Облікова картка дисертації

I. Загальні відомості

Державний обліковий номер: 0823U101234

Особливі позначки: відкрита

Дата реєстрації: 10-11-2023

Статус: Наказ про видачу диплома

Реквізити наказу МОН / наказу закладу: №НСВС/11/24 від 23.01.2024

II. Відомості про здобувача

Власне Прізвище Ім'я По-батькові:

1. Матійко Александра Андріївна
2. Aleksandra A. Matiiko

Кваліфікація:

Ідентифікатор ORCID ID: 0000-0002-6947-5958

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: Безпека державних інформаційних ресурсів

Дата захисту: 04-01-2024

Спеціальність за освітою: Кібербезпека

Місце роботи здобувача: Інститут спеціального зв'язку та захисту інформації Національного технічного університету України "Київський політехнічний інститут імені Ігоря Сікорського "

Код за ЄДРПОУ: 34979237

Місцезнаходження: вул. Верхньоключова, буд. 4, корпус 27, Київ, 03056, Україна

Форма власності: Державна

Сфера управління: Адміністрація Державної служби спеціального зв'язку та захисту інформації України

Ідентифікатор ROR:

III. Відомості про організацію, де відбувся захист

Шифр спеціалізованої вченої ради (разової спеціалізованої вченої ради): ДФ 26.002.41; ID 3025

Повне найменування юридичної особи: Національний технічний університет України "Київський політехнічний інститут імені Ігоря Сікорського"

Код за ЄДРПОУ: 02070921

Місцезнаходження: проспект Берестейський, буд. 37, Київ, 03056, 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: Національний технічний університет України "Київський політехнічний інститут імені Ігоря Сікорського"

Код за ЄДРПОУ: 02070921

Місцезнаходження: проспект Берестейський, буд. 37, Київ, 03056, Україна

Форма власності: Державна

Сфера управління: Міністерство освіти і науки України

Ідентифікатор ROR:

V. Відомості про дисертацію

Мова дисертації: Українська

Коди тематичних рубрик: 20.56.01

Тема дисертації:

1. Метод побудови обґрунтовано стійких симетричних NTRU-подібних шифросистем

2. Method of constructing provable secure NTRU-like encryption schemes

Реферат:

1. Дисертаційна робота присвячена вирішенню актуальної наукової задачі, яка полягає у розробці методу побудови симетричних NTRU-подібних шифросистем, що є обґрунтовано стійкими відносно атак на основі підібраних відкритих текстів. Протягом останніх років проведено значну кількість досліджень у галузі квантових технологій та квантових комп'ютерів, які використовують квантово-механічні явища для розв'язання обчислювальних задач, що є практично нерозв'язними за допомогою звичайних комп'ютерів. У зв'язку з тим, що поява квантового комп'ютера є лише питанням часу, виникає загроза поточному стану захищеності спеціальних інформаційно-комунікаційних систем. Це зумовлює необхідність створення нових криптосистем, які є стійкими до квантових атак. Сьогодні NTRU-подібні шифросистеми утворюють однин з найперспективніших класів постквантових криптосистем. Майже третина усіх криптосистем і протоколів,

поданих до відкритого конкурсу зі стандартизації асиметричних постквантових криптопримітивів NIST PQC, належать до решіткових або NTRU-подібних. Окрім того, новітній постквантовий алгоритм відкритого шифрування, стандартизований в Україні (ДСТУ 8961:2019 «Скеля»), також є NTRU-подібним. Прогрес у решіткової криптографії стимулює створення симетричних постквантових шифросистем, стійкість яких базується на складності розв'язанні лише однієї обчислювальної задачі. Поряд з тим, єдина відома на сьогодні симетрична NTRU-подібна шифросистема (NTRUCipher) виявляється вразливою відносно певних атак. В роботі вперше отримано аналітичні співвідношення для оцінювання ймовірності оборотності випадкових поліномів, які використовуються в NTRU-подібних шифросистемах. На відміну від відомого співвідношення для ймовірності оборотності випадкового рівноймовірного елементу кільця зрізаних поліномів, отримані співвідношення є справедливими для більш загальної схеми формування випадкових поліномів. Вони базуються на застосуванні апарату перетворення Фур'є розподілів ймовірностей на скінченному полі та надають змогу оцінювати (а в окремих практично важливих випадках – обчислювати) значення ймовірності оборотності випадкових поліномів, що використовуються в ролі компонентів секретних ключів NTRU-подібних шифросистем. Удосконалено аналітичні співвідношення для оцінювання ймовірності помилкового розшифрування повідомлень в NTRU-подібних шифросистемах. На відміну від раніше відомих, отримані співвідношення є справедливими для усіх видів сучасних NTRU-подібних шифросистем (як асиметричних, так і симетричних). Окрім того, вони дозволяють оцінювати ймовірність помилкового розшифрування повідомлень в NTRU-подібних шифросистемах при фіксованому ключі, надаючи, таким чином, більш адекватну інформацію про частоту виникнення помилок при розшифруванні. Дістав подальший розвиток метод оцінювання стійкості симетричних шифросистем NTRUCipher та NTRUCipher+ за рахунок дослідження трьох додаткових атак на ці шифросистеми. Для зазначених атак отримано аналітичні оцінки складності та показано, що, принаймні, одна з них може бути реалізована в режимі реального часу (хоча й не дозволяє відновлювати ключі шифросистем, а тільки відрізняти послідовності їхніх шифрованих повідомлень від суто випадкової послідовності). Вперше запропоновано метод побудови обґрунтовано стійких симетричних NTRU-подібних шифросистем. Показано, що на відміну від відомих симетричних NTRU-подібних шифросистем, запропоновані шифросистеми мають обґрунтовану стійкість відносно атак на основі підібраних відкритих повідомлень, яка базується на складності еталонної обчислювально складної задачі Decision-Ring-LWE. Практичне значення одержаних результатів полягає в тому, що дисертанткою розроблено програмні реалізації, які дозволяють в режимі реального часу обчислювати значення параметрів для побудови запропонованих обґрунтовано стійких NTRU-подібних шифросистем, обчислювати ймовірність оборотності випадкових поліномів та ймовірність помилкового розшифрування повідомлень у довільних NTRU-подібних шифросистемах. Крім того, отримані в роботі результати дозволяють: - зменшити ймовірність необоротності випадкового полінома в кільці Rn.q (з 0,5 до 1,5·10^-2) за рахунок належного вибору параметрів q і n NTRU-подібної шифросистеми; - вибирати параметри NTRU-подібних шифросистем, що забезпечують належне (мале) значення ймовірності помилкового розшифрування повідомлень при фіксованому секретному ключі; - встановити, що трудомісткість BKW-атаки на шифросистему NTRUCipher+ є в 2^15-2^69 разів вище в порівнянні з трудомісткістю аналогічної атаки на шифросистему NTRUCipher; - довести, що шифросистема NTRUCipher+ є цілком вразливою відносно розрізнювальної атаки, яка може бути реалізована в режимі реального часу (при цьому найбільше значення обсягу матеріалу, потрібного для реалізації атаки становить t=2^19); – обирати параметри NTRU-подібних шифросистем, які гарантують їхню стійкості на заздалегідь визначеному рівні □ (зокрема n=631, q=2693, d=56 при □=2^128, n=883, q=8089, d=168 при □=2^256).

2. Ph.D thesis is devoted to solving actual scientific problem of development the method of constructing NTRU-like encryption schemes that are provable secure against chosen plaintext attacks. In recent years, numerous researches has been carried out in the field of quantum technologies and quantum computers, which use quantum mechanical phenomena to solve computational problems that are practically unsolvable with the help of conventional computers. Due to the fact that the appearance of a quantum computer is only a matter of time, there is a threat to the current state of security of special information and communication systems. This

necessitates the creation of new cryptosystems that are security to quantum attacks. Today, NTRU-like cryptosystems form one of the most promising classes of post-quantum cryptosystems. Almost a third of all cryptosystems and protocols submitted to the NIST post-quantum competition (PQC) are lattice or NTRU-like. In addition, the latest post-quantum public-key encryption algorithm standardized in Ukraine (DSTU 8961:2019 “Skelya”) is also NTRU-like. Progress in lattice cryptography stimulates the creation of symmetric post-quantum encryption schemes, the security of which is based on the complexity of solving only one particular problem. Along with that, the only symmetric NTRU-like encryption scheme known today (NTRUCipher) is vulnerable to certain attacks. For the first time, analytical relations for estimating the probability of reversibility of random polynomials used in NTRU-like encryption schemes were obtained. In contrast to the known relation for the probability of reversibility of a random equiprobable element of a truncated polynomials ring, the obtained relations are valid for a more general scheme of random polynomials formation. They are based on the application of the Fourier transformation of probability distributions on a finite field and make it possible to estimate (and in some practically important cases to calculate) the probability value of reversibility of random polynomials used as components of secret keys of NTRU-like encryption schemes. Analytical relations for estimating decryption failure probability in NTRU-like encryption schemes were improved. Unlike the previously known ones, the obtained relations are valid for all types of modern NTRU-like encryption schemes (both asymmetric and symmetric one). In addition, they make it possible to estimate the decryption failure probability of messages in NTRU-like encryption schemes for a fixed key, thus providing more adequate information about the frequency of decryption failure. The method of estimating the security of symmetric encryption schemes NTRUCipher and NTRUCipher+ due to the research of three additional attacks on these encryption schemes was further developed. Analytical estimates of complexity for the mentioned attacks were obtained and it was shown that at least one of them can be implemented in real time (although it does not allow to recover the keys of encryption schemes but only to distinguish the sequences of their encrypted messages from a purely random sequence). For the first time, the method of constructing provable secure NTRU-like encryption schemes was proposed. It is shown that, in contrast to known symmetric NTRU-like encryption schemes, the proposed encryption schemes have provable security against chosen plaintext attacks, which is based on the complexity of reference computational Decision-Ring-LWE problem. The practical significance of the obtained results consist in developing the software implementations that allow in real time to calculate the parameters values for constructing proposed provable secure NTRU-like encryption schemes, to calculate the probability of reversibility of random polynomials and the decryption failure probability in arbitrary NTRU-like encryption schemes. In addition, the results obtained in this thesis allow: - reduce the probability of irreversibility of a random polynomial in the ring Rn.q (from 0,5 to 1,5·10^-2) due to proper selection of parameters q and n of NTRU-like encryption scheme; - choose the parameters of NTRU-like encryption schemes that provide an appropriate (small) value of decryption failure probability of messages for a fixed secret key; - establish that complexity of BKW-attack on the NTRUCipher+ encryption scheme is in 2^15-2^69 times higher compared to the complexity of a similar attack on the NTRUCipher encryption scheme; - prove that the NTRUCipher+ encryption scheme is quite vulnerable to a distinguishing attack that can be implemented in real time (at the same time, the largest value of the material’s amount required to implement the attack is t=2^19); - choose parameters of NTRU-like encryption schemes that guarantee their security at a predetermined level □ (in particular n=631, q=2693, d=56 at □=2^128, n=883, q=8089, d=168 at □=2^256).

Державний реєстраційний номер ДіР: 0119U102099, 0120U101801

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:

- Алексейчук А. Н., Матийко А. А. Оценки вероятности обратимости случайных многочленов, используемых в модифицированной версии криптосистемы NTRU. Радиотехника. 2017. № 189. С. 38–46.
- Олексійчук А. М., Матійко А. А. Оцінки ймовірності помилкового розшифрування повідомлень у шифросистемі NTRUEncrypt при фіксованому ключі. Захист інформації. 2018. Т. 20, № 2. С. 89–94.
- Матійко А. А. Порівняльний аналіз алгоритмів шифрування NTRUEncrypt та NTRUCipher. Математичне та комп'ютерне моделювання. Серія: Технічні науки. 2019. Вип. 19. С. 81–87.
- Матійко А.А. BKW-атака на шифросистеми NTRUCipher та NTRUCipher+. Information Technology and Security. 2020. Т. 8, № 2. С. 164–176.
- Олексійчук А. М., Матійко А. А. ШВИДКА РОЗРІЗНЮВАЛЬНА АТАКА НА ШИФРОСИСТЕМУ NTRUCipher+. Захист інформації. 2020. Т. 22, № 3. С. 183–189.
- Матійко А.А. Оцінки стійкості шифросистем NTRUCipher та NTRUCipher+ відносно BKW-атаки. Фізико-математичне моделювання та інформаційні технології. 2021. Вип. 33. С. 28–32.
- Олексійчук А. М., Матійко А. А. Метод побудови обґрунтовано стійких симетричних NTRU-подібних шифросистем. Information Technology and Security. 2022. Т. 10, № 2. С. 165–176.
- Alekseychuk A. N., Matiyko A. A. Achievable Upper Bound for the Sup-Norm of the Product of Elements of the Ring of Truncated Polynomials and its Application to the Analysis of NTRU-Like Cryptosystems. Cybernetics and Systems Analysis. 2021. Vol. 57, № 2. P. 190–195.
- Alekseychuk A. N., Matiyko A. A. Distinguishing Attack on the NTRUCipher Encryption Scheme. Cybernetics and Systems Analysis. 2022. Vol. 58, № 2. P. 186-190.

Наукова (науково-технічна) продукція: технології

Соціально-економічна спрямованість: забезпечення промисловості чи населення новим видом інформаційно-комунікаційних послуг

Охоронні документи на ОПІВ:

Впровадження результатів дисертації: Впроваджено

Зв'язок з науковими темами:

VI. Відомості про наукового керівника/керівників (консультанта)

Власне Прізвище Ім'я По-батькові:

1. Олексійчук Антон Миколайович

2. Anton M. Oleksiichuk

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

Ідентифікатор ORCID ID: 0000-0003-4385-4631

Додаткова інформація: https://www.scopus.com/authid/detail.uri?authorId=6504165390

Повне найменування юридичної особи: Інститут спеціального зв'язку та захисту інформації Національного технічного університету України "Київський політехнічний інститут імені Ігоря Сікорського "

Код за ЄДРПОУ: 34979237

Місцезнаходження: вул. Верхньоключова, буд. 4, корпус 27, Київ, 03056, Україна

Форма власності: Державна

Сфера управління: Адміністрація Державної служби спеціального зв'язку та захисту інформації України

Ідентифікатор ROR:

VII. Відомості про офіційних опонентів та рецензентів

Офіційні опоненти

Власне Прізвище Ім'я По-батькові:

1. Гнатюк Сергій Олександрович

2. Sergiy Gnatyuk

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

Ідентифікатор ORCID ID: 0000-0003-4992-0564

Додаткова інформація: https://www.scopus.com/authid/detail.uri?authorId=36184129600; https://scholar.google.com/citations?hl=uk&user=H8oHKbYAAAAJ&view_op=list_works&sortby=pubdate; https://www.researchgate.net/profile/Sergiy-Gnatyuk

Повне найменування юридичної особи: Національний авіаційний університет

Код за ЄДРПОУ: 01132330

Місцезнаходження: проспект Любомира Гузара, буд. 1, Київ, 03058, Україна

Форма власності: Державна

Сфера управління: Міністерство освіти і науки України

Ідентифікатор ROR:

Власне Прізвище Ім'я По-батькові:

1. Олійников Роман Васильович

2. Roman V. Oliynykov

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

Ідентифікатор ORCID ID: 0000-0002-3494-0493

Додаткова інформація: https://scholar.google.com.ua/citations?user=9ZHTlHYAAAAJ&hl; https://www.scopus.com/authid/detail.uri?authorId=36104503000

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

Код за ЄДРПОУ: 02071205

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

Форма власності: Державна

Сфера управління: Міністерство освіти і науки України

Ідентифікатор ROR:

Рецензенти

Власне Прізвище Ім'я По-батькові:

1. Конюшок Сергій Миколайович

2. Sergii M. Koniushok

Кваліфікація: к. т. н., доц., 05.13.21

Ідентифікатор ORCID ID: 0000-0003-4121-1464

Додаткова інформація: https://scholar.google.com/citations?user=Pr75GyMAAAAJ&hl=uk

Повне найменування юридичної особи: Інститут спеціального зв'язку та захисту інформації Національного технічного університету України "Київський політехнічний інститут імені Ігоря Сікорського "

Код за ЄДРПОУ: 34979237

Місцезнаходження: вул. Верхньоключова, буд. 4, корпус 27, Київ, 03056, Україна

Форма власності: Державна

Сфера управління: Адміністрація Державної служби спеціального зв'язку та захисту інформації України

Ідентифікатор ROR:

Власне Прізвище Ім'я По-батькові:

1. Яковлєв Сергій Володимирович
2. Serhii V. Yakovliev

Кваліфікація: к. т. н., 05.13.21

Ідентифікатор ORCID ID: 0000-0002-5647-5043

Додаткова інформація: https://scholar.google.com/citations?hl=uk&user=40BUMd0AAAAJ

Повне найменування юридичної особи: Національний технічний університет України "Київський політехнічний інститут імені Ігоря Сікорського"

Код за ЄДРПОУ: 02070921

Місцезнаходження: проспект Берестейський, буд. 37, Київ, 03056, Україна

Форма власності: Державна

Сфера управління: Міністерство освіти і науки України

Ідентифікатор ROR:

VIII. Заключні відомості

Власне Прізвище Ім'я По-батькові голови ради	Савчук Михайло Миколайович
Власне Прізвище Ім'я По-батькові головуючого на засіданні	Савчук Михайло Миколайович
Відповідальний за підготовку облікових документів	Матійко Александра Андріївна
Реєстратор	УкрІНТЕІ

Керівник відділу УкрІНТЕІ, що є відповідальним за реєстрацію наукової діяльності

Юрченко Тетяна Анатоліївна