Облікова картка дисертації

I. Загальні відомості

Державний обліковий номер: 0825U001703

Особливі позначки: відкрита

Дата реєстрації: 14-05-2025

Статус: Наказ про видачу диплома

Реквізити наказу МОН / наказу закладу: Наказ ХНУ імені В. Н. Каразіна № 0302-3к/1042 від 17.06.2025 р.

II. Відомості про здобувача

Власне Прізвище Ім'я По-батькові:

1. Кандій Сергій Олегович
2. Serhii Kandii

Кваліфікація:

Ідентифікатор ORCID ID: 0000-0003-0552-8341

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: Кібербезпека

Дата захисту: 02-06-2025

Спеціальність за освітою: Безпека інформаційних і комунікаційних систем

Місце роботи здобувача: Харківський національний університет імені В. Н. Каразіна

Код за ЄДРПОУ: 02071205

Місцезнаходження: майдан Свободи, 4, Харків, Харківський р-н., 61022, Україна

Форма власності: Державна

Сфера управління: Міністерство освіти і науки України

Ідентифікатор ROR:

III. Відомості про організацію, де відбувся захист

Шифр спеціалізованої вченої ради (разової спеціалізованої вченої ради): PhD 8436

Повне найменування юридичної особи: Харківський національний університет імені В. Н. Каразіна

Код за ЄДРПОУ: 02071205

Місцезнаходження: майдан Свободи, 4, Харків, Харківський р-н., 61022, Україна

Форма власності: Державна

Сфера управління: Міністерство освіти і науки України

Ідентифікатор ROR:

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

Повне найменування юридичної особи: Харківський національний університет імені В. Н. Каразіна

Код за ЄДРПОУ: 02071205

Місцезнаходження: майдан Свободи, 4, Харків, Харківський р-н., 61022, Україна

Форма власності: Державна

Сфера управління: Міністерство освіти і науки України

Ідентифікатор ROR:

V. Відомості про дисертацію

Мова дисертації: Українська

Коди тематичних рубрик: 20.54.02, 20.54.04, 20.56.01

Тема дисертації:

1. Методи та моделі оцінки захищеності асиметричних криптографічних перетворень на решітках від існуючих та потенційних атак

2. Methods and models for evaluating the security of lattice-based asymmetric cryptographic transformations against existing and potential attacks

Реферат:

1. Дисертаційна робота присвячена розв'язанню актуальної задачі: аналізу та розробці методів та моделей для підвищення захищеності асиметричних криптографічних систем на решітках. Мета і завдання дослідження. Метою дослідження є аналіз та розробка методів та моделей для підвищення захищеності асиметричних криптографічних систем на решітках від існуючих та потенційних атак. У першому розділі дисертації (Аналіз сучасних тенденцій у квантово-стійкій криптографії) на основі проведеного аналізу показано, що розвиток квантових алгоритмів обумовлений двома техніками – квантовим пошуком та квантовою вибіркою Фур'є. Обґрунтовано, що криптографія на решітках є стійкою до застосування цих технік. Розкриті вимоги до квантово-стійкої криптографії. Розкрита сутність доказової безпеки та моделей безпеки IND-CCA (Indistinguishability under Adaptive Chosen Chiphertext Attack) для механізмів інкапсуляції ключів та EUF-CMA (Existentially unforgeable under adaptive chosen message attacks) для електронних підписів. Наведено

відомості з теорії решіток та теорії квантових обчислень. У другому розділі дисертації (Аналіз та порівняння моделей редукції решіток) обґрунтовано, що фактор Ерміта відіграє важливу роль при аналізі моделей редукції решіток. Проведено серію експериментів, що направлені на визначення точності існуючих асимптотичних оцінок фактору Ерміта на криптографічно значущих розмірностях решіток. Показано, що істинне значення фактору Ерміта швидко наближається до асимптотичних оцінок і на криптографічно значущих розмірностях можливо вважати помилку апроксимації фактору Ерміта незначною. Проведено порівняльний аналіз існуючих симуляторів редукції решіток. Для порівняння симуляторів проведено ряд експериментів на решітках малої розмірності. Показано, що симулятор Альбрехта–Лі дає найменшу середньоквадратичну помилку серед усіх симуляторів. Для NTRU решіток розкрито сутність розрідженої підрешітки. Отримано перший науковий результат: Вперше виконано кількісне порівняння точності моделей редукції решіток із застосуванням метрики середньоквадратичної помилки для моделі GSA (Geometric Series Assumption) та симуляторів редукції решіток. Попередні дослідження фокусувалися на якісних або суто теоретичних оцінках якості роботи моделей. Отримані оцінки дозволяють кількісно оцінювати якість роботи симуляторів в залежності від параметрів решіток для оцінки захищеності від класичних та квантових атак. У третьому розділі дисертації (Методи оцінки складності криптографічних задач з теорії решіток) наведено класифікацію існуючих атак на криптографічні перетворення на решітках. Для атак вкладення та декодування запропонована удосконалена модель оцінки складності атаки, що базується на проведеному у другому розділі аналізі. Для атак декодування запропонований метод визначення оптимальних параметрів атаки. Удосконалено методику оцінювання складності криптографічної задачі SIS (Shortest Integer Solution), що відрізняється від існуючих тим, що у даній методиці враховується алгебраїчна структура решіток під час аналізу процесів редукції для оцінки параметрів та характеристик атак на їх основі. У четвертому розділі дисертації (Оцінка захищеності механізмів інкапсуляції ключів на алгебраїчних решітках) уточнено оцінки захищеності механізмів інкапсуляції ключів ДСТУ 8961:2019 та Crystals–Kyber. Показано, що врахування структури алгебраїчних решіток, згідно до методу, що був розроблений в розділі 3, дає більші оцінки безпеки, ніж класична модель GSA. Вперше було отримано узагальнений доказ IND–CCA безпеки перетворень, що використовуються в стандарті ДСТУ 8961:2019, у моделі квантового випадкового оракула. Попередні дослідження не вивчали IND–CCA безпеку перетворень ДСТУ 8961:2019 у моделі квантового випадкового оракула. У п’ятому розділі дисертації (Оцінка захищеності електронних підписів на алгебраїчних решітках) уточнено оцінки захищеності електронних підписів Falcon та Crystals–Dilithium. Показано, що врахування структури алгебраїчних решіток, згідно до методу, що був розроблений в розділі 3, дає більші оцінки безпеки, ніж класична модель GSA. Для електронного підпису Falcon отримали подальший розвиток обґрунтування оцінки атаки відновлення ключів, що використовує обчислення з плаваючою крапкою, для алгоритмів електронного підпису на основі решіток, що дало змогу підвищити безпеку електронних підписів на решітках.

2. The thesis is devoted to solving a relevant problem: the analysis and development of methods and models to enhance the security of lattice–based asymmetric cryptographic systems. In the first chapter of the dissertation (Analysis of Modern Trends in Quantum–Resistant Cryptography), the conducted analysis demonstrates that the advancement of quantum algorithms is driven by two key techniques: quantum search and quantum Fourier sampling. It is substantiated that lattice–based cryptography remains resistant to these techniques. The chapter outlines the requirements for quantum–resistant cryptography and explores the concept of provable security, along with security models such as IND–CCA (Indistinguishability under Adaptive Chosen Ciphertext Attack) for key encapsulation mechanisms and EUF–CMA (Existential Unforgeability under Adaptive Chosen Message Attack) for digital signatures. Additionally, fundamental concepts from lattice theory and quantum computing theory are presented. In the second chapter of the dissertation (Analysis and Comparison of Lattice Reduction Models), it is substantiated that the Hermite factor plays a crucial role in analyzing lattice reduction models. A series of experiments was conducted to assess the accuracy of existing asymptotic estimates of the Hermite factor for cryptographically significant lattice dimensions. The results demonstrate that the true value of the Hermite factor quickly converges to its asymptotic estimates, and for cryptographically relevant dimensions, the approximation

error can be considered negligible. A comparative analysis of existing lattice reduction simulators was performed. To evaluate these simulators, several experiments were conducted on low–dimensional lattices. The findings indicate that the Albrecht–Lee simulator produces the lowest root–mean–square error among all tested simulators. For NTRU lattices, the concept of a sparse sublattice is explored in detail. First Scientific Contribution: For the first time, a quantitative comparison of the accuracy of lattice reduction models was performed using the root–mean–square error metric for both the Geometric Series Assumption (GSA) model and lattice reduction simulators. Previous studies primarily focused on qualitative or purely theoretical assessments of model accuracy. The obtained estimates enable a quantitative evaluation of simulator performance based on lattice parameters, contributing to the assessment of security against both classical and quantum attacks. In the third chapter of the dissertation (Methods for Assessing the Complexity of Cryptographic Problems in Lattice Theory), a classification of existing attacks on lattice–based cryptographic transformations is provided. For embedding and decoding attacks, an enhanced complexity assessment model is proposed, based on the analysis conducted in the second chapter. For decoding attacks, a method for determining optimal attack parameters is introduced. Additionally, the evaluation methodology for the complexity of the Shortest Integer Solution (SIS) problem has been improved. Unlike existing methods, this approach incorporates the algebraic structure of lattices when analyzing the reduction processes used to estimate the parameters and characteristics of attacks based on SIS. In the fourth chapter of the dissertation (Security Assessment of Key Encapsulation Mechanisms on Algebraic Lattices), the security estimates of the DSTU 8961:2019 and CRYSTALS–Kyber key encapsulation mechanisms were refined. The findings demonstrate that considering the structure of algebraic lattices, according to the method developed in Chapter 3, results in higher security estimates compared to the classical Geometric Series Assumption (GSA) model. First Scientific Contribution: For the first time, a generalized IND–CCA security proof for transformations used in DSTU 8961:2019 was obtained within the Quantum Random Oracle Model (QROM). Previous studies had not explored the IND–CCA security of DSTU 8961:2019 transformations in the QROM framework. In the fifth chapter of the dissertation (Security Assessment of Digital Signatures on Algebraic Lattices), the security estimates of the Falcon and CRYSTALS–Dilithium digital signature schemes were refined. The findings demonstrate that considering the structure of algebraic lattices, according to the method developed in Chapter 3, results in higher security estimates compared to the classical Geometric Series Assumption (GSA) model. For the Falcon digital signature scheme, further development was made in justifying the evaluation of key recovery attacks that utilize floating–point computations for lattice–based signature algorithms. This advancement has contributed to enhancing the security of lattice–based digital signatures.

Державний реєстраційний номер ДіР:

Пріоритетний напрям розвитку науки і техніки: Інформаційні та комунікаційні технології

Стратегічний пріоритетний напрям інноваційної діяльності: Розвиток сучасних інформаційних, комунікаційних технологій, робототехніки

Підсумки дослідження: Нове вирішення актуального наукового завдання

Публікації:

- Gorbenko I.D., Yesina M.V., Kandy S.O., Ostryanska Ye. V. Generation of general system parameters for Falcon cryptosystem for 256, 384, and 512 security bits // Telecommunications and Radio Engineering. 2022. Vol. 81, Is. 2. P. 49–59. DOI:10.1615/TelecomRadEng.2022037071. URL:https://www.dl.begellhouse.com/journals/0632a9d54950b268,33bd45d917452b68,54c5c714496ce4ca.html.
- Potii O.V., Kachko O.G., Kandii S.O., Kaptol Y.Y. Determining the effect of a floating point on the Falcon Digital Signature Algorithm Security // Eastern–European Journal of Enterprise Technologies. 2024. Vol. 1, Is. 9. P. 52–59. DOI:10.15587/1729–4061.2024.295160.
- Kachko O.G., Gorbenko Y.I., Kandii S.O., Kaptol Y.Y. Improving protection of falcon electronic signature software implementations against attacks based on Floating Point Noise // Eastern–European Journal of

Enterprise Technologies. 2024. Vol. 4, Is. 9, P. 6–17. DOI:10.15587/1729–4061.2024.310521. URL: https://journals.uran.ua/eejet/article/view/310521.
- Gorbenko Yu.I., Kandii S.O. Comparison of security arguments of promising key encapsulation mechanisms // Radiotekhnika. 2022. Vol. 210. P. 22–36. DOI:10.30837/rt.2022.3.210.02. URL: http://rt.nure.ua/article/view/268561/264140.
- Kandiy S.O., Gorbenko I.D. Security analysis of promising key encapsulation mechanisms in the core–SVP model // Radiotekhnika. 2023. Vol. 212. P. 66–84. DOI:10.30837/rt.2023.1.212.06. URL: http://rt.nure.ua/article/view/286564.
- Kandii S.O., Gorbenko I.D. Analysis of DSTU 8961:2019 in the quantum random Oracle Model // Radiotekhnika. 2023. Vol. 214. P. 7–16. DOI:10.30837/rt.2023.3.214.01. URL: http://rt.nure.ua/article/view/297798/290701.
- Kandii S.O., Gorbenko I.D. Refinement of security estimates of quantum–resistant standards of asymmetric encryption taking into account the structure of q–arry lattices // Radiotekhnika. 2024. Vol 218. P. 76–92 DOI:10.30837/rt.2024.3.218.06 URL: http://rt.nure.ua/article/view/318798/309118.
- Kandii S.O., Gorbenko I.D. Assessing the influence of the algebraic structure of q–ary lattices on the complexity of cryptanalysis of problems on lattices // Radiotekhnika. 2024. Vol. 217. P. 79–99. DOI:10.30837/rt.2024.2.217.07. URL: http://rt.nure.ua/article/view/310856.

Наукова (науково-технічна) продукція:

Соціально-економічна спрямованість:

Охоронні документи на ОПІВ:

Впровадження результатів дисертації: Впроваджено

Зв'язок з науковими темами: 0121U109939

VI. Відомості про наукового керівника/керівників (консультанта)

Власне Прізвище Ім'я По-батькові:

1. Горбенко Іван Дмитрович

2. Ivan Gorbenko

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

Ідентифікатор ORCID ID: 0009-0003-6979-8946

Додаткова інформація:

Повне найменування юридичної особи: Харківський національний університет імені В. Н. Каразіна

Код за ЄДРПОУ: 02071205

Місцезнаходження: майдан Свободи, 4, Харків, Харківський р-н., 61022, Україна

Форма власності: Державна

Сфера управління: Міністерство освіти і науки України

Ідентифікатор ROR:

VII. Відомості про офіційних опонентів та рецензентів

Офіційні опоненти

Власне Прізвище Ім'я По-батькові:

1. Толюпа Сергій Васильович

2. Serhii Toliupa

Кваліфікація: д. т. н., професор, 05.12.02

Ідентифікатор ORCID ID: 0000-0002-1919-9174

Додаткова інформація:

Повне найменування юридичної особи: Київський національний університет імені Тараса Шевченка

Код за ЄДРПОУ: 02070944

Місцезнаходження: вул. Володимирська, буд. 60, Київ, 01033, Україна

Форма власності:

Сфера управління: Міністерство освіти і науки України

Ідентифікатор ROR: Не застосовується

Власне Прізвище Ім'я По-батькові:

1. Корченко Олександр Григорович

2. Korchenko Oleksandr H.

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

Ідентифікатор ORCID ID: Не застосовується

Додаткова інформація:

Повне найменування юридичної особи: Державний університет інформаційно-комунікаційних технологій

Код за ЄДРПОУ: 38855349

Місцезнаходження: вул. Солом'янська, буд. 7, Київ, 03110, Україна

Форма власності: Державна

Сфера управління: Міністерство освіти і науки України

Ідентифікатор ROR:

Власне Прізвище Ім'я По-батькові:

1. Чевардін Владислав Євгенович

2. Vladyslav Chevardin

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

Ідентифікатор ORCID ID: 0000-0002-1070-4568

Додаткова інформація:

Повне найменування юридичної особи: Військовий інститут телекомунікацій та інформатизації імені Героїв Крут

Код за ЄДРПОУ: 24978555

Місцезнаходження: вул. Московська, буд. 45/1, Київ, 01011, Україна

Форма власності: Державна

Сфера управління: Міністерство оборони України

Ідентифікатор ROR:

Рецензенти

Власне Прізвище Ім'я По-батькові:

1. Олійников Роман Васльович
2. Roman Oliynykov

Кваліфікація: д. т. н., професор, 05.13.05

Ідентифікатор ORCID ID: 0000-0002-3494-0493

Додаткова інформація:

Повне найменування юридичної особи: Харківський національний університет імені В. Н. Каразіна

Код за ЄДРПОУ: 02071205

Місцезнаходження: майдан Свободи, 4, Харків, Харківський р-н., 61022, Україна

Форма власності: Державна

Сфера управління: Міністерство освіти і науки України

Ідентифікатор ROR:

VIII. Заключні відомості

Власне Прізвище Ім'я По-батькові голови ради	Єсін Віталій Іванович
Власне Прізвище Ім'я По-батькові головуючого на засіданні	Єсін Віталій Іванович
Відповідальний за підготовку облікових документів	Шевченко Андрій Олександрович
Реєстратор	УкрІНТЕІ
Керівник відділу УкрІНТЕІ, що є відповідальним за реєстрацію наукової діяльності	Юрченко Тетяна Анатоліївна