ВІДГУК
офіційного опонента

професора кафедри безпеки інформаційних систем і технологій Харківського національного університета ім.В.Н.Каразіна, д.т.н., Олійникова Романа Васильовича

на дисертацію Касянчука Михайла Миколайовича
«Методи опрацювання багаторозрядних чисел в асиметричних криптосистемах на основі модулярної арифметики»,
подану на здобуття наукового ступеня доктора технічних наук
за спеціальністю 05.13.21 – «Системи захисту інформації»

Актуальність теми дисертаційної роботи. Постійне вдосконалленя методів криптоаналізу і розвиток обчислювальних засобів, разом із подальшим зростанням рівня критичності інформаційно-телекомунікаційних систем загального призначення призводить к суттєвому збільшенню вимог до стійкості криптографічних систем і протоколів. Крім того, з'являються додаткові вимоги щодо зниження ризиків, викликаних можливою появою квантового комп'ютера для криптоаналізу та першими етапами його впровадження. Все це призводить до необхідності збільшення стійкості криптографічних засобів, в тому числі через використання більших довжин ключів традиційних асиметричних перетворень. Водночас, це призводить к зниженню продуктивності засобів криптографічного захисту інформації та зростанню вартості забезпечення необхідного рівня стійкості у разі застосування вже існуючих підходів щодо реалізації перетворень. Напрямок досліджень, орієнтований на вдосконалення ефективності багаторазрядних чисел на основі модулярної арифметики в асиметричних криптосистемах, є актуальним і необхідним як в теоретичному, так і прикладному аспектах. Це також підтверджується представленням напрямку на міжнародних наукових конференціях, конгресах та симпозіумах в Україні та за кордоном, і нізкою держбюджетних та госпдоговорних тем, в рамках яких виконана дисертаційна робота.

Ступінь обґрунтованості наукових положень, висновків та рекомендацій. Автором виконано ґрунтовний аналіз сучасних методів, алгоритмів та засобів опрацювання багаторозрядних чисел в асиметричних криптосистемах на основі модулярної арифметики. За результатами цього аналізу виділено переваги та недоліки відомих методів, обґрунтовано висновок про доцільність розроблення нових методів та засобів опрацювання багаторозрядних чисел в асиметричних криптосистемах. На основі цього аналізу обґрунтовано сформулювана мета і завдання роботи, виділені об'єкт та предмет дослідження. Основні припущення, покладені в основу теоретичних досліджень, є коректними. Наукові результати отримані на основі апробованого математичного апарату і не суперечать відомим уявленням теорії. Подальша практична перевірка теоретичних результатів продемонструвала високий ступінь їх адекватності в обраному класі задач. Результати опубліковані у фахових виданнях і мають низку актів впровадження у державних і комерційних установах, навчальних закладах Україні та за її кордонами.

Зв'язок з науковими програмами, планами, темами. Дисертаційна робота виконана у рамках науково-дослідних держбюджетних та госпдоговірних робіт 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).

Достовірність отриманих результатів. Достовірність викладених в дисертації основних наукових положень, висновків і результатів, отриманих здобувачем, забезпечується коректними постановками розв'язуваних у роботі задач та подальшим їх теоретичним аналізом, висновки якого узгоджуються з одержаними практичними результатами. Достовірність отриманих результатів також підтверджується узгодженістю теоретичних положень з практичними даними, належною апробацією на міжнародних конференціях і семінарах, а також впровадженням результатів дисертаційної роботи.

Оцінка змісту дисертації, її завершеності й оформлення. Структура дисертації відповідає дійсним вимогам. Дисертація складається з анотації, вступу, семи розділів, висновків, списку використаних джерел та додатків.

У вступі виконано обґрунтування актуальність теми досліджень; наведений зв'язок роботи з науковими програмами, планами, темами; сформульована мета і основні задачі досліджень; наведена наукова новизна і практичне значення отриманих результатів; описаний особистий внесок здобувача; надані дані про апробацію, публікації та впровадження результатів.

У першому розділі наведений аналіз відомих результатів напряму досліджень разом із базовими математичними положеннями.

У другому розділі викладені основні методи виконання модулярних аріфметичних операцій.

Третій розділ містить опис низки запропонованих методів і алгоритмів побудови досконалої форми системи залишкових класів, разом із аналізом їхніх властивостей.

Четвертий розділ присвячений методам побудови трьохмодульної модифікованої досконалої форми системи залишкових класів із відповідним аналізом і обґрунтуванням, а також чисельними прикладами.

У п'ятому розділі запропоновані теоретичні основи побудови багатомодульної модифікованої досконалої форми системи залишкових класів на основі факторизації, наведені приклади побудови відповідних конструкцій, а також інші напрямки прикладного застосування.

Шостий розділ описує програмну реалізацію запропонованих методів і алгоритмів та модель апаратного модулю для перетворень.

У сьомому розділі наведені результати експериментальних досліджень властивостей запропонованих методів і алгоритмів, а також порівняння із відомими методами.

У висновках наведений стислий опис отриманих теоретичних і прикладних результатів, із чисельними оцінками виграшу у порівнянні із вже відомими методами.

У додатки винесені акти впровадження результатів досліджень та вихідні коди розроблених програм.

Всі положення, що винесені на захист, мають належне викладення в тексті дисертаційної роботи. Зміст дисертації відповідає її назві. Робота написана та оформлена відповідно до дійсних нормативних документів.

Наукова новизна результатів дисертації. Аналіз дисертаційної роботи дозволяє зробити висновок, що здобувачем у процесі досліджень отримані такі нові наукові результати.

А) 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;

- 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;

- 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;

- 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;

- 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;

- 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;

- 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.

Б) Удосконалено і отримали подальший розвиток:

- 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;

- 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.

Теоретичне та практичне значення роботи. Представлені в роботі методи та методологія для вирішення актуальної науково-прикладної проблеми підвищення ефективності опрацювання багаторозрядних чисел в асиметричних криптосистемах на основі використання матрично- та векторно-модульного підходу виконання операцій модулярного множення та експоненціювання для зменшення часової складності для вдосконалення продуктивності криптографічних алгоритмів є важливим теоретичним розвитком відповідного напряму. Суттєве практичне значення має розроблене програмне забезпечення для прискорення асиметричних криптографічних перетворень у кільцях цілих чисел та їх допоміжних перетворень, а також апаратна модель асиметричної криптосистеми. Практична значущість додатково підкреслюється низкою актів впровадження у державних і комерційних установах, навчальних закладах Україні та за її кордонами.

Повнота викладу основних результатів у наукових виданнях та апробація. Основні положення дисертаційної роботи опубліковані в 76 наукових працях, у тому числі у 30 статтях у фахових виданнях (з них п’ять одноосібних), 5 у виданнях, індексованих базами Scopus і Web of Science (з них одна одноосібна), 3 у періодичних виданнях іноземних держав (з них одна також одноосібна). Результати пройшли необхідну апробацію на багатьох міжнародних наукових і науково-технічних конференціях, на яких опубліковано 40 матеріалів

і тез доповідей (з них п’ять одноосібних), з яких 14, що проіндексовані базами Scopus і Web of Science, розділи у 5 колективних монографіях.

Відповідність дисертації встановленим вимогам. При загальній оцінки дисертаційної роботи слід зазначити, що вона є завершеним і цілісним дослідженням з чіткою структурою і логічним викладом матеріалу, узагальнює дослідження автора, написана сучасною науково-технічною мовою. Оформлення дисертації проведено згідно з дійсними вимогами щодо докторських дисертацій. Стиль викладу результатів досліджень, наукових положень, висновків і рекомендацій забезпечує доступність її сприйняття.

Відповідність змісту автореферату основним положенням дисертації. Оформлення автореферату за своїм обсягом, структурою та змістом відповідає чинним вимогам. Зміст автореферату повністю розкриває зміст основних наукових положень дисертаційної роботи.

Рекомендації щодо використання результатів дисертації. Отримані автором методи і алгоритми доцільно використати у відповідних установах при розробці наступного покоління програмних, апаратно-програмних і апаратних комплексів криптографічного захисту інформації. Теоретичні результати, отримані при проведенні досліджень, доцільно застосувати в профільних науково-дослідних і навчальних закладах України.

Зауваження по дисертаційній роботі. Серед недоліків дисертації слід зазначити такі:

1. У третьому розділі дисертації наведений опис низки методів (побудови ДФ СЗК та ін.) і оцінки їхньої складності, але відсутній формальний опис запропонованих методів із аналітичним обґрунтуванням отриманих оцінок складності. У п’ятому розділі (стор. 209) висновки щодо кількості наборів модулів зроблені на основі чисельних досліджень, без аналітичного обґрунтування.

2. У своїх роботах автором розвинута досконала та модифікована досконала форма залишкових класів, але у тексті дисертації не наводиться формальне визначення цих термінів.

3. У формулюваннях наукової новизни, в пунктах, де отримані результати є удосконаленням або подальшим розвитком вже існуючих, не вказана відмінність від відомих результатів. У формулюваннях практичних результатів заявлено про меншу обчислювальною складність перетворень в порівнянні з відомими методами, але чисельні дані є тільки у тексті дисертації та її висновках.

4. У першому розділі (стор.45) є твердження, що довжина ключа 1024 біти вважається прийнятним варіантом. Але NIST SP 800-131A у якості такого (acceptable) допускає лише ключ довжиною від 2048 бітів.

5. Перший розділ дисертації містить не тільки огляд нових актуальних результатів у напряму досліджень, але й навчальні відомості, які відомі фахівцям із відповідною освітою (теорема Ейлера та ін.).

6. З листингу програми на стор. 228 випливає, якщо різниця між двома елементами пар має протилежний знак, то метод поверне 0 (return p1.a - p2.a + p1.b - p2.b), тобто при цієї

умови пари вважаються рівними. Крім того, використаний власний клас Pair, що відрізняється від стандартного класу Pair з JDK.

Не зрозуміло пояснення щодо роботи програми на стор.231: “отриманий добуток факторизується. Після цього перевіряється кількість елементів отриманої множини множників. Якщо кількість елементів більша одиниці (число не просте)”.

Добуток двох елементів кільця цілих чисел може бути простим виключно коли один з множників простий, а інший - одиниця. Перевірка такої умови (принанні, попередня) значно швидша, ніж факторизація та наступний підрахунок кількости множників.

7. У п.5.5 наведені додаткові корисні напрямки застосування отриманих результатів досліджень, але таки додаткові напрями знаходяться за межами обраної спеціальності (05.13.21).

Загальні висновки по дисертаційній роботі. Тема і зміст дисертації Касянчука М.М. відповідають паспорту спеціальності 05.13.21 – «Системи захисту інформації». Дисертаційна робота є завершеним науковим дослідженням і містить нові науково обґрунтовані результати, що в сукупності вирішують важливу науково-прикладну проблему підвищення ефективності опрацювання багаторозрядних чисел в асиметричних криптосистемах.

Автореферат оформлений згідно діючих вимог, що висуваються до докторських дисертацій, повністю розкриває сутність дисертації та коректно описує одержані наукові результати та висновки у роботі.

Вважаю, що дисертаційна робота Касянчука Михайла Миколайовича «Методи опрацювання багаторозрядних чисел в асиметричних криптосистемах на основі модулярної арифметики» відповідає вимогам Порядку присудження наукових ступенів, затвердженого Постановою Кабінету Міністрів України від 24.07.2013 р. №567 (із відповідними змінами), а її автор заслуговує на присудження наукового ступеня доктора технічних наук за спеціальністю 05.13.21 – «Системи захисту інформації».

Офіційний опонент:
доктор технічних наук, доцент,
професор кафедри безпеки
інформаційних систем і технологій
Харківського національного
університета ім.В.Н.Каразіна Р.В. Олійников

ПІДПИС ЗАСВІДЧУЮ
Начальник відділу кадрів