МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
НАЦІОНАЛЬНИЙ АВІАЦІЙНИЙ УНІВЕРСИТЕТ

КАСЯНЧУК МИХАЙЛО МИКОЛАЙОВИЧ

УДК 004.056.53

МЕТОДИ ОПРАЦЮВАННЯ БАГАТОРОЗРЯДНИХ ЧИСЕЛ В АСИМЕТРИЧНИХ КРИПТОСИСТЕМАХ НА ОСНОВІ МОДУЛЯРНОЇ АРИФМЕТИКИ

05.13.21 – системи захисту інформації

Автореферат
дисертації на здобуття наукового ступеня
доктора технічних наук

Київ – 20___

Дисертацією є рукопис.

Робота виконана на кафедрі кібербезпеки Тернопільського національного економічного університету Міністерства освіти і науки України.

Наукові консультанти: доктор технічних наук, професор
Николайчук Ярослав Миколайович,
Тернопільський національний економічний університет,
завідувач кафедри спеціалізованих комп'ютерних систем, академік Міжнародної академії інформатики;

доктор технічних наук, професор,
Карпінський Микола Петрович,
Університет у Бєльсько-Бялій (Польща),
завідувач кафедри інформатики та автоматики.

Офіційні опоненти: доктор технічних наук, професор
Білецький Анатолій Якович,
Національний авіаційний університет,
професор кафедри електроніки,
заслужений діяч науки і техніки України,
лауреат Державної премії України,
заслужений професор Національного
авіаційного університету;

доктор технічних наук, професор
Казакова Надія Феліксівна,
Одеський державний екологічний університет,
професор кафедри інформаційних технологій;

доктор технічних наук, доцент
Олійников Роман Васильович,
Харківський національний університет ім.В.Н.Каразіна,
професор кафедри безпеки інформаційних систем
і технологій.

Захист відбудеться «___» _____ 20__ р. о ___ годині на засіданні спеціалізованої вченої ради Д 26.062.17 при Національному авіаційному університеті за адресою: 03058, м.Київ, пр. Любомира Гузара, 1, корпус 11, ауд. 111.

З дисертацією можна ознайомитись у науково-технічній бібліотеці Національного авіаційного університету за адресою: 03058, м.Київ, пр. Любомира Гузара, 1.

Автореферат розісланий «___» _____ 20___ р.

Учений секретар
спеціалізованої вченої ради,
д.т.н., доцент Гнатюк С.О

ЗАГАЛЬНА ХАРАКТЕРИСТИКА РОБОТИ

Обгрунтування вибору теми дослідження. На даний час інтенсивна комп'ютеризація усіх видів людської діяльності приводить до повсякденного використання телекомунікаційних систем та мереж. Представлена у цифровому вигляді інформація повинна бути надійно захищена від різних видів загроз, таких як несанкціонований доступ, модифікація, руйнування, підробка електронного цифрового підпису тощо. Це досягається засобами криптографічного захисту.

Важливу роль під час захисту інформаційних потоків відіграють асиметричні криптосистеми. Вони усувають основний недолік симетричних криптосистем: необхідність надійного каналу обміну ключем. Значний вклад в розвиток асиметричної криптографії зробили такі зарубіжні та вітчизняні вчені: У. Діффі, М. Хеллманн, Р. Меркле, Р. Райвест, А. Шамір, Л. Адлеман, М. Рабін, Т. Ель-Гамаль, М. Манассі, О. Василенко, Е. Маховенко, І.Горбенко та інші.

Основними операціями в найпоширеніших асиметричних криптосистемах RSA, Рабіна, Ель-Гамаля, є модулярне множення та модулярне експоненціювання. Однак методи, які найчастіше використовуються для їх реалізації (стандартний, Шенхаге-Штрасена, Монтгомері, Карацуби-Офмана) характеризуються значною часовою та/або апаратною складністю. Пришвидшити процес виконання обчислень дозволяють матрично- та векторно-модульні методи, але вони не набули значного поширення для асиметричних криптосистем.

Крім того, в зв'язку із збільшенням довжини ключа все більше стали проявлятися недоліки двійкової системи числення, а саме, її багаторозрядність, строго послідовна структура, наявність міжрозрядних переносів тощо, які в значній мірі сповільнюють виконання арифметичних операцій.

Найперспективнішим шляхом підвищення швидкодії сучасних обчислювальних систем є розпаралелення процесу обробки інформації. Цією властивістю володіє система залишкових класів (СЗК). Вона дозволяє істотно поліпшити параметри обчислювальних систем у порівнянні з пристроями, побудованими на тій же фізико-технологічній базі і які працюють у позиційних системах числення. Значний теоретичний та прикладний внесок у розвиток СЗК та її застосування в обчислювальній техніці зробили такі вчені: І. Акушський, Д. Юдицький, В. Амербаєв, В. Торгашев, В. Краснобаєв, Я. Николайчук, В. Яцків, М. Червяков, О. Фінько, А. Омонді (A. Omondi), Б. Премкумар (B. Premkumar), А. Молахоссеіні (A. Molahosseini), А.Мохан (A.Mohan) та інші.

Хоча СЗК не позбавлена недоліків (труднощі при виконанні операцій ділення, порівняння, визначення переповнення розрядної сітки), однак її успішно можна застосовувати для додавання, віднімання, піднесення до степеня, множення цілих багаторозрядних чисел, що є важливо для асиметричної криптографії. Безсумнівна перевага СЗК - це можливість виконання операцій над числами, які менші за вибрані модулі, розпаралелення процесу обчислень та відсутність міжрозрядних переносів.

Ще одним з недоліків СЗК, який сповільнив її розвиток, є складність при переведенні чисел із СЗК у позиційну систему числення. Найбільш відомі підходи на основі китайської теореми про залишки (КТЗ) або алгоритму Гарнера передбачають пошук оберненого елемента за модулем та множення на нього, що може привести до переповнення розрядної сітки. Уникнути виконання цієї операції

дозволяє досконала (ДФ) та модифікована досконала форми (МДФ) СЗК, що є перспективним, проте найменш розвиненим підходом використання СЗК при опрацюванні багаторозрядних чисел в асиметричних криптосистемах, оскільки на даний час відсутні методи побудови системи модулів, які задовольняють умови ДФ та МДФ СЗК.

Таким чином, на сучасному етапі розвитку науки і техніки в процесі функціонування асиметричних криптосистем існує таке об'єктивне *протиріччя* між потребою у збільшенні довжини ключа, який забезпечує високу стійкість до криптоаналізу та конфіденційність даних, з одного боку, та збільшенням часової складності, зменшенням швидкодії відповідного програмного та апаратного забезпечення при реалізації асиметричних криптосистем.

Враховуючи викладене, *актуальною науково-технічною проблемою* є підвищення ефективності опрацювання багаторозрядних чисел на основі використання векторно-модульних методів модулярного множення та експоненціювання, ДФ та МДФ СЗК для зменшення часової складності, підвищення швидкодії алгоритмів, спеціалізованого програмного і апаратного забезпечення в асиметричних криптосистемах.

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 Тернопільського національного економічного 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), «Світлодіодне підсвічування зовнішньої реклами», «Теоретичні основи та апаратні засоби підвищення продуктивності роботи безпровідних сенсорних мереж» (Державний реєстраційний номер 0117U000414).

Мета і завдання дослідження. Метою дисертаційного дослідження є розробка методів, засобів та методології опрацювання багаторозрядних чисел в асиметричних криптосистемах для зменшення обчислювальної складності, підвищення швидкодії алгоритмів, спеціалізованого програмного і апаратного забезпечення. Для досягнення поставленої мети у дисертаційній роботі необхідно розв'язати наступні задачі:

1) проаналізувати сучасні методи, алгоритми та засоби опрацювання багаторозрядних чисел в асиметричних криптосистемах на основі модулярної арифметики з метою визначення перспектив підвищення їх ефективності на основі матрично- та векторно-модульних методів, використання різних форм СЗК;

2) удосконалити векторно-модульний метод модулярного множення та експоненціювання;

3) розробити алгоритмічне забезпечення для реалізації криптосистем RSA та Ель-Гамаля на основі векторно-модульного алгоритму модулярного множення та модулярного експоненціювання;

4) розробити методи пошуку оберненого елемента за модулем та здійснити їх програмну і апаратну реалізацію;

5) розробити метод пошуку мультистепеневої функції за модулем;

6) розробити метод пошуку модулів СЗК, які дозволяють аналітично обчислювати коефіцієнти базисних чисел;

7) розробити методи побудови системи модулів ДФ та МДФ СЗК;

8) удосконалити метод Ферма для факторизації багаторозрядних чисел;

9) розробити програмну реалізацію операції множення в цілочисельній та МДФ СЗК, сумісного виконання алгоритму Евкліда та множення, методів модулярного множення, експоненціювання, методів факторизації багаторозрядних чисел;

10) розробити трьохмодульну криптосистему Рабіна та її VHDL-модель;

11) розробити методологію опрацювання багаторозрядних чисел в асиметричних криптосистемах.

Об'єкт дослідження – процеси опрацювання багаторозрядних чисел в асиметричних криптосистемах на основі модулярної арифметики.

Предмет дослідження – методи, алгоритми та засоби для зменшення обчислювальної складності при опрацюванні багаторозрядних чисел в асиметричних криптосистемах на основі модулярної арифметики.

Методи дослідження. Проведені дослідження базуються на використанні математичних основ алгебри і теорії чисел (для розробки методів побудови ДФ та МДФ СЗК, реалізації КТЗ), теорії алгоритмів (для оцінки часової складності відомих та розроблених методів), методів криптографії (для розробки трьохмодульної криптосистеми Рабіна), програмування (для реалізації методів побудови ДФ та МДФ СЗК, дослідження модулярного експоненціювання, факторизації та пошуку оберненого елемента), схемотехнічного проектування (для дослідження методів пошуку оберненого елемента та трьохмодульної криптосистеми Рабіна), теорії множин (для побудови методології опрацювання багаторозрядних чисел в асиметричних криптосистемах), статистики (для обробки експериментальних результатів).

Наукова новизна отриманих результатів полягає в наступному:

1) отримали подальший розвиток методи модулярного множення та експоненціювання в асиметричних криптосистемах, які за рахунок використання матрично- та векторно-модульних методів характеризуються меншою часовою та апаратною складністю в порівнянні з відомими;

2) вперше розроблено методи пошуку оберненого елемента за модулем та виконання китайської теореми про залишки на основі додавання модуля та додавання залишку, які за рахунок використання модулярних операцій додавання модуля або залишку дають можливість розпаралелити процес пошуку оберненого елемента за модулем і, відповідно, зменшити часову складність даної операції при її використанні в асиметричних криптосистемах;

3) вперше розроблено метод пошуку мультистепеневої функції за модулем, який за рахунок двократного використання функції Ейлера, виконання арифметичних дій над операндами, меншими від заданого модуля, та переходу до лінійної конгруенції, дозволяє уникнути виконання операції модулярного експоненціювання багаторозрядних чисел, відповідно зменшуючи часову складність;

4) вперше розроблено метод пошуку набору модулів системи залишкових класів, який за рахунок обчислення коефіцієнтів базисних чисел на основі аналітичних виразів при відновленні десяткового числа із системи залишкових класів забезпечує уникнення громіздкої операції знаходження мультиплікативного оберненого елемента за модулем, відповідно зменшуючи часову складність та збільшуючи швидкодію обчислювальних систем;

5) вперше розроблено методи побудови наборів модулів досконалої форми системи залишкових класів на основі дробових перетворень та факторизації, які за рахунок уникнення виконання операції пошуку мультиплікативного оберненого елемента за модулем та множення на нього дозволяють зменшити часову та апаратну складності при переведенні чисел із системи залишкових класів в десяткову систему числення;

6) вперше розроблено методи побудови трьох- та багатомодульної модифікованої досконалої форми системи залишкових класів, які за рахунок використання аналітичних виразів, отриманих на основі дробових перетворень, факторизації, теореми Вієта, розв’язку систем конгруенцій, дозволяють зменшити розрядність операндів під час проміжних обчислень, уникнути виконання операції пошуку оберненого елемента за модулем та множення на нього і, відповідно, зменшити часову складність при відновленні десяткового числа із системи залишкових класів. Обґрунтовано доцільність використання модифікованої досконалої форми системи залишкових класів в асиметричних криптосистемах замість існуючої цілочисельної форми;

7) удосконалено метод Ферма для факторизації багаторозрядних чисел, який за рахунок заміни операції добування квадратного кореня та піднесення до квадрату на кожній ітерації на обчислювально простіші операції додавання і віднімання дає можливість зменшити розрядності операндів, спростити процедуру пошуку факторизованих чисел та підвищити швидкодію обчислень для множників різної розрядності;

8) вперше розроблено трьохмодульну криптосистему Рабіна, яка за рахунок узагальнення методів побудови модифікованої досконалої форми системи залишкових класів та їх використання дозволила підвищити швидкодію процесів шифрування та розшифровування блоків відкритого тексту в порівнянні із звичайною цілочисельною формою та розширити блок шифрування без зменшення стійкості криптосистеми;

9) вперше розроблено методологію опрацювання багаторозрядних чисел, яка за рахунок використання матрично- та векторно-модульних методів пошуку залишку, модулярного множення та експоненціювання, знаходження оберненого елемента на основі додавання модуля, а також використання досконалої та модифікованої досконалої форм системи залишкових класів дозволяє забезпечити

зменшення обчислювальної складності, підвищення швидкодії алгоритмів, спеціалізованого програмного і апаратного забезпечення та побудувати єдину стратегію опрацювання багаторозрядних чисел в асиметричних криптосистемах.

Практичне значення одержаних результатів.

1. Розроблено алгоритмічне забезпечення для реалізації криптосистем RSA та Ель-Гамаля на основі векторно-модульного методу модулярного множення та модулярного експоненціювання, які характеризується меншою обчислювальною складністю шифрування/розшифрування в порівнянні з відомими.

2. Здійснено програмну та апаратну реалізацію методів пошуку оберненого елемента за модулем, що дозволило виявити переваги запропонованих методів над існуючими.

3. Розроблено алгоритмічне забезпечення для пошуку модулів ДФ та МДФ СЗК на основі дробових перетворень, факторизації, теореми Вієта, розв'язку систем конгруенцій, що дозволило уникнути виконання операції оберненого елемента за модулем та множення на нього при переведенні чисел з СЗК в десяткову систему числення, та обґрунтовано доцільність використання МДФ СЗК в асиметричних криптосистемах.

4. Програмно реалізовано та досліджено виконання множення в цілочисельній та МДФ СЗК, сумісне виконання алгоритму Евкліда та множення у криптосистемі Рабіна, методів модулярного експоненціювання в криптосистемі RSA, методів факторизації, що дозволило показати зменшення обчислювальної складності при використанні запропонованих методів.

5. Побудовано VHDL-модель трьохмодульної криптосистеми Рабіна на основі цілочисельної та МДФ СЗК, отримано відповідні часові характеристики, які показують зменшення часової складності при використанні МДФ СЗК.

Результати досліджень впроваджені або плануються до впровадження (підтверджено відповідними актами) в Управлінні Державної служби спеціального зв'язку та захисту інформації України в Тернопільській області (від 8.07.2019 р.), Управлінні Державної служби України з надзвичайних ситуацій в Тернопільській області (від 8.07.2019 р.), ТзОВ НВФ «Інтеграл» (№2507-01 від 25.07.2019 р.), ТзОВ ТКБР «Стріла» (№288 від 19.07.2019 р.), компанії «CONNECT» (ФОП Яконюк Р.А.) (від 10.07.2019 р.), науковому процесі Громадської організації «Міжнародна академія інформації» (від 10.07.2019 р.), використані при виконанні п'яти науково-дослідних робіт у Тернопільському національному економічному університеті (ТНЕУ) (від 11.07.2019 р.), у навчальному та науковому процесах Університету у Бельсько-Бялій (Польща) (від 16.07.2019 р.), факультету комп'ютерних інформаційних технологій ТНЕУ (від 9.07.2019 р.), фізико-математичного факультету Тернопільського національного педагогічного університету ім. В.Гнатюка (№928-33/03 від 10.07.2019 р.), Академії ГУСПОЛ (Чеська Республіка) (від 10.07.2019 р.).

Особистий внесок здобувача. Наукові положення, які містяться в дисертації, отримані здобувачем особисто. У друкованих працях, опублікованих у співавторстві, автору належить: [2, 47] – запропоновано методи опрацювання багаторозрядних чисел в СЗК, [3] – обґрунтовано застосування СЗК в криптографічних засобах захисту інформації, [4, 37] – запропоновано метод пошуку

залишку багаторозрядних чисел за модулем, [6] – запропоновано метод побудови п’ятимодульної МДФ СЗК, [7] – запропоновано метод підбору модулів для аналітичного обчислення коефіцієнтів базисних чисел, [8, 9] – запропоновано методи побудови МДФ СЗК, [10] – проведено чисельні розрахунки для побудови термо- або п’єзоелектричного сенсора на основі СЗК, [12, 13, 38, 42, 52] – проведено аналітичні розрахунки методів факторизації багаторозрядних чисел на основі властивостей квадратичних лишків в СЗК та компактного кодування багаторозрядних двійкових чисел відповідно, [15] – розроблена методологія опрацювання багаторозрядних чисел в асиметричних криптосистемах, [16] – розроблено алгоритмічне забезпечення криптосистеми Рабіна на основі операції додавання, [17, 30] - розроблено математичне забезпечення для вибору параметрів еліптичних кривих при шифруванні, [18, 19, 40] – запропоновано методи та здійснено інтерпретацію експериментальних чисельних результатів пошуку оберненого елемента за модулем, [20] – запропоновано метод розширення набору модулів МДФ СЗК, [21] – запропоновано метод сумісного виконання алгоритму Евкліда та множення, [22, 41] – запропоновано трьохмодульний метод шифрування Рабіна з використанням різних форм СЗК, [25, 28, 31, 44, 53] – запропоновано методи модулярного експоненціювання та модулярного множення, [26] – проведено чисельні дослідження алгоритму пошуку символів Якобі, [27, 34, 45] – запропоновано методи аналітичного пошуку модулів ДФ СЗК, [29, 49] – розроблено алгоритми опрацювання інформаційних потоків у комп’ютерних системах, [32] – запропоновано метод побудови криптоалгоритмів RSA і Ель-Гамаля в розмежованій СЗК, [33, 35] – розроблено алгоритми пошуку найбільшого спільного дільника та перетворень КТЗ на основі СЗК, [36, 51] – запропоновано метод захисту комп’ютерної мережі на основі асиметричного шифрування та апарату еліптичних кривих, [39] – розроблено алгоритм реалізації криптоалгоритму RSA на основі векторно-модульного методу модулярного множення та експоненціювання, [43] – проведено чисельні розрахунки перевірки багаторозрядних чисел на простоту, [46] – запропоновано метод пошуку дискретного логарифма в СЗК, [48] – розроблено матричні алгоритми опрацювання інформаційних потоків, [50] – проведено огляд сучасних алгоритмів і методів біометричної ідентифікації особи, [54] – розроблено метод обчислення мультистепеневої функції.

Апробація результатів дисертації. Основні результати дисертаційної роботи доповідались і обговорювались на таких міжнародних та вітчизняних конференціях, школах, семінарах, як: проблемно-наукова міжгалузева конференція «Інформаційні проблеми комп’ютерних систем, юриспруденції, енергетики, економіки, моделювання та управління», Україна (2008-2012 роки); Міжнародна конференція «Теоретичні та прикладні аспекти побудови програмних систем» (2008), Міжнародний симпозіум «Питання оптимізації обчислень» Інституту кібернетики імені В.М. Глушкова НАН України (2009, 2013, 2015, 2017 роки), Всеукраїнська школа–семінар молодих вчених і студентів «Сучасні комп’ютерні інформаційні технології» (Тернопіль) (2011-2019 роки), Міжнародна науково-практична конференція «Сучасні інформаційні та електронні технології» (Одеса) (2014 рік), Міжнародна конференція «Захист інформації і безпека інформаційних систем» (Львів) (2014 рік), VII Міжнародна школа-семінар «Теорія прийняття рішень»

(Ужгород) (2014 рік), проблемно–наукова міжгалузева конференція «Юриспруденція та проблеми інформаційного суспільства» (Тернопіль-Бучач), Міжнародна науково-технічна конференція «Актуальні задачі сучасних технологій» (Тернопіль) (2017 рік), науково-технічна конференція «Інформаційні моделі, системи та технології» (Тернопіль) (2018 рік), Міжнародна науково-технічна конференція «Безпека інформаційних технологій» (Україна-Єгипет) (2019), IEEE International Conference on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications (2005, 2015, 2017, 2019 роки), International Conference «Advanced Computer Systems and Network: Design and Application» (2009 рік), International Conference «Modern Problems of Radio Engineering, Telecommunications and Computer Science» (L'viv) (2010, 2012, 2014, 2016, 2018 роки), International Conference «The Experience of Designing and Application of CAD Systems in Microelectronics» (L'viv) (2011, 2015, 2017 роки), International Conference on Control, Automation and Systems (Korea) (2016), Inter University Conference of Students, PhD Students and Young Scientists «Engineer of XXI Century» (Poland) (2016, 2017 роки), International Conference «Advanced Computer Information Technology» (Czech Republic) (2018, 2019).

Публікації. За матеріалами дисертації опубліковано 76 друкованих праць (56 основних з яких наведено в авторефераті), з яких 30 статей у фахових виданнях (5 одноосібних), в тому числі 5 індексовано у наукометричних базах Scopus та Web of Science (1 одноосібна), 3 - у періодичних виданнях іноземних держав (1 одноосібна); 40 - у матеріалах та тезах доповідей конференцій (5 одноосібних), з яких 14 проіндексовані наукометричними базами Scopus та Web of Science; 1 авторська та розділи у 5 колективних монографіях.

Обсяг і структура дисертації. Дисертація складається з анотації, змісту, вступу, семи розділів, загальних висновків, списку використаних джерел, додатків та має 287 сторінок основного тексту, 92 рисунки, 84 таблиці, 38 сторінок додатків. Список літератури загалом містить 346 найменувань і займає 38 сторінок. Загальний обсяг роботи 380 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 та досліджено сучасний стан опрацювання багаторозрядних чисел в асиметричних криптосистемах, визначено переваги та недоліки розглянутих методів, а також напрямки підвищення ефективності використання СЗК в асиметричних криптосистемах.

Наведено основні положення теорії чисел, яка є основою асиметричних криптосистем. Здійснено детальний аналіз найбільш поширених асиметричних криптосистем, основними операціями у яких є пошук оберненого елемента, модулярне множення та експоненціювання. Вони характеризуються значною часовою складністю і при розрядностях ключа порядку 1024 біт проявляються

недоліки двійкової арифметики (велика розрядність, міжрозрядні переноси, строга послідовність виконання обчислень), що сповільнює виконання арифметичних операцій. Одним із напрямків підвищення швидкодії є використання матричних та векторних методів, у яких порівняно невисока часова складність (табл. 1) (n_0-розрядність операндів) поєднується з простотою програмної та апаратної реалізацій.

Таблиця 1 – Часова складність алгоритмів модулярного множення

Назва алгоритму	Часова складність
Стандартний	n_0^2
Шенхаге-Штрасена	$n_0 \cdot \log_2 n_0 \log_2(\log_2 n_0)$
Карацуби	$n_0^{\log_2 3} = n_0^{1,585}$
Монтгомері	$n_0 \cdot \log_2 n_0$
Матрично-модульний	$n_0 \cdot \log_2 n_0$
Векторно-модульний	$(n_0 \cdot \log_2 n_0)/2$

Проведена систематизація найбільш відомих методів факторизації, яка використовується при побудові ДФ та МДФ СЗК. Відомі на даний час методи є складними і вимагають значних обчислювальних ресурсів для багаторозрядних чисел.

Можливостями розпаралелення виконання операцій додавання, множення, піднесення до степеня володіє непозиційна СЗК. Представленню десяткового числа N у СЗК відповідають його найменші невід'ємні залишки $b_i = A \bmod p_i$ у системі взаємно простих модулів p_i. Діапазон обчислень має лежати в межах $0 \le A \le P-1$, де $P = \prod_{i=1}^{k} p_i$, k – кількість модулів. Операції виконуються незалежно по кожному модулю. Перехід у десяткову систему числення відбувається на основі КТЗ:

$$A = \left(\sum_{i=1}^{k} b_i B_i \right) \bmod P, \qquad (1)$$

де $B_i = P_i m_i$, $P_i = P / p_i$, базисні числа m_i шукаються з виразу $m_i = P_i^{-1} \bmod p_i$.

Необхідність обчислення оберненого елемента у цілочисельній формі істотно збільшує складність відновлення десяткового числа із СЗК. Це є, поряд з труднощами при виконанні ділення та порівняння чисел, основним недоліком, який стримував розвиток СЗК. Однак аналіз літературних джерел показує, що в багатьох задачах використання СЗК разом з паралельними обчисленнями дозволяє значно збільшити продуктивність обчислювальних систем. Одним із шляхів для спрощення процедури відновлення десяткового числа за його залишками є застосування ДФ та запропонованої в дисертації МДФ СЗК, у яких відповідно виконуються умови $m_i = P_i^{-1} \bmod p_i = 1$, $m_i = P_i^{-1} \bmod p_i = \pm 1$. Це дозволяє уникнути пошуку оберненого елемента за модулем та множення на нього в (1) (табл. 2).

Таблиця 2 – Характеристики форм СЗК

Форма СЗК	Відновлення десяткового числа	m_i	Пошук оберненого елемента	Множення на m_i в (1)	Перевищення модуля P
Звичайна	$A=\left(\sum_{i=1}^{k} b_i P_i m_i\right) \bmod P$	$P_i^{-1} \bmod p_i$	+	+	Значне
ДФ	$A=\left(\sum_{i=1}^{k} b_i P_i\right) \bmod P$	1	-	-	Значне
МДФ	$A=\left(\sum_{i=1}^{k} b_i P_i m_i\right) \bmod P$	±1	-	-	Незначне

Наведені чинники визначають розробку та використання нових підходів (зокрема, векторно-модульного методу, ДФ та МДФ СЗК) до підвищення швидкодії асиметричних криптосистем як важливу та актуальну проблему, від вирішення якої залежить ефективність захисту інформаційних потоків.

У другому розділі представлено схему адміністративного алгоритму (рис. 1), в якому показано застосування розроблених методів в асиметричних криптосистемах RSA, Рабіна та Ель-Гамаля, а також проведені теоретичні дослідження виконання модулярних операцій над багаторозрядними числами.

Для зменшення часової складності в асиметричних криптосистемах, зокрема, RSA та Ель-Гамаля, пропонується використати метод векторно-модульного експоненціювання. Показник степеня виразу $A^e (\bmod n)$ (A – блок відкритого тексту, e, n – відкритий ключ криптосистеми RSA), потрібно записати за степенями двійки і використати співвідношення $A^e \bmod n = \left(\prod_{i=0}^{n_0-1} \left(A^{e_i 2^i}\right) \bmod n\right) \bmod n = \prod_{i=0}^{n_0-1} f_i^{e_i} \bmod n$, де n_0 – розрядність степеня e, e_i=0 або 1, $f_i = A^{2^i} \bmod n$, причому $f_i = \left(f_{i-1}\right)^2 \bmod n$. Тоді шуканий результат можна отримати, перемноживши ті значення f_i, для яких відповідні e_i=1 (табл. 3). Отже, операція модулярного експоненціювання замінюється модулярним множенням. Часова складність зменшується з $O(n_0^3)$ до $O(\frac{1}{4} n_0^2 \log_2 n_0)$.

При модулярному множенні двох чисел $f_i f_j \bmod n$ одне з них (наприклад, f_j) також потрібно представити за степенями двійки: $f_j = \sum_{l=0}^{r_0-1} s_l \cdot 2^l$, де $s_l = 0,1$, r_0 – розрядність числа f_j. Далі для використання векторно-модульного методу будується табл. 4 відповідно з елементами l, s_l та λ_l, причому $\lambda_0 = 2^0 f_i \bmod n$, $\lambda_l = 2 \cdot \lambda_{l-1} \bmod n$.

Результат модулярного множення двох чисел знаходиться згідно формули $f_i f_j \bmod n = \left(\sum_{l=0}^{r_0-1} s_l \cdot \lambda_l\right) \bmod n$, тобто множення замінюється додаванням тих λ_l, для яких відповідні s_l рівні 1, що призводить до зменшення часової складності з $O(n_0^2)$ до $O(\frac{1}{2} n_0 \log_2 n_0)$, причому операції виконуються над числами значно меншої розрядності.

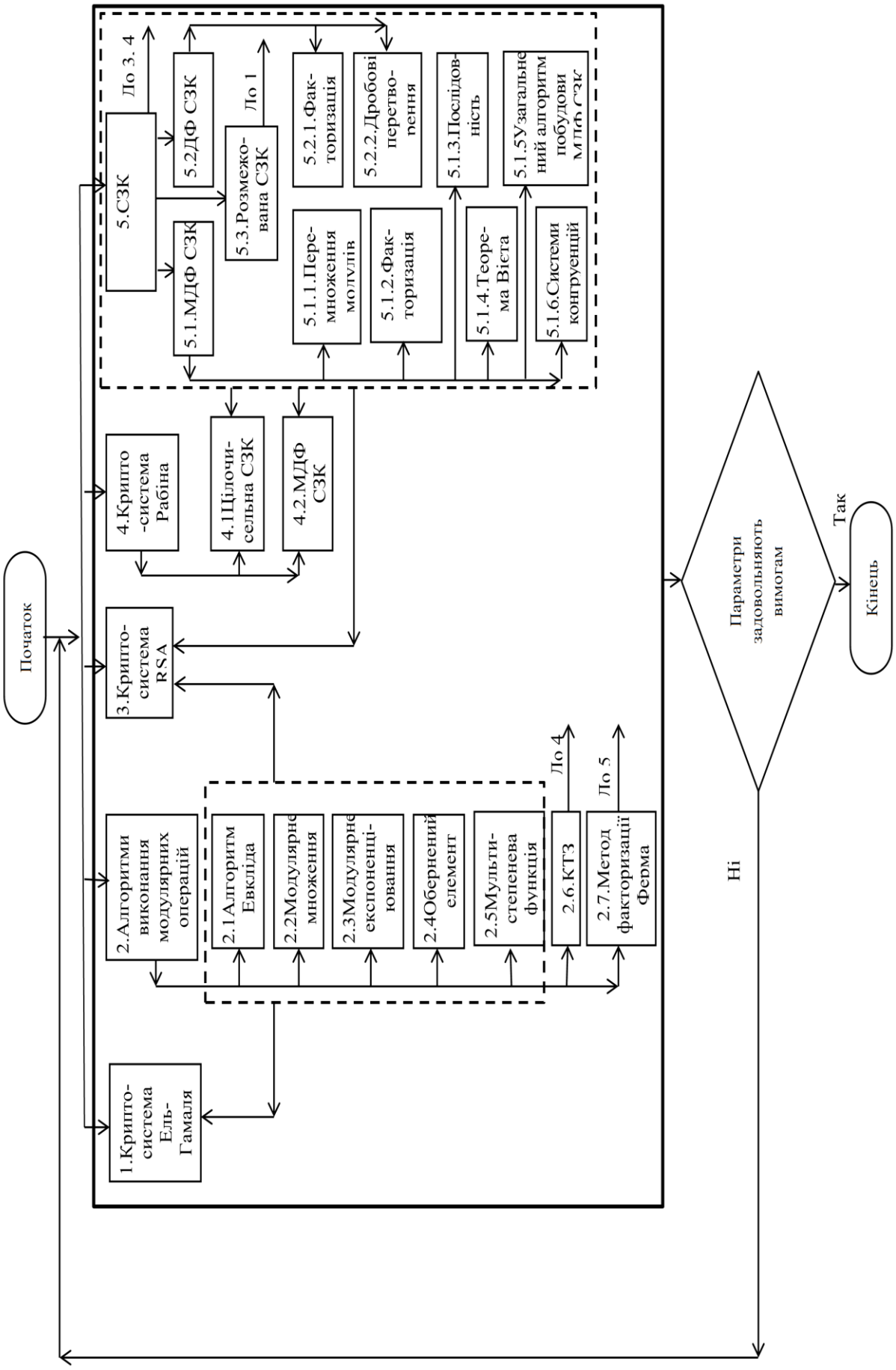

Рис. 1 – Схема адміністративного алгоритму використання розроблених методів в асиметричних криптосистемах

Таблиця 3 - Вектор піднесення до степеня

i	n_0-1		3	2	1	0
e_i	e_{n_0-1}	…	e_3	e_2	e_1	e_0
f_i	$A^{2^{n_0-1}} \bmod n$	…	$A^{2^3} \bmod n$	$A^{2^2} \bmod n$	$A^{2^1} \bmod n$	$A^{2^0} \bmod n$

Таблиця 4 - Представлення вектор-рядків модулярного множення

l	r_0-1	…	2	1	0
s_l	s_{r_0-1}	…	s_2	s_1	s_0
λ_l	$\lambda_{r_0-1}= 2\cdot\lambda_{r_0-2} \bmod n$	…	$\lambda_2= 2\cdot\lambda_1 \bmod n$	$\lambda_1= 2\cdot\lambda_0 \bmod n$	$\lambda_0= 2^0 f_i \bmod n$

У роботі вперше представлено алгоритмічне забезпечення криптосистем RSA та Ель-Гамаля, а також пошуку найбільшого спільного дільника на основі векторно - модульного методу, уникнувши громіздкої операції ділення.

Для спрощення пошуку оберненого елемента $a=b^{-1} \bmod p=1$ вперше пропонується такий метод. До модуля p додається 1 і перевіряється, чи ділиться націло отримане число на a. Якщо не ділиться, то далі до отриманого числа потрібно послідовно додавати модуль до тих пір, поки результат ділення не буде цілим числом, яке і буде шуканим оберненим елементом. Математично це записується так: $p_{01} = p+1;\ b_{01} = (p+1)/a;\ p_{11} = 2\cdot p+1;\ b_{11} = (2\cdot p+1)/a;$ …, $p_{i1} = (i+1)\cdot p+1;\ b_{i1} = ((i+1)\cdot p+1)/a;\ b_i \in Z.$

Для зменшення чисел, які використовуються у даній процедурі, додається не модуль, а залишок $p_{00}=p \bmod a$ до тих пір, поки остача від ділення отриманого результату на число a не буде дорівнювати 0. Математичний запис матиме такий вигляд: $b_{02} = (p_{00}+1) \bmod a;$ $b_{12} = (b_{02}+p_{00}) \bmod a;$ $b_{22} = (b_{12}+p_{00}) \bmod a;$ …, $b_{i2} = (b_{i-1\ 2}+p_{00}) \bmod a = 0.$ Обернений елемент шукається за формулою $b = a^{-1} \bmod p = \left((i+1)p+1\right)\Big/a.$

На відміну від розширеного алгоритму Евкліда, запропоновані методи дозволяють розпаралелити процес пошуку оберненого елемента на декілька потоків. Початок обчислень в кожному потоці для обох методів відповідно визначається так: $N_0 = \left(\left[\frac{(j-1)a}{z}\right]+1\right)p+1;$ $N_1 = \left(\left(\left[\frac{(j-1)a}{z}\right]+1\right)p_{00}+1\right) \bmod a,$ де j - номер потоку, z - кількість потоків. Максимальна кількість ітерацій в кожному потоці становитиме $a/z+1$.

Загальна часова складність пошуку оберненого елемента запропонованим методом, вважаючи max $i=a/z+1$, становить $O\left((a/z+1)\left(\frac{n_0}{2}+\log_2 n_0/2\right)\right)$. Класичний метод з використанням розширеного алгоритму Евкліда приводить до такого результату: $O(n_0^3)$.

Отже, розроблені методи дозволяють уникати складних операцій, зокрема, ділення з остачею, та проводити обчислення над числами значно

меншої розрядності в порівнянні з класичним методом пошуку оберненого елемента за модулем з використанням алгоритму Евкліда та його наслідку.

Запропоновані методи додавання модуля та залишку можна використати для відновлення десяткового числа за його залишками, уникнувши виконання операції пошуку оберненого елемента. Нехай маємо систему:

$$\begin{cases} A \bmod p_1 = r_1; \\ A \bmod p_2 = r_2; \\ \quad \ldots. \\ A \bmod p_k = r_k. \end{cases} \qquad (2)$$

Перше рівняння (2) можна записати у вигляді $A=\gamma_1 p_1+r_1$, де $\gamma_1=0, 1, 2, \ldots$. Це означає, що для пошуку числа A до залишку потрібно додати модуль p_1 стільки разів, щоб виконувалось друге рівняння (2). Далі необхідно додавати добуток модулів p_1p_2, поки не буде виконуватися третє рівняння (2). Процес продовжується до тих пір, поки не буде виконуватися останнє рівняння (2). Математично це записується таким чином: $A_1=r_1$; $A_2=A_1+\gamma_1 p_1=r_1+\gamma_1 p_1$; $A_2 \bmod p_2=r_2$; $A_3=A_2+\gamma_2 p_1 p_2=r_1+\gamma_1 p_1+\gamma_2 p_1 p_2$; $A_3 \bmod p_3=r_3;\ldots$, $A_i= A_{i-1}+\gamma_{i-1} p_1 p_2 \ldots p_{i-1}$; $A_i \bmod p_i=r_i;\ldots$, $A_k= A=A_{k-1}+\gamma_{k-1} p_1 p_2 \ldots p_{k-1}$; $A_k \bmod p_k=r_k$. Даний метод подібний до алгоритму Гарнера, однак у ньому уникається пошук оберненого елемента за модулем для отримання відповідних коефіцієнтів.

Для зменшення чисел, які використовуються у запропонованому методі, можна додавати не добуток модулів, а залишок цього добутку від ділення на відповідний модуль. Математичний запис даного методу виглядає таким чином: $A_1=r_1$; $p_{11}=p_1 \bmod p_2$; $A_2= A_1+\gamma_1 p_1$; $A_2 \bmod p_2=r_2$; $p_{12} =(p_1p_2) \bmod p_3$; $A_3=A_2+\gamma_2 p_1 p_2$; $A_3 \bmod p_3=r_3$; $p_{13} =(p_1p_2p_3) \bmod p_4;\ldots$, $A_i= A_{i-1}+\gamma_{i-1} p_1 p_2 p_3 \ldots p_{i-1}$; $A_i \bmod p_i=r_i$; $p_{1i} = =(p_1p_2 \ldots p_i) \bmod p_{i+1}$; …, $A_k=A=A_{k-1}+\gamma_{k-1} p_1 p_2 p_3 \ldots p_{k-1}$; $A_k \bmod p_k=r_k$.

Отже, розроблені методи дозволяють уникати виконання складних операцій, зокрема, ділення з остачею і пошуку оберненого елемента, та проводити обчислення над числами значно меншої розрядності в порівнянні з класичною КТЗ та алгоритмом Гарнера.

Запропоновані методи дозволяють розпаралелити процес виконання КТЗ. Початок обчислень в кожному потоці для методів додавання добутку модулів та залишку від добутку модулів, починаючи від найбільшого, визначається з такого виразу: $A_{1i}=\left[\frac{P}{z}\right](j-1)+1+\left(p_1-\left(\left[\frac{P}{z}\right](j-1)+1\right)\bmod p_1+r_1\right)\bmod p_1$, де z-кількість потоків, j – номер потоку.

У випадку, коли показник степеня при модулярному експоненціюванні можна записати у вигляді степеня, вперше розроблено метод пошуку мультистепеневої функції за модулем: $x=a^{b^c} \bmod p$. За рахунок двократного використання функції Ейлера відбувається перехід до лінійної конгруенції, яка розв’язується стандартними методами теорії чисел. Даний метод дозволяє істотно зменшити обчислювальну складність за рахунок уникнення громіздкої операції модулярного експоненціювання багаторозрядних чисел та виконання арифметичних дій над операндами, меншими від заданого модуля.

Удосконалено метод Ферма для факторизації багаторозрядних чисел, у класичному варіанті якого використовуються обчислювально складні операції піднесення до квадрату та пошуку квадратного кореня, із застосуванням додавання і віднімання на основі властивості, що квадрати цілих чисел можна представити у вигляді суми непарних чисел, кількість яких дорівнює даному числу: $s^2=\sum_{i=1}^{s}(2i-1)$. Тому, знайшовши значення $w_1=\lceil\sqrt{n}\rceil$ та $q_{11}(x)=(w_1+1)^2-n$, де $n=q\cdot p$ – число, яке потрібно факторизувати, виконується така послідовність операцій: $q_{1i}=q_{1\,i-1}-r_{1\,i-1}$, $r_{11}=1$, $r_{1\,i-1}=2i-3=r_{1\,i-2}+2$, $i=2, 3, \ldots$ до тих пір, поки для деякого i не буде виконуватись умова: $q_{1i}-r_{1i}\le 0$. При виконанні строгої нерівності подальші обчислення відбуваються таким чином: $w_2=w_1+1$; $q_{21}=q_{1i}+2\ w_2+1-r_{1i}$, $r_{21}=r_{1i}+2$. Пошук наступних значень q_{2i}, r_{2i} здійснюється аналогічно до попереднього випадку.

В загальному випадку зазначені розрахунки можна описати такими виразами: $q_{j\,i+1}=q_{ji}-r_{ji}\le 0$, $r_{j\,i+1}=r_{ji}+2$, якщо $q_{ji}-r_{ji}>0$; $q_{j+1\ \ 1}=q_{ji}+2m_j+\ +1-r_{ji}\le 0$, $r_{j\ i+1}=r_{ji}+2$, якщо $q_{ji}-r_{ji}<0$. При виконанні умови $q_{ji}-r_{ji}=0$ визначаються шукані величини, які будуть натуральними числами. Слід зазначити, що в цьому випадку значення параметра j відповідає кількості кроків у класичному та удосконаленому методах Ферма.

У третьому розділі розроблені теоретичні основи для аналітичного пошуку коефіцієнтів базисних чисел та методи побудови ДФ СЗК. Розглянуто набір модулів у такому вигляді:

$$\begin{cases} p_1=2^u-1; \\ p_2=2^u+1; \\ p_3=2^{2u}+1; \\ p_4=2^{4u}+1; \\ \quad\ldots. \\ p_i=2^{u\cdot 2^{i-2}}+1; \\ \quad\ldots. \\ p_{k-1}=2^{u\cdot 2^{k-3}}+1; \\ p_k=2^{u\cdot 2^{k-2}}+1. \end{cases} \qquad (3)$$

Даний підбір модулів дозволяє обчислити аналітично необхідні обернені елементи за модулем згідно формули:

$$m_1=\frac{2^u}{2^{k_1}}=2^{u-k_1};\ m_i=\begin{cases} 2^{u\cdot 2^{i-2}}-2^{u\cdot 2^{i-2}-k_i}+1, & \text{при } a_i \text{ непарному}; \\ 2^{u\cdot 2^{i-2}-k_i}, & \text{при } a_i \text{ парному}, \end{cases} \qquad (4)$$

де k_i та a_i визначаються з рівностей: $k-1=a_1u+k_1;\ k-(i-1)=2^{i-2}ua_i+k_i$.

У ДФ СЗК підбір модулів такий, що $m_i=P_i^{-1}\bmod p_i=1$. Даний вираз можна трансформувати в умову $\sum_{i=1}^{k}\frac{1}{p_i}=\gamma+\frac{1}{\prod_{i=1}^{k}p_i}$, де $\gamma=1, 2, \ldots$.

Дослідження цього рівняння для великої кількості модулів є досить громіздкою задачею. Розрахунки показують, що для ДФ СЗК p_1=2, p_2=3. Поклавши γ=1, що відповідає найбільшому діапазону обчислень при заданій кількості модулів, можна отримати умови для знаходження будь-якого варіанту набору, для прикладу, з шести модулів ДФ СЗК:

$$(6p_3p_4)^2-(p_4(p_3-6)-6p_3)=ab,\ (6p_3p_4+a,b)\bmod(p_4(p_3-6)-6p_3)=0, \quad (5)$$

де введено позначення: $p_{5,6}=\dfrac{6p_3p_4+a,b}{p_4(p_3-6)-6p_3}$.

Ліва частина першого рівняння (5) має бути факторизована, на основі чого визначаються параметри a та b. Нехай для прикладу p_3=7. Тоді модуль p_4 має бути не менше 43, оскільки набір 2, 3, 7, 41 утворює ДФ СЗК. Звідси отримується: $ab=(42\cdot 43)^2-1=1805\cdot 1807=5\cdot 19\cdot 19\cdot 13\cdot 139$. Використавши всі можливі перестановки множників, можна отримати 12 варіантів наборів з 6 модулів ДФ СЗК при заданих 2, 3, 7, 43, які представлені в табл. 5 в порядку зростання p_5. Видно, що модуль p_5 зростає повільно. В той же час, p_6 істотно спадає із збільшенням номера набору модулів.

Таблиця 5 - Можливі варіанти наборів з 6 модулів ДФ СЗК при заданих модулях 2, 3, 7, 43

№	a	b	p_5	p_6
1	1	5·19·19·13·139	1807	3263441
2	5	19·19·13·139	1811	654133
3	13	5·19·19·139	1819	252701
4	19	5·19·13·139	1825	173471
5	5·13	19·19·139	1871	51985
6	5·19	19·13·139	1901	36139
7	139	5·19·19·13	1945	25271
8	19·13	5·19·139	2053	15011
9	19·19	5·13·139	2167	10841
10	5·139	19·19·13	2501	6499
11	5·13·19	19·139	3041	4447
12	5·19·19	13·139	3611	3613

Використання ДФ СЗК дозволяє, наприклад, спростити обчислення в КТЗ. При цьому усувається виконання громіздкої операції пошуку оберненого елемента за модулем та множення на нього при переході із СЗК в десяткову систему числення, а застосовуються тільки операції додавання та множення, що успішно можна використати в асиметричних криптосистемах, зокрема, в криптосистемі Рабіна.

У четвертому розділі розроблені теоретичні основи та методи побудови трьохмодульної МДФ СЗК, узагальнення результатів яких дозволяє побудувати систему з будь-якої кількості модулів, що утворюють МДФ СЗК.

Оскільки недоліком ДФ СЗК є те, що модулі швидко зростають, тому у роботі запропонована МДФ СЗК, в якій $m_i=P_i^{-1}\bmod p_i=\pm 1$.

Обчислення, аналогічні попереднім при γ=0, приводять до такого виразу: $\frac{1}{p_1}+\frac{1}{p_2}+\frac{1}{p_3}=\pm\frac{1}{p_1 p_2 p_3}$. На відміну від ДФ СЗК, у якій найменші модулі набувають строго визначених значень (p_1=2, p_2=3), у МДФ СЗК найменші модулі можуть бути будь-які. Звідси можна отримати $\pm 1+p_1^2=ab$ (введено позначення: $p_{2,3}=a,b-p_1$).

Ліва частина останнього рівняння повинна бути факторизована, на основі чого визначаються параметри a та b. Отже, даний вираз визначає умову для побудови МДФ СЗК з трьох модулів. Нехай p_1=7. Тоді отримаємо: $p_{2,3}=a,b-7$ і $ab=\pm 1+49=\begin{cases}50=2\cdot 5\cdot 5;\\ 48=2\cdot 2\cdot 2\cdot 2\cdot 3.\end{cases}$ Усі можливі варіанти з трьох модулів для МДФ СЗК при p_1=7 представлені в табл. 6.

Таблиця 6 - Можливі варіанти систем з трьох модулів для МДФ СЗК при p_1=7 (в дужках – розрядність в двійковій системі числення)

№	p_1	ab	a	b	p_2	p_3	P
1	7 (3)	48	1	48	-6 (3)	41 (6)	1722 (11)
2			-1	-48	-8 (4)	-55 (6)	3080 (12)
3			2	24	-5 (3)	17 (5)	595 (10)
4			-2	-24	-9 (4)	-31 (5)	1953 (11)
5			3	16	-4 (3)	9 (4)	252 (9)
6			-3	-16	-10 (4)	-23 (5)	1610 (11)
7			4	12	-3 (2)	5 (3)	105 (7)
8			-4	-12	-11 (4)	-19 (5)	1463 (11)
9			6	8	-1 (1)	1 (1)	7 (3)
10			-6	-8	-13 (4)	-15 (4)	1365 (11)
11		50	1	50	-6 (3)	43 (6)	1806 (11)
12			-1	-50	-8 (4)	-57 (6)	3192 (12)
13			2	25	-5 (3)	18 (5)	630 (10)
14			-2	-25	-9 (4)	-32 (6)	2016 (11)
15			5	10	-2 (2)	3 (2)	42 (6)
16			-5	-10	-12 (4)	-17 (5)	1428 (11)

На рис. 2 представлений характер зміни значень модулів p_2 та p_3 в порядку зростання абсолютної величини p_2. Як видно з рисунка, модуль p_2 відносно повільно зростає. В той же час, графік для значення модуля p_3 зростає інтенсивніше, доходить до максимуму приблизно посередині номерного діапазону модулів, а потім спадає майже до значення модуля p_2.

Слід зазначити, що найбільший діапазон обчислень буде в тому випадку, коли кожен наступний модуль є на одиницю більший від добутку абсолютних величин попередніх.

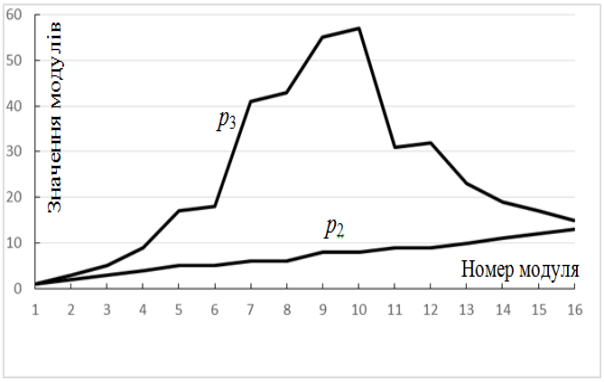

Рис. 2 - Характер зміни значень модулів p_2 та p_3 в порядку зростання абсолютної величини p_2

Крім того, з табл. 6 видно, що при застосуванні даних модулів МДФ СЗК розрядність чисел, над якими виконуються арифметичні операції, зменшується в 2-3 рази.

Ще один метод побудови трьохмодульної МДФ СЗК ґрунтується на теоремі Вієта. З умови МДФ СЗК можна отримати рівняння $p_2 p_3 + p_1(p_2 + p_3) = \pm 1$, в яке входять добуток та сума невідомих модулів p_2 та p_3. Для їх пошуку введемо позначення $p_2 p_3 = \chi p_1 \pm 1$. Тоді, відповідно, $p_2 + p_3 = -\chi$. За допомогою теореми Вієта можна побудувати квадратне рівняння, цілочисельними коренями якого будуть значення шуканих модулів: $x^2 + \chi x + \chi p_1 \pm 1 = 0$. Знайшовши дискримінант та ввівши позначення $\chi^2 - 4(\chi p_1 \pm 1) = (\chi - 2(p_1 + \rho))^2$ можна отримати: $\chi = 2p_1 + \rho + \frac{p_1^2 \pm 1}{\rho}$.

Отже, МДФ СЗК з трьох модулів існує, коли виконується умова $(p_1^2 \pm 1) \bmod \rho = 0$. Це означає, що параметр ρ обмежується інтервалом $\rho = \pm\sqrt{p_1^2 \pm 1}$. При p_1=7 параметр ρ∈[-6; 6] і в результаті отримується 16 варіантів значень модулів p_2, p_3, які відповідають представленим в табл. 6.

Ще один метод побудови трьохмодульної МДФ СЗК базується на розв'язку системи конгруенцій. Згідно умовам МДФ СЗК, повинна виконуватися система: $\begin{cases} p_2 p_3 \bmod p_1 = \pm 1 \\ p_1 p_3 \bmod p_2 = \pm 1. \\ p_1 p_2 \bmod p_3 = \pm 1 \end{cases}$ Після складних математичних перетворень можна отримати остаточний вираз для знаходження третього модуля: $p_3 = p_1 + \frac{p_1^2 \pm 1}{p_2 - p_1}$. Звідси випливає умова, при виконанні якої існує третій модуль для МДФ СЗК: $p_1^2 \bmod (p_2 - p_1) = \pm 1$. Два останні рівняння пояснюють, чому при заданому p_1 не для всіх p_2 можна підібрати третій модуль для МДФ СЗК.

У випадку багаторозрядних чисел, коли задана різниця між другим та першим модулями (p_2-p_1=q<p_1, причому p_1 і q повинні бути взаємно простими), їх можна представити у вигляді p_1=qn-r, p_2=qn-r+q і побудувати відповідну систему рівнянь для МДФ СЗК:

$$\begin{cases}(qn-r)p_3 \bmod (qn-r+q) = qp_3 \bmod (qn-r+q) = \mp 1, \\ (qn-r+q)p_3 \bmod (qn-r) = qp_3 \bmod (qn-r) = \pm 1, \\ (qn-r)(qn-r+q) \bmod p_3 = \pm 1. \end{cases} \quad (6)$$

Аналогічно до попереднього шукається значення третього модуля: $p_3 = qn(n+1) - r(2n+1) + \frac{r^2 \pm 1}{q}$, який можна знайти при умові $r^2 \bmod q = \pm 1$.

У роботі наведено приклад для q=5, r=2, а також побудова МДФ СЗК на основі послідовності Фібоначчі, коли третій модуль дорівнює сумі абсолютних величин двох попередніх.

У **п'ятому розділі** розроблено теоретичні основи побудови багатомодульної МДФ СЗК, для чого найзручніше вибрати метод факторизації. Нехай у системі $\begin{cases} M_1 \bmod p_1 = \pm 1 \\ \dots \\ M_k \bmod p_k = \pm 1 \end{cases}$ невідомі два останні модулі p_{k-1} p_k. Тоді

$$\begin{aligned} & p_{k-1}p_k(p_2p_3 \dots p_{k-2} + p_1p_3 \dots p_{k-2} + \dots + p_1p_2 \dots p_{k-3}) + \\ & + p_1p_2 \dots p_{k-2}(p_{k-1} + p_{k-2}) = \pm 1. \end{aligned} \quad (7)$$

Ввівши позначення $p_{k-1,k} = \frac{a,b - p_1p_2 \dots p_{k-2}}{p_2p_3 \dots p_{k-2} + p_1p_3 \dots p_{k-2} + \dots + p_1p_2 \dots p_{k-3}}$, після відповідних математичних перетворень можна отримати умову, яка повинна виконуватися для побудови багатомодульної МДФ СЗК:

$$\pm(p_2p_3 \dots p_{k-2} + p_1p_3 \dots p_{k-2} + \dots + p_1p_2 \dots p_{k-3}) + (p_1p_2p_{k-2})^2 = ab. \quad (8)$$

Ліва частина (8) факторизується, на основі чого визначаються параметри a та b. Крім того, модулі p_k та p_{k-1} мають бути цілими числами, тому: $(a,b - p_1p_2 \dots p_{k-2}) \bmod (|p_2p_3 \dots p_{k-2} + p_1p_3 \dots p_{k-2} + \dots + p_1p_2 \dots p_{k-3}|) = 0$. Два останні вирази є умовами для пошуку будь-якої кількості модулів МДФ СЗК, два з яких невідомі.

Для прикладу запропонованого методу можна розглянути МДФ СЗК, яка складається з чотирьох модулів. Умови побудови МДФ СЗК відповідно трансформуються:

$$p_{3,4} = \frac{a,b - p_1p_2}{p_1 + p_2}; \pm(p_1 + p_2) + (p_1p_2)^2 = ab; (a,b - p_1p_2) mod (p_1 + p_2) = 0. \quad (9)$$

Модулі p_1 і p_2 повинні мати різні знаки. Очевидно, що, вважаючи модуль p_1 додатнім, найбільше варіантів буде, коли p_2=-(p_1+1), оскільки в цьому випадку третя умова (9) зникає. Перші дві матимуть такий вигляд: $p_{3,4} = -(a,b + p_1^2 + p_1)$; $\pm 1 + (p_1(p_1+1))^2 = ab$. Нехай p_1=7, p_2=-8. Тоді $p_{3,4} = -(a,b + 56)$ і $ab = \pm 1 + 3136 = \begin{cases} 3135 = 3 \cdot 5 \cdot 11 \cdot 19 \\ 3137 = 71 \cdot 73. \end{cases}$ Усі можливі варіанти систем з чотирьох модулів для МДФ СЗК при p_1=7, p_2=-8 подані в табл. 7 (в дужках вказана розрядність модулів та діапазона обчислень у двійковій системі

числення). На рис. 3 представлений характер зміни значень модулів p_3 та p_4 в порядку зростання абсолютної величини модуля p_3.

Таблиця 7 - Можливі варіанти систем з чотирьох модулів для МДФ СЗК при p_1=7, p_2=-8 (в дужках – розрядність в двійковій системі числення)

№	p_1, p_2	ab	a	b	p_3	p_4	P
1	7 (3), -8 (4)	3135	1	3135	-57 (6)	-3191 (12)	10185672 (24)
2			-1	-3135	-55 (6)	3079 (12)	9483320 (24)
3			3	1045	-59 (6)	-1101 (11)	3637704 (22)
4			-3	-1045	-53 (6)	989 (10)	2935352 (22)
5			5	627	-61 (6)	-683 (10)	2333128 (22)
6			-5	-627	-51 (6)	571 (10)	1630776 (21)
7			11	285	-67 (7)	-341 (9)	1279432 (21)
8			-11	-285	-45 (6)	229 (8)	577080 (20)
9			15	209	-71 (7)	-265 (9)	1053640 (21)
10			-15	-209	-41 (6)	153 (8)	351288 (19)
11			19	165	-75 (7)	-221 (8)	928200 (20)
12			-19	-165	-37 (6)	109 (7)	225848 (18)
13			33	95	-89 (7)	-151 (8)	752584 (20)
14			-33	-95	-23 (5)	39 (6)	50232 (16)
15			55	57	-111 (7)	-113 (7)	702408 (20)
16			-55	-57	-1 (1)	1 (1)	56 (6)
17		3137	1	3137	-57 (6)	-3193 (12)	10192056 (24)
18			-1	-3137	-55 (6)	3081 (12)	9489480 (24)

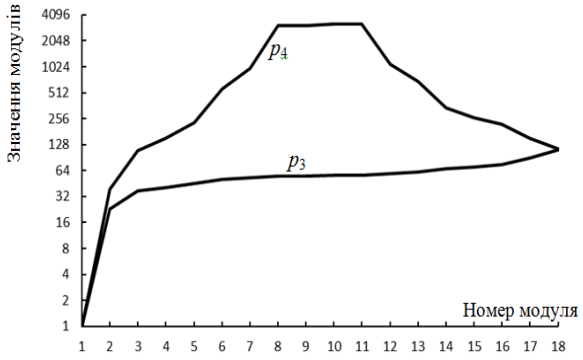

Рис. 3 - Характер зміни значень модулів p_3 та p_4 при p_1=7, p_2=-8 в порядку зростання абсолютної величини модуля p_3 згідно таблиці 7

Як видно з рисунка, модуль p_3 відносно повільно зростає. В той же час, графік для значення модуля p_4 зростає інтенсивніше, доходить до плоского максимуму приблизно посередині номерного діапазону модулів, а потім спадає до значення модуля p_3. Слід зазначити, що найбільший діапазон обчислень буде в тому випадку, коли кожен наступний модуль є на одиницю більший від добутку абсолютних величин попередніх модулів.

Крім того, з табл. 7 видно, що при застосуванні даних модулів МДФ СЗК розрядність чисел, над якими виконуються арифметичні операції, зменшується в 2-3 рази.

Чисельні розрахунки показують, що для p_1=7 в інших випадках, крім p_2=-8, найбільша кількість варіантів буде при p_2=-9 та p_2=-11.

На рис. 4 показані графіки залежності значень модулів p_3 та p_4 (суцільною лінією – для p_2=-9, пунктирною - для p_2=-11). Видно, що модуль p_3 відносно повільно збільшується. Графік для значення модуля p_4 збільшується інтенсивніше, приходить до плоского максимуму (причому для p_2=-9 максимум ширший) посередині номерного діапазону модулів, а потім спадає.

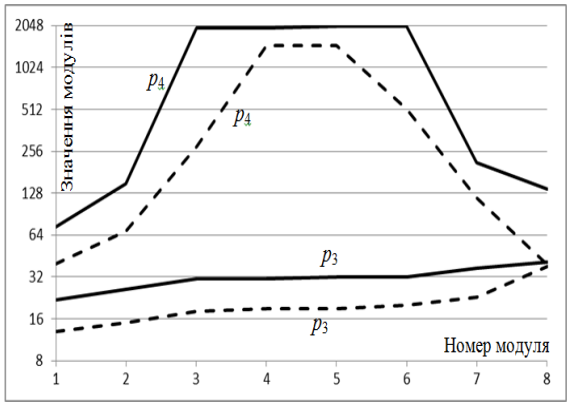

Рис. 4 – Характер змін значень модулів p_3 та p_4 при p_1=7, p_2=-9 (суцільна лінія) і p_2=-11 (пунктирна лінія) в залежності від номера модуля

У роботі наведено також приклад побудови п’ятимодульної МДФ СЗК, метод розширення набору модулів МДФ СЗК та застосування МДФ СЗК для побудови розподіленого термо- або п’єзоелектричного сенсора.

У шостому розділі здійснена програмна реалізація методів підбору модулів для ДФ та МДФ СЗК, а також розроблено трьохмодульну криптосистему Рабіна на основі звичайної цілочисельної та МДФ СЗК. Програмна реалізація виконана на мові програмування Java.

Для факторизації чисел можна використати одну зі сторонніх бібліотек. Робота програми складається з таких етапів: знаходження добутку модулів; факторизація отриманого добутку; перебір всіх можливих комбінацій отриманих чисел; перевірка отриманих комбінацій на відповідність умові, що забезпечує цілочисельні модулі; обчислення модулів для чисел, що відповідають умові.

Для побудови трьохмодульної криптосистеми Рабіна з метою шифрування більшого блоку відкритого тексту вибирається три великих простих числа *p, q і r*. Тоді обчислюється значення $n = p \cdot q \cdot r$, де число n — відкритий ключ, а *p, q* і *r* – закритий. Шифрування повідомлення *A* (текст) відбувається за допомогою відкритого ключа n за формулою $A' = A^2 \bmod n$.

При розшифруванні вводяться додаткові допоміжні величини $k = A' \bmod p$; $l = A' \bmod q$; $d = A' \bmod r$. Значення x, y і z шукаються з порівнянь $x^2 \equiv k(\bmod p)$, $y^2 \equiv l(\bmod q)$, $z^2 \equiv d(\bmod r)$.

Для розшифрування потрібно розв’язати вісім систем порівнянь, що утворюються як комбінації можливих варіантів пошуку відкритого повідомлення: $\begin{cases} A_i \equiv x_1(\bmod p), \\ A_i \equiv y_1(\bmod q), \\ A_i \equiv z_1(\bmod r), \end{cases}$ де i=1, …, 8, x_1=x або p-x, y_1=y або q-y, z_1=z або

r-z. Далі на основі КТЗ: $A_i = (x_1 \cdot B_1 + y_1 \cdot B_2 + z_1 \cdot B_3) \bmod n$, де $B_j = S_j m_j$, j=1, 2, 3, $S_1 = \frac{n}{p}$, $S_2 = \frac{n}{q}$, $S_3 = \frac{n}{r}$, m_j шукається з виразів $(S_j m_j) \bmod p, q, r = 1$.

Задача суттєво спрощується, коли модулі p, q, r підібрано так, що вони утворюють МДФ СЗК (m_i=±1). Це дозволяє уникнути виконання громіздкої процедури пошуку оберненого елемента за модулем та множення на m_i.

Нижче наведено приклад одного з восьми випадків розшифровування, з якого отримується правильний результат, для трьох варіантів підбору модулів (1 – модулі утворюють звичайну цілочисельну СЗК, 2 – модулі утворюють МДФ СЗК, результат обчислюється на основі КТЗ за допомогою останньої формули, 3 - модулі утворюють МДФ СЗК, результат обчислюється при умові, що m_i=±1):

1. p=11, q=13, r=17, n= 2431, A=1031; A_6=(8·1·221+4·8·187+ +11·5·143) mod2431 = (1768+5984+7865) mod2431 =15617 mod2431 = 1031;

2. p=11, q=17, r=31, n= 5797. A=1031; A_7 = (8·10·527+11·1·341+ +8·1·187) mod5797 = (42160+3751+1496) mod5797 =47407 mod5797 = 1031;

3. p=11, q=17, r=31, n= 5797. A=1031; A_7 = (-8·1·527+11·1·341+ +8·1·187) mod5797 = (-4216+3751+1496) mod5797 =1031 mod5797 = 1031.

Видно, що в третьому випадку проміжні обчислення набувають менших значень, ніж у двох інших.

На основі розробленої VHDL-моделі було проведено дослідження трьохмодульного криптоалгоритму Рабіна. Для звичайної цілочисельної СЗК (p=11, q=13, r=17 ; Word = 1024 – блок для шифрування) був отриманий час 1,4 мікросекунди, з використанням МДФ СЗК (p=11, q=17, r=31) час опрацювання становив 650 нс, тобто зменшився більш, ніж у 2 рази. Крім того, даний метод при виборі модулів одного порядку має перевагу перед класичним у стійкості за рахунок збільшення блоку відкритого тексту для шифрування.

У сьомому розділі наведено результати експериментальних досліджень опрацювання багаторозрядних чисел в асиметричних криптосистемах з використанням різних форм СЗК.

Для експериментального дослідження модулярного експоненціювання для криптосистеми RSA були вибрані чотири методи:

1) бінарний або метод пониження степеня за допомогою квадратів, який описується таким виразом:

$$N = a^x \bmod p = \left(a^{x-2x_1} a_1^{x_1-2x_2} \ldots a_i^{x_i-2x_{i+1}} \ldots\right) \bmod p = \left(\prod_{i=0}^{[\log_2 x]} a_i^{x_i-2x_{i+1}}\right) \bmod p, \quad (10)$$

де a_0=a, x_0=x, $a_i = a_{i-1}^2 \bmod p$; $x_i = \left[\frac{x_{i-1}}{2}\right]$;

2) метод пониження степеня за допомогою кубів (3-арний), який можна записати аналогічно (10):

$$N = a^x \bmod p = \left(a^{x-3x_1} a_1^{x_1-3x_2} \ldots a_i^{x_i-3x_{i+1}} \ldots\right) \bmod p = \left(\prod_{i=0}^{[\log_3 x]} a_i^{x_i-3x_{i+1}}\right) \bmod p, \quad (11)$$

де $a_0=a$, $x_0=x$, $a_i = a_{i-1}^3 \bmod p$; $x_i = \left[\frac{x_{i-1}}{3}\right]$;

3) використання звичайної цілочисельної СЗК, далі відбувається пониження степеня бінарним методом і відновлення десяткового запису числа;

4) використання модифікованої досконалої форми (МДФ) СЗК.

Для модулярного піднесення до степеня $a^x \ mod \ p$ в залежності від розрядності n_0 та кількості одиничок у двійковому записі числа (ваги Хемінга) параметри a, x та p визначалися таким чином: $a=r(n_0\text{-}3, \Delta)$, $x=r(n_0, \Delta)$, де цілочисельна функція $r(n_0,\Delta)=2^{n_0}-1-\left[RND\cdot\left[\frac{\Delta\cdot n_0}{100}\right]\right]$, $0<RND<1$ – випадкова величина, заданий параметр Δ набуває дискретних значень 0, 10, 30, 50 та 80 і вказує, що при $\Delta=0$ вага Хемінга чисел $a=2^{n_0}-1$ та $x=2^{n_0-3}-1$ дорівнює їх розрядності. Збільшення цього параметра означає, що Δ% молодших розрядів у двійковому записі a та x може змінитися випадковим чином під дією функції *RND*.

Для кожного методу піднесення до степеня використовувався один і той самий модуль, який залежить від розрядності числа x і є добутком трьох попарно взаємно простих співмножників $p=p_1\cdot p_2\cdot p_3$, що утворюють МДФ СЗК: $p_1 = 2^{\left[n_0/3\right]+1}$, $p_2=2p_1\text{-}1$, $p_3=2p_1+1$. Отримані результати при $\Delta=0$ наведені в табл. 8 (у першому стовпчику 1 – пониження степеня за допомогою квадратів, 2 – за допомогою кубів, 3 – СЗК, 4 – МДФ СЗК).

Таблиця 8 - Час виконання операції модулярного експоненціювання різними способами

Розрядність	8	16	32	64	128	256	512	1024	2048	4096
1	14	24	55	108	254	746	2251	10727	64628	405196
2	12	23	44	91	200	655	2162	11987	75411	466016
3	58	83	159	299	628	1430	3430	10366	37564	216596
4	62	72	150	266	610	1340	3195	9956	36861	208496

Як слідує з таблиці, швидкість піднесення до степеня за модулем істотно залежить від методу, яким воно виконується. Так, при малих розрядностях (до 256 включно) методи СЗК та МДФ СЗК істотно поступаються в часі двом іншим (приблизно в 2-4 рази), а найшвидше модулярне експоненціювання виконується методом пониження степеня за допомогою кубів. Це ж стосується випадку, коли $n_0=512$ і $\Delta=0$. Для інших Δ і тієї ж розрядності мінімальний час буде при використанні бінарного методу, а СЗК та МДФ СЗК вже відстають приблизно в 1,5 раза і, починаючи з $n_0=1024$ вони дають мінімальний час. При інших значеннях Δ залежності носять приблизно такий самий характер.

Для дослідження у криптосистемі Рабіна сумісного виконання алгоритму Евкліда, в якому для чисел a і b виконується послідовність операцій $a = r_0\cdot q_1 + r_1,\ q_1 = b,\ 0 \le r_1 < r_0$; $r_0 = r_1\cdot q_2 + r_2,\ 0 \le r_2 < r_1$; …,

$r_{k-2} = r_{k-1} \cdot q_k + r_k$, $0 \le r_k < r_{k-1}$; $r_{k-1} = r_k \cdot q_{k+1} + 0$, та множення в останньому пропонується використати проміжні та кінцеві результати алгоритму Евкліда таким чином: $a \cdot b = r_0^2 q_1 + r_1^2 q_2 + r_2^2 q_3 + \ldots + r_{k-1}^2 q_k + r_k$. Слід відмітити, що кількість доданків у цьому рівнянні відповідає кількості кроків у алгоритмі Евкліда. Хоча даний метод передбачає виконання більшої кількості арифметичних операцій, однак вони виконуватимуться над числами меншої розрядності. Суттєвим кроком для підвищення швидкодії буде наявність таблиці квадратів у пам'яті комп'ютера, хоча це приводить до збільшення використання ресурсів обчислювальної системи. На рис. 5 представлено графічні залежності середнього часу сумісного виконання алгоритму Евкліда та перемноження класичним (t_1) та запропонованим (t_2) методами у випадку, коли розрядність n_0 простих чисел a, яким присвоювалося значення найменшого простого числа, що перевищувало 2^{n_0}, перебуває в межах від 16 до 44 біт. Число b набувало 10000 різних значень. Як видно з рисунка, графіки розміщені практично паралельно. При великих розрядностях ($n_0 \ge 40$) інтенсивність зростання t_2 зменшується. Збільшення швидкодії становить приблизно 1,3.

Факторизація є необхідною при побудові ДФ та МДФ СЗК. На рис. 6 наведено часові характеристики програмної реалізації класичного (крива 1), вдосконаленого (крива 2) методів Ферма, а також запропонованого алгоритму (крива 3) для розрядності 32 біти при p=4294952719. Число q набуває 1000 різних значень, вибраних рівномірно із послідовності всіх 32-бітних простих чисел.

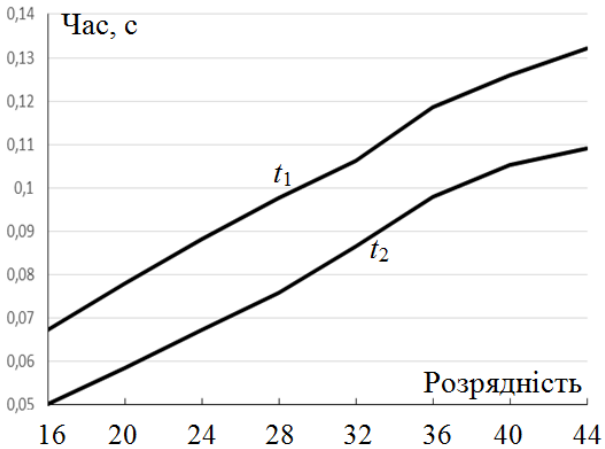

Рис. 5 - Графічна залежність середнього часу сумісного виконання алгоритму Евкліда та перемноження класичним (t_1) та запропонованим (t_2) методами від розрядності числа a

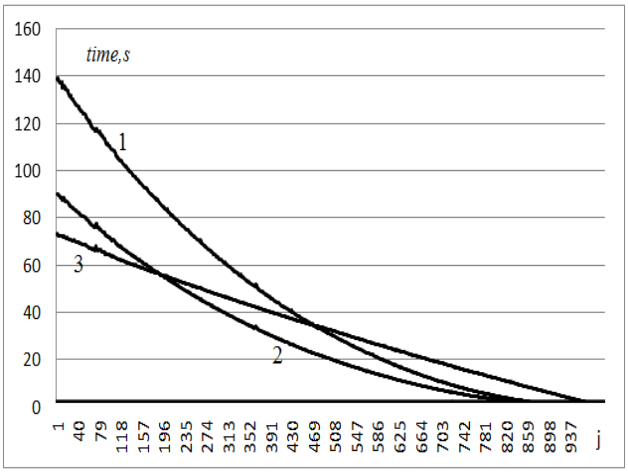

Рис. 6 - Часові характеристики програмної реалізації методів факторизації для множників розрядністю 32 біт (j – номер числа)

Усі графіки носять спадаючий характер, що свідчить про зменшення часу факторизації із зменшенням різниці між множниками, добуток яких факторизується.

Запропонований алгоритм, зменшення часу для якого відбувається лінійно, має перевагу перед двома іншими при малих значеннях q. При збільшенні q найменшим часом характеризується вдосконалений алгоритм

Ферма. Подальше зростання q приводить до того, що запропонований метод використовує найбільше часу в порівнянні з двома іншими. Отже, запропонований метод доцільно застосовувати тоді, коли велика різниця між числами, добуток яких потрібно факторизувати.

На рис. 7 показано графічну залежність середнього часу пошуку оберненого елемента на основі додавання модуля (штрихова лінія) та залишку (суцільна лінія) від кількості паралельних потоків z при n_0=1021 (рис. 7а) та n_0=65521 (рис. 7б), які є найбільшими простими десяти- та шістнадцятирозрядними числами.

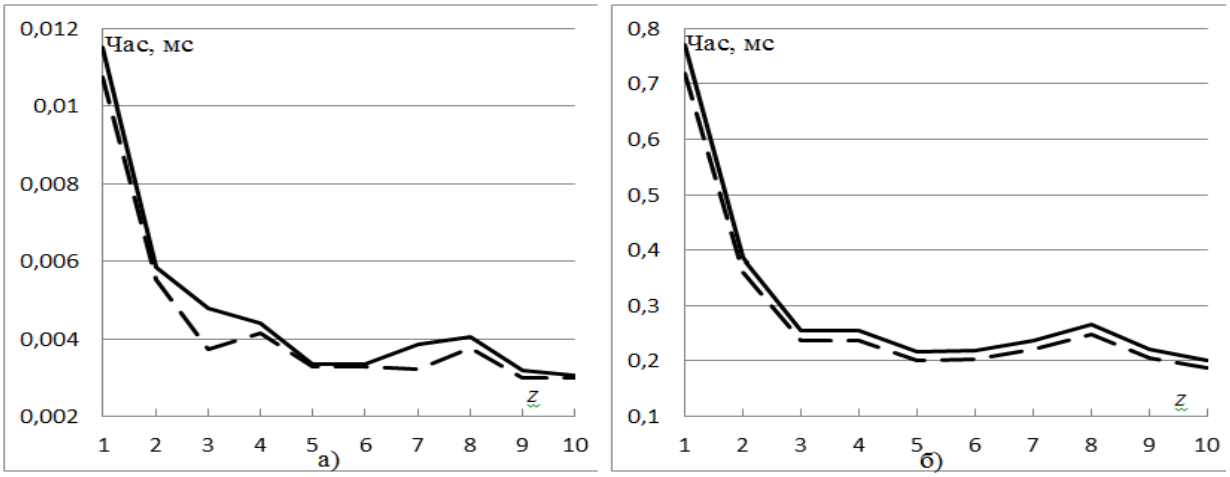

Рис. 7 - Графічна залежність середнього часу пошуку оберненого елемента на основі додавання модуля (штрихова лінія) та залишку (суцільна лінія) від кількості паралельних потоків при n_0=1021 (рис. 7а) та n_0=65521 (рис. 7б)

З рис. 7 видно, що в обох випадках метод додавання модуля володіє більшою швидкодією, ніж додавання залишку.

На рис. 8 показано графічну залежність середнього часу пошуку оберненого елемента на основі розширеного алгоритму Евкліда (крива 1) та запропонованих методів додавання модуля (штрихові лінії 3, 5) та залишку (суцільні лінії 2, 4) при z=1 (криві 2, 3) і z=6 (криві 3,5) від розрядності модуля.

Число a пробігає значення від 2 до 2^{n_0}-1 з кроком 1. Як видно з рис. 8, при використанні алгоритму Евкліда із збільшенням розрядності чисел час збільшується дуже повільно. При n_0=19 час різко зростає і далі знову наступає практично горизонтальна ділянка графіка. В обох запропонованих методах середній час збільшується приблизно параболічно, причому метод додавання модуля має більшу швидкодію. При z=1, тобто без розпаралелення, алгоритм Евкліда випереджає запропоновані алгоритми при n_0=17,5, а для z=6 – при n_0=19,5. Це вказує на необхідність розпаралелення процесу обчислень для зменшення часу пошуку оберненого елемента.

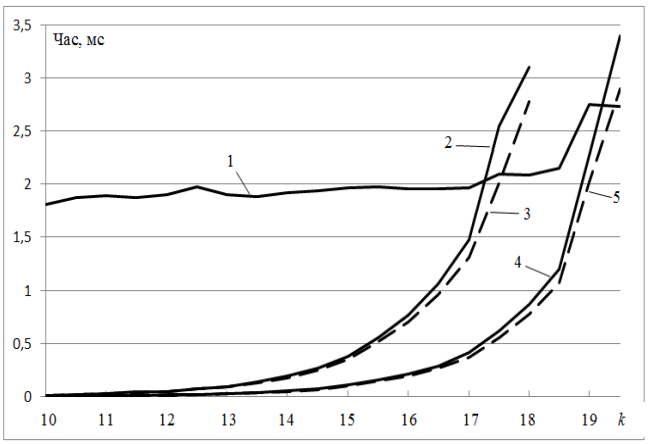

Рис. 8 – Графічна залежність часу пошуку оберненого елемента на основі розширеного алгоритму Евкліда (крива 1) та запропонованих методів додавання модуля (криві 3, 5) та залишку (криві 2, 4) при z=1 (криві 2, 3) та z=6 (криві 4,5) від розрядності модуля

Програмно - апаратну реалізацію методів пошуку оберненого елемента за модулем було здійснено на базі середовища розробки Aldec Active-HDL 9.1. При пошуку $60000^{-1}\text{mod}65537$ час роботи системи зменшився із 2,8974 мс (на основі алгоритму Евкліда) до 2,65275 мс (на основі запропонованого методу додавання залишків), тобто приблизно в 1,09 разів.

При дослідженні часових параметрів програмно-апаратної реалізації вищеназваними методами вибиралося число p=65537. Число a змінювалося від 5000 до 65000 з кроком 5000. Результати наведено в табл. 9, з якої видно, що тільки у двох із тринадцяти випадків при a=40000 та a=45000 запропонований метод поступається класичному, що пояснюється необхідністю виконання великої кількості операцій додавання.

Таблиця 9 - Часові затрати обчислення оберненого елемента за модулем

N п/п	a	$a^{-1}\text{mod}p$	Час роботи, *ns*	
			Розширений алгоритм Евкліда	Метод додавання залишку
1.	5000	20015	201300	113540
2.	10000	42776	4277500	652750
3.	15000	50363	5036200	1152750
4.	20000	21388	2138700	652750
5.	25000	4003	400200	152750
6.	30000	57950	5794900	2652750
7.	35000	40309	4030800	2152750
8.	40000	10694	1069300	3552750
9.	45000	60479	5542000	6553550
10.	50000	34770	3476900	2652750
11.	55000	37567	3756600	3152750
12.	60000	28975	2897400	2652750
13.	65000	56994	4845000	3553450
Сер. час	-	-	3343600	2280619

Середній час пошуку оберненого елемента за допомогою алгоритму Евкліда (3343600 ns) в 1,47 разів більший від аналогічного параметра з використанням додавання залишків (2280619 ns).

Експериментальне дослідження програмної реалізації трьохмодульного криптоалгоритму Рабіна здійснювалося на основі розробленої VHDL-моделі. У табл. 10 наведено час t_{1i} та t_{2i} (i=1, 2) виконання відповідно двома розглянутими методами для деяких значень простих модулів, які утворюють МДФ СЗК, та блоків відкритого тексту F_1=131071 та F_2=229376. Час для різних чисел позначений відповідно t_{j1} та t_{j2} (j=1, 2).

Таблиця 10 – Час виконання трьохмодульного криптоалгоритму Рабіна

№	p	q	r	P	F_1=131071		F_2=229376	
					t_{11}	t_{12}	t_{21}	t_{22}
1	41	71	97	282367	4100	1000	4100	1300
2	43	71	109	332777	4200	3000	4200	1900
3	41	53	181	393313	4100	900	4100	1800
4	29	31	449	403651	2900	800	2900	1300
5	37	41	379	574943	3700	1500	3700	2200
6	53	89	131	617927	5300	3200	5300	1000
7	59	79	233	1086013	5900	5500	5900	5100
8	67	101	199	1346633	6700	2900	6700	3000
9	59	71	349	1461961	7300	7200	5900	2400
10	41	43	881	1553203	5000	4900	11900	11800
11	67	89	271	1615973	6700	3600	6700	4900
12	53	59	521	1629167	9900	9800	5300	4000
13	71	101	239	1713869	7100	4600	7100	2200
14	61	71	433	1875323	6100	4200	6100	3500
15	79	131	199	2059451	7900	3200	7900	3000
16	97	109	881	9314813	9700	4900	11900	11800

Видно, що для модулів, які утворюють МДФ СЗК, використання значення m_i=±1 зменшує час криптоперетворень. При шифруванні F_1 для модулів p=41, q=53, r=181 досягається максимальна перевага приблизно в 4,6 разів. В цей же час існують модулі криптоперетворень (p=53, q=59, r=521), для яких спостерігається мінімальна перевага в 1,01 разів. Це пояснюється різною кількістю ітерацій при пошуку оберненого елемента.

У криптоперетворенні блоку F_2 максимальна і мінімальна переваги у 5,3 та 1,008 разів відповідно спостерігаються при використанні модулів p=53, q=89, r=131 та p=97, q=109, r=881. В середньому час виконання операцій при використанні МДФ СЗК для F_1 та F_2 зменшився відповідно у 1,58 і 1,63 рази, що свідчить про переваги використання МДФ СЗК.

Для експериментального дослідження множення в трьохмодульній СЗК були розглянуті чотири випадки побудови системи модулів:

1) модулі СЗК сильно відрізняються один від одного;

2) модулями є три послідовних числа, перше і третє з яких непарні: $p_1 \approx \left\lceil \sqrt[3]{2^{2n_0}} \right\rceil$, $p_2 = p_1+1$, $p_3 = p_1+2$;

3) модулі обчислюються за формулами $p_2 = p_1+1$, $p_3 = p_1(p_1+1)-1$;

4) модулі обчислюються за формулами $p_2 = 2p_1-1$, $p_3 = 2p_1+1$.

У всіх випадках добуток модулів є мінімальним, але перевищував 2^{2n_0}. В третьому та четвертому випадках системи модулів утворюють МДФ СЗК. Перший множник був фіксованим $p=2^{n_0}-1$, другий змінювався з відповідним кроком, щоб отримати 1000 значень добутків. Обчислення проводилися за формулами звичайної СЗК. Результати представлені на рис. 9. На рис. 10 представлені графіки множення для третього (крива 1) та четвертого (крива 2) випадків з використанням виразів для МДФ СЗК.

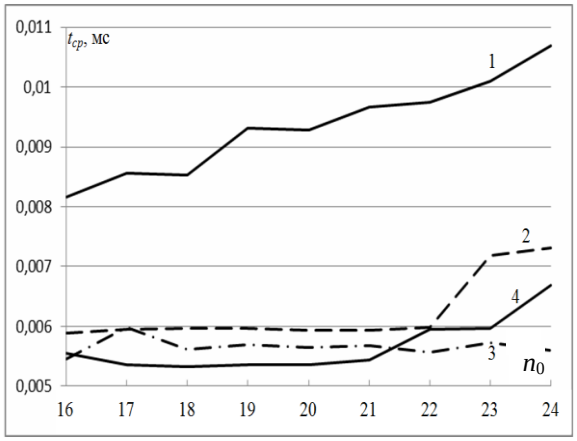

Рис. 9 - Графіки залежності середнього часу виконання операції множення в СЗК від розрядності чисел

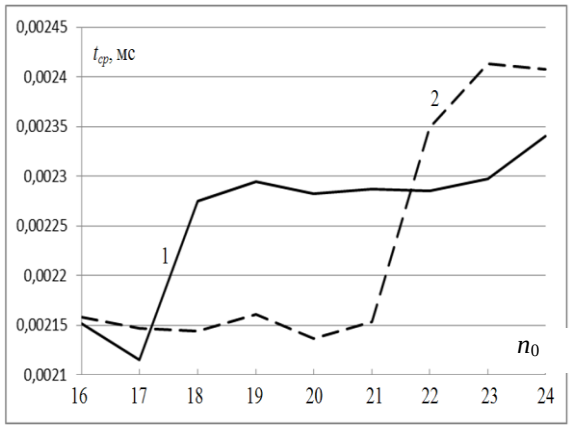

Рис. 10 - Графіки залежності середнього часу виконання операції множення від розрядності при використанні формул для МДФ СЗК

Аналіз рисунків показує, що середній час обчислень в МДФ СЗК зменшується приблизно в 2,5-3 рази.

Крім того, в заключному розділі дисертаційної роботи розроблено методологію опрацювання багаторозрядних чисел в асиметричних криптосистемах, структурно-аналітичне відображення якої представлено на рис. 11. Вона охоплює вісім базових етапів.

Етап 1. Формування множини блоків відкритого тексту. На першому етапі користувачу необхідно сформувати множину блоків відкритого тексту $BT = \left\{ \bigcup_{i=1}^{z_1} BT_i \right\} = \left\{ BT_1, BT_2, ..., BT_{z_1} \right\}$, ($z_1$ – кількість блоків відкритого тексту). Крім того, визначаються можливі загрози, які виникають при передачі даних у вигляді блоків зашифрованого тексту. В результаті формується множина загроз $MЗ = \left\{ \bigcup_{i=1}^{z_2} MЗ_i \right\} = \left\{ MЗ_1, MЗ_2, ..., MЗ_{z_2} \right\}$, ($z_2$ – їх кількість).

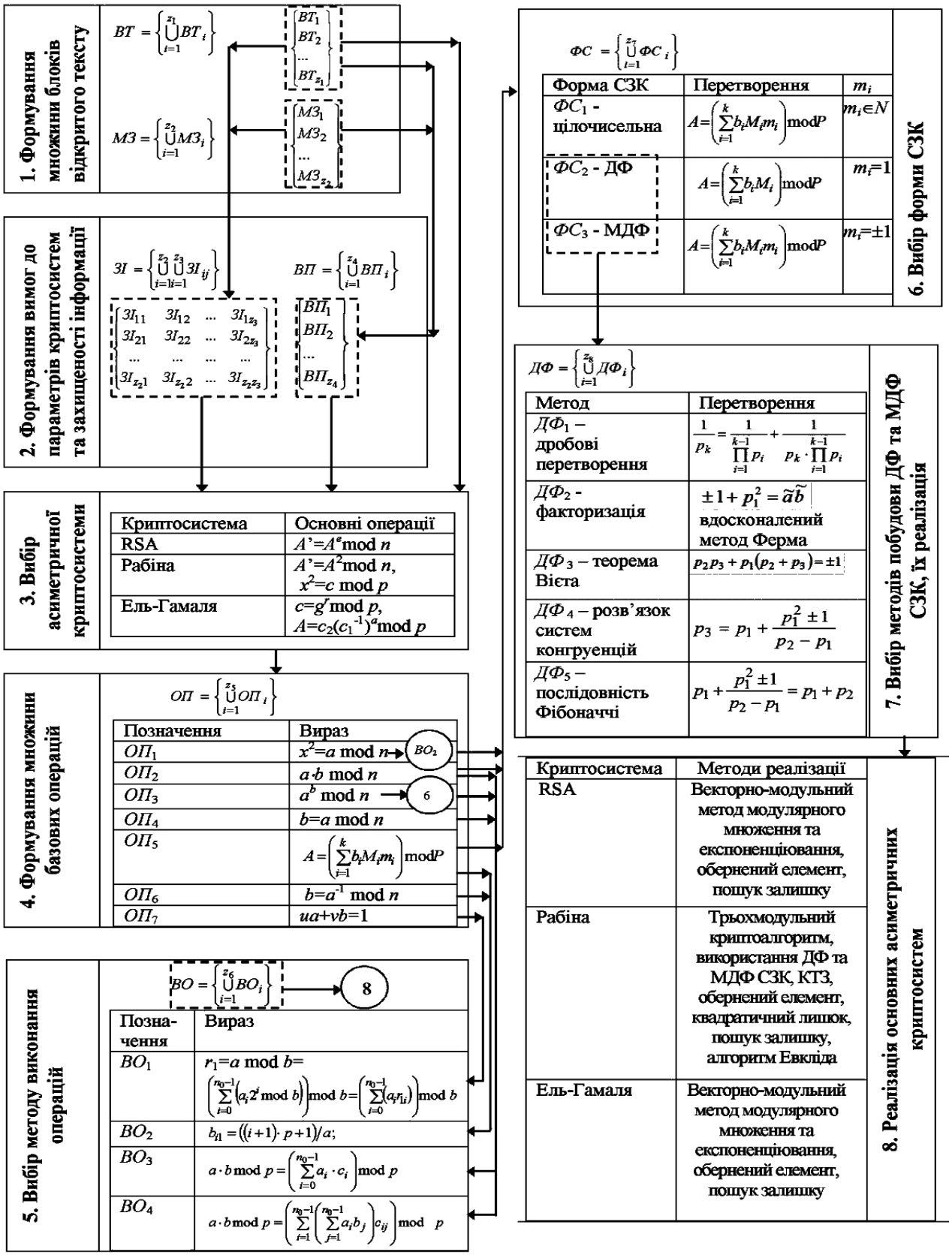

Рис. 11 – Структурно-аналітичне відображення методології опрацювання багаторозрядних чисел в асиметричних криптосистемах

Етап 2. Формування вимог до параметрів криптосистем та захищеності інформації. На основі вказаних множин відбувається формування вимог у вигляді матриці до кількісних показників захищеності інформації $ЗІ = \left\{ \bigcup_{i=1}^{z_2} \bigcup_{j=1}^{z_3} ЗІ_{ij} \right\}$ і параметрів криптосистем $ВП = \left\{ \bigcup_{i=1}^{z_4} ВП_i \right\} = \{ВП_1, ВП_2, ..., ВП_{z_4}\}$. Для кожного блоку відкритого тексту $ВТ_i, i \in [1, z_1]$ та кожної можливої загрози $МЗ_i, i \in [1, z_2]$ ставиться у відповідність множина показників захищеності $ЗІ_i = \left\{ \bigcup_{j=1}^{z_3} ЗІ_{ij} \right\} = \{ЗІ_{i1}, ЗІ_{i2}, ..., ЗІ_{iz_3}\}$, де z_3 – кількість можливих показників для i-ої загрози, та множина вимог до параметрів криптосистеми $ВП_i, i \in [1, z_4]$ (z_4 – кількість вимог).

Етап 3. Вибір асиметричної криптосистеми. Третій етап призначений для вибору асиметричної криптосистеми, найбільш поширеними з яких є RSA, Рабіна та Ель-Гамаля, згідно визначених у попередньому етапі вимог до їх параметрів. Для генерації ключів криптосистем, шифрування та розшифровування використовуються такі операції: пошук залишку, квадратного кореня за модулем, найбільшого спільного дільника, оберненого елемента, використання розширеного алгоритму Евкліда, (КТЗ), модулярне множення та модулярне експоненціювання.

Етап 4. Формування множини базових операцій. На четвертому етапі формується відповідна множина базових операцій $ОП = \left\{ \bigcup_{i=1}^{z_5} ОП_i \right\} = \{ОП_1, ОП_2, ..., ОП_{z_5}\}$, $i \in [1, z_5]$, де z_5 – кількість операцій.

Етап 5. Вибір методу виконання операцій. На п’ятому етапі відбувається формування множини методів виконання операцій, визначених на попередньому етапі: $BO = \left\{ \bigcup_{i=1}^{z_6} BO_i \right\} = \{BO_1, BO_2, ..., BO_{z_6}\}$, $i \in [1, z_6]$, де z_6 – кількість методів. Зокрема, пошук залишку, модулярне множення та експоненціювання може виконуватися матрично- або векторно-модульним методом, усі інші – методом додавання модуля або добутку модулів.

Етап 6. Вибір форми СЗК. Більшість з описаних на четвертому етапі операцій можна виконувати на основі СЗК, множина форм якої формується на шостому етапі: $ФС = \left\{ \bigcup_{i=1}^{z_7} ФС_i \right\} = \{ФС_1, ФС_2, ..., ФС_{z_7}\}$, $i \in [1, z_7]$, де z_7 – кількість форм СЗК. Поряд із звичайною цілочисельною формою, найбільш перспективними для застосування в асиметричних криптосистемах є ДФ та МДФ СЗК.

Етап 7. Вибір методів побудови ДФ та МДФ СЗК. На сьомому етапі формується множина методів побудови ДФ та МДФ СЗК:

$ДФ = \left\{ \bigcup_{i=1}^{z_8} ДФ_i \right\} = \{ДФ_1, ДФ_2, ..., ДФ_{z_8}\}$, $i \in [1, z_8]$, де z_8 – кількість методів. У дисертації розроблені методи на основі дробових перетворень, факторизації, теореми Вієта, розв'язку систем конгруенцій та послідовності Фібоначчі.

Етап 8. Реалізація основних асиметричних криптосистем. Восьмий етап передбачає реалізацію вибраної асиметричної криптосистеми (RSA, Рабіна, зокрема трьохмодульної, або Ель-Гамаля) з базовими модулярними операціями (етап 4) на основі вибору методу їх виконання (етап 5) або з використанням відповідних форм СЗК (етап 6), методи побудови яких визначені на етапі 7.

Розроблена методологія за рахунок використання матрично та векторно-модульних методів пошуку залишку, модулярного множення та експоненціювання, знаходження оберненого елемента на основі додавання модуля, використання ДФ та МДФ СЗК дозволяє забезпечити зменшення часової складності, підвищення швидкодії алгоритмів, спеціалізованого програмного і апаратного забезпечення в асиметричних криптосистемах

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 опрацювання багаторозрядних чисел на основі використання матрично- та векторно-модульного підходу до виконання операцій модулярного множення та експоненціювання, ДФ та МДФ СЗК для зменшення часової складності, підвищення швидкодії алгоритмів, спеціалізованого програмного і апаратного забезпечення в асиметричних криптосистемах. При цьому отримано такі основні теоретичні й практичні результати і наукові висновки:

1. Проведено аналіз сучасних методів, алгоритмів та засобів опрацювання багаторозрядних чисел в асиметричних криптосистемах на основі модулярної арифметики. Встановлено, що відомі методи модулярного множення та експоненціювання характеризуються значною часовою та/або апаратною складністю і не володіють властивістю розпаралелення процесу обчислень. Крім того, при опрацюванні багаторозрядних чисел все більше стали проявлятися недоліки двійкової системи числення, яка використовується в сучасних обчислювальних системах. Результати проведеного аналізу дали можливість визначити завдання дисертаційного дослідження щодо розробки методів та засобів опрацювання багаторозрядних чисел в асиметричних криптосистемах.

2. Удосконалено методи модулярного множення, модулярного експоненціювання та пошуку найбільшого спільного дільника з використанням векторно-модульних перетворень у розмежованій системі числення залишкових класів, який дає можливість замінити операції піднесення до степеня та множення на, відповідно, множення та додавання малорозрядних залишків. Це

дозволило, у порівнянні з відомими методами, зменшити обчислювальну складність модулярного множення та експоненціювання в 2-4 рази. Розроблено алгоритмічне забезпечення пошуку найбільшого спільного дільника, криптосистем RSA та Ель-Гамаля на основі векторно-модульного методу модулярного множення та експоненціювання.

3. Розроблено методи пошуку мультиплікативного оберненого елемента за модулем та реалізації китайської теореми про залишки на основі додавання модуля та додавання залишку, які не містять громіздких операцій ділення з остачею та піднесення до степеня, дозволяють виконувати розпаралелення процесу обчислень та зменшити обчислювальну складність даної операції при застосуванні в асиметричних криптосистемах. Встановлено, що при програмно-апаратній реалізації час обчислень зменшується майже в 1,5 рази в порівнянні з класичними методами.

4. Розроблено метод пошуку мультистепеневої функції за модулем, який забезпечує уникнення операції піднесення багаторозрядних чисел до степеня за модулем шляхом переходу до розв'язування лінійної конгруенції, виконання арифметичних дій над операндами, меншими від заданого модуля, та, відповідно, зменшення часової складності при опрацюванні мультистепеневої функції в асиметричних криптосистемах.

5. Розроблено загальний метод побудови спеціальних модулів системи залишкових класів у вигляді $p_1=2^u-1$, $p_2=2^u+1$, …, $p_i = 2^{u\cdot 2^{i-2}}+1$, …, $i=3, 4, \ldots$, який забезпечує аналітичний пошук коефіцієнтів базисних чисел при відновленні десяткового числа із системи залишкових класів, уникнувши операції знаходження мультиплікативного оберненого елемента за модулем.

6. Запропоновано методи побудови модулів досконалої форми системи залишкових класів на основі дробових перетворень та факторизації, що дозволяє уникнути виконання операцій знаходження мультиплікативного оберненого елемента за модулем та множення на нього при переведенні чисел із системи залишкових класів у десяткову систему числення.

7. Розроблено методи побудови трьох- та багатомодульної модифікованої досконалої форми системи залишкових класів на основі факторизації, теореми Вієта, розв'язку систем конгруенцій. Дана форма забезпечує уникнення виконання операції пошуку мультиплікативного оберненого елемента за модулем та множення на нього при переведенні чисел із системи залишкових класів у десяткову систему числення. За допомогою програмної реалізації встановлено, що використання трьохмодульної модифікованої досконалої форми при перемноженні двох чисел підвищує швидкодію обчислень в 2,5-3 рази. Обґрунтовано доцільність її використання в асиметричних криптосистемах і показано, що при програмній реалізації криптосистеми RSA збільшення швидкодії наступає при використанні чисел розрядністю не менше 1024 біти в порівнянні з відомими методами.

8. Удосконалено метод Ферма для факторизації багаторозрядних чисел, який в порівнянні з класичним методом Ферма забезпечує заміну громіздкої операції пошуку квадратного кореня операцією додавання, зменшення

розрядності операндів та спрощення методу факторизації. На основі програмної реалізації встановлено, що запропонований метод ефективніший від класичного методу Ферма для множників різної розрядності.

9. Розроблено метод сумісного виконання алгоритму Евкліда та перемноження двох багаторозрядних чисел для використання у криптосистемі Рабіна та проведено експериментальне дослідження часових характеристик класичним та розробленим методами над числами різної розрядності. Показано, що в переважній більшості розглянутих випадків запропонований метод характеризується більшою швидкодією, середній час виконання операцій зменшується приблизно в 1,3 рази.

10. Розроблено трьохмодульну криптосистему Рабіна на основі звичайної цілочисельної та модифікованої досконалої форм системи залишкових класів, яка дозволяє розширити блок шифрування відкритого тексту. Показано, що застосування модифікованої досконалої форм системи залишкових класів забезпечує зменшення значень операндів та кількість арифметичних операцій, необхідних при розшифруванні. Отримані за допомогою VHDL-моделей часові характеристики показують, що використання модифікованої досконалої форми зменшує час шифрування та розшифрування приблизно в 1,5 рази.

11. Розроблено методологію опрацювання багаторозрядних чисел на основі запропонованих методів, яка дозволяє забезпечити зменшення часової складності, підвищення швидкодії алгоритмів, спеціалізованого програмного і апаратного забезпечення в асиметричних криптосистемах. Застосування цієї методології дає можливість використовувати розроблені методи в єдиній стратегії опрацювання багаторозрядних чисел у галузі асиметричних криптосистем і ефективно будувати швидкодіючі криптографічні системи захисту інформації.

12. Комп’ютерне моделювання за допомогою розробленого програмного та програмно-апаратного забезпечення на основі застосування спеціалізованої бібліотеки А.Ленстра, об’єктно орієнтованої мови С++, програмного інтерпретатора Python, засобів VHDL для проектування на ПЛІС підтверджує основні результати, які отримані теоретично.

ОСНОВНІ ПУБЛІКАЦІЇ ЗДОБУВАЧА ЗА ТЕМОЮ ДИСЕРТАЦІЇ

1. Касянчук М. М. Досконала форма системи залишкових класів: методи побудови та застосування (Монографія). Тернопіль: Економічна думка (ТНЕУ), 2019. 224 с.
2. 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.
3. 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.

4. 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.
5. Касянчук М. Алгоритми побудови модифікованої досконалої форми системи залишкових класів. *Спеціалізовані комп'ютерні технології в інформатиці: Колективна монографія*. Під ред. Я.Николайчука. Тернопіль: Бескиди, 2017. С. 580-604. Р. 11.
6. 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.
7. Nykolaychuk Ya.M., Kasianchuk M.M., Yakymenko I.Z. Theoretical Foundations for the Analytical Computation of Coefficients of Basic Numbers of Krestenson's Transformation. *Cybernetics and Systems Analysis*. 2014. Vol. 50, № 5. P. 649-654 (Scopus).
8. Nykolaychuk Ya.M., Kasianchuk M.M., Yakymenko I.Z. Theoretical Foundations of the Modified Perfect form of Residue Number System. *Cybernetics and Systems Analysis*. 2016. Vol. 52, №2. P. 219-223 (Scopus).
9. Kasianchuk M.N., Nykolaychuk Ya.N., Yakymenko I.Z. Theory and Methods of Constructing of Modules System of the Perfect Modified Form of the System of Residual Classes. *Journal of Automation and Information Sciences*. 2016. Vol.48, №8. P.56-63 (Scopus).
10. Iakymenko I., Kasianchuk M., Kinakh I., Karpinski M. Construction of distributed thermal or piezoelectric sensor based on residue systems. *Przeglad Elektrotechniczny*. 2017. №1. P. 290-294 (Scopus).
11. Касянчук М. Построение модифицированной совершенной формы системы остаточных классов с использованием факторизации. *Радиоэлектроника, информатика, управление*. 2017. Vol.42, №3. P.53-59 (Web of Science).
12. Николайчук Я.М., Ивасьев С.В., Якименко И.З., Касянчук М.Н. Метод факторизации многоразрядных чисел на основе свойств квадратичности вычетов в системе остаточных клас сов. *Вестник Брестского государственного технического университета. Физика, математика, информатика*. 2015. № 5(95). С. 45–45.
13. Николайчук Я.Н., Ивасьев С.В., Якименко И.З., Касянчук М.Н. Метод компактной кодировки простых многоразрядных чисел в двоичной системе исчисления. *Вестник Брестского государственного технического университета. Физика, математика, информатика*. 2016. №5 (96). С. 21-23.
14. Касянчук М.Н. Экспериментальное исследование программной реализации системы остаточных классов и ее модифицированной совершенной формы.

Вестник Брестского государственного технического университета. Физика, математика, информатика. 2017. №5 (97). С. 53-57.

15. Касянчук М., Карпінський М., Казмірчук С. Методологія опрацювання багаторозрядних чисел в асиметричних криптосистемах/ *Захист інформації*. 2019. Т.21, №2. С. 65- 73.
16. Касянчук М.М., Якименко І.З., Івасьєв С.В. Криптосистема Рабіна на основі операції додавання. *Математичне та комп'ютерне моделювання: Технічні науки.* 2019. В.19. С.145-150.
17. Якименко І.З., Тимошенко Л.М., Касянчук М.М. Вибір параметрів еліптичних кривих у задачах шифрування інформаційних потоків. *Сучасна спеціальна техніка*. 2018. № 2. С. 63–71.
18. 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.
19. 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.
20. 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.
21. 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.
22. 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.
23. Касянчук М.М. Побудова модифікованої досконалої форми системи залишкових класів на основі розв'язку систем конгруенцій. *Науковий збірник Національного лісотехнічного університету України*. 2016. Т.26, №7. С. 372-377.
24. Касянчук М.М. Побудова трьохмодульної модифікованої досконалої форми системи залишкових класів на основі розв'язку квадратного рівняння. *Інформатика та математичні методи в моделюванні*. 2016. Т.6, №1. С. 19–25.
25. 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.

26. 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.
27. 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.
28. Николайчук Я. М., Касянчук М.М., Якименко І.З., Івасьєв С.В. Ефективний метод модулярного множення в теоретико-числовому базисі Радемахера–Крестенсона. *Вісник Національного університету «Львівська політехніка». Комп'ютерні системи та мережі*. 2014. № 806. С. 195-199.
29. 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.
30. 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 Радемахера-Крестенсона. *Вісник Національного університету «Львівська політехніка» «Комп'ютерні системи та мережі»*. 2012. №745. С. 190–197.
31. 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–Радемахера. *Інформатика та математичні методи в моделюванні*. 2011. №2. С. 123–130.
32. Касянчук М.М., Якименко І.З., Волинський О.І., Пітух І.Р. Теорія алгоритмів RSA та Ель–Гамаля в розмежованій системі числення Радемахера–Крестенсона. *Вісник Хмельницького національного університету. Технічні науки.* 2011. №3. С. 265-273.
33. Касянчук М.М., Якименко І.З., Николайчук Я.М. Теорія алгоритмів пошуку найбільшого спільного дільника у базисі Крестенсона. *Вісник Тернопільського національного технічного університету.* 2011. Т.16, №1. С. 154–161.
34. Касянчук М.М. Концепція теоретичних положень досконалої форми перетворення Крестенсона та його практичне застосування. *Оптико-електронні інформаційно-енергетичні технології*. 2010. №2 (20). С. 43-47.
35. Касянчук М.М., Николайчук Я.М., Якименко І.З. Теорія алгоритмів перетворень китайської теореми про залишки в матрично розмежованому базисі Радемахера–Крестенсона. *Вісник Національного університету «Львівська політехніка» «Комп'ютерні системи та мережі»*. 2010. №688. С. 118–124.
36. Яциковська У.О. Касянчук М.М., Трембач Р.Б. Удосконалена система захисту комп'ютерної мережі на підставі асиметричного шифрування. *Вісник Східноукраїнського національного університету імені Володимира Даля*. 2009. №6(136). Ч.1. С. 57–60.

37. 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. Ceske Budejovice (Czech Republic). 2019. P. 175-178 (Scopus).
38. Ivasiev S., Yakymenko I., Kasianchuk M., Shevchuk R., Tymoshenko L. The Method of Factorizing Multi-Digit Numbers Based on the Operation of Adding Odd Numbers. *Advanced Computer Information Technology* (*ACIT–2018*): Proceedings of the International Conference. Ceske Budejovice (Czech Republic). 2018. P. 232-235 (Scopus).
39. Yakymenko I.Z., Kasianchuk M.M., Ivasiev S.V., Melnyk A.M., Nykolaichuk Ya.M. Realization of RSA cryptographic algorithm based on vector-module method of modular exponention. *Modern Problems of Radio Engineering, Telecommunications and Computer Science* (*TCSET–2018*): Proceedings of the XIV–th International Conference. L'viv–Slavske. 2018. P.550-554 (Scopus).
40. Rajba T. Klos-Witkowska A., Ivasiev S., Yakymenko I., Kasianchuk M. Research of Time Characteristics of Search Methods of Inverse Element by the Module. *Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications* (*IDAACS–2017*): Proceedings of the 2017 IEEE 9th International Conference. Bucharest, Romania. V.1. September, 2017. P.82–85 (Scopus).
41. Kasianchuk M. Yakymenko I., Pazdriy I., Melnyk A., Ivasiev S. Rabin's modified method of encryption using various forms of system of residual classes. *The Experience of Designing and Application of CAD Systems in Microelectronics* (*CADSM-2017*): Proceedings of the XIV International Conference. Polyana-Svalyava. 2017. P.222-224 (Scopus).
42. 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. P.1484–1486 (Scopus).
43. 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, Telecommunica-tions and Computer Science* (*TCSET–2016*): Proceedings of the XIII–th International Conference. L'viv–Slavske. 2016. P.534-536 (Scopus).
44. 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. P.161–163 (Scopus).
45. 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. P.168-171 (Scopus).

46. 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. P.93 (Scopus).
47. Kasjanchuk M., Yakymenko I., Ivasiev S., Nykolaychuk Ya. Fundamental theoretical and algorithmic principles of the applied tasks decision of theory of numbers and construction of the high-performance special processors on their basis. *The Experience of Designing and Application of CAD Systems in Microelectronics* (*CADSM-2011*): Proceedings of the XI International Conference. Polyana-Svalyava. 2011. P.168-169 (Scopus).
48. Yakymenko I., Kasyanchuk M., Nykolaychuk Ya. Matrix Algorithms of Processing of the Information Flow in Computer Systems Based on Theoretical and Numerical Krestenson's Basis. *Modern Problems of Radio Engineering, Telecommunications and Computer Science* (*TCSET–2010*): Proceedings of the X–th International Conference. L'viv–Slavske. 2010. P.241 (Scopus).
49. Grynchyshyn T., Yakymenko I., Nykolaychuk Ya., Kasyanchuk M. The Theoretical Basis of Bisignal Formation of Information Flow in Computer Systems with Open Optical Signals. *Modern Problems of Radio Engineering, Telecommunications and Computer Science* (*TCSET–2010*): Proceedings of the X–th International Conference. L'viv–Slavske. 2010. P.222 (Scopus).
50. Andrijchuk V.A., Kuritnyk I.P., Kasyanchuk M.M., Karpinski M.P. Modern Algorithms and Methods of the Person Biometric Identification. *Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications* (*IDAACS–2005*): Proceedings of the Third IEEE Workshop. Sofia, Bulgaria. 2005. P.403–406 (Scopus).
51. Карпінський М., Кінах Я., Яциковська У., Якименко І., Касянчук М. Удосконалення архітектури комп'ютерної мережі для програмної реалізації криптоаналітичних алгоритмів. *Інформаційні моделі, системи та технології*: Матеріали V науково-технічної конференції. Тернопіль. 2018. С. 93.
52. Николайчук Я.М., Якименко І.З., Івасьєв С.В., Касянчук М.М. Метод збереження простих великорозрядних чисел у базисі Радемахера. *Питання оптимізації обчислень* (*ПОО-XXXVII*): Матеріали Міжнародної молодіжної математичної школи. Київ: Інститут кібернетики імені В.М. Глушкова НАН України. 2015. С. 159-161.
53. Касянчук М.М., Якименко І.З., Николайчук Я.М., Івасьєв С.В. Векторно-модульний метод множення багаторозрядних чисел в базисі Радемахера-Крестенсона. *Захист інформації і безпека інформаційних систем – 2014*: Матеріали Міжнародної конференції. Львів. 2014. С. 53-54.
54. Задірака В.К., Николайчук Я.М., Касянчук М.М. Теоретичні основи та високопродуктивний алгоритм обчислення мультистепеневої функції в базисі Крестенсона. *Інформаційні проблеми комп'ютерних систем, юриспруденції, енергетики, економіки, моделювання та управління* (*ПНМК-*

2010): Матеріали Міжнародної проблемно-наукової міжгалузевої конференції. 2010. Т.1, В.6. С. 30-32.

55. Kasianchuk M. Conception of theoretical bases of the accomplished form of Krestenson's transformation and its practical application. *Advanced Computer Systems and Network: Design and Application* (*ACSN–2009*): Proceedings of the 4–th International Conference. L'viv. 2009. P.299–301.
56. Касянчук М.М. Теорія та математичні закономірності досконалої форми системи залишкових класів. *Питання оптимізації обчислень* (*ПОО–XXXV*): Праці Міжнародного симпозіуму. Київ–Кацивелі. 2009. Т.1. С. 306–310.

АНОТАЦІЯ

Касянчук М.М. Методи опрацювання багаторозрядних чисел в асиметричних криптосистемах на основі модулярної арифметики. – Рукопис.

Дисертація на здобуття наукового ступеня доктора технічних наук за спеціальністю 05.13.21 – «Системи захисту інформації». – Національний авіаційний університет, Київ, 20__.

Дисертаційна робота присвячена вирішенню актуальної науково-практичної проблеми підвищення ефективності опрацювання багаторозрядних чисел на основі використання векторно-модульних методів модулярного множення та експоненціювання, ДФ та МДФ СЗК. Розроблено методи пошуку оберненого елемента за модулем та виконання КТЗ на основі додавання модуля та додавання залишку. Розроблено метод пошуку мультистепеневої функції за модулем. Розроблено методи пошуку набору модулів СЗК, який забезпечує уникнення громіздкої операції знаходження мультиплікативного оберненого елемента за модулем. Обґрунтовано доцільність використання МДФ СЗК в асиметричних криптосистемах. Удосконалено метод Ферма для факторизації багаторозрядних чисел. Розроблено трьохмодульну криптосистему Рабіна, яка дозволила розширити блок шифрування. Розроблено методологію опрацювання багаторозрядних чисел, застосування якої дає можливість використовувати розроблені методи в єдиній стратегії опрацювання багаторозрядних чисел в асиметричних криптосистем.

Ключові слова: асиметричні криптосистеми, модулярна арифметика, система залишкових класів, багаторозрядні числа, досконала та модифікована досконала форми, векторно-модульний метод, китайська теорема про залишки, мультиплікативний обернений елемент, факторизація.

АННОТАЦИЯ

Касянчук М.Н. Методы обработки многоразрядных чисел в асимметричных криптосистемах на основе модулярной арифметики. – Рукопись.

Диссертация на соискание ученой степени доктора технических наук по специальности 05.13.21 – «Системы защиты информации». – Национальный авиационный университет, Киев, 20__.

Диссертация посвящена решению актуальной научно-практической проблемы повышения эффективности обработки многоразрядных чисел на основе использования векторно-модульных методов модулярного умножения и экспоненциирования, совершенной и модифицированной совершенной форм системы остаточных классов. Разработаны методы поиска обратного элемента по модулю и выполнения китайской теоремы об остатках на основе добавления модуля и добавления остатка, которые дают возможность распараллелить процесс вычислений. Разработан метод поиска мультистепенной функции по модулю. Разработаны методы поиска набора модулей системы остаточных классов, который обеспечивает избежание громоздкой операции нахождения мультипликативного обратного элемента по модулю. Обоснована целесообразность использования модифицированной совершенной форм системы остаточных классов в асимметричных криптосистемах. Усовершенствован метод Ферма для факторизации многоразрядных чисел. Разработана трехмодульная криптосистема Рабина, которая позволила повысить быстродействие процессов шифрования и расшифровки блоков по сравнению с обычной целочисленной формой и расширить блок шифрования. Разработана методология обработки многоразрядных чисел, применение которой дает возможность использовать разработанные методы в единой стратегии обработки многоразрядных чисел в области асимметричных криптосистем.

Ключевые слова: асимметричные криптосистемы, модулярная арифметика, система остаточных классов, многоразрядные числа, совершенная и модифицированная совершенная формы, векторно-модульный метод, китайская теорема об остатках, мультипликативный обратный элемент, факторизация.

ABSTRACT

Kasianchuk M. Methods of multi-digit numbers processing in asymmetric cryptosystems based on modular arithmetic. – Manuscript.

Thesis for a Doctor of Technical Science degree in specialty 05.13.21 – «Information security systems». – National Aviation University, Kyiv, 20__.

The thesis is devoted to solving the urgent scientific and practical problem of increasing the efficiency of multi-digit numbers processing based on the use of vector-modular operations of modular multiplication and exponentiation, the perfect (PF) and the modified perfect forms (MPF) of the residue number system (RNS) to reduce time complexity, increase speed algorithms, specific software and hardware in asymmetric cryptosystems.

The methods for searching the inverse element by modulo and performing the Chinese Remainder Theorem based on adding a module and adding a remainder were developed, which make it possible to parallelize the process of searching for the inverse element by modulo and, correspondingly, reduce the time complexity of this operation when it is used in asymmetric cryptosystems by using modular operation of adding the module or remainder. A method has been developed for searching for a multi-degree function by modulo, which avoids the operation of modular exposure of multi-digit numbers due to the double use of the Euler function, performing

arithmetic operations on operands, less than a given module, and switching to linear congruence. Also, the method has been proposed for exploration of a set of RNS modules, which, by calculating the coefficients of basic numbers based on analytical expressions when restoring a decimal number from a RNS, avoided the cumbersome operation of finding the multiplicative inverse element by modulo, respectively reducing the time complexity and increasing the speed of computing systems. Methods for constructing sets of PF RNS modules on the basis of fractional transformations and factorization were developed, which could reduce the time and hardware complexity when converting numbers from RNS to a decimal number system by avoiding the search for a multiplicative inverse element by modulo and multiplying by it. Also, methods for constructing a three- and multi-module MPF RNS were discovered, which, through the use of analytical expressions obtained on the basis of fractional transformations, factorization, Viet's theorem, and solutions of congruence systems, could reduce the length of operands in intermediate calculations, and avoided the operation of searching for the inverse element modulo and multiplying by it, reducing, respectively, the time complexity when restoring a decimal number from RNS. The expediency of using the MPF RNS in asymmetric cryptosystems instead of the existing integer form was substantiated. The Fermat's method for multi-digit numbers factorization has been improved, which made it possible to reduce the lengths of operands, simplify the search for factorization of digits, and increase the speed of calculations for factors of different lengths by replacing the square root extraction and squaring at each iteration with computationally simple addition and subtraction operations. A three-module Rabin's cryptosystem was developed, which allowed to increase the speed of encryption and decryption processes compared to the usual integer form and to expand the encryption block without reducing the stability of the cryptosystem due to the generalization of the methods for constructing MPF RNS and their using. Also we have discovered the methodology of multi-digit numbers processing, which, through the use of matrix and vector-modular methods for finding the remainder, modular multiplication and exponentiation, finding the inverse element by adding a module or remainder, and also using the PF and MPF RNS, allowed to reduce the computational complexity and improve performance algorithms, specialized software and hardware in asymmetric cryptosystems. The application of presented methodology makes its possible to use the developed methods in a universal strategy for multi-digit numbers processing in the field of asymmetric cryptosystems and to efficiently build of high-speed cryptographic information protection systems.

Keywords: asymmetric cryptosystems, modular arithmetic, Residue Number System, multi-digit numbers, perfect and modified perfect forms, vector-modular method, Chinese Remainder Theorem, multiplicative inverse element, factorization.

Підписано до друку 25.11.2019.
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.