *Inżynier XXI Wieku: VII Międzynarodowa Konferencja studentow oraz doktorantow, 08.12.2017: monografia*, 1st ed., Vol.2., Bielsko – Biała (Poland): Akademia Techniczno-Humanistyczna w Bielsku-Białej, 2017, pp. 123-130. Chapter in monograph.

Матеріали конференцій:

32. Yakymenko I., Kasianchuk M., Martyniuk O., Martyniuk S., Martyniuk A., Yakymenko Y. A Symmetric Cryptoalgorithm in a Polynomial Hierarchical Residual Number System. *Proceedings International Conference on Advanced Computer Information Technologies*, ACIT., 2025, pp. 501-504. DOI: 10.1109/ACIT65614.2025.11185808

33. Yakymenko I., Martyniuk O., Martyniuk S., Yakymenko Y., Kasianchuk M. Hierarchical Encryption in a Residual Number System. *Proceedings International Conference on Advanced Computer Information Technologies*, ACIT., 2024, pp. 496–499 (Scopus). DOI: 10.1109/ACIT62333.2024.10712567

34. Shevchuk R., Yakymenko I., Kasianchuk M. Encryption Using Residue Number System: Research Trends and Future Challenges. *Proceedings International Conference on Advanced Computer Information Technologies*, ACIT2024, 2024, pp. 552–559 (Scopus). DOI: 10.1109/ACIT62333.2024.10712566

35. Shevchuk R., Karpinski M., Kasianchuk Yakymenko I., Melnyk A., Tykhyi R. Software for Improve the Security of Kubernetes-based CI/CD Pipeline. *Proceedings International Conference on Advanced Computer Information*

Technologies, ACIT2023, 2023, pp. 420–425. (Scopus). DOI: 10.1109/ACIT58437.2023.10275654

36. Yakymenko I., Kasianchuk M., Shylinska I., Shevchuk R., Yatskiv V., Karpinski M. Polynomial Rabin Cryptosystem Based on the Operation of Addition. *12th International Conference on Advanced Computer Information Technologies*, ACIT 2022, 2022, pp. 345–350. DOI:10.1109/ACIT54803.2022.9913089 (Scopus).

37. Yakymenko I., Kasianchuk M., Yatskiv V., Shevchuk R., Koval V., Yatskiv S. Sustainability and Time Complexity Estimation of Cryptographic Algorithms Main Operations on Elliptic Curves. *2021 11th International Conference on Advanced Computer Information Technologies (ACIT)*. pp. 494-498 (Scopus). DOI: 10.1109/ACIT52158.2021.9548534

38. Mykhailo Kasianchuk, Ihor Yakymenko, Vasyl Yatskiv, Stepan Ivasiev, Andriy Sverstiuk. Same Bit-Size Moduli Formation of Residue Number System for Application in Asymmetric Cryptography. *IntelITSIS 2021*. pp. 301-308.

39. Yakymenko I., Shylinska I., Kasianchuk M., Bilovus L., Gomotiuk O. Algorithmic Support for Rabin Three-Modular Cryptosystem Based on the Operation of Addition. *IEEE 15th International Conference on Computer Sciences and Information Technologies (CSIT)*. 2020. pp. 328-331 (Scopus).

40. Kasianchuk M., Yakymenko I., Karpinski M., Shevchuk R., Karpinskyi V., Shylinska I. Theoretical Bases for Reducing the Time Complexity of the Rabin Cryptosystem. *Conference on Computer Science and Information Technologies*. 2020. pp. 628-639. (Scopus). DOI: 10.1007/978-3-030-63270-0_43

41. Ivasiev S., Kasyanchuk M., Yakymenko I., Gomotiuk O., Shylinska I., Bilovus L. Algorithmic support for Rabin cryptosystem implementation based on addition.*10th International Conference on Advanced Computer Information Technologies (ACIT)*. 2020. pp. 779-782. (Scopus). DOI: 10.1109/ACIT49673.2020.9208923

42. Yakymenko I., Kasianchuk M., Ivasiev S., Shevchuk R., Batko Y., Vasylkiv V. Method for Determining Prime and Relatively Prime Numbers of 2^n+k Type Based on the Periodicity Property. *10th International Conference on Advanced Computer Information Technologies (ACIT)*, Deggendorf, Germany. 2020. pp. 751–754. https://doi.org/10.1109/ACIT49673.2020.9208812 (Scopus).

43. Yakymenko I., Kasianchuk M., Gomotiuk O., Tereshchuk G., Ivasiev S., Basistyi P. Elgamal cryptoalgorithm on the basis of the vector-module method of modular exponentiation and multiplication. *IEEE 15th International Conference on Advanced Trends in Radioelectronics, Telecommunications and Computer Engineering (TCSET)*. 2020. pp. 926-929. (Scopus). DOI: 10.1109/TCSET49122.2020.235572

44. Karpinski M., Rajba S., Zawislak S., Warwas K., Kasianchuk M., Ivasiev S., Yakymenko I. A method for decimal number recovery from its residues based on the addition of the product modules, *2019 10th IEEE International Conference on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications (IDAACS)*. Metz, France. 2019. pp.13-17. https://doi.org/10.1109/IDAACS.2019.8924395. (Scopus).

45. Kasianchuk M., Yakymenko I., Ivasiev S., Shevchuk R., Tymoshenko L. The method of factorizing multi-digit numbers based on the operation of adding odd numbers. *CEUR Workshop Proceedings 8th International Conference Advanced Computer Information Technologies ACIT*. June 2018. 2018, pp. 232-235, (Scopus).

46. Ivasiev S., Yakymenko I., Kasianchuk M., Shevchuk R., Karpinski M., Gomotiuk O. Effective algorithms for finding the remainder of multi-digit numbers. *Advanced Computer Information Technology (ACIT–2019): Proceedings of the International Conference*. 2019, pp. 175-178. (Scopus). DOI: 10.1109/ACITT.2019.8779899

47. Yakymenko I., Kasianchuk M., Ivasiev S., Melnyk A., Nykolaichuk Y. Realization of RSA cryptographic algorithm based on vector-module method of modular exponention. *In Proceedings of the 2018 14th International Conference on Advanced Trends in Radioelecrtronics*. Telecommunications and Computer Engineering (TCSET), Lviv-Slavske, Ukraine, 20–24 February 2018. 2018. pp. 550–554.

48. Якименко І.З., Касянчук М.М., Кінах Я.І., Власюк І.М., Суслін В.В. Удосконалення реалізації асиметричних криптоалгоритмів на основі системи залишкових класів. *Матеріали VI Всеукраїнської школи-семінару молодих вчених і студентів «Сучасні комп'ютерні інформаційні технології» (ACIT)*. 2018. с. 79.

49. Карпінський, М. П., Кінах, Я. І., Яциковська, У. О., Якименко, І. З., Касянчук, М. М. Удосконалення архітектури комп'ютерної мережі для програмної реалізації криптоаналітичних алгоритмів. *Матеріали V науково-технічної конференції „Інформаційні моделі, системи та технології".* 2018. С. 93.

50. Карпінський М. П., Кінах Я. І., Войтенко, О. С., Паславський, В. Р., Якименко, І. З., Касянчук, М. М. Теоретичний аналіз інформаційної безпеки в комп'ютерних мережах. *Збірник тез доповідей VI Міжнародної науково-технічної конференції молодих учених та студентів „Актуальні задачі сучасних технологій". 2*, 2017. С.81-82.

51. Rajba T., Klos-Witkowska A., Ivasiev S., Yakymenko I., Kasianchuk M. Research of time characteristics of search methods of inverse element by the module in: Proc. *IEEE 9th Intern. Conf. on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications (IDAACS-2017)* (Bucharest, Romania. 21–23 Sept, 2017), 2017. pp. 82–85. https://doi.org/10.1109/IDAACS.2017.8095054. (Scopus).

52. Kasianchuk M., Yakymenko I., Pazdriy I., Melnyk A., Ivasiev S., Rabin's modified method of encryption using various forms of system of residual classes. *14th International Conference The Experience of Designing and Application of CAD Systems in Microelectronics (CADSM)*, 2017. pp. 222-224. (Scopus). DOI: 10.1109/CADSM.2017.7916120

53. Якименко І.З. Методологія криптографічного захисту інформації на основі цілочисельної, модифікованої досконалої та поліноміальної систем залишкових класів, *Матеріали XIV Міжнародної науково-технічної конференції ITSec-2025 Безпека інформаційних технологій*, 22-24 травня 2025, м. Тернопіль (Україна). 2025. С. 224-228.

54. Karpiński M., Ivasiev S., Yakymenko I., Kasianchuk M., Gancarczyk T. Advanced method of factorization of multi-bit numbers based on Fermat's theorem in the system of residual classes. *International Conference on Control, Automation and Systems* (*ICCAS–2016*): Proceedings. Gyeongju, Korea. V.1. 2016. pp.1484–1486 (Scopus). DOI: 10.1109/ICCAS.2016.7832500

55. Nykolaychuk Ya., Ivas'ev S., Yakymenko I., Kasianchuk M. Test of verification of multidigit numbers on simplicity on the basis of method of vector and modular multiplication. *Modern Problems of Radio Engineering, Telecommunications and Computer Science* (*TCSET–2016*): *Proceedings of the XIII–th International Conference.* L'viv–Slavske. 2016. pp.534-536 (Scopus). DOI: 10.1109/TCSET.2016.7452107

56. Kozaczko D., Ivasiev S., Yakymenko I., Kasianchuk M. Vector Module Exponential in the Remaining Classes System. *Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications* (*IDAACS–2015*): Proceedings of the 2015 IEEE 8th International Conference. Warsaw, Poland. V.1. 2015. pp.161–163 (Scopus). DOI: 10.1109/IDAACS.2015.7340720

57. Kasianchuk M., Yakymenko I., Pazdriy I., Zastavnyy O. Algorithms of findings of perfect shape modules of remaining classes system. *The Experience of Designing and Application of CAD Systems in Microelectronics* (*CADSM-2015*): Proceedings of the XIII International Conference. Polyana-Svalyava. 2015. pp.168-171 (Scopus). DOI: 10.1109/CADSM.2015.7230866

58. Ivas'ev S., Kasyanchuk M., Yakymenko I., Nykolaychuk Ya. Fundamental Backgrounds of the Discrete Logarithms Theory in the Rademacher–Krestenson's Basis. *Modern Problems of Radio Engineering, Telecommunications and Computer Science* (*TCSET–2012*): Proceedings of the XI–th International Conference. L'viv–Slavske. 2012. 93 P. (Scopus).

59. Касянчук М.М., Якименко І.З., Тимошенко Л.М., Івасьєв С.В., Николайчук Я.М. Векторно-модульний метод модулярного множення. *Сучасні інформаційні та електронні технології: Матеріали Міжнародної науково-практичної конференції.* Одеса. 2014, С. 152.

Патенти:

60. Пат. 159225 Україна МПК G06F 7/00 (2025.01). Накопичуючий синхронізований двійковий суматор / Николайчук Я.М., Грига В.М., Якименко І.З., Грига Л.П., № u 2024 04320 заявл. 03.09.2024; опубл. 08.05.2025, Бюл. №19/2025.

61. Пат. 160091 Україна МПК G06F7/04. Пристрій порівняння даних, представлених у непозиційній системі залишкових класів / Николайчук Я.М., Якименко І.З., Івасьєв С.В, Грига В.М. № u202404328 заявл. 03.09.2024; опубл. 06.08.2025, Бюл. № 32/2025.

АНОТАЦІЯ

І.З. Якименко Методи та засоби криптографічного захисту інформації на основі системи залишкових класів. – Рукопис.

Дисертація на здобуття наукового ступеня доктора технічних наук за спеціальністю 05.13.21 – «Системи захисту інформації». – Державний університет інформаційно-комунікаційних технологій, Київ, 20__.

Дисертаційна робота присвячена вирішенню актуальної науково-практичної проблеми підвищення ефективності захисту інформаційних потоків на основі заміни в алгоритмах шифрування операції множення операцією додавання, використання цілочисельної, модифікованої досконалої форми, поліноміальної та ієрархічної СЗК для розробки нових криптографічних алгоритмів. Розроблено симетричний криптоалгоритм у СЗК та побудовано аналітичні вирази оцінки стійкості. Розроблено високопродуктивні симетричні та асиметричні криптоалгоритми на основі СЗК та її МДФ шляхом довільної заміни базисних чисел, що дозволило підвищити рівень захисту даних та стійкість до криптоаналітичних атак. Розроблено криптографічний алгоритм, в якому шифрування відкритого тексту у вигляді залишків відбувається за допомогою КТЗ, а розшифрування – на основі операції пошуку залишків за відповідними модулями. Розроблено одно- та двоключові симетричні криптографічні методи в ПСЗК, криптоаналіз яких потребує вирішення NP-повної задачі. Розроблено симетричні методи шифрування/розшифрування інформаційних потоків в ІЗСК та ІПСЗК, які за рахунок представлення зашифрованого тексту наборами залишків за відповідними модулями (ключами) та розпаралення процесу обчислень дають змогу підвищити стійкість криптоалгоритму та збільшити його швидкодію. Отримали подальший розвиток поліноміальний, дво- та тримодульний цілочисельні асиметричні криптосистеми Рабіна на основі операції додавання. Отримав подальший розвиток метод пошуку оберненого полінома в кільці $Z[x]$ на основі методу невизначених коефіцієнтів, що дало змогу зменшити часову складність. Розроблено методологію криптографічного захисту інформації в СЗК, застосування якої дає можливість забезпечити збільшення стійкості, зменшення часової складності, підвищення швидкодії алгоритмів, спеціалізованого програмного забезпечення та побудувати єдину стратегію захисту інформаційних потоків.

Ключові слова: симетричний та асиметричний криптографічні алгоритми, система залишкових класів, модифікована досконала форма, векторно-модульний метод, китайська теорема про залишки, поліноміальна система залишкових класів, ієрархічна система залишкових класів.

ABSTRACT

Yakymenko I. Methods and Means of Cryptographic Information Protection Based on the Residue Number System. – Manuscript. Dissertation for the degree of Doctor of Technical Sciences in specialty 05.13.21 – "Information Security Systems". – State University of Telecommunications, Kyiv, 2026.

The dissertation is devoted to solving the urgent scientific and practical problem of improving the efficiency of information flow protection by replacing the

multiplication operation with addition in encryption algorithms, and by using integer, modified perfect, polynomial, and hierarchical residue number systems (RNS) for the development of new cryptographic algorithms. A symmetric cryptographic algorithm based on RNS was developed, along with analytical expressions for evaluating its resistance. High-performance symmetric and asymmetric cryptographic algorithms based on RNS and its modified perfect form were designed by arbitrary substitution of base numbers, which increased data protection levels and resistance to cryptanalytic attacks.

A cryptographic algorithm was developed in which encryption of plaintext is carried out using the Chinese Remainder Theorem (CRT), and decryption is based on residue recovery for the respective moduli. One-key and two-key symmetric cryptographic methods in the polynomial residue number system (PRNS) were proposed, the cryptanalysis of which requires solving an NP-complete problem. Symmetric encryption/decryption methods for information flows in hierarchical integer and polynomial RNS (HIRNS and HPRNS) were designed, which—through representation of ciphertext as sets of residues with respect to corresponding moduli (keys) and parallelization of computation—allow improved algorithm resistance and increased processing speed.

Further development was given to polynomial, two-modulus, and three-modulus integer asymmetric cryptosystems Rabin based on addition operations. The method of finding an inverse polynomial in the ring Z[x] using the method of undetermined coefficients was also advanced, reducing computational complexity. A methodology for cryptographic information protection in RNS was developed, the application of which makes it possible to ensure increased resistance, reduced time complexity, enhanced performance of algorithms and specialized software, and to build a unified strategy for information flow protection.

Keywords: symmetric and asymmetric cryptographic algorithms, residue number system, modified perfect form, vector-modular method, Chinese Remainder Theorem, polynomial residue number system, hierarchical residue number system.

Підписано до друку 03.02.2026.
Формат 60х 84/16. Гарнітура Times New Roman.
Папір офсетний 80 г/м2. Друк офсетний.
Ум. друк. арк. 1,9. Обл.-вид. арк. 1,9.
Наклад 100 прим. Зам. № 11/19/1-2

Віддруковано у видавничому центрі "Вектор"
46018, м. Тернопіль, вул. Львівська, 12,
Тел. 8 (0352) 40-08-12

Свідоцтво про внесення суб'єкта видавничої справи
до державного реєстру видавців, виготівників
і розповсюджувачів видавничої продукції
серія ТР № 46 від 07 березня 2013р.
ФОП Осадца Ю.В.