Отримано
31.03.2025 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
Гулаку Геннадію Миколайовичу

ВІДГУК

офіційного опонента **ОПІРСЬКОГО Івана Романовича**,
доктора технічних наук, професора, завідувача кафедри захисту інформації
Національного університету «Львівська політехніка»,
на дисертаційне дослідження **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

Методологія криптографії є надзвичайно важливим інструментом, що значно впливає на державну безпеку та діяльність комерційних організацій, забезпечуючи надійний захист конфіденційної інформації від пошкоджень чи перехоплення під час її передачі, обробки в реальному часі та збереження.

Перші асиметричні криптосистеми з відкритими ключами, створені Діффі та Геллманом півстоліття тому, базувалися на субекспоненційній складності та використанні арифметики у скінченних кільцях і полях. Через десятиліття з'явилися системи на еліптичних кривих, які мали експоненційну складність і значно перевершували попередників за швидкодією та довжиною модулів.

Розвиток сучасних комп'ютерів стрімко триває. Уже є дані про створення квантових комп'ютерів, які за потужністю значно перевершують класичні. Наприклад, комп'ютер IBM Quantum поступово досягає заявленої мети в понад 4000+ кубітів, відкриваючи нові горизонти, недоступні сучасній фізичній електроніці.

Це вимагає підготовки до появи квантових комп'ютерів, які можуть зробити багато існуючих криптосистем неефективними, особливо вразливими до їх атак асиметричні системи. Актуальним стає питання про те, які криптосистеми залишатимуться дієздатними у постквантову еру та як їх слід розвивати. Однією з перспективних постквантових систем є система Діффі-Геллмана на ізогеніях

еліптичних кривих, що вирізняється мінімальною довжиною ключа. Проте й вона має певні недоліки, що робить дослідження й удосконалення цієї системи надзвичайно актуальним завданням.

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. Напрям дисертаційного дослідження безпосередньо пов'язаний з реалізацією доктрини інформаційної безпеки України, Стратегії інформаційної безпеки та Стратегії кібербезпеки України. 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).

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

Зміст дисертаційної роботи повною мірою розкриває тему наукового дослідження та відповідає визначеним меті, завданням, об'єкту та предмету дослідження. Розроблені автором і викладені у дисертаційній роботі наукові положення, висновки та рекомендації є аргументованими та обґрунтованими, чітко і послідовно сформульованими.

Отримані наукові результати та висновки дисертаційної роботи характеризуються належним рівнем обґрунтованості та достовірності, оскільки

при її підготовці:

1) опрацьовано значну кількість літературних джерел зарубіжних і вітчизняних вчених, проаналізовано нормативно-правове забезпечення та приділено значну увагу дослідженню та можливості впровадження іноземного досвіду;

2) використано широкий спектр загальнонаукових і спеціальних методів дослідження – логічного узагальнення, аналізу і синтезу, наукового абстрагування та системного підходу, а також методи теорії ймовірностей та математичної статистики; методи моделювання систем;

3) здійснена численна апробація результатів дослідження, про що свідчить перелік наукових праць здобувача;

4) результати наукових досліджень прийняті до впровадження в діяльність Інституту програмних систем Національної академії наук України. Дисертаційна робота Абрамова С.В. є оригінальною науковою працею, яка виконана на належному теоретичному та методичному рівнях. Робота має послідовну та логічну структуру і є комплексним, завершеним науковим дослідженням. Зміст роботи та багатогранність висвітленої проблеми свідчать про високий рівень наукової компетентності автора.

Викладене вище дає можливість висловити позитивний висновок стосовно наукового рівня, достовірності подання в дисертації матеріалу, теоретичних обґрунтувань і аргументації всіх положень, практичного значення висновків і рекомендацій.

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

У дисертаційній роботі Абрамова С.В. сформульовано та обґрунтовано ряд наукових положень, висновків і рекомендацій, які відзначаються наявністю наукової новизни. До положень, що відображають наукову новизну дисертаційного дослідження, можна віднести результати, отримані дисертантом самостійно, а саме:

- запропоновано і обґрунтовано метод підвищення швидкодії криптосистеми CSIDH за рахунок використання двох нециклічних кривих

моделі цих систем удосконалено за рахунок інкапсуляції ключа, рандомізації

було запропоновано використати у криптографії алгебраїчні властивості еліптичних кривих.»

- Різні позначення одної й тої самої величини:

а. Спочатку порядок кривої позначається N_E (стор. 65) а потім #E (стор. 138).

б. Початкова крива інколи позначається як $E_d^{(0)}$ (стор. 131) а інколи як E_0 (стор. 83)

- Схеми виконані не в одному стилі

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 захисту інформації
Національного університету
«Львівська політехніка» Іван ОПІРСЬКИЙ

Підпис д.т.н., професора Опірського І.Р. засвідчую
Вчений секретар Національного університету
«Львівська політехніка», к.т.н., доцент Роман БРИЛИНСЬКИЙ