Отримано
28.03.2025 р
Голова спеціалізованої
вченої ради
ДФ 26.133.080
д. т. н. проф.
Г.М. Гулак

Голові спеціалізованої вченої ради
ДФ 26.133.080 у Київському столичному університеті імені Бориса Грінченка
доктору технічних наук, професору
професору кафедри інформаційної та кібернетичної безпеки імені професора Володимира Бурячка Факультету інформаційних технологій та математики Київського столичного університету імені Бориса Грінченка
Гулаку Геннадію Миколайовичу

РЕЦЕНЗІЯ

КОРШУН Наталії Володимирівни, доктора технічних наук, професора, професора кафедри інформаційної та кібернетичної безпеки імені професора Володимира Бурячка на дисертацію **АБРАМОВА Сергія Вадимовича** «Моделі та методи підвищення швидкодії алгоритму CSIDH на основі суперсингулярних скручених кривих Едвардса» подану на здобуття ступеня доктора філософії за спеціальністю 125 Кібербезпека.

1. Актуальність теми дослідження

Наразі очікується поява квантових комп'ютерів, вони мають здатність ефективно вирішувати завдання, які класичні комп'ютери вирішують дуже довго, наприклад, розкладання на прості множники або знаходження дискретних логарифмів. Це робить традиційні криптосистеми вразливими до атак із використанням квантових алгоритмів, таких як алгоритм Шора.

У відповідь на ці погрози вчені розробляють нові криптографічні алгоритми, які є стійкими до атак з використанням квантових комп'ютерів.

Квантові комп'ютери ще не досягли стадії, на якій вони можуть ефективно зламати поточні криптосистеми, але очікується, що це відбудеться в майбутньому, можливо, протягом кількох десятиліть. Проте, криптографічні стандарти та протоколи мають бути підготовлені заздалегідь, щоб забезпечити безпеку у довгостроковій перспективі. Це вимагає розробки, тестування та впровадження постквантових алгоритмів, що може тривати багато часу.

Національний інститут стандартів і технологій США (NIST) вже розпочав процес стандартизації постквантових криптографічних алгоритмів, обравши

кілька кандидатів для створення стійких до квантових атак криптографічних рішень. Це стане основою для майбутніх систем, які будуть використовуватись у різних сферах, включаючи електронну комерцію, захист даних та фінансові транзакції.

Хоча квантові комп'ютери ще не стали повсякденною реальністю, необхідно вже зараз розробляти інфраструктуру для їхньої можливої появи. Постквантові криптосистеми повинні бути інтегровані в існуючі системи для забезпечення безпеки.

Таким чином, актуальність постквантових криптосистем сьогодні надзвичайно висока, і вона тільки збільшуватиметься у майбутньому. Актуальність полягає в їхній здатності забезпечити захист інформації в умовах появи квантових обчислень, що робить їх невід'ємною частиною майбутніх безпекових технологій.

2. Зв'язок теми дисертаційної роботи з науковими планами, програмами, фундаментальними та прикладними дослідженнями

Дисертація виконувалась в Київському столичному університеті імені Бориса Грінченка.

Результати наукових досліджень були використані на кафедрі інформаційної та кібернетичної безпеки імені професора Володимира Бурячка факультету інформаційних технологій та математики Київського столичного університету імені Бориса Грінченка в рамках науково-дослідної роботи: «Методи та моделі забезпечення кібербезпеки інформаційних систем переробки інформації та функціональної безпеки програмно-технічних комплексів управління критичної інфраструктури» (№ 0122U200483, КСУБГ, м. Київ).

Також результати наукових досліджень прийняті до впровадження в діяльність Київського столичного університету імені Бориса Грінченка (акт від 12.09.2024 року) та Інституту програмних систем Національної академії наук України (акт від 02.09.2024 року).

3. Ступінь обґрунтованості наукових положень, висновків і рекомендацій та їхня достовірність

Отримані наукові результати та висновки дисертаційної роботи характеризуються належним рівнем обґрунтованості, що підтверджується аналізом значної кількості наукової та технічної літератури та використанням загальнонаукових та спеціальних методів дослідження, зокрема методів теорії чисел; теорії поля; теорії графів; теорії функцій; теорії алгоритмів; теорії односторонніх функцій; теорії складності алгоритмів; теорії ймовірностей та математичної статистики; абстрактної алгебри; алгебраїчної геометрії; математичного і комп'ютерного моделювання.

Достовірність, отриманих в дисертації результатів, ґрунтується на комплексному, експериментальному і теоретичному вивченні моделей і методів криптосистем Діффі-Геллмана на основі еліптичних кривих Едвардса. опробуванню у публікаціях і докладах на конференціях. Перелік наукових праць дисертанта та довідки щодо впровадження результатів дослідження засвідчують фаховий підхід здобувача до обрання дослідницької проблематики та високий рівень його наукової компетентності.

4. Новизна наукових положень, висновків і рекомендацій, сформульованих у дисертації

Представлені в дисертації положення, концептуальні засади, структура, постановка завдань та їх вирішення, узагальнені висновки є результатом реалізації авторських ідей і самостійно виконаної наукової праці. У дисертаційній роботі Абрамова С.В. обґрунтовано низку концептуальних положень, узагальнень та висновків, які відповідають критеріям наукової новизни, зокрема:

- запропоновано і обґрунтовано метод підвищення швидкодії криптосистеми CSIDH за рахунок використання двох нециклічних кривих Едвардса з випадковим вибором, замість одної циклічної кривої. Це у зрівнянні з CSIDH вдвічі збільшує швидкість обчислення алгоритму.

- запропоновано метод інкапсуляції ключа CSIKE з рандомізацією вибору ізогеній і одним сеансом передачі одного відкритого ключа замість двох у CSIDH. Це дозволяє удвічі скоротити час на обмін ключами і усуває загрозу атаки сторонніми каналами..
- удосконалено метод обчислення ізогеній і вибору їх структури, що дає відповідно прискорення обчислення алгоритму більш ніж у 2^3 разів та скорочення діапазону ізогеній, що дає лінійну оцінку прискорення алгоритму в 1,5 рази.

-набув подальшого розвитку метод шифрування CRS на несуперсингулярних (ординарних) кривих Едвардса. Замість двох ізоморфних криптосистем в алгоритмі CSIDH перехід до НКЕ породжує чотири незалежні криптосистеми з можливістю паралельних обчислень. Це дає оцінку виграшу швидкості обчислень у чотири рази. Оцінка загального виграшу швидкості обчислень досягає $3 \cdot 2^9$ разів.

Слід підкреслити, що отримані результати розширюють попередні наукові дослідження проблем захисту інформації на основі криптосистеми Діффі-Геллмана на еліптичних кривих Едвардса.

5. Теоретична цінність і практична значущість наукових результатів

Наукові положення, висновки та рекомендації дисертаційної роботи Абрамова С.В. мають теоретичну цінність і практичну значущість. Отримані результати є певним внеском у розвиток інформаційної та кібернетичної безпеки.

Теоретичне значення дослідження, в умовах очікування появи квантових комп'ютерів, полягає в обґрунтуванні необхідності та дослідженні можливості вдосконалення методів захисту інформації на основі модифікованої криптосистеми CSIDH на ґрунті еліптичних суперсингулярних нециклічних кривих Едвардса.

Практичне значення отриманих результатів полягає у готовності створених методів і моделей для застосування у реальних криптосистемах для підвищення

кібербезпеки інформаційно-комунікаційних систем державного і приватного сектору, що є критично важливими для функціонування держави у постквантових умовах.

Запропоновані рішення були впроваджені у межах виконання державних науково-дослідних програм в Інституті проблем математичних машин і систем НАН України, де вони використовувались для вдосконалення криптографічного захисту інформації. Крім того, розробки інтегровані в освітній процес Київського столичного університету імені Бориса Грінченка, що сприяє підготовці висококваліфікованих фахівців.

6. Повнота викладення наукових результатів дисертації в опублікованих працях

У наукових публікаціях у повному обсязі висвітлено наукові результати дисертації відповідно до мети та поставлених завдань. Основні результати дисертації висвітлено у 11 наукових публікаціях, із них усі у співавторстві: 1 стаття (у співавторстві) у наукових виданнях, включених на дату опублікування до переліку наукових фахових видань України; 3 статті (з них усі у співавторстві) у періодичних наукових виданнях, проіндексованих в наукометричних базах даних Scopus і Web of Science Core Collection; 7 публікацій (з них 5 у співавторстві) у яких додатково відображено результати дисертації.

Основні положення, висновки і результати дослідження викладались і у процесі виступів і обговорень на науково-практичних міжнародних конференціях.

7. Відсутність (наявність) порушення академічної доброчесності

Аналіз тексту дисертації, а також публікації здобувача свідчать про відсутність ознак порушення вимог академічної доброчесності. Зокрема, дисертаційна робота містить посилання на джерела інформації у випадку використання ідей, розробок, тверджень, відомостей; відповідає нормам законодавства про авторське право і суміжні права; відображає прагнення автора

надати достовірну інформацію про результати власної наукової діяльності, використані методики досліджень та інформаційні ресурси. Посилання на першоджерела є коректними, навмисних спотворень не виявлено.

8. **Дискусійні положення, недоліки та зауваження до дисертації**

Принципових зауважень щодо структури, основних положень та концепції дисертації АБРАМОВА С.В. немає. Оцінюючи загалом позитивно наукове і практичне значення отриманих дисертантом результатів, висловлюю зауваження і рекомендації до окремих положень дисертації.

1. В постквантової криптографії існує багато криптоалгоритмів. Було б цікаво перевірити як розробки Абрамова С.В. можна було б застосувати до інших криптоалгоритмів і як це допоможе поліпшити їх якість.

2. В розділі 2 стверджується, що використання нециклічних кривих Едвардса приводить до подвоєння швидкодії або довжини секретного ключа. Варто було б більш детально пояснити механізм цього подвоєння.

3. Метод обчислення ізогеній, який використовує автор є досить складним і тому було б доцільним докладніше його описати та навести алгоритми. Крім того, залишилося нез'ясованим, як саме скорочення діапазону ступенів ізогеній дає лінійну оцінку прискорення в 1,5 рази.

4. В тексті дисертаційної роботи відмічені певні неточності та помилки технічного характеру:

- Про функції операції (*) сказано мимохідь, немає чіткого її визначення.

- Операції $[3^7, 5^{-5}, 7^8]$ на вигляд збігаються з операцією піднесення до степеня, можливо верхні індекси треба було б взяти у дужки, наприклад, $3^{(7)}$, $5^{(-5)}$, $7^{(8)}$.

- Деякий текст повторюється:

Стор. 61 криві Едвадса мають рекордно малу довжину ключа.

Стор. 60 Алгоритм CSIDH має найменшу серед відомих алгоритмів PQC довжину ключа.

Наведені зауваження і дискусійні моменти вказують на деякі суперечливі

аспекти дослідження, проте загалом вони засвідчують складність і багатогранність обраної теми, її практичну важливість та актуальність і суттєво не впливають на якісні характеристики дисертаційної роботи.

9. **Загальна оцінка дисертації і наукових публікацій щодо їхнього наукового рівня з урахуванням дотримання академічної доброчесності та щодо відповідності вимогам**

Дисертаційна робота Абрамова Сергія Вадимовича на тему «Моделі та методи підвищення швидкодії алгоритму CSIDH на основі суперсингулярних скручених кривих Едвардса» є завершеним науковим дослідженням, яке за актуальністю, достовірністю отриманих результатів, їхньою науковою новизною і практичною цінністю відповідає вимогам «Порядку присудження ступеня доктора філософії та скасування рішення разової спеціалізованої вченої ради закладу вищої освіти, наукової установи про присудження ступеня доктора філософії», затвердженого Постановою Кабінету Міністрів України від 12 січня 2022 року №44, а її автор, Абрамов Сергій Вадимович, заслуговує на присудження ступеня доктора філософії за спеціальністю 125 Кібербезпека.

Рецензент:

Доктор технічних наук, професор,
професор кафедри інформаційної та кібернетичної безпеки імені професора Володимира Бурячка
Київського столичного університету імені Бориса Грінченка

Наталія КОРШУН

КИЇВСЬКИЙ СТОЛИЧНИЙ УНІВЕРСИТЕТ ІМЕНІ БОРИСА ГРІНЧЕНКА
Код ЄДРПОУ 45307965
ВЛАСНИЙ ПІДПИС
Н. Коршун (ПІБ) ЗАСВІДЧУЮ
Київ. ... (посада)