Отримано
31.03.2025р
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,
Гулаку Геннадію Миколайовичу

РЕЦЕНЗІЯ

ЖДАНОВОЇ Юлії Дмитрівни, кандидата фізико-математичних наук, доцента, доцента кафедри інформаційної та кібернетичної безпеки імені професора Володимира Бурячка Київського столичного університету імені Бориса Грінченка 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

Актуальність теми дослідження обумовлена потребою у вдосконаленні захищеності та підвищенні швидкодії постквантових криптосистем, зокрема алгоритму CSIDH, який є одним з провідних у сфері асиметричної постквантової криптографії. З огляду на очікуване створення потужних квантових комп'ютерів, які становлять загрозу сучасним криптосистемам, що базуються на складності задач факторизації та дискретного логарифмування, цей напрямок має велике значення.

Технологія CSIDH на ізогеніях еліптичних кривих має стійкість до квантових атак, проте демонструє обмежену швидкодію. Застосування нециклічних суперсингулярних кривих Едвардса підвищує захищеність, але ускладнює обчислення. Однак вона має недоліки: невисоку швидкодію і уразливість до атак побічними каналами. Для модифікації CSIDH пропонуються такі рішення, як рандомізований вибір кривих, оптимізація і спрощення обчислення ізогеній, інкапсуляція ключів, а також використання паралельних обчислень.

Модернізація алгоритму CSIDH є актуальною для ґарантування безпеки передачі конфіденційної інформації в умовах розвитку квантових обчислень та еволюції методів криптоаналізу.

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 у 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 мають високий рівень обґрунтованості, що підтверджується детальним аналізом значного обсягу наукової й технічної літератури, а також застосуванням загальнонаукових і спеціалізованих методів дослідження. Серед них – методи теорії чисел, теорії скінченних полів, теорії графів, теорії алгоритмів, теорії складності алгоритмів, теорії ймовірностей та математичної статистики, алгебраїчної геометрії, а також математичного і комп'ютерного моделювання. Апробація дослідження підтверджується науковими публікаціями здобувача і документами про впровадження отриманих результатів.

Достовірність висновків ґрунтується на їхній внутрішній несуперечливості, а також на детальному вивченні моделей і методів криптосистем Діффі-Геллмана з використанням еліптичних кривих Едвардса, результати яких висвітлено у публікаціях.

Дисертація Абрамова С.В. є оригінальною науковою працею, яка виконана на високому теоретичному та методологічному рівні. Вона має чітку логічну структуру та є завершеним і комплексним дослідженням. Зміст роботи і багатогранність викладеної тематики свідчать про професійний підхід автора до вибору 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 порівнянні 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 вдвічі скоротити час обміну 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 (НКЕ). 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 значну теоретичну цінність і практичну важливість. Отримані результати є певним внеском у розвиток інформаційної та кібернетичної безпеки.

Теоретична цінність дослідження полягає в обґрунтуванні необхідності вдосконалення методів захисту інформації з використанням модифікованої криптосистеми CSIDH, що базується на еліптичних суперсингулярних нециклічних кривих Едвардса, в умовах появи квантових комп'ютерів.

Практична значущість полягає у готовності розроблених методів і моделей до впровадження у реальні криптосистеми для посилення кібербезпеки інформаційно-комунікаційних систем державного та приватного секторів, що є критично важливим у постквантову епоху.

Запропоновані розробки були впроваджені у межах виконання державних науково-дослідних програм в Інституті проблем математичних машин і систем НАН України, де вони застосовувались для підвищення рівня криптографічного захисту інформації. Окрім цього, розробки інтегровані в освітній процес Київського столичного університету імені Бориса Грінченка, що сприяє підготовці висококваліфікованих фахівців спеціальності «Кібербезпека».

6. Повнота викладення наукових результатів дисертації в опублікованих працях

Основні результати дисертації висвітлено в 11 наукових публікаціях, з 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), в яких додатково відображено результати дисертації.

Основні положення, висновки і результати дослідження викладались у процесі виступів та обговорень на науково-практичних міжнародних конференціях. Наукові результати дисертації повною мірою висвітлено у наукових публікаціях.

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, вважаємо за необхідне відзначити деякі дискусійні положення та зауваження до дисертації.

1. У другому розділі роботи запропоновано і обґрунтовано метод підвищення швидкодії криптосистеми CSIDH шляхом використання замість одної циклічної повної кривої Едвардса двох нециклічних кривих з випадковим вибором однієї з кривих пари. Втім не висвітлено механізм, який гарантував би рівномірність вибору та унеможливлював передбачення.
2. В побудованій моделі інкапсуляції ключа CSIKE було б доцільним вказати розподіл ймовірностей, який може бути використаний для рандомізації ступіня ізогенії на кожному кроці ланцюжка ізогеній.
3. В описі методу CRS на НКЕ та поділу секретів Діффі-Геллмана на ізогеніях ординарних нециклічних кривих Едвардса стверджується, що замість двох ізоморфних криптосистем в алгоритмі CSIDH перехід до НКЕ породжує чотири незалежні криптосистеми з можливістю паралельних обчислень. Проте не вказано, як саме відбувається це породження і як визначається їх незалежність.
4. Текст дисертаційної роботи містить певні неточності та помилки технічного характеру:

- Початкова крива інколи позначається як E_0 (стор. 83), а інколи як $E_d^{(0)}$ (стор. 131)
- Для одного й того самого поняття використовується два терміна: кручений, скручений (стор. 6)
- Одне скорочення використовується для різних термінів НКЕ несуперсингулярні (стор. 90) і нециклічні (стор. 100)
- Для одного типу атаки використовується два терміни: сторонніми каналами і побічними каналами.

Крім того, текст містить певну кількість друкарських помилок, та помилок перекладу, зокрема математичних термінів.

- Для поняття оберненої функції використаний неправильний термін «зворотна функція» (стор. 33)
- замість «скінченні поля» використаний неправильний термін «кінцеві поля» (стор. 42).
- Операція «додавання» неправильно навивається операцією «складання», замість «піднесення до степеня» використовується «зведення у ступінь» (стор. 43).

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, цілісним науковим дослідженням, виконана на актуальну тему, містить елементи наукової новизни та має теоретичне й практичне значення. Оформлення роботи 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:
кандидат фізико-математичних наук, доцент, доцент кафедри інформаційної та кібернетичної безпеки імені професора Володимира Бурячка Київського столичного університету імені Бориса Грінченка

Юлія ЖДАНОВА

КИЇВСЬКИЙ СТОЛИЧНИЙ УНІВЕРСИТЕТ ІМЕНІ БОРИСА ГРІНЧЕНКА
Код ЄДРПОУ 45307965
ВЛАСНИЙ ПІДПИС
Ю. Жданової ЗАСВІДЧУЮ
(ПІБ)
(посада)