Отримано
28.03.2025р
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

ВІДГУК

офіційного опонента **СМІРНОВА Олексія Анатолійовича**,
доктора технічних наук, професора, завідувача кафедри кібербезпеки та програмного забезпечення Центральноукраїнського національного технічного університету
на дисертаційну роботу **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

Найважливішим завданням у забезпеченні інформаційної безпеки держави є створення та підтримка умов, що забезпечують надійний захист державних і приватних інформаційних ресурсів, а також безпечну їх обробку, зберігання та передачу. Розвиток криптографічних методів, що використовуються для захисту цих ресурсів, відіграє важливу роль у підвищенні інформаційної безпеки держави в цілому.

Стрімкий прогрес у квантових обчисленнях суттєво змінив криптографічний ландшафт. Через значну обчислювальну потужність квантових комп'ютерів класичні криптографічні алгоритми, які є основою сучасної цифрової безпеки, можуть бути скомпрометовані. Ця загроза зумовлює нагальну потребу у переході до постквантової криптографії (PQC) – сфери, яка досліджує алгоритми, стійкі до квантових атак.

Існуючі стандартні криптосистеми більше не відповідають сучасним вимогам безпеки, оскільки зростання обчислювальних можливостей техніки та збільшення обсягів передачі інформації потребують надійнішого захисту. Це призводить до скорочення терміну життя старих криптосистем і створює

невідкладну потребу у модернізації або розробці нових, більш швидких криптосистем.

У 2015 році було запропоновано використання властивостей еліптичних кривих у формі Едвардса в криптосистемах. Їх перевагою є висока швидкість скалярного множення точок та знижена вразливість до атак із застосуванням інформації з побічного каналу. Це актуалізує дослідження еліптичних кривих Едвардса над простими полями для впровадження в сучасні, більш ефективні криптосистеми.

Сьогодні значна увага дослідників спрямована на вивчення протоколів CSIDH на основі кривих Едвардса, які виявляються перспективними для використання в асиметричних постквантових криптосистемах.

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

Дисертація виконана на кафедрі інформаційної та кібернетичної безпеки імені професора Володимира Бурячка Київського столичного університету імені Бориса Грінченка відповідно до теми науково-дослідної роботи та індивідуального плану аспіранта Київського столичного університету імені Бориса Грінченка.

Дисертаційна робота виконана відповідно до планів наукової і науково-технічної діяльності 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, КУБГ, 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).

Обрана тема відповідає доктрини інформаційної безпеки України, Стратегії інформаційної безпеки та Стратегії кібербезпеки України.

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 складності алгоритмів; теорії ймовірностей та математичної статистики; абстрактної алгебри; алгебраїчної геометрії; математичного і комп'ютерного моделювання.

Достовірність, отриманих в дисертації результатів, ґрунтується на комплексному, вивченні моделей і методів криптосистем Діффі-Гельмана на основі еліптичних кривих Едвардса, випробуванню у публікаціях і впровадженнях. 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-Гельмана 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 основі 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 за спеціальністю Кібербезпека.

6. Повнота викладення наукових результатів дисертації в опублікованих працях

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.

Аналіз публікацій автора дозволяє зробити висновок про повноту викладення основних наукових положень дисертаційного дослідження у науковій літературі. Також зазначено особистий внесок здобувача у тих наробках, які виконано колективно.

7. Відсутність (наявність) порушення академічної доброчесності

У дисертації та наукових публікаціях Абрамова С.В. відсутні порушення академічної доброчесності. Запозичень матеріалу без посилання на відповідне джерело не виявлено. Перевірка проводилася сертифікованою програмою Turnitin.

8. Дискусійні положення та недоліки дисертаційної роботи

Відзначаючи позитивні сторони роботи Абрамова С.В., слід звернути увагу на певні зауваження та дискусійні положення, які потребують додаткової аргументації.

1. У постквантовому середовищі існує досить багато типів криптосистемі, резистентних до квантових атак. Порівняння їх з розробками дисертанта значно підвищили би наукову цінність роботи.

2. У загальному вигляді крива Едвардса має два параметри A та D, але у роботі криві ідентифікуються тільки параметром D, а параметр A майже не використовується. Це певним чином порушує строгість подання цього питання і потребує обґрунтування.

3. В описі удосконалення методу обчислення ізогеній відбувається заміна обчислення ізогенних функцій $\varphi(R)$ на обчислення параметра d. Варто було б детальніше пояснити, як саме відбувається така заміна, які математичні перетворення при цьому використовуються.

4. Текст дисертаційної роботи містить ряд помилок і зауважень технічного характеру:
   - Одне скорочення використовується для різних термінів НКЕ несуперсингулярні стор. 90 і нециклічні стор. 100
   - Трикратне повторення:
   - стор 38 Головна перевага еліптичної криптографії полягає в тому
   - стор 39 Переваги шифрування на основі еліптичних кривих
   - стор 42 інтерес до еліптичної криптографії обумовлений перевагами
   - В тексті присутні певні граматичні та пунктуаційні помилки;

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 дисертаційної роботи, її відповідність встановленим 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.

Офіційний опонент:
доктор технічних наук, професор
завідувач кафедри кібербезпеки
та програмного забезпечення
Центральноукраїнського національного
технічного університету Олексій СМІРНОВ

Підпис професора Смірнова О.А. засвідчую:
Проректор з наукової роботи та міжнародних зв'язків
Центральноукраїнського національного технічного університету,
кандидат технічних наук, доцент Андрій ТИХИЙ
“____” _____ 2025 року