Облікова картка дисертації

I. Загальні відомості

Державний обліковий номер: 0825U000720

Особливі позначки: відкрита

Дата реєстрації: 04-03-2025

Статус: Захищена

Реквізити наказу МОН / наказу закладу:

II. Відомості про здобувача

Власне Прізвище Ім'я По-батькові:

1. Абрамов Сергій Вадимович
2. Serhii Abramov

Кваліфікація:

Ідентифікатор ORCID ID: Не застосовується

Вид дисертації: доктор філософії

Аспірантура/Докторантура: так

Шифр наукової спеціальності: 125

Назва наукової спеціальності: Кібербезпека та захист інформації

Галузь / галузі знань: інформаційні технології

Освітньо-наукова програма зі спеціальності: «Інформаційна безпека держави»

Дата захисту: 15-04-2025

Спеціальність за освітою: Комп'ютерні науки

Місце роботи здобувача: Київський столичний університет імені Бориса Грінченка

Код за ЄДРПОУ: 02136554

Місцезнаходження: вул. Бульварно-Кудрявська, 18/2, Київ, 04053, Україна

Форма власності: Державна

Сфера управління: Департамент освіти і науки, молоді та спорту виконавчого органу Київської міської ради (Київської міської державної адміністрації)

Ідентифікатор ROR:

III. Відомості про організацію, де відбувся захист

Шифр спеціалізованої вченої ради (разової спеціалізованої вченої ради): PhD 7894

Повне найменування юридичної особи: Київський столичний університет імені Бориса Грінченка

Код за ЄДРПОУ: 02136554

Місцезнаходження: вул. Бульварно-Кудрявська, 18/2, Київ, 04053, Україна

Форма власності: Державна

Сфера управління: Департамент освіти і науки, молоді та спорту виконавчого органу Київської міської ради (Київської міської державної адміністрації)

Ідентифікатор ROR:

IV. Відомості про підприємство, установу, організацію, в якій було виконано дисертацію

Повне найменування юридичної особи: Київський столичний університет імені Бориса Грінченка

Код за ЄДРПОУ: 02136554

Місцезнаходження: вул. Бульварно-Кудрявська, 18/2, Київ, 04053, Україна

Форма власності: Державна

Сфера управління: Департамент освіти і науки, молоді та спорту виконавчого органу Київської міської ради (Київської міської державної адміністрації)

Ідентифікатор ROR:

V. Відомості про дисертацію

Мова дисертації: Українська

Коди тематичних рубрик: 20.56, 20.56.01

Тема дисертації:

1. Моделі та методи підвищення швидкодії алгоритму CSIDH на основі суперсингулярних скручених кривих Едвардса

2. Models and Methods for Improving the Performance of the CSIDH Algorithm based on Supersingular Twisted Edwards Curves

Реферат:

1. Дисертаційна робота присвячена вирішенню актуального наукового завдання, сутність якого полягає в підвищенні у постквантових умовах захищеності і швидкодії криптосистем на основі комутативної суперсингулярної ізогенії Діффі-Геллмана (від англ. Commutative Supersingular Isogeny Diffie–Hellman, CSIDH), який є одним з лідерів асиметричних постквантових криптосистем. Алгоритм пропонується будувати на ґрунті ізогеній нециклічних суперсингулярних кривих Едвардса як пар квадратичного кручення. Використання еліптичних кривих Едвардса значно підвищує захищеність криптоалгоритму, але при цьому збільшується складність обчислення алгоритму і відповідно зменшується його швидкодія. Тому є актуальною проблема підвищення швидкодії за рахунок модифікації цього алгоритму.

2. The dissertation is devoted to solving an urgent scientific problem, the essence of which is to increase the security and performance of cryptosystems based on the Commutative Supersingular Isogeny Diffie-Hellman, which is one of the leaders in asymmetric post-quantum cryptosystems, in post-quantum conditions. The algorithm is proposed to be built based on isogenies of noncyclic supersingular Edwards curves as pairs of quadratic torsion. The use of elliptic Edwards curves significantly increases the security of the cryptoalgorithm, but it increases the complexity of the algorithm's computation and, accordingly, reduces its performance. Therefore, the problem of improving performance by modifying this algorithm is relevant.

Державний реєстраційний номер ДіР:

Пріоритетний напрям розвитку науки і техніки: Фундаментальні наукові дослідження з найбільш важливих проблем розвитку науково-технічного, соціально-економічного, суспільно-політичного, людського потенціалу для забезпечення конкурентоспроможності України у світі та сталого розвитку суспільства і держави

Стратегічний пріоритетний напрям інноваційної діяльності: Освоєння нових технологій транспортування енергії, впровадження енергоефективних, ресурсозберігаючих технологій, освоєння альтернативних джерел енергії

Підсумки дослідження: Теоретичне узагальнення і вирішення важливої наукової проблеми

Публікації:

- Bessalov, A., Kovalchuk, L., & Abramov, S. (2022). Randomization of CSIDH Algorithm on Quadratic and Twisted Edwards Curves. Electronic Professional Scientific Journal "Cybersecurity: Education, Science, Technique", 1(17), 128–144. https://doi.org/10.28925/2663-4023.2022.17.128144.
- Bessalov, A., & Abramov, S. (2022). Special Properties of the Point Addition Law for Non-Cyclic Edwards Curves. Cybernetics and Systems Analysis, 58(683), 851–861. https://doi.org/10.1007/s10559-023-00518-w (Scopus Q3).
- Bessalov, V., & Abramov, S. (2023). PQC CSIKE Algorithm on Non-Cyclic Edwards Curves. Cybernetics and Systems Analysis, 59(6), 867–879. https://doi.org/10.1007/s10559-023-00622-x (Scopus Q3).
- Bessalov, A., Sokolov, V., & Abramov, S. (2024). Efficient Commutative PQC Algorithms on Isogenies of Edwards Curves. Cryptography, 8(3), 1–17. https://doi.org/10.3390/cryptography8030038 (Scopus Q2, WoS Q2).

Наукова (науково-технічна) продукція:

Соціально-економічна спрямованість:

Охоронні документи на ОПІВ:

Впровадження результатів дисертації: Впроваджено

Зв'язок з науковими темами: 0122U200483

VI. Відомості про наукового керівника/керівників (консультанта)

Власне Прізвище Ім'я По-батькові:

1. Соколов Володимир Юрійович

2. Volodymyr Y. Sokolov

Кваліфікація: к. т. н., доцент, 05.13.06

Ідентифікатор ORCID ID: 0000-0002-9349-7946

Додаткова інформація:

Повне найменування юридичної особи: Київський столичний університет імені Бориса Грінченка

Код за ЄДРПОУ: 02136554

Місцезнаходження: вул. Бульварно-Кудрявська, 18/2, Київ, 04053, Україна

Форма власності: Державна

Сфера управління: Департамент освіти і науки, молоді та спорту виконавчого органу Київської міської ради (Київської міської державної адміністрації)

Ідентифікатор ROR:

VII. Відомості про офіційних опонентів та рецензентів

Офіційні опоненти

Власне Прізвище Ім'я По-батькові:

1. Смірнов Олексій Анатолійович
2. OLEKSII SMIRNOV

Кваліфікація: д.т.н., професор, 21.05.01

Ідентифікатор ORCID ID: Не застосовується

Додаткова інформація:

Повне найменування юридичної особи: Центральноукраїнський національний технічний університет

Код за ЄДРПОУ: 02070950

Місцезнаходження: просп. Університетський, буд. 8, Кропивницький, Кропівницький р-н., 25006, Україна

Форма власності:

Сфера управління: Міністерство освіти і науки України

Ідентифікатор ROR: Не застосовується

Власне Прізвище Ім'я По-батькові:

1. Опірський Іван Романович
2. Ivan R. Opirskyi

Кваліфікація: д. т. н., професор, 05.13.21

Ідентифікатор ORCID ID: Не застосовується

Додаткова інформація:

Повне найменування юридичної особи: Національний університет "Львівська політехніка"

Код за ЄДРПОУ: 02071010

Місцезнаходження: вул. Степана Бандери, буд. 12, Львів, 79013, Україна

Форма власності: Державна

Сфера управління: Міністерство освіти і науки України

Ідентифікатор ROR:

Рецензенти

Власне Прізвище Ім'я По-батькові:

1. Жданова Юлия Дмитриевна
2. YULIIA ZHDANOVA

Кваліфікація: к. ф.-м. н., доц., 01.01.05

Ідентифікатор ORCID ID: Не застосовується

Додаткова інформація:

Повне найменування юридичної особи: Київський столичний університет імені Бориса Грінченка

Код за ЄДРПОУ: 02136554

Місцезнаходження: вул. Бульварно-Кудрявська, 18/2, Київ, 04053, Україна

Форма власності: Державна

Сфера управління: Департамент освіти і науки, молоді та спорту виконавчого органу Київської міської ради (Київської міської державної адміністрації)

Ідентифікатор ROR:

Власне Прізвище Ім'я По-батькові:

1. Коршун Наталія Володимирівна
2. Nataliia Korshun

Кваліфікація: д. т. н., професор, 05.12.13

Ідентифікатор ORCID ID: 0000-0003-2908-970X

Додаткова інформація:

Повне найменування юридичної особи: Київський столичний університет імені Бориса Грінченка

Код за ЄДРПОУ: 02136554

Місцезнаходження: вул. Бульварно-Кудрявська, 18/2, Київ, 04053, Україна

Форма власності: Державна

Сфера управління: Департамент освіти і науки, молоді та спорту виконавчого органу Київської міської ради (Київської міської державної адміністрації)

Ідентифікатор ROR:

VIII. Заключні відомості

Власне Прізвище Ім'я По-батькові голови ради Гулак Геннадій Миколайович

Власне Прізвище Ім'я По-батькові головуючого на засіданні	Гулак Геннадій Миколайович
Відповідальний за підготовку облікових документів	Сало Ганна Вікторівна
Реєстратор	УкрІНТЕІ
Керівник відділу УкрІНТЕІ, що є відповідальним за реєстрацію наукової діяльності	Юрченко Тетяна Анатоліївна