ВІДГУК

офіційного опонента, професора кафедри безпеки інформаційних систем і технологій Харківського національного університету імені В.Н. Каразіна доктора технічних наук, професора Кузнецова Олександра Олександровича на дисертацію Ковтун Марії Григорівни «Методи удосконалення арифметичних операцій у полях, кільцях та алгебраїчних кривих для криптографічних застосувань», подану на здобуття наукового ступеня кандидата технічних наук за спеціальністю 05.13.21 – системи захисту інформації.

1. Актуальність теми дисертації

Стратегією кібербезпеки України (затвердженою Указом Президента України від 15 березня 2016 року № 96) та Доктриною інформаційної безпеки України (затвердженою Указом Президента України від 25 лютого 2017 року № 47/2017) визначено принципи, пріоритети та напрями забезпечення інформаційної та кібербезпеки України. Серед головних пріоритетів та напрямків забезпечення інформаційної та кібербезпеки визначено низку задач з впровадження послуг та механізмів захисту інформації, зокрема з безпечного функціонування і розвитку національного інформаційного простору та його інтеграції у європейський і світовий інформаційний простір; забезпечення розвитку інформаційно-комунікаційних технологій та інформаційних ресурсів України; забезпечення захищеності державної таємниці та іншої інформації, вимоги щодо захисту якої встановлені законом; розвитку і захисту технологічної інфраструктури забезпечення інформаційної та кібербезпеки України, тощо.

Відповідно до вимог та основних положень законів України «Про електронний цифровий підпис», «Про електронні документи та електронний документообіг», «Про електронні довірчі послуги» в Україні створена національна система електронного цифрового підпису, яка надає послуги виготовлення та обслуговування сертифікатів відкритих ключів більше трьох мільйонів користувачів, іде її подальше впровадження в економіку, освіту, науку, державне управління, виробництво, оборону тощо. Широке застосування електронних довірчих послуг здійснюється в ЄС, США тощо, яке суттєво поліпшило виконання електронних операцій на цифрових електронних ринках та у державному управлінні. В той же час практичний досвід експлуатації таких систем в Україні та за кордоном показує, що з часом навантаження на розгорнуту інфраструктуру стрімко зростає. Зокрема, підвищується кількість звернень до всіх складових національної системи електронного цифрового підпису та, як наслідок, виникає загроза відмови в обслуговуванні або стрімкої деградації з якості надання електронних довірчих послуг. Обмежена обчислювальна потужність програмно-технічних комплексів акредитованих центрів сертифікації ключів з часом не відповідає підвищеним вимогам. Це обумовлює об'єктивне протиріччя між підвищеними вимогами до швидкості

обробки електронних запитів із наданням відповідних послуг безпеки та існуючим станом і можливостями інформаційно-телекомунікаційних систем центрів сертифікації ключів.

Таким чином, підвищення швидкодії криптографічних операцій у інформаційно-телекомунікаційних системах центрів сертифікації ключів Національної системи електронного цифрового підпису на основі розробки та удосконалення методів арифметичних операцій над числами, поліномами і точками еліптичних кривих зі зменшеною обчислювальною складністю є надзвичайно важливою та актуальною науково-технічною задачею, яка тісно пов'язана із виконанням завдань та положень, визначених Стратегією кібербезпеки України та законами України «Про електронний цифровий підпис», «Про електронні документи та електронний документообіг», «Про електронні довірчі послуги», тощо.

2. Ступінь обґрунтованості наукових положень, висновків і рекомендацій, сформульованих в дисертації

2.1. У першому розділі дисертаційної роботи проведено аналіз програмно-технічних комплексів центрів сертифікації ключів, зроблено огляд сучасних і перспективних криптографічних перетворень з відкритим ключем, зокрема, проаналізовано поточний стан безпеки класичних криптосистем стосовно квантових комп'ютерів. На основі проведеного аналізу та узагальнення відомих результатів з різних літературних джерел автором формалізовано постановку задач наукового дослідження, зроблено певні висновки стосовно обробки програмно-технічними комплексами акредитованих центрів сертифікації ключів великої кількісті запитів (криптографічних транзакцій), сформульовано вимоги щодо швидкості формування та перевірки електронних підписів та роботи комплексів в режимі реального часу. Також відзначено перспективність переходу до криптоперетворень на кривих Едвардса.

Недоліки та зауваження за першим розділом дисертації:

- назва розділу «Особливості функціонування програмно-технічного комплекси криптографічного захисту інформації ЦСК» написано з помилкою, речення є не узгодженим;
- інколи застосовуються нестандартизовані визначення та жаргонні терміни, наприклад, «…з точки зору процесора..» (стор. 41 дисертації та стор. 7 автореферату);
- автор правильно відмічає перспективність квантової криптографії (стор. 37 дисертації), але не можна погодитися з відсутністю поточного прикладного значення цього напрямку. Як приклад можна навести розпочатий минулого року міжнародний відкритий конкурс постквантової криптографії, який проводиться національним інститутом стандартів і технологій США (NIST). За результатами цього конкурсу вже у 2022 році заплановано введення в дію низки стандартів постквантової криптографії із поступовою заміною діючих стандартів асиметричної

криптографії. Отже наукові дослідження та дискусійні питання, які стосуються діючих стандартів асиметричної криптографії, зокрема і тих криптоперетворень, що розглядаються в дисертації, вже через кілька років втратять свою актуальність та затребуваність. Однак отримані в дисертації результати будуть затребувані на перехідний період, який, як правильно відмічає автор дисертації, буде пов'язаний із побудовою квантових комп'ютерів із великим числом кубітів, достатнім для ефективного криптоаналізу існуючих асиметричних криптосистем;

- за текстом дисертації зустрічаються певні стилістичні вади та помилки. Зокрема, відповідно до ДСТУ 3008:2015 «Інформація та документація. Звіти у сфері науки і техніки. Структура та правила оформлювання» рисунки та таблиці дозволено нумерувати в межах розділу, тобто номер рисунка або таблиці складається з номера розділу та порядкового номера рисунка або таблиці, відокремлених крапкою, наприклад, «Таблиця 2.1» – перша таблиця другого розділу. В дисертації застосовується нумерація рисунків та таблиць в межах підрозділу, наприклад «Таблиця 1.3.2». На таблицю 1.2.2 за текстом дисертації немає посилання.

2.2. У другому розділі «Розробка методу підвищення швидкодії арифметичних операцій над цілими числами» проведено дослідження методу ділення «в стовпчик» великих цілих чисел та запропоновано удосконалення методу. Зроблено оцінку обчислювальної складності та наведено результати експериментальних оцінок швидкодії розробленого методу. Досліджено продуктивність удосконаленого методу для Національної системи електронного цифрового підпису України, зроблено певні висновки, зокрема, наведено оцінку обчислювальної складності методу прототипу та удосконаленого методу, показано виграш щодо зменшення кількості обчислювально складних операцій порівняння за рахунок арифметичних операцій, які швидше виконуються сучасними процесорами із можливістю розпаралелювання.

Недоліки та зауваження за другим розділом дисертації:

- другий розділ присвячений удосконаленню методу ділення великих цілих чисел в стовпчик для криптосистеми RSA, хоча в меті та завданнях роботи про криптосистему RSA не йдеться. Це застаріла система, яку необхідно замінювати на більш ефективні перетворення в групі точок ЕК;
- деякі таблиці містять вибіркові оцінки певних параметрів, які отримані за лише одним спостереженням. З наведених даних складно з'ясувати точність та достовірність наведених оцінок, переконатися в конструктивності певних висновків. Наприклад, у таблиці 2.5.1 дисертації (у таблиці 3 автореферату) наводяться результати експериментальної оцінки часу генерації ключів RSA, причому задекларований виграш складає від 7% до 14%. Яка точність наведених експериментальних оцінок? Якщо можлива похибка у 20% тоді наведені значення не конструктивні, довіряти їм не можна.

2.3. Третій розділ дисертації «Розробка методів підвищення швидкодії арифметичних операцій у двійковому полі» присвячено дослідженню операцій мультиплікативного інвертування на основі розширеного алгоритму Евкліда та його удосконаленню, розробці методу автоматизації приведення довільного полінома за фіксованим модулем у двійковому полі та оцінці обчислювальної складності. В розділі наводяться також результати експериментальних оцінок швидкодії розробленого методу, швидкодії реалізацій операції мультиплікативного інвертування на основі розширеного алгоритму Евкліда, швидкодії реалізацій операції приведення по модулю, результати оцінки продуктивності удосконалених методів для Національної системи електронного цифрового підпису України. У висновках наголошено про зменшення обчислювальної складності запропонованих методів, що підтверджується експериментальними оцінками, та про виграш при використанні запропонованих методів для Національної системи електронного цифрового підпису України.

Недоліки та зауваження за третім розділом дисертації:

- зазвичай отримання нових позитивних якостей відбувається за рахунок певних втрат ресурсів чи часу, тобто кожне вдосконалення є, певною мірою, обміном, за рахунок якого вдається досягти цільового результату. Але автор ці питання зовсім ігнорує і не вказує за рахунок яких втрат досягаються певні позитивні якості. Наприклад, зменшення обчислювальної складності найчастіше досягається за рахунок збільшення ємнісної складності, тобто шляхом обміну додаткових витрат пам'яті на певний виграш у кількості операцій. Необхідно було вказати відповідні втрати для всіх здобутих удосконалень (ділення великих цілих чисел в стовпчик, мультиплікативного інвертування, здобуття кореня в полі, пошуку біраціонально еквівалентних кривих);
- деякі висновки подано у формі анотацій, наприклад, п. 6 «Розроблено метод автоматизації приведення довільного полінома за фіксованим модулем у двійковому полі (тричлена, п'ятичлена)». Це є найпоширенішою помилкою здобувачів. У висновках зазвичай наводять оцінку одержаних результатів і їх відповідність сучасному рівню наукових і технічних знань, наголошують на кількісних та якісних показниках здобутих результатів, їх прикладному значенні та можливості практичного впровадження, тощо.

2.4. У четвертому розділі «Розробка методу вилучення коренів в двійковому полі» дисертації досліджуються операції здобуття кореня в двійковому полі, розробляються удосконалені методи здобуття кубічного кореня та n-вимірного кореня. Проводиться оцінка обчислювальної складності та наводяться результати експериментальних оцінок швидкодії. У висновках наголошено на здобутому виграші в обчислювальної складності удосконалених алгоритмів та на результатах статистичного тестування щодо часу реалізації різних методів.

До недоліків, як і в попередньому розділі, слід віднести певну однобічність зроблених оцінок, зокрема, необхідно було вказати відповідні втрати для всіх здобутих удосконалень, тобто зазначити що є «платою» за досягнення цільового результату.

2.5. У п'ятому розділі «Розробка методу підвищення швидкодії та захищеності криптографічних перетворень на еліптичних кривих у двійковому полі» розробляється удосконалений метод скалярного множення точок еліптичної кривої з проміжними обчисленнями на кривій Едвардса, досліджуються процедури пошуку біраціонально еквівалентних повних кривих Едвардса до кривих Вейерштрасса у двійковому полі, наводяться оцінки обчислювальної складності та результати експериментальних оцінок швидкодії розробленого методу, досліджується продуктивність його використання на двійкових кривих Едвардса для Національної системи електронного цифрового підпису України. У висновках наголошено на кількісних та якісних показниках здобутих результатів, зокрема, наведено оцінки виграшу при застосуванні запропонованого методу.

Недоліки та зауваження:

- На оцінки обчислювальної складності, які наведено в більшості таблиць, впливає багато різних факторів, зокрема конфігурації операційної системи, спеціалізованого програмного забезпечення, компіляторів, характеристики обчислювальної системи, на якій проводилися експериментальні дослідження, тощо. В дисертації не пояснюється з яких міркувань було обрано ці налаштування, який вплив вони мають на отримані оцінки та на зроблені висновки і рекомендації. Зокрема, не зрозумілим виглядає застосування різних обчислювальних систем для проведення досліджень у різних частинах роботи. Наприклад, оцінка часу виконання транзакцій з ЕЦП (таблиця 1 автореферату) проводилася за допомогою обчислювальної системи з процесором Intel Core i7-6700 2,60 GHz, під управлінням ОС Windows 10 x86-64; експериментальні дослідження методу ділення великих цілих чисел в стовпчик (таблиця 2 автореферату) проводилися за допомогою іншої обчислювальної системи з процесором Intel Core i3 M350 (PC1) і Intel Xeon E5 - 2640 (PC2) під управлінням ОС Windows 7 SP1 x86-64; дослідження удосконаленого розширеного алгоритму Евкліда для мультиплікативного інвертування - на мобільних процесорах Intel Core i3 M350 і настільних процесорах Intel Core i5-3570, Intel Core i5-4670 під управлінням ОС Windows 7 SP1 x86-64 і т.д. Чому не можна було провести всі дослідження на однакових платформах, навіть якщо їх буде декілька? Яким чином зміняться відносні показники швидкодії при зміні обчислювальної або операційної системи? Чи буде спостерігатися задекларований виграш при застосуванні інших конфігурацій компіляторів або використовуючи системи із інтерпретаторами?

3. Достовірність отриманих результатів

Достовірність результатів дисертаційної роботи підтверджується збіжністю отриманих результатів експериментальних досліджень шляхом імітаційного та комп'ютерного моделювання з теоретичними результатами та аналітичними співвідношеннями. Достовірність отриманих результатів обґрунтовується їх несуперечністю основним положенням математичного апарату теорії складності алгоритмів, теорії чисел, теорії груп, полів, кілець, прикладної криптології, методів математичного та комп'ютерного моделювання, теорії ймовірностей та математичної статистики.

4. Новизна отриманих результатів

У дисертаційній роботі Ковтун М.Г. «Методи удосконалення арифметичних операцій у полях, кільцях та алгебраїчних кривих для криптографічних застосувань» отримано теоретичне узагальнення та нове вирішення актуальної науково-прикладної задачі, яка полягає в розробці та удосконаленні методів арифметичних перетворень над числами, поліномами і точками еліптичної кривої зі зменшеною обчислювальною складністю для підвищення швидкодії інформаційно-телекомунікаційних систем центрів сертифікації ключів Національної системи електронного цифрового підпису України.

Отримано такі **науково обґрунтовані результати**.

- вперше розроблено метод автоматизації приведення довільного полінома за фіксованим модулем, що враховує степені членів для заданого тричлена та п'ятичленна, що не приводиться, для різних цільових апаратних платформ;
- удосконалено метод скалярного множення в групі точок еліптичної кривої, який за рахунок проміжних обчислень на кривій Едвардса дозволяє підвищити стійкість до атак на реалізацію та підвищити швидкодію при генерації ключів, накладанні та перевірці електронного підпису;
- удосконалено метод здобуття n-вимірного кореня на прикладі кубічного кореня, який за рахунок розкладу показника степеню за допомогою адитивного ланцюга на множники, дозволяє зменшити обчислювальну складність алгоритму пошуку бірaціонально еквівалентних кривих Едвардса до кривих Вейерштрасса;
- удосконалено метод ділення «в стовпчик» великих цілих чисел, який за рахунок спрощення операції порівняння великих чисел, враховуючи двійкову довжину чисел, проведення операцій зсуву, додавання і віднімання за значущими словами, дозволяє знизити обчислювальну складність звичайного та розширеного алгоритму Евкліда;
- удосконалено метод мультиплікативного інвертування на основі розширеного алгоритму Евкліда, який дозволяє знизити обчислювальну

складність при генерації ключів, накладанні та перевірці електронного підпису.

5. Завершеність, стиль викладення, публікації

5.1. Аналіз сукупності наукових результатів і положень, характеристику яких наведено в пп. 2-4, дозволяє зробити висновок про їх внутрішню єдність і засвідчує особистий внесок автора у науку. У дисертаційній роботі отримано розвиток методів арифметичних перетворень над числами, поліномами і точками еліптичної кривої зі зменшеною обчислювальною складністю для підвищення швидкодії інформаційно-телекомунікаційних систем центрів сертифікації ключів Національної системи електронного цифрового підпису України.

5.2. Дисертація є завершеною науковою роботою, виконаною і оформленою відповідно до встановлених вимог.

5.3. Дисертаційна робота написана зрозуміло і грамотно, науково-технічна термінологія використовується коректно, структура роботи логічна.

5.4. Основні результати досліджень опубліковані досить повно у в 20 наукових публікаціях: 7 наукових статей (4 – у міжнародних рецензованих виданнях, що входять до баз даних Scopus та 3 – у вітчизняних фахових наукових журналах), 1 розділ колективної монографії, 3 патенти України на корисну модель, 9 матеріалів та тез доповідей.

5.5. Структура і зміст автореферату повністю відповідає тексту дисертації.

6. Практична значимість

6.1. В дисертаційній роботі розроблено спеціальне програмне та математичне забезпечення та практичні рекомендації щодо впровадження отриманих наукових та практичних результатів, зокрема:

- алгоритму ділення великих цілих чисел «в стовпчик», який дозволив підвищити швидкодію в 1,5-3 разів для чисел однакової довжини починаючи з довжини числа 512 біт, і з 128 біт для випадку, коли різниця в довжині між діленим та дільником складає 2 рази;
- алгоритму мультиплікативного інвертування на основі розширеного алгоритму Евкліда, який дозволив підвищити швидкодію реалізації в 1.2-1.8 разів відносно алгоритму прототипу;
- алгоритму побудови процедури приведення за фіксованим модулем, який дозволяє будувати алгоритми для поліномів, що не приводяться, на різних цільових платформах, що дозволяють збільшити швидкодію операції приведення за модулем у 34-197 разів зі зростанням двійкової довжини відносно звичайного побітового алгоритму;
- алгоритму здобуття n-вимірного кореня на прикладі здобуття кубічного кореня, який дозволив зменшити обчислювальну складність в 4-4.9 разів і

підвищити швидкодію в 2,8-3,7 разів зі зростанням двійкової довжини елемента поля;

- алгоритму скалярного множення на основі удосконаленого методу з використанням проміжних обчислень на кривій Едвардса, який дозволив підвищити швидкодію скалярного множення на 6%, формування підпису на 5-7% та перевірки підпису на 6-7%.

6.2. Розроблене спеціальне програмне та математичне забезпечення реалізовано у бібліотеках криптографічних примітивів «Шифр+v.2.1» системи криптографічного захисту інформації «Шифр-Х.509», що має дійсний позитивний експертний висновок Держспецзв'язку України від 16.05.2017 №04/03/02- 1674 (Акт від 29.09.2017 р. №12/09-17).

6.3. Отримані наукові та практичні результати дисертаційних досліджень впроваджено у навчальний процес кафедри безпеки інформаційних технологій НАУ (Акт від 18.01.2018 р.).

7. Недоліки та зауваження

Основні недоліки та зауваження викладено при аналізі наукових результатів дисертанта (п.2). Додатково слід зазначити, що при розкритті наукових результатів в авторефераті описано підходи, за рахунок яких вдалося отримати нові позитивні якості, але самі результати докладно не описано. Зокрема, необхідно було навести обчислювальні алгоритми: ділення великих цілих чисел в стовпчик (2 розділ), мультиплікативного інвертування (3 розділ), здобуття кореня в полі (4 розділ), пошуку біраціонально еквівалентних кривих (5 розділ) та вказати, чим саме вони відрізняються від відомих алгоритмів. Застосована стилістика викладення результатів ускладнює критичний аналіз здобутих результатів та їх порівняння із відомими напрацюваннями.

Але вищеозначені недоліки та зауваження не впливають на загальний позитивний висновок про дисертаційну роботу.

8. Загальні висновки

8.1. Дисертація є закінченою науково-дослідною роботою, яка містить теоретичне узагальнення та нове рішення актуальної науково-прикладної задачі, яка полягає в розробці та удосконаленні методів арифметичних перетворень над числами, поліномами і точками еліптичної кривої зі зменшеною обчислювальною складністю для підвищення швидкодії інформаційно-телекомунікаційних систем центрів сертифікації ключів Національної системи електронного цифрового підпису України.

8.2. Зміст дисертації відповідає паспорту спеціальності 05.13.21 – системи захисту інформації.

8.3. Дисертаційна робота Ковтун М.Г. «Методи удосконалення арифметичних операцій у полях, кільцях та алгебраїчних кривих для криптографічних застосувань» має певну наукову новизну і практичну

значимість у галузі безпеки інформаційних технологій, відповідає вимогам п. 9-14 "Порядку присудження наукових ступенів", а її автор заслуговує присудження наукового ступеня кандидата технічних наук.

Професор кафедри безпеки інформаційних систем і технологій
Харківського національного університету імені В.Н. Каразіна
доктор технічних наук, професор О.О. КУЗНЕЦОВ

"13" ЧЕРВНЯ 2018 р.

Підпис доктора технічних наук,
професора КУЗНЕЦОВА О.О. засвідчую.

Підпис О.О. Кузнецов
ЗАСВІДЧУЮ
Учений секретар Харківського національного
університету імені В.Н.Каразіна