Голові спеціалізованої вченої
ради Д 26.062.17
Національного авіаційного університету
03680, м. Київ, проспект
Космонавта Комарова,1

ВІДГУК
офіційного опонента
на дисертацію Ковтун Марії Григорівни
на тему «Методи удосконалення арифметичних операцій у полях, кільцях та алгебраїчних кривих для криптографічних застосувань», поданої на здобуття наукового ступеня кандидата технічних наук за спеціальністю 05.13.21 – «Системи захисту інформації»

Детальний аналіз дисертації Ковтун М.Г. «Методи удосконалення арифметичних операцій у полях, кільцях та алгебраїчних кривих для криптографічних застосувань» дозволяє сформулювати наступні узагальнені висновки щодо актуальності, ступеня обґрунтованості основних наукових положень, висновків, рекомендацій, достовірності наукової новизни, практичного значення, а також загальної оцінки роботи.

Актуальність. Світові глобалізаційні процеси відображаються і в Україні – відбувається автоматизація управлінських процесів, що дозволяє ліквідувати багато рутинних операцій, підвищуючи комфортність та продуктивність роботи. В Україні розгорнуто Національну систему електронного цифрового підпису (ЕЦП), яка дозволяє забезпечити юридичну значущість процесів електронного документообігу, завдяки тому, що ЕЦП прирівнюється до власноручного підпису. Кількість сфер де використовується ЕЦП зростає, а також налагоджується інтероперабельність (розгорнуто гілки для RSA та ECDSA у Центральному засвідчувальному органі) між іноземними системами. Це вимагає від Національної системи ЕЦП – постійної модернізації, оскільки кількість звернень до складових частин, центрів сертифікації ключів, зростає. Також з'являються періодичні сезонні імпульси, викликані здачею податкової звітності, торгів, закупівель, подачею деклараціями держслужбовцями тощо, можуть створити певні навантаження, які призведуть до неякісного обслуговування. Тому як до Національної системи ЕЦП, так і до центрів сертифікації ключів (ЦСК), висувають жорсткі вимоги щодо швидкодії та надійності.

Дисертаційна робота Ковтун Марії Григорівни спрямована на *розв'язання актуальної науково-технічної задачі*, яка має практичне та теоретичне значення. Зокрема, направлена підвищення швидкодії криптографічних операцій у інформаційно-телекомунікаційних системах ЦСК Національної системи ЕЦП, шляхом зменшення обчислювальної складності алгоритмів криптографічних перетворень на основі розробки та удосконалення методів арифметичних операцій над числами, поліномами і точками еліптичної кривої зі зменшеною обчислювальною складністю.

Одержані автором результати роботи відображені у звітах держбюджетних НДР Національного авіаційного університету «Квантово-криптографічні методи захисту критичної інформаційної інфраструктури держави» (д.р. № 0117U006770), «Методи забезпечення конфіденційності державних інформаційних ресурсів в інформаційно-комунікаційних системах» (№ 61/09.01.08), «Новітні технології криптографічного захисту інформації» (№ 100/14.01.06).

Оцінка обґрунтованості та достовірності наукових положень, висновків та рекомендацій.

Ступінь обґрунтованості наукових положень, висновків та рекомендації у дисертації обумовлена коректністю застосувань сучасних методів оцінки складності алгоритмів та теорії алгоритмів (для аналізу складності алгоритму скалярного множення та арифметичних операцій у групі точок еліптичної кривої (ЕК), полях та кільцях); теорії криптографії (для аналізу криптографічних перетворень, побудованих на ЕК, полях та кільцях); ймовірності та комбінаторики (для аналізу складності алгоритмів); теорії еліптичних кривих (для удосконалення арифметичних операцій на ЕК у формі Вейерштрасса та Едвардса, пошуку біраціонально еквівалентних відображень кривої Вейерштрасса до кривої Едвардса); теорії кілець, полів та ідеалів (для удосконалення методів мультиплікативного інвертування у полі $GF(2^m)$, здобуття кубічного кореня у полі $GF(2^m)$, приведенням полінома за фіксованим модулем у полі $GF(2^m)$, ділення великих цілих чисел у полі $GF(p)$ та кільці цілих чисел).

Робота має чітку послідовність постановки задач та отриманих рішень, достатню доказову базу та аргументованість результатів.

У вступі автором представлена загальна характеристика роботи, обґрунтована актуальність наукової теми, сформульовані мета та задачі, відображено наукову новизну та практичну цінність отриманих результатів і висновків, наведено дані щодо їх апробації та впровадження.

У першому розділі проаналізовано вітчизняну та зарубіжну літературу за темою дисертаційного дослідження. Розглянуто побудову та функціонування інформаційно-телекомунікаційних систем (ІТС) ЦСК Національної системи ЕЦП. Розглянуто існуючі методи арифметичних операцій, на основі яких було обрано методи для удосконалення з метою підвищення швидкодії роботи ІТС ЦСК, доповнено класифікацію по методам ділення великих цілих чисел та приведення за модулем. Також був проведений аналіз розробки квантових комп'ютерів та квантового криптоаналізу.

Другий розділ спрямований на удосконалення методу ділення великих цілих чисел для криптосистеми RSA, який розглядає два випадки: однакова двійкова довжина – кількість машинних слів діленого та дільника однакові, двійкова довжина діленого в 2 рази перевищує довжину дільника (результат отриманий після операції множення або піднесення до квадрату). Проведений аналіз методу прототипу, дозволив виявити недоліки, які вдалося усунути в удосконаленому методі, який застосовувався в звичайному та розширеному

алгоритмі Евкліда: перевірка двох чисел на простоту, та знаходження оберненого елемента.

Знизити обчислювальну складність операції ділення і підвищити швидкодію реалізації вдалося за рахунок наступних підходів: при порівнянні великих цілих чисел порівнювати номера старших бітів, а в разі їх рівності, проводити порівняння лише за значимими словами; проводити зсуви за одну ітерацію, знаючи різницю (більше 0) номерів старших бітів. При зсувах вправо використовувати лише значущі слова, а вліво – значущі слова, з урахуванням можливого переносу; проводити операцію віднімання за значущими словами, оскільки зменшуване більше від'ємника.

Наводиться оцінка обчислювальної складності, перевірка статистичної гіпотези щодо однорідності двох незалежних вибірок – часу реалізації методу прототипу та удосконаленого та практична реалізація, а також вплив модифікованого методу при генерації ключів RSA.

У третьому розділі розглядається удосконалення методу мультиплікативного інвертування у двійковому полі на основі розширеного алгоритму Евкліда, та розробляється метод автоматизації приведення довільного полінома (тричлена, п'ятичлена) за фіксованим модулем.

При аналізі методу мультиплікативного алгоритму Евкліда було виявлено ряд аспектів для подальшого удосконалення: застосування методів «наступного відповідного», «врахування значущих елементів», проводити операції додавання і зсуву поліномів лише за значущими словами, застосування алгоритму-трюку «обчислення номера старшого значущого біта» в машинному слові, без операції галуження.

Запропонований метод автоматизації приведення довільного полінома за фіксованим модулем (на прикладі, тричлена та п'ятичлена), дозволяє будувати послівні алгоритми приведення довільного полінома, отриманого в результаті множення або піднесення до квадрату у двійковому полі (довжина якого становить подвійну довжину полінома, що не приводиться) в не залежності від степенів полінома, що не приводиться.

Наводиться оцінка обчислювальної складності, перевірка статистичної гіпотези щодо однорідності двох незалежних вибірок – часу реалізації методу мультиплікативного інвертування Евкліда та удосконаленого. Також представлена практична реалізація удосконаленого і розробленого методів, вплив при формуванні та перевірці ЕЦП згідно ДСТУ 4145-2002.

У четвертому розділі удосконалено метод здобуття n-вимірного кореня в полі $GF(2^m)$, де m – непарне, на прикладі кубічного кореня, за допомогою розкладу адитивного ланцюга показника степеню на множники, який дозволяє підвищити швидкодію пошуку біраціонально еквівалентних кривих Едвардса до кривих Вейерштрасса, представлених в ДСТУ 4145-2002, за рахунок зменшення кількості трудомістких операцій множення. Наводиться оцінка обчислювальної складності, перевірка статистичної гіпотези щодо однорідності двох незалежних вибірок – часу реалізації методів прототипу та удосконаленого. Представлено розклади адитивного ланцюга для полів з

ДСТУ 4145-2002, оцінку обчислювальної складності, перевірку статистичної гіпотези щодо однорідності двох незалежних вибірок – часу реалізації методів прототипу та удосконаленого. Також представлена практична реалізація удосконаленого і розробленого методів.

П'ятий розділ спрямований на використання двійкових біраціонально еквівалентних кривих Едвардса до кривих Вейерштрасса з ДСТУ 4145-2002: пропонується використовувати більш захищені криві при реалізації скалярного множення в операціях формування та перевірки ЕЦП. Приводиться удосконалений метод пошуку біраціонально еквівалентних кривих з використанням здобуття кубічного кореня. Наводиться практична реалізація методів прототипу та удосконаленого скалярного множення при формуванні та перевірці ЕЦП за стандартом ДСТУ 4145-2002.

У додатках приведені акти впровадження результатів дисертаційної роботи, патенти України на корисну модель, приведені знайдені біраціонально еквівалентні криві Едвардса до відповідних кривих Вейерштрасса (ДСТУ 4145-2002, NIST FIPS 186-4) у двійковому полі, параметри та результати статистичного дослідження на значущість оцінки часу методів прототипу та удосконаленого, результати експериментальних оцінок швидкодії операції скалярного множення, формуванню і перевірки ЕЦП.

Для основних положень дисертації та змісту автореферату характерна повна ідентичність. Крім того, варто зауважити, що дисертаційна робота відповідає формулі та паспорту спеціальності 05.13.21 – системи захисту інформації.

Наукове та практичне значення отриманих результатів.

1. *Вперше розроблено метод* автоматизації приведення довільного полінома за фіксованим модулем у полі GF(2^m), який враховує степені членів для заданого тричлена та п'ятичленна, що не приводиться, для різних цільових апаратних платформ, що дозволяє будувати алгоритми приведення за фіксованим модулем з меншою обчислювальною складністю по відношенню з побітовим методом.

2. *Удосконалено метод* скалярного множення в групі точок ЕК над полем GF(2^m), який за рахунок проміжних обчислень на кривій Едвардса, при $d_1 = d_2$, дозволяє підвищити стійкість до атак на реалізацію та підвищити швидкодію операції СК при генерації ключів, накладанні та перевірці ЕЦП за алгоритмами ДСТУ 4145-2002 та ECDSA.

3. *Удосконалено метод* здобуття $\sqrt[n]{\cdot}$ – вимірного кореня в полі GF(2^m), де m – непарне, на прикладі кубічного кореня, який за рахунок розкладу показника степеню за допомогою адитивного ланцюга на множники, дозволяє зменшити обчислювальну складність алгоритму пошуку біраціонально еквівалентних кривих Едвардса до кривих Вейерштрасса з ДСТУ 4145-2002 та рекомендованих NIST FIPS 186-4.

4. *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, під час генерації загальних параметрів криптосистеми RSA.

5. *Удосконалено метод* мультиплікативного інвертування на основі розширеного алгоритму Евкліда у полі $GF(2^m)$, який за рахунок використання інформації про двійкову довжину параметрів рівняння Безу: відмова від обчислення степеню полінома, а лише уточнення, зсуви і додавання лише за значущими словами, дозволяє знизити обчислювальну складність при генерації ключів, накладанні та перевірці ЕЦП за алгоритмами ДСТУ 4145-2002 та ECDSA.

Основні положення і результати дисертаційної роботи викладено 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. Також вони пройшли апробацію на міжнародних та всеукраїнських наукових конференціях, семінарах.

Значення результатів для науки та практики.

Практична цінність роботи полягає у тому, що удосконалені методи можуть застосуватися для підвищення ефективності криптографічних перетворень компонентів (центрів сертифікації ключів) Національної системи електронного цифрового підпису.

Отримані результати дисертаційної роботи впроваджено у навчальний процес кафедри безпеки інформаційних технологій Національного авіаційного університету та у науково-програмних розробках (бібліотеці криптографічних примітивів) ТОВ «Сайфер ЛТД», що підтверджено відповідними актами впровадження.

Дискусійні положення та зауваження щодо дисертаційного дослідження.

1. В дисертації пропонуються методи для підвищення інформаційно-телекомунікаційних систем Національної системи ЕЦП, але в самій темі дисертації мова не йдеться.

2. Практична реалізація на різних цільових платформах з використанням різного набору інструкцій та операційних систем проводиться лише у 5-му розділі для скалярного множення, формуванні та перевірці ЕЦП, але чому не проводиться для інших методів?

3. У 3-му розділі представляється удосконалений метод інвертування, який за часом реалізації не сильно відрізняється від методу прототипу, навіть дивлячись на вплив для Національної системи ЕЦП.

4. В 5-му розділі удосконаленню підлягає метод пошуку біраціонально еквівалентних кривих з двома параметрами, і результати показали, що швидкодія на стандартизованих кривих Вейерштрасса краща, тому постає питання чи потрібен удосконалений метод взагалі.

5. Рис. 3.3.2 трохи не інформативний, оскільки не видно нижніх коефіцієнтів при словах, що підлягають складанню.

6. У якості методу прототипу ділення великих цілих чисел було обрано найпростіший метод ділення «у стовпчик», однак добре відомі методи Бурнікеля- Ціглера та Баррета не розглядалися.

Слід зауважити, що наведені зауваження та недоліки не є принциповими щодо вирішення науково-практичного завдання, яке є суттю дослідження, суттєво не впливають на загальне позитивне враження від роботи, не зменшують її якості, а також наукової цінності та практичності.

Загальна оцінка дисертаційної роботи.

У цілому дисертаційна робота Ковтун М.Г. є закінченою науковою працею, яка містить нові науково обґрунтовані теоретичні та експериментальні результати, що у сукупності є суттєвими для розвитку теорії криптографії та захисту інформації. Одержані наукові результати можуть також застосовуватися в інших галузях науки і техніки, де

Дисертаційна робота «Методи удосконалення арифметичних операцій у полях, кільцях та алгебраїчних кривих для криптографічних застосувань» повністю відповідає чинним вимогам МОН України, зокрема «Порядку присудження наукових ступенів», затвердженого постановою КМУ від 24.07.2013 р. № 567 (зі змінами), а її автор Ковтун Марія Григорівна заслуговує присудження наукового ступеня кандидата технічних наук за спеціальністю 05.13.21 – системи захисту інформації.

Офіційний опонент
Завідувач кафедри кібербезпеки та програмного забезпечення,
Центральноукраїнського національного технічного університету
доктор технічних наук, професор О.А. Смірнов

Підпис професора Смірнова О.А. засвідчую:
Проректор з наукової роботи Центральноукраїнського національного технічного університету,
доктор економічних наук, професор О.М. Левченко

“ 7 ” червня 2018 року