ЗАТВЕРДЖУЮ
Проректор з наукової роботи НАУ
Харченко В.П. _____
«___» _____ 2020 р.

ВІДГУК

офіційного опонента 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. Останнє десятиліття характеризується інтенсивною комп'ютеризацією усіх видів людської діяльності, що 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 симетричної та асиметричної криптографії, які не позбавлені певних недоліків. Зокрема, симетричним методам характерна проблема розподілу секретних ключів, а асиметричні є порівняно повільними і потребують значних обчислювальних ресурсів. 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. Однак збільшення об'ємів передачі конфіденційної інформації істотно загострює існуючі протиріччя між збільшенням довжини ключа, який забезпечує високу стійкість до криптоаналізу, та підвищенням вимог до швидкодії криптографічних алгоритмів

Тому вважаю, що дисертаційна робота Касянчука Михайла Миколайовича, яка присвячена розробці та дослідженню нових ефективних методів модулярного множення та експоненціювання багаторозрядних чисел на основі векторно-модульних підходів, а також використанню системи залишкових класів (СЗК), зокрема її модифікованої досконалої форми (МДФ СЗК), для розпаралелення процесів виконання арифметичних операцій, зменшення часової складності, підвищення швидкодії асиметричних криптографічних алгоритмів є важливою та актуальною і, відповідно, має теоретичне та практичне значення.

Також актуальність і практичне значення даного наукового дослідження 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 дослідницької роботи Касянчука М.М. можна зробити висновок, що найбільш суттєвими науковими результатами, які одержані в дисертації, є такі:

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

2) вперше розроблено метод пошуку мультистепеневої функції за модулем, який дозволяє уникнути виконання операції модулярного експоненціювання багаторозрядних чисел, відповідно зменшуючи часову складність;

3) 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;

4) вперше розроблено методи побудови трьох- та багатомодульної модифікованої досконалої форми системи залишкових класів, які 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;

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 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)

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 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. Побудова дисертації відповідає прийнятим для наукового дослідження вимогам. Дисертація складається з анотації, вступу, семи розділів, загальних висновків, додатків, загального списку використаних джерел.

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

У **першому розділі** проведено дослідження сучасного стану науково-технічної проблеми, пов'язаної з розробкою методів опрацювання багаторозрядних чисел в асиметричних криптосистемах, визначено переваги та недоліки розглянутих методів, а також напрямки підвищення ефективності використання різних форм СЗК в асиметричних криптосистемах.

У другому розділі представлено схему адміністративного алгоритму, який описує 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 пропонується використати векторно-модульний метод модулярного множення та експоненціювання. Згідно даного підходу представлено алгоритмічне забезпечення криптосистем RSA та Ель-Гамаля, а також пошуку найбільшого спільного дільника, уникнувши громіздкої операції ділення.

Крім того, на основі додавання модуля та залишку розроблено методи пошуку оберненого елемента за модулем та відновлення десяткового числа за його залишками, які дозволяють розпаралелити процес виконання обчислень, уникнути виконання операції ділення з остачею та зменшити розрядність операндів.

Також розроблено метод пошуку мультистепеневої функції за модулем та удосконалено метод Ферма для факторизації багаторозрядних чисел, в якому використовується тільки операція додавання.

Третій розділ присвячений розробці теоретичних основ аналітичного пошуку коефіцієнтів базисних чисел та побудови ДФ СЗК за допомогою дробових перетворень та факторизації. Використання ДФ СЗК дозволяє спростити обчислення при відновленні десяткового числа із його залишків. При цьому усувається виконання громіздкої операції пошуку оберненого елемента за модулем та множення на нього при переході із СЗК у десяткову систему числення, а застосовуються тільки операції додавання та множення, що успішно можна використати в асиметричних криптосистемах, зокрема, в криптосистемі Рабіна.

У четвертому розділі представлено теоретичні основи та методи побудови трьохмодульної МДФ СЗК за допомогою перемноження модулів, факторизації, теореми Віста, розв'язку систем конгруенцій, використання послідовності Фібоначчі. Встановлено, що при застосуванні знайдених модулів розрядність операндів, над якими виконуються проміжні арифметичні обчислення, зменшується в 2-3 рази. Найбільший діапазон обчислень буде в тому випадку, коли кожен наступний модуль на одиницю більший від добутку абсолютних величин попередніх. Крім того, використання МДФ СЗК дозволяє уникнути виконання операції пошуку оберненого елемента за модулем та множення на нього і, відповідно, зменшити часову складність при відновленні десяткового числа із СЗК. Обґрунтовано доцільність використання МДФ СЗК в асиметричних криптосистемах замість існуючої цілочисельної форми.

Отримані результати можна узагальнити для багатомодульної МДФ СЗК, розробці методів побудови якої присвячений **п'ятий розділ**. Обґрунтовано, що найдоцільніше вибрати метод на основі факторизації. 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, що дозволяє за необхідності збільшити діапазон обчислень за рахунок введення нових модулів, які утворюють МДФ СЗК.

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. 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. Отримані за допомогою VHDL-моделей часові характеристики показують, що використання МДФ СЗК зменшує час шифрування та розшифрування приблизно в 1,5 рази.

У сьомому розділі наведено результати експериментальних досліджень опрацювання багаторозрядних чисел в асиметричних криптосистемах з використанням різних форм СЗК. Здійснено програмну реалізацію методів модулярного експоненціювання для застосування в криптосистемі RSA, факторизації, запропоновано метод сумісного виконання алгоритму Евкліда та перемноження двох багаторозрядних чисел для використання у криптосистемі Рабіна та проведено експериментальне ення часових характеристик класичним та розробленим методами над числами рядності. Наведено результати дослідження часових характеристик програмної амно-апаратної реалізації методів пошуку оберненого елемента. Проведено ментальні дослідження часових характеристик VHDL-моделей трьохмодульної системи Рабіна з використанням звичайної цілочисельної форми та МДФ СЗК.

Отримані результати підтверджують достовірність основних теоретичних ожень, практичних застосунків та висновків наукової роботи.

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.

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

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

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

Рекомендації щодо використання результатів дисертації. Теоретичні та практичні результати дисертаційної 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. 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.

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 працею 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. Зміст автореферату повністю відповідає основним положенням і висновкам дисертації.

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

1. У першому розділі, зокрема, в пунктах 1.1 та 1.2, крім аналізу теоретичних основ алгебри і теорії чисел та найбільш поширених асиметричних криптосистем, доцільно було б детально і критично розглянути їх основні недоліки, виділивши ті з них, які дозволяє усунути дана робота.

2. Аналізуючи найбільш поширені асиметричні криптосистеми, автор використовує класичні схеми (рис. 1.4-1.6) криптосистем RSA, Рабіна та Ель-Гамаля, однак відсутні посилання на першоджерела.

3. У висновку до рис. 2.7 автор вказує, що «запропоновані алгоритми потребують менше часу для виконання операцій». Дане твердження доцільно було б підтвердити кількісними характеристиками.

4. В темі роботи присутній термін «багаторозрядні числа». Однак для експериментальних досліджень вони використані тільки у модулярному експоненціюванні.

5. Відсутні порівняння складностей розроблених в розділі 2 методів (зокрема, 2.10, 2.11) з існуючими. Відсутні числові значення, вказано тільки загальні переваги.

6. В четвертому розділі (зокрема, пункт 4.7) немає прив'язки розроблених методів до асиметричних криптосистем, хоча у висновку сказано «наведено приклади застосування розроблених методів та обґрунтовано доцільність використання трьохмодульної МДФ СЗК в асиметричних криптосистемах.

7. При формуванні наукової новизни, практичної цінності та висновків автор наголошує на розробленні великої низки нових методів, методології, алгоритмічного, програмного, та програмно-апаратного забезпечення, проте відсутні патенти на корисну модель, винахід чи промисловий зразок. Наявність патентів на отримані автором наукові та практичні результати підвищили б вагомість роботи, ступінь її новизни та практичне значення.

Висновки. Незважаючи на вказані зауваження та недоліки, загалом оцінка дисертаційної роботи Касянчука Михайла Миколайовича позитивна. Загалом вона характеризується внутрішньою єдністю, виконана на належному науковому рівні та є завершеною працею. В ній отримано нові науково обґрунтовані результати, що в сукупності вирішують важливу науково-прикладну проблему підвищення ефективності опрацювання багаторозрядних чисел в асиметричних криптосистемах.

За актуальністю, науковою новизною, практичною значущістю та сформульованими науковими положеннями вважаю, 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, а її автор заслуговує на присудження наукового ступеня доктора технічних наук за спеціальністю 05.13.21 – «Системи захисту інформації».

Офіційний опонент:

доктор технічних наук, професор,
заслужений діяч науки і техніки України,
лауреат Державної премії України,
професор кафедри електроніки
Національного авіаційного університету Білецький А.Я.

16.03.2020