Голові спеціалізованої вченої
ради Д 26.062.17
Національного авіаційного університету
03058, м. Київ, пр. Любомира Гузара, 1

ВІДГУК
офіційного опонента
професора кафедри інформаційних технологій
Одеського державного екологічного університету,
д.т.н., професора Казакової Надії Феліксівни
на дисертаційну роботу Касянчука Михайла Миколайовича
на тему "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 обраної теми.

Стрімкий розвиток сучасних інформаційних технологій та поширення телекомунікаційних систем і мереж, крім надання якісних інформаційних послуг, зумовлюють суттєве збільшення ризиків та можливих загроз інформаційній безпеці, загострюють існуючі протиріччя між необхідністю обробки та передачі великих обсягів інформації у зазначені терміни та підвищення вимог до їх безпеки. Однак недоліки, притаманні двійковій системі числення, що найбільш поширена в сучасних обчислювальних системах, сповільнюють процес опрацювання багаторозрядних чисел при їх використанні в асиметричних криптосистемах, основними операціями в яких є модулярне множення та модулярне експоненціювання. Сучасні методи, які найчастіше використовуються для реалізації вказаних арифметичних операцій, характеризуються значною часовою та/або апаратною складністю. Тому на даний час гостро постає проблема підвищення швидкодії опрацювання багаторозрядних чисел в асиметричних криптосистемах. Одним із шляхів її вирішення є застосування системи залишкових класів (СЗК), яка дозволяє розпаралелити процес обчислень, та векторно-модульного підходу для виконання модулярного множення та експоненціювання. Тому вважаю, що тема дисертаційної роботи Касянчука Михайла Миколайовича є **актуальною**.

Також актуальність і практичне значення даної наукової роботи підтверджується виконанням ряду держбюджетних та госпдоговірних тем: "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), в яких здобувач виступав керівником, відповідальним виконавцем та виконавцем.

Наукова новизна результатів роботи.

На основі аналізу результатів дисертаційної роботи Касянчука М.М. можна зробити висновок, що найбільш суттєвими науковими результатами, які одержані в дисертації, є такі:

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 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;

3) 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;

4) 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;

5) 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;

6) 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.

Ступінь обґрунтованості та достовірність наукових положень, висновків і рекомендацій, сформульованих у дисертації підтверджується коректною постановкою завдань, науковою обґрунтованістю теоретичних положень, використанням апробованого математичного апарату, узгодженістю теоретичних положень з результатами експериментальних досліджень, опублікованими науковими працями у фахових виданнях та відповідними актами впровадження у діяльність Управління Державної служби спеціального зв'язку та захисту інформації України в Тернопільській області, Управління Державної служби України з надзвичайних ситуацій в Тернопільській області, ТзОВ НВФ «Інтеграл», ТзОВ ТКБР «Стріла», компанії «CONNECT» (ФОП Яконюк Р.А.), науковий процес Громадської організації «Міжнародна академія інформації», при виконанні п'яти науково-дослідних робіт у Тернопільському національному економічному університеті (ТНЕУ), у навчальному та науковому процесах Університету у Бельсько-Бялій (Польща), факультету комп'ютерних інформаційних технологій Тернопільського національного

економічного університету, фізико-математичного факультету Тернопільського національного педагогічного університету ім. В.Гнатюка, Академії ГУСПОЛ (Чеська Республіка).

Достовірність наукових положень, висновків і рекомендацій, які наведені в дисертаційній роботі, обґрунтовані наступними положеннями:

– строгість, коректність та достовірність результатів, які наведені в дисертаційній роботі, базуються на використанні при дослідженнях сучасного математичного апарату і методів моделювання, які є адекватними виконаним розрахункам;

– передумови, які обрані для постановки мети та вирішення задач дисертаційного дослідження, в достатній мірі аргументовані та виключають неоднозначні трактування;

– обговоренням результатів на семінарах, симпозіумах та конференціях різного рівня, науковими публікаціями здобувача основних результатів дисертаційного дослідження, його окремих матеріалів та сформульованих рекомендацій у фахових виданнях за переліками МОН України та у зарубіжних виданнях;

– методи та пропоновані рішення відповідають теоретичним положенням та практиці, які є базовими для дослідження систем захисту інформації, а також в достатній мірі корелюються з аналогічними теоретико-практичними роботами інших авторів;

– нові технології, а також пропоновані моделі та методи, які запропоновані в роботі, добре узгоджуються та не суперечать існуючим стандартам в галузі захисту інформації;

– актами впровадження отриманих результатів у науково-дослідні розробки та у виробництво.

Таким чином, викладені наукові положення, висновки та рекомендації є повністю обґрунтованими, а достовірність теоретичних положень підтверджується експериментальними даними та результатами верифікації запропонованих моделей, методів та методології.

Теоретичне та практичне значення роботи. Представлені в роботі методи та методологія опрацювання багаторозрядних чисел в асиметричних криптосистемах на основі векторно-модульного підходу модулярного множення та експоненціювання, а також використання досконалої (ДФ) та модифікованої досконалої форм (МДФ) СЗК, орієнтованих на створення засобів, що розширюють функціональні можливості сучасних систем опрацювання багаторозрядних чисел, є важливим теоретичним внеском у наукову спеціальність 05.13.21 – «Системи захисту інформації». Практичне значення отриманих результатів полягає у розробці на основі запропонованих методів алгоритмічного забезпечення для реалізації криптосистем RSA та Ель-Гамаля; програмного забезпечення для побудови ДФ та МДФ СЗК, пошуку оберненого елемента, модулярного множення та експоненціювання в цілочисельній та МДФ СЗК, сумісного виконання алгоритму Евкліда та множення, факторизації; програмно-апаратного забезпечення для пошуку оберненого елемента та реалізації трьохмодульної криптосистеми Рабіна. Вказані реалізації дозволяють розширити функціональні можливості сучасних обчислювальних систем при опрацюванні багаторозрядних чисел в асиметричних криптосистемах.

Цінною рисою дисертації є те, що створена теоретична база забезпечує побудову та впровадження методів опрацювання багаторозрядних чисел в асиметричних криптосистемах. Розроблені методи орієнтовані на сучасну елементну базу, що дає змогу їх подальшого широкого практичного застосування при створенні подібних систем.

Оцінка змісту дисертації, її завершеності й оформлення.

Структура дисертації та її оформлення відповідає прийнятим для наукового дослідження вимогам. 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 складає 380 сторінок..

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** наведено основні положення алгебри і теорії чисел, проаналізовано найбільш поширені асиметричні криптосистеми та методи факторизації, розглянуто теоретичні основи СЗК та напрямки підвищення ефективності їх використання при опрацюванні багаторозрядних чисел в асиметричних криптосистемах, визначено переваги та недоліки існуючих методів.

У другому розділі представлено схему адміністративного алгоритму, який описує застосування розроблених методів в асиметричних криптосистемах RSA, Рабіна та Ель-Гамаля.

Розроблено методи пошуку залишку, модулярного множення, модулярного експоненціювання та пошуку найбільшого спільного дільника з використанням матричних та векторно-модульних перетворень у розмежованій системі числення залишкових класів, що дозволяє зменшити обчислювальну складність при виконанні цих операцій. Запропоновано методи пошуку оберненого елемента за модулем на основі додавання модуля та додавання залишку, який дозволяє виконувати розпаралелення процесу обчислень та зменшити обчислювальну складність даної операції при застосуванні в асиметричних криптосистемах.

Розроблено алгоритмічне забезпечення для пошуку найбільшого спільного дільника, криптосистем RSA та Ель-Гамаля на основі векторно-модульного методу модулярного множення та модулярного експоненціювання. Запропоновано метод реалізації китайської теореми про залишки на основі додавання добутку модулів та залишку від добутку модулів. Розроблено метод пошуку мультистепеневої функції за модулем. Крім того, удосконалено метод Ферма для факторизації багаторозрядних чисел на основі використання на кожній ітерації тільки операцій додавання та віднімання.

У **третьому розділі** проаналізовано сучасний стан та напрямки підвищення ефективності використання різних форм СЗК, зокрема, її ДФ та МДФ, в асиметричних криптосистемах. Розроблено загальний алгоритм пошуку модулів СЗК, який дає змогу аналітично визначати коефіцієнти базисних чисел, уникнувши громіздкої операції знаходження оберненого елемента за модулем. Запропоновано алгоритм побудови модулів ДФ СЗК на основі дробових перетворень та факторизації, продемонстровано використання ДФ СЗК у китайській теоремі про залишки.

У четвертому розділі розроблено різні методи побудови трьохмодульної МДФ СЗК, зокрема, на основі перемноження модулів, факторизації, теореми Вієта, розв'язку систем конгруенцій, використання послідовності Фібоначчі. Дана форма забезпечує зменшення обчислювальної складності при переведенні чисел із СЗК у позиційну систему числення за рахунок уникнення виконання операції пошуку оберненого елемента за модулем та множення на нього. Розроблено метод побудови трьохмодульної МДФ СЗК на основі розв`язку систем конгруенцій для багаторозрядних чисел, коли відома різниця між двома першими модулями. Наведено приклади застосування розроблених методів.

У **п'ятому розділі** узагальнено методи для побудови багатомодульної МДФ СЗК, наведено приклади та на основі графічних залежностей досліджено поведінку модулів і діапазону обчислень для чотирьох- та п'ятимодульної МДФ СЗК, що дозволяє обґрунтувати вибір системи модулів в залежності від класу задач, які необхідно розв`язати. Розроблено метод розширення набору модулів МДФ СЗК для збільшення діапазону обчислень. Розроблено метод побудови розподіленого термо- або п`єзоелектричного сенсора на основі звичайної цілочисельної та МДФ СЗК, який дозволяє визначити опір кожного резистора при відомому значенні загального опору їх послідовного з`єднання.

У шостому розділі за допомогою мови програмування Java здійснена програмна реалізація методів підбору модулів ДФ та МДФ СЗК. Крім того, розроблено трьохмодульну криптосистему Рабіна на основі звичайної цілочисельної та МДФ СЗК, який дозволяє розширити блок шифрування без зменшення криптостійкості алгоритму. Показано, що застосування МДФ СЗК забезпечує зменшення значень операндів та кількість арифметичних операцій, необхідних при розшифруванні.

Сьомий розділ присвячений експериментальним дослідженням програмних та програмно-апаратних реалізацій арифметичних операцій асиметричних криптосистем на основі запропонованих методів, а також розроблена методологія опрацювання багаторозрядних чисел в асиметричних криптосистемах. Зокрема, здійснено програмну реалізацію методів модулярного експоненціювання для застосування в криптосистемі RSA, експериментальні дослідження якої показали переваги використання МДФ СЗК при розрядностях, більших 1024 біти. Запропоновано та програмно реалізовано метод сумісного виконання алгоритму Евкліда та перемноження двох багаторозрядних чисел для використання у криптосистемі Рабіна. Показано, що середній час виконання операцій зменшується приблизно в 1,3 рази. На основі експериментальних досліджень програмної реалізації методів факторизації встановлено, що запропонований метод факторизації особливо ефективним є для множників різної розрядності. На основі дослідження програмної та програмно-апаратної реалізації методів пошуку оберненого елемента встановлено, що час обчислень запропонованим методом зменшується приблизно в 1,5 разів. На основі експериментального дослідження часових характеристик VHDL-моделей трьохмодульного криптоалгоритму Рабіна встановлено, що використання МДФ СЗК дозволяє зменшити час шифрування/розшифровування приблизно в 1,5 разів. Отримані результати підтверджують достовірність основних теоретичних положень, практичних розробок та висновків наукової роботи.

Крім того, розроблено методологію опрацювання багаторозрядних чисел в асиметричних криптосистемах на основі запропонованих методів, застосування якої дає можливість використовувати розроблені методи в єдиній стратегії опрацювання багаторозрядних чисел у галузі асиметричних криптосистем і ефективно будувати швидкодіючі криптографічні системи захисту інформації.

У **висновках** стисло сформульовано основні наукові та практичні результати дисертаційної роботи.

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

Таким чином, усі положення винесені на захист, висвітлені в тексті дисертації. Зміст дисертаційної роботи відповідає її назві. Дисертація написана науковою мовою та оформлена відповідно до існуючих нормативних документів.

Рекомендації щодо використання результатів дисертації. Запропоновані у роботі математичні моделі, методи та алгоритми можуть бути використані для побудови високоефективної системи опрацювання багаторозрядних чисел, яка є складовою комплексної системи захисту інформації. Теоретичні та практичні результати роботи доцільно використовувати в установах як державного, так і приватного секторів, а також в науково-дослідних та навчальних закладах України, які займаються питаннями, пов'язаними із розробкою та аналізом ефективності функціонування криптографічних систем захисту інформаційних потоків.

Повнота викладу результатів в опублікованих працях, апробація роботи. Основні результати дисертації достатньо повно **відображені в** 76 друкованих працях (в авторефераті наведено 56), 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.

Дисертаційна робота написана зрозуміло і грамотно, науково-технічна література використовується коректно. Опубліковані роботи в повній мірі охоплюють основні результати дисертаційних досліджень.

Зміст дисертації відповідає паспорту спеціальності 05.13.21 – Системи захисту інформації, а саме пунктам 1, 3: Теоретичні, методологічні, технічні, технологічні й організаційні основи створення комплексних систем захисту інформації, зокрема інформації, що зберігається, оброблюється і передається в комп'ютерних системах і мережах; шифри, шифросистеми, криптографічні протоколи та способи вибору систем криптозахисту, адекватних прийнятій політиці безпеки інформації.

Дисертація є завершеною кваліфікаційною роботою з науковими положеннями, які характеризуються внутрішньою єдністю. Аналіз сукупності наукових результатів, поданих у роботі Касянчука М.М., дає змогу зробити висновок про їх цілісність і засвідчує особистий внесок автора в науку щодо розроблення теоретичних основ для підвищення ефективності опрацювання багаторозрядних чисел в асиметричних криптосистемах.

Автореферат дисертації.

У авторефераті дисертації з необхідною повнотою відображено загальну характеристику, основний зміст та висновки дисертації.

Зміст автореферату відображає основні положення дисертаційного дослідження та відповідає поставленій науково-технічній проблемі та сформульованим задачам..

Зауваження та питання дискусійного характеру

Незважаючи на належний рівень виконаних наукових досліджень, до дисертаційної роботи виносяться такі зауваження:

1. У першому розділі доцільно було б більше уваги звернути на відомі методи модулярного множення та експоненціювання, виділивши їх основні недоліки.
2. В п.1.3 проаналізовано кілька методів факторизації, однак в роботі використовується тільки метод Ферма. Доцільно було б провести порівняльний аналіз з іншими методами, зокрема, решета числового поля.
3. Пункт 5.5 про застосування МДФ СЗК у технічних системах, зокрема, побудова термо- або п'єзоелектричного сенсора, в принципі не має відношення до систем захисту інформації.
4. Робота перенасичена таблицями та викладками математичних розрахунків. Деякі з них можна було б винести в додатки (наприклад, з п. 5.3 та 5.5). Це ж саме стосується фрагментів програмного коду з 6 розділу.
5. Позначення параметрів у блок-схемах не завжди відповідають позначенням аналогічних параметрів у тексті дисертації.
6. На рис. 7.2 побудовано графік залежності часу модулярного експоненціювання від ваги Хемінга, однак параметр Δ змінюється нерівномірно, тому графік не зовсім коректно відображає отриману залежність.
7. У роботі відсутнє дослідження запропонованої трьохмодульної криптосистеми Рабіна на вразливість до різних типів атак.

Зазначені недоліки суттєво не впливають на загальне позитивне враження від роботи, не зменшують її якості, а також наукової та практичної цінності. Вони не є визначальними і можуть бути враховані як деякі напрямки подальших досліджень.

Висновки.

Отже, на основі вивчення дисертації, автореферату дисертації та праць здобувача, опублікованих за темою дисертації, встановлено:

1. За змістом, актуальністю, ступенем новизни, обґрунтованістю, науковою та практичною значимістю одержаних результатів дисертаційна робота Касянчука Михайла Миколайовича «Методи опрацювання багаторозрядних чисел в асиметричних криптосистемах на основі модулярної арифметики» відповідає паспорту спеціальності 05.13.21 – Системи захисту інформації.

2. Дисертаційна робота є завершеною науковою працею у якій вирішено актуальну науково-прикладну науково-прикладну проблему підвищення 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. В ній отримано нові науково обґрунтовані результати, що в сукупності вирішують важливу науково-прикладну проблему підвищення ефективності опрацювання багаторозрядних чисел в асиметричних криптосистемах.

4. Робота повністю відповідає вимогам, які висуваються до робіт на здобуття наукового ступеня доктора технічних наук, зокрема пп. 9, 10, 12 положення про «Порядок присудження наукових ступенів», затвердженого постановою Кабінету Міністрів України №567 від 24.07.2013 р. (зі змінами), а її автор а її автор, Касянчук Михайло Миколайович, заслуговує на присудження наукового ступеня доктора технічних наук за спеціальністю 05.13.21 – «Системи захисту інформації».

Офіційний опонент:
Професор кафедри інформаційних технологій
Одеського державного екологічного університету,
доктор технічних наук за спеціальністю
05.13.21 – «Системи захисту інформації», професор Н.Ф.Казакова

Підпис професора Казакової Н.Ф. засвідчую,
Проректор з наукової роботи
Одеського державного екологічного Університету
доктор географічних наук, професор Ю.С.Тучковенко

Вчений секретар
Одеського державного екологічного Університету
кандидат економічних наук, доцент О.П.Павленко