Національний технічний університет України
«Київський політехнічний інститут імені Ігоря Сікорського»
Міністерство освіти і науки України

Національний технічний університет України
«Київський політехнічний інститут імені Ігоря Сікорського»
Міністерство освіти і науки України

Кваліфікаційна наукова
праця на правах рукопису

МАТІЙКО АЛЕКСАНДРА АНДРІЇВНА

УДК 621.391:519.2:004.056.55

ДИСЕРТАЦІЯ
МЕТОД ПОБУДОВИ ОБҐРУНТОВАНО СТІЙКИХ СИМЕТРИЧНИХ NTRU-ПОДІБНИХ ШИФРОСИСТЕМ

125 – «Кібербезпека»
12 – «Інформаційні технології»

Подається на здобуття наукового ступеня доктора філософії
Дисертація містить результати власних досліджень. Використання ідей, результаті і текстів інших авторів мають посилання на відповідне джерело
_____А.А. Матійко

Науковий керівник
Олексійчук Антон Миколайович, доктор технічних наук, доцент

Київ – 2023

АНОТАЦІЯ

Матійко А.А. Метод побудови обґрунтовано стійких симетричних NTRU-подібних шифросистем – Кваліфікаційна наукова праця на правах рукопису.

Дисертація на здобуття наукового ступеня доктора філософії з галузі знань 12 Інформаційні технології за спеціальністю 125 Кібербезпека. – Національний технічний університет України “Київський політехнічний інститут імені Ігоря Сікорського”, Київ, 2023.

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 численні дослідження у галузі квантових комп’ютерів, які використовують квантово-механічні явища для розв’язання обчислювальних задач, що є практично нерозв’язними за допомогою звичайних комп’ютерів. Оскільки створення квантових комп’ютерів є лише питанням часу, це серйозно загрожує конфіденційності та цілісності інформації у спеціальних інформаційно-комунікаційних системах. Виходячи з цього, у 2016 р. Національний інститут стандартів і технологій США оголосив відкритий конкурс зі стандартизації асиметричних постквантових криптопримітивів. Майже третина усіх криптосистем і протоколів, представлених на цьому конкурсі, належить до NTRU-подібних. (Зауважимо, що асиметрична шифросистема NTRU є на сьогодні однією з найшвидших та представляє широкий клас постквантових криптосистем з однойменною назвою, стійкість яких базується на складності знаходження коротких векторів у деяких решітках в евклідовому просторі). До того ж, новітній постквантовий алгоритм відкритого шифрування, стандартизований в Україні (ДСТУ 8961:2019 «Скеля») також є NTRU-подібним.

Однією з актуальних задач сучасної криптології є створення постквантових симетричних шифросистем, стійкість яких, аналогічно асиметричним, базується на складності розв'язанні лише однієї обчислювальної задачі. Зауважимо, що сучасні блокові чи потокові шифри не володіють такою властивістю. При цьому тривіальний метод побудови симетричних шифросистем, виходячи з асиметричних (шляхом "засекречування відкритого ключа"), виявляється цілком неприйнятним, оскільки не гарантує стійкості отриманих шифросистем відносно певних атак на основі підібраних відкритих текстів.

Єдиною відомою на сьогодні симетричною NTRU-подібною шифросистемою є алгоритм NTRUCipher, запропонований в 2017 р. Розробником шифросистеми проведено попередній аналіз її стійкості та наведено рекомендації стосовно вибору параметрів, які гарантують її стійкість відносно розглянутих ним атак. Поряд з тим, як показують подальші дослідження, шифросистема NTRUCipher є вразливою відносно деяких інших атак, причому природний спосіб модифікувати цю шифросистему задля підвищення її стійкості не приводить до успіху. Як наслідок, постає потреба у створенні методів побудови обґрунтовано стійких симетричних NTRU-подібних шифросистем, які відрізняються за сутністю від відомої.

Таким чином, існує певне протиріччя між потребами практики в обґрунтовано стійких постквантових (зокрема, NTRU-подібних) симетричних шифросистемах та відсутністю методів побудови таких шифросистем. Зазначене протиріччя приводить до наукової задачі, яка полягає у розробці методу побудови симетричних NTRU-подібних шифросистем, що є обґрунтовано стійкими відносно атак на основі підібраних відкритих текстів.

Для розв'язання поставленої наукової задачі використано методи теорії скінченних полів, теорії дискретного перетворення Фур'є на скінченних

абелевих групах, лінійної алгебри, теорії ймовірностей та кореляційного криптоаналізу.

Метою дисертаційної роботи є створення обґрунтовано стійких симетричних NTRU-подібних шифросистем для систем захисту інформації в інформаційно-комунікаційних системах.

Об’єктом дослідження у дисертаційній роботі є процес перетворення інформації з використанням сучасних NTRU-подібних шифросистем, а предметом дослідження – методи побудови та обґрунтування стійкості зазначених шифросистем відносно атак на основі підібраних відкритих текстів.

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 $R_{n.q}$ (з 0,5 до $1{,}5\cdot 10^{-2}$) 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 $2^{15} \div 2^{69}$ 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 λ (зокрема $n = 631$, $q = 2693$, $d = 56$ при $\lambda = 2^{128}$, $n = 883$, $q = 8089$, $d = 168$ при $\lambda = 2^{256}$).

Наукові та практичні результати дисертаційної роботи реалізовані в Службі зовнішньої розвідки України в результаті виконання НДР “Дорадо” та НДР “Сарган”, а також в науково-технічних розробках АТ “Інститут інформаційних технологій”.

Ключові слова: кібербезпека, криптоаналіз, постквантова криптографія, криптосистеми на основі решіток, статистичні атаки, NTRU-подібні шифросистеми, обґрунтування стійкості, ймовірність помилкового розшифрування.

ABSTRACT

Matiyko A. Method of constructing provable secure NTRU-like encryption schemes. – Qualifying scientific work as a manuscript.

Ph.D thesis in the field of knowledge 12 Information technologies in specialty 125 Cybersecurity. – National technical university of Ukraine “Igor Sikorsky Kyiv Polytechnic Institute”, Kyiv, 2023.

This 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 have been carried out in the field of quantum computers, which use quantum mechanical phenomena to solve computational problems that are practically unsolvable with the help of conventional computers. Since the creation of quantum computers is only a matter

of time, it seriously threatens the confidentiality and integrity of information in special information and communication systems. Based on this, in 2016 the US National Institute of Standards and Technology announced an open competition for the standardization of asymmetric post-quantum crypto primitives. Almost a third of all cryptosystems and protocols presented at this competition belong to NTRU-like. (Note that the NTRU asymmetric encryption scheme is currently one of the fastest and represents a wide class of post-quantum cryptosystems with the same name, the security of which is based on difficulty of finding short vectors in some lattices in Euclidean space). In addition, the latest post-quantum public-key encryption algorithm standardized in Ukraine (DSTU 8961:2019 “Skelya”) is also NTRU-like.

One of the most important problem in the field of cryptology is the design of symmetric encryption schemes, whose security, similarly to the asymmetric one, is based on the complexity of solving only one particular problem. Note that modern block or stream ciphers do not have this property. At the same time, the trivial method of constructing symmetric encryption schemes, based on asymmetric ones (by “secrecy of the public key”), turns out to be completely unacceptable, since it does not guarantee the security of received encryption schemes against chosen plaintext attack.

The only symmetric NTRU-like encryption scheme known today is the NTRUCipher, which was proposed in 2017. The developer of encryption scheme conducted a preliminary analysis of its security and gave recommendations regarding the selection of parameters that guarantee its security against attacks considered by him. In addition, further research shows that NTRUCipher is vulnerable to several other attacks, and the natural way to modify this encryption scheme to make it more robust does not lead to success. As a result, there is a need to create methods of constructing provable secure NTRU-like encryption schemes, which differ in essence from the known one.

Thus, there is a certain contradiction between the needs of practice in provable secure post-quantum (in particular, NTRU-like) symmetric encryption

schemes and the lack of methods for constructing such encryption schemes. This contradiction leads to a scientific problem, which consists in the development of a method of constructing provable secure NTRU-like encryption schemes against chosen-plaintext attacks.

The methods of finite field theory, discrete Fourier transform theory on finite Abelian groups, linear algebra, probability theory, and correlation cryptanalysis were used to solve the scientific problem.

The aim of Ph.D thesis is to create provable secure symmetric NTRU-like encryption schemes for information security systems in information and communication systems.

The object of research in Ph.D thesis is a process of information transformation using modern NTRU-like encryption schemes, and the subject of research is methods of constructing and security evaluation of encryption schemes against chosen-plaintext 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 $R_{n.q}$ (з 0,5 до $1{,}5 \cdot 10^{-2}$) 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 $2^{15} \div 2^{69}$ 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 λ (in particular $n = 631,\ q = 2693$, $d = 56$ at $\lambda = 2^{128}$, $n = 883,\ q = 8089,\ d = 168$ at $\lambda = 2^{256}$).

Scientific and practical results of the thesis were implemented at the Foreign Intelligence Service of Ukraine (in the research scientific works «Dorado» and «Sargan») and in the scientific and technical developments of JSC «Institute of Information Technologies».

Key words: cybersecurity, cryptanalysis, post-quantum cryptography, lattice-based cryptosystems, statistical attacks, NTRU-like encryption schemes, provable security, decryption failure probability.

Список основних публікацій здобувачки:

1. Алексейчук А. Н., Матийко А. А. Оценки вероятности обратимости случайных многочленов, используемых в модифицированной версии криптосистемы NTRU. *Радиотехника*. 2017. № 189. С. 38–46.

2. Олексійчук А. М., Матійко А. А. Bounds of decryption failure probability in NTRUEncrypt encryption scheme for a fixed key. *Ukrainian Information Security Research Journal*. 2018. Vol. 20, no. 2. DOI: https://doi.org/10.18372/2410-7840.20.12276.

3. Matiyko A. A. The Comparative Analysis of NTRUCipher and NTRUEncrypt Encryption Schemes. *Mathematical and computer modelling. Series: Technical sciences*. 2019. No. 19. P. 81–87. DOI: https://doi.org/10.32626/2308-5916.2019-19.81-87.

4. Matiyko A. BKW-attack on NTRUCIPHER and NTRUCIPHER+ enctyption schemes. *Collection "Information Technology and Security"*. 2020.

Vol. 8, no. 2. P. 164–176. DOI: https://doi.org/10.20535/2411-1031.2020.8.2.222599.

5. Олексійчук А. М., Матійко А. А. ШВИДКА РОЗРІЗНЮВАЛЬНА АТАКА НА ШИФРОСИСТЕМУ NTRUCipher+. *Ukrainian Information Security Research Journal*. 2020. Т. 22, № 3. С. 183–189. DOI: https://doi.org/10.18372/2410-7840.22.14981.

6. Matiyko A. Security estimates of the NTRUCipher and NTRUCipher+ encryption schemes against BKW-attack. *Physico-mathematical modelling and informational technologies*. 2021. No. 33. P. 28–32. DOI: https://doi.org/10.15407/fmmit2021.33.028.

7. Matiyko A., Alekseychuk A. Method for design secure symmetric NTRU-like encryption schemes. *Collection "Information Technology and Security"*. 2022. Vol. 10, no. 2. P. 165–176. DOI: https://doi.org/10.20535/2411-1031.2022.10.2.270406.

8. 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, no. 2. P. 190–195. DOI: https://doi.org/10.1007/s10559-021-00343-z.

9. Alekseychuk A. N., Matiyko A. A. Distinguishing Attack on the NTRUCipher Encryption Scheme. *Cybernetics and Systems Analysis*. 2022. Vol. 58, no. 2. P. 186-190. DOI: https://doi.org/10.1007/s10559-022-00449-y.

10. Олексійчук А. М., Матійко А. А. Оцінки ймовірності оборотності випадкових многочленів, що використовуються в модифікованій версії криптосистеми NTRU. *Безпека інформації в інформаційно-телекомунікаційних системах* : XIX Міжнар. науково-практ. конф., м. Буча, 25–26 трав. 2017 р. С. 82.

11. Олексійчук А. М., Матійко А. А. Оцінки ймовірності помилкового розшифрування повідомлень у шифросистеми NTRUEncrypt при фіксованому ключі. *Безпека інформації в інформаційно-телекомунікаційних*

системах : XX Міжнар. науково-практ. конф., м. Буча, 22–24 трав. 2018 р. С. 37.

12. Олексійчук А. М., Матійко А. А., Грицай В. А. Оцінка трудомісткості BKW-атаки на симетричну криптосистему NTRUCipher. *Актуальні питання застосування спеціальних інформаційно-телекомунікаційних систем* : Наукова-практ. конф. курсантів (студентів), аспірантів, докторантів та молодих уч., м. Київ, 23–24 черв. 2020 р. С. 80.

13. Олексійчук А. М., Матійко А. А. Швидка розрізнювальна атака на шифросистему NTRUCIPHER+. *Інформаційно-телекомунікаційні системи і технології та кібербезпека: нові виклики, нові завдання* : Наукова-практ. конф., м. Київ, 18–19 листоп. 2020 р. С. 31.

14. Олексійчук А. М., Матійко А. А., Грицай В. А. Дослідження стійкості симетричних NTRU-подібних шифросистем відносно атак на основі підібраних відкритих текстів. *Інформаційно–телекомунікаційні системи і технології та кібербезпека: нові виклики, нові завдання* : Наукова-практ. конф., м. Київ, 24 листоп. 2020 р. – 25 листоп. 2021 р. С. 47.

15. Олексійчук А. М., Матійко А. А. Метод побудови обґрунтовано стійких симетричних NTRU-подібних шифросистем. *Актуальні питання застосування спеціальних інформаційно-комунікаційних систем* : V науково-практ. конф. курсантів (студентів), аспірантів, докторантів та молодих уч., м. Київ, 29 листоп. 2022 р. С. 33.

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ

NIST – National Institute of Standards and Technology;

LWE – Learning With Errors;

SVP_γ – Shortest Vector Problem with parameter $\gamma \geq 1$;

CVP_γ – Closest Vector Problem with parameter $\gamma \geq 1$;

BDD_γ – Bounded Distance Decoding with parameter $\gamma \geq 1$;

CPA – chosen-plaintext attack;

ММП – метод максимуму правдоподібності;

СР – система рівнянь;

ОС – операційна система.

ВСТУП

Актуальність теми. Протягом останніх років проведено численні дослідження у галузі квантових комп'ютерів, які використовують квантово-механічні явища для розв'язання обчислювальних задач, що є практично нерозв'язними за допомогою звичайних комп'ютерів. Оскільки створення квантових комп'ютерів є лише питанням часу, це серйозно загрожує конфіденційності та цілісності інформації у спеціальних інформаційно-комунікаційних системах. Виходячи з цього, у 2016 р. Національний інститут стандартів і технологій США оголосив відкритий конкурс зі стандартизації асиметричних постквантових криптопримітивів. Майже третина усіх криптосистем і протоколів, представлених на цьому конкурсі, належить до NTRU-подібних. (Зауважимо, що асиметрична шифросистема NTRU є на сьогодні однією з найшвидших та представляє широкий клас постквантових криптосистем з однойменною назвою, стійкість яких базується на складності знаходження коротких векторів у деяких решітках в евклідовому просторі). До того ж, новітній постквантовий алгоритм відкритого шифрування, стандартизований в Україні (ДСТУ 8961:2019 «Скеля») також є NTRU-подібним.

Однією з актуальних задач сучасної криптології є створення постквантових симетричних шифросистем, стійкість яких, аналогічно асиметричним, базується на складності розв'язанні лише однієї обчислювальної задачі. Зауважимо, що сучасні блокові чи потокові шифри не володіють такою властивістю. При цьому тривіальний метод побудови симетричних шифросистем, виходячи з асиметричних (шляхом "засекречування відкритого ключа"), виявляється цілком неприйнятним, оскільки не гарантує стійкості отриманих шифросистем відносно певних атак на основі підібраних відкритих текстів.

Єдиною відомою на сьогодні симетричною NTRU-подібною шифросистемою є алгоритм NTRUCipher, запропонований в 2017 р. Розробником шифросистеми проведено попередній аналіз її стійкості та наведено рекомендації стосовно вибору параметрів, які гарантують її стійкість відносно розглянутих ним атак. Поряд з тим, як показують подальші дослідження, шифросистема NTRUCipher є вразливою відносно деяких інших атак, причому природний спосіб модифікувати цю шифросистему задля підвищення її стійкості не приводить до успіху. Як наслідок, постає потреба у створенні методів побудови обґрунтовано стійких симетричних NTRU-подібних шифросистем, які відрізняються за сутністю від відомої.

Таким чином, існує певне протиріччя між потребами практики в обґрунтовано стійких постквантових (зокрема, NTRU-подібних) симетричних шифросистемах та відсутністю методів побудови таких шифросистем. Зазначене протиріччя приводить до *наукової задачі, яка полягає у розробці методу побудови симетричних NTRU-подібних шифросистем, що є обґрунтовано стійкими відносно атак на основі підібраних відкритих текстів*, розв’язанню якої присвячено дану дисертаційну роботу.

Зв'язок роботи з науковими програмами, планами, темами. Робота над дисертацією проводилася в рамках виконання науково-дослідних робіт “Дорадо” (номер держреєстрації 0119U102099) та “Сарган” (номер держреєстрації 0120U101801) на замовлення Служби зовнішньої розвідки України та відповідно до планів науково-дослідної роботи Інституту спеціального зв’язку та захисту інформації Національного технічного університету України “Київський політехнічний інститут імені Ігоря Сікорського”.

Мета та задачі досліджень. *Метою дисертаційної роботи* є створення обґрунтовано стійких симетричних NTRU-подібних шифросистем для систем захисту інформації в інформаційно-комунікаційних системах.

Для досягнення поставленої мети **необхідно розв'язати такі окремі задачі дослідження:**

1. Провести аналіз відомих методів побудови та оцінювання й обґрунтування стійкості NTRU-подібних шифросистем.

2. Отримати аналітичні співвідношення для ймовірності оборотності випадкових поліномів, які використовуються в NTRU-подібних шифросистемах.

3. Отримати аналітичні співвідношення для оцінювання ймовірності помилкового розшифрування повідомлень в NTRU-подібних шифросистемах при фіксованому ключі.

4. Отримати аналітичні оцінки складності статистичних атак на симетричні шифросистеми NTRUCipher та NTRUCipher+.

5. Розробити метод побудови симетричних NTRU-подібних шифросистем, які мають обґрунтовану стійкість відносно атак на основі підібраних відкритих текстів.

Об'єктом дослідження у дисертаційній роботі є процес перетворення інформації з використанням сучасних NTRU-подібних шифросистем, а *предметом дослідження* – методи побудови та обґрунтування стійкості зазначених шифросистем відносно атак на основі підібраних відкритих текстів.

Методи дослідження. Основу дисертаційних досліджень складають теоретичні дослідження (математичні методи оцінювання та обґрунтування стійкості симетричних NTRU-подібних шифросистем). Для розв'язання окремої задачі 2 використано методи теорії скінченних полів і теорії дискретного перетворення Фур'є на скінченних абелевих групах. Задачу 3 розв'язано за допомогою методів теорії ймовірностей та лінійної алгебри, а задачі 4, 5 – з використанням методів теорії скінченних полів, теорії ймовірностей та кореляційного криптоаналізу. Для проведення чисельних розрахунків та програмної реалізації запропонованих шифросистем

використано PyCharm – інтегроване середовище розробки для мови програмування Python.

Наукова новизна отриманих результатів. Підсумком вирішення перелічених вище окремих задач є такі нові наукові результати, що висуваються на захист.

1. *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.

2. *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.

3. *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).

4. *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 отриманих результатів. Представлені в дисертаційній роботі нові наукові та практичні результати дозволяють:

– зменшити ймовірність необоротності випадкового полінома в кільці $R_{n.q}$ (з 0,5 до $1{,}5\cdot 10^{-2}$) 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 $2^{15} \div 2^{69}$ 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 λ (зокрема $n = 631$, $q = 2693$, $d = 56$ при $\lambda = 2^{128}$, $n = 883$, $q = 8089$, $d = 168$ при $\lambda = 2^{256}$).

Дисертантом розроблено також комп’ютерні програми, 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.

Наукові та практичні *результати дисертаційної роботи реалізовані* в Службі зовнішньої розвідки України – в результаті виконання НДР “Дорадо” (акт від 27.09.2022) та НДР “Сарган“ (акт від 27.09.2022) та в науково-технічних розробках АТ “Інститут інформаційних технологій” (акт від 24.11.2022).

Особистий внесок здобувача. У статті [1] та тезах доповіді [10] здобувачем отримано аналітичні співвідношення, які дозволяють оцінювати ймовірність оборотності випадкових поліномів, що використовуються в ролі ключів в NTRU-подібних шифросистемах; у статті [2] та тезах доповіді [11] дисертантом отримано аналітичні співвідношення для оцінювання ймовірності помилкового розшифрування повідомлень при фіксованому ключі у шифросистемі NTRUEncrypt, а у статті [8] – узагальнення цих співвідношень для довільної NTRU-подібної шифросистеми; у статті [5] та тезах доповіді [13] здобувачу належать оцінки трудомісткості швидкої розрізнювальної атаки на шифросистему шифросистеми NTRUCipher+, а також висновок про недоцільність практичного використання цієї шифросистеми. Нарешті у статті [7] та тезах доповіді [15] дисертантом запропоновано метод побудови симетричних NTRU-побідних шифросистем, що є обґрунтовано стійкими відносно атак на основі підібраних відкритих текстів.

Апробація результатів дисертації. Результати дисертаційних досліджень доповідалися та обговорювалися на XIX та XX Міжнародних науково-практичних конференціях “Безпека інформації в інформаційно-телекомунікаційних системах” (Київ, 2017-2018), Міжнародному науковому симпозіумі “Питання оптимізації обчислень (ПОО-XLVI)” (м. Київ, 2019), Науково-практичній конференції курсантів (студентів), аспірантів, докторантів та молодих учених “Актуальні питання застосування

спеціальних інформаційно-телекомунікаційних систем" (Київ, 2020), Науково-практичних конференціх "Інформаційно-телекомунікаційні системи і технології та кібербезпека: нові виклики, нові завдання" (Київ, 2020 та 2021 роки), Міжнародній науковій конференції "Питання оптимізації обчислень (ПОО-XLVII)" (м. Львів), V науково-практичній конференції курсантів (студентів), аспірантів, докторантів та молодих учених "Актуальні питання застосування спеціальних інформаційно-комунікаційних систем" (Київ, 2022).

Публікації. Основні наукові результати дисертаційної роботи опубліковано в 9 наукових працях (з них 3 без співавторів), з яких 7 наукових статей [1 – 7] в наукових фахових виданнях України та 2 наукові статті [8, 9] індексуються у міжнародній наукометричній базі даних Scopus, 6 тез доповідей на науковому симпозіумі, наукових та науково-практичних конференціях [10 – 15].

Структура роботи та її обсяг. Дисертація складається з анотації, змісту, переліку умовних позначень, вступу, чотирьох розділів, загальних висновків, додатків, списку використаних джерел (в кінці кожного розділу основної частини дисертації) і має 158 сторінок основного тексту, 3 рисунки, 18 таблиць, 20 сторінок додатків. Список використаних джерел містить 162 найменування і займає 24 сторінки. Загальний обсяг дисертаційної роботи – 178 сторінок.

РОЗДІЛ 1

АНАЛІЗ СУЧАСНОГО СТАНУ ТА НАПРЯМІВ РОЗВИТКУ МЕТОДІВ ПОБУДОВИ NTRU-ПОДІБНИХ ШИФРОСИСТЕМ

1.1. Аналіз ролі та перспектив розвитку постквантових криптосистем в системах захисту інформації сучасних інформаційно-комунікаційних систем

Протягом останнього десятиліття спостерігається активізація досліджень в галузі квантових комп'ютерів – пристроїв, що використовують квантово-механічні явища для розв'язання математичних задач, які є обчислювально складними для звичайних комп'ютерів.

У 1985 р. Д. Дойч [1] описав побудову квантових логічних елементів для "універсального квантового комп'ютера". Пізніше П. Шор [2] розробив алгоритм, який розкладає цілі числа на множники за допомогою квантового комп'ютера. Основною одиницею інформації для квантових комп'ютерів є кубіти, які являють собою "квантовий еквівалент" бітів у класичних комп'ютерах. Нагадаємо, що біт може перебувати лише в одному із станів: 1 або 0. Однак кубіти не обмежуються тільки цими станами та можуть існувати у так званих суперпозиціях. Іншими словами, кубіт може існувати в станах 0, 1 або лінійній комбінації обох станів. Саме ця властивість кубітів забезпечує "паралелізм" квантових обчислень (експоненційне збільшення обсягу інформації, яка обробляється), що виключає необхідність перебору всіх можливих значень в деяких обчислювальних алгоритмах [3].

Можливість створення потужних квантових комп'ютерів ставить під загрозу більшість класичних криптосистем із відкритим ключем. Отже, конфіденційність та цілісність інформації у спеціальних інформаційно-комунікаційних системах в цілому опиняються під загрозою. Протокол Діффі-Геллмана [4], криптосистеми RSA [5] та Ель-Гамаля [6],

криптосистеми на основі еліптичних кривих [7] є прикладами класичних асиметричних криптосистем і протоколів, стійкість яких базується на складності розв'язання задач теорії чисел (таких як факторизація чи дискретне логарифмування). Проте усі зазначені криптосистеми є вразливими для квантових комп'ютерів. Зокрема, шифросистема RSA з довжиною ключа 2048 бітів забезпечує належний захист від класичних атак, але не від квантових. Більш того, шифр "Калина" [8 – 10] з довжиною ключа 256 бітів забезпечує стійкість відносно квантових атак на рівні 2^{128}, тоді як збільшення довжини ключа шифросистеми RSA у 7,5 разів майже не впливає на її стійкість відносно таких атак [11].

Сьогодні над створенням квантових комп'ютерів працює багато провідних компаній: IBM [12, 13], D-Wave Systems [14, 15], Microsoft [16], Google [17], Intel [18], Amazon [19], IonQ [20] тощо. Наприклад, компанія Amazon відносно нещодавно почала роботу над створенням квантового комп'ютера і в 2021 році оголосила про відкриття Центру квантових обчислень AWS (Amazon Web Services) у Пасадені, штат Каліфорнія. Компанія співпрацює з Каліфорнійським технологічним інститутом, щоб сприяти новому поколінню науковців у сфері квантових обчислень і стимулювати їхні зусилля зі створення відмовостійкого квантового комп'ютера. До того ж Amazon пропонує послугу квантових обчислень, яка дозволяє клієнтам прискорити власні дослідження зі створення квантових проектів та моделювання квантових алгоритмів. В свою чергу, D-Wave Systems є першою в світі організацією, яка продала комерційний квантовий комп'ютер. Його остання версія D-Wave Advantage має процесорну архітектуру з понад 5000 кубітами та 15-канальним підключенням кубітів [21].

У зв'язку з вищесказаним відчувається нагальна потреба у створенні нових, постквантових, криптографічних систем, які залишаться стійкими за умови існування потужних квантових комп'ютерів [22]. Тому у 2016 році

Національний інститут стандартів і технологій (NIST) оголосив відкритий конкурс з розробки нових стандартів постквантових криптосистем та протоколів [23].

В даний час ця розробка здійснюється, в основному, на основі таких об’єктів (рис. 1.1) [24, 25]:

– лінійних блокових кодів;
– решіток в евклідовому просторі;
– ґеш-функцій;
– ізогеній еліптичних кривих;
– квадратичних систем булевих рівнянь.

Необхідно зазначити, що до постквантових відносять також сучасні потокові та блокові шифри (за умови належного збільшення довжини їхніх ключів) [26].

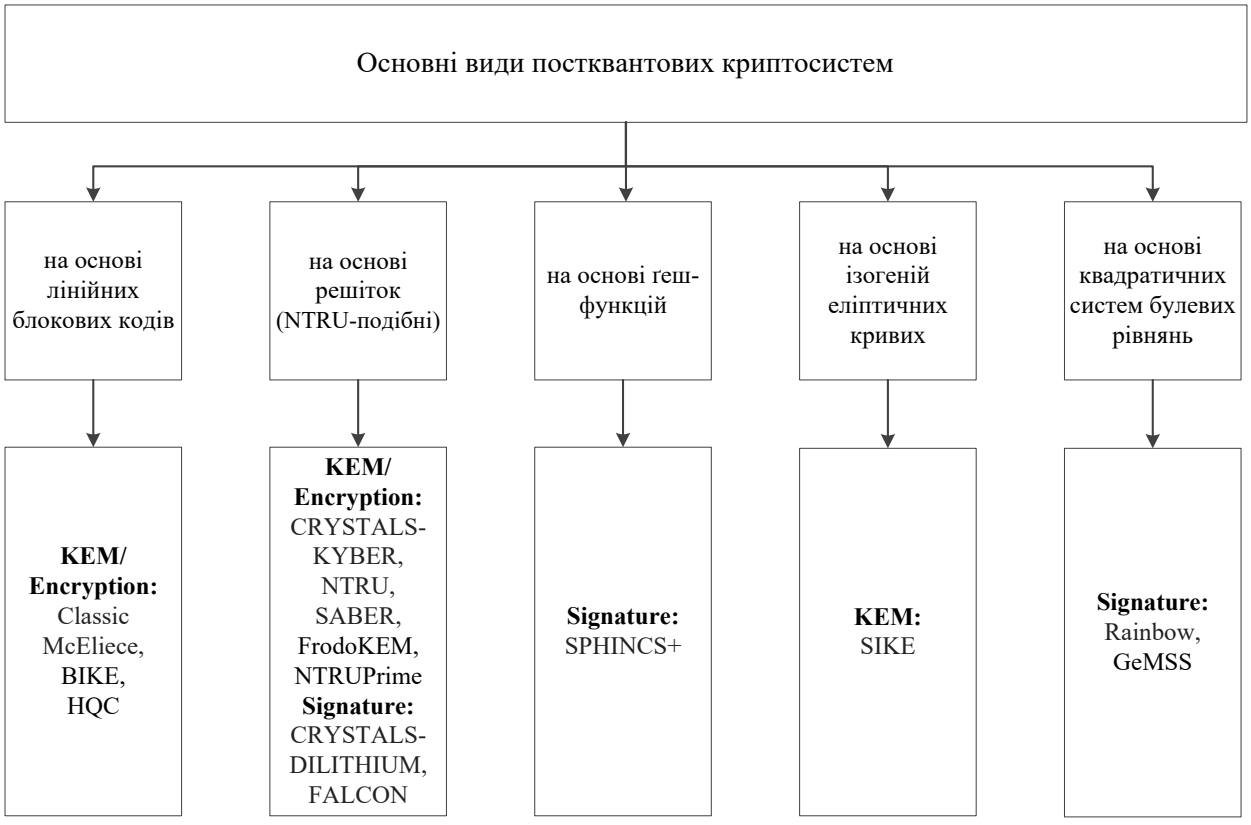

Рисунок 1.1. Основні види та приклади постквантових криптосистем

Стійкість кодових криптосистем базується на складності деяких задач теорії кодування і теорії вивідування (learning theory) [24, 25, 27]. Ці криптосистеми будуються на основі відомих класів завадостійких кодів (таких як коди Гоппи [28]), що можуть бути “замасковані” під суто випадкові блокові коди, декодування яких є обчислювально складною задачею. Недоліком цих криптосистем є достатньо великі довжини ключів, потрібні для забезпечення належної стійкості.

Зауважимо, що усі кодові схеми цифрового підпису, подані до конкурсу NIST, виявилися нестійкими, а переможцями в номінації протоколів інкапсуляції ключів (KEM) стали Classic McEliece [27, 29], BIKE [30] та HQC [31] (рис. 1.1). При цьому алгоритм Classic McEliece обрано першим фіналістом, а BIKE та HQC – альтернативними кандидатами.

Стійкість криптосистем на основі ґеш-функцій базується на складності задач пошуку прообразу значення ґеш-функції або обчислення її колізії [24, 25, 32]. Такі криптосистеми потребують менше обчислювальних припущень при обґрунтуванні стійкості в порівнянні з алгоритмами, що будуються на основі задач теорії чисел (наприклад, RSA чи DSA). Складність пошуку колізії ґеш-функції з довжиною значень n бітів за допомогою класичного алгоритму становить $2^{n/2}$, проте квантовий алгоритм Гровера [33] розв’язує цю задачу зі складністю $2^{n/3}$. Схему цифрового підпису Sphincs+ [34], що базується на ґеш-функціях, обрано як альтернативне рішення у третьому раунді конкурсу NIST [23].

Криптосистеми на основі квадратичних систем булевих рівнянь [35] базуються на складності розв’язання довільних систем квадратних рівнянь від декількох змінних над полем з двох елементів. Наразі такі схеми шифрування не дуже ефективні, оскільки мають великі за довжиною відкриті ключі та характеризуються тривалим часом розшифрування. Проте ситуація зі схемами цифрового підпису виявляється трохи кращою. З дев’ятнадцяти схем підпису, поданих до конкурсу NIST, сім базуються на квадратичних

системах булевих рівнянь, при цьому дві з цих семи пройшли до третього раунду. В результаті схема Rainbow [36] обрана як один із трьох фіналістів, а схема GeMMS [37] – як альтернативний кандидат. Ці схеми характеризуються дуже короткими розмірами підписів (усього 33 байти), але їхнім недоліком є досить великий розмір відкритих ключів (160 КБ або більше).

Криптосистеми на основі ізогеній еліптичних кривих запропоновані в 2006 році [38] і, таким чином, є найновітнішими серед сучасних видів постквантових криптосистем. Ізогенія – це відображення між двома еліптичними кривими, що є гомоморфізмом [39]. Пізніше запропоновано використовувати ізогенії суперсингулярних кривих [40] для підвищення стійкості та зменшення часу виконання операцій шифрування та розшифрування даних. Стійкість таких криптосистем ґрунтується на припущенні про обчислювальну складність задачі пошуку шляху в графі ізогеній суперсингулярної еліптичної кривої. Головними перевагами таких криптосистем є відносно невеликі за довжиною ключі. Лише одну криптосистему на основі ізогеній, а саме SIKE [41], подано на конкурс NIST, яка і стала альтернативним кандидатом.

Нарешті, одним з найперспективніших класів постквантових криптосистем є решіткові, зокрема, NTRU-подібні [11], криптосистеми. Для цього є декілька причин. По-перше, їхня стійкість базується на складності розв’язання декількох добре відомих обчислювально складних задач (таких як SVP_γ чи LWE; див. нижче підрозділ 1.2). По-друге, ці криптосистеми надають змогу створювати різноманітні криптографічні примітиви (такі як схеми гомоморфного чи функціонального шифрування [42]). По-третє, вони забезпечують високу швидкість шифрування поряд з помірними довжинами ключів (наприклад, алгоритм NTRUEncrypt виявляється майже в 100 разів швидше за RSA [43]).

Приблизно третина криптосистем, поданих до конкурсу NIST, побудована на основі решіток. При цьому в якості фіналістів обрано шифросистеми Kyber [44], NTRU [45], SABER [46], а також схеми цифрового підпису Chrystal-Dilithium [47] і Falcon [48].

Таким чином, створення у найближчій перспективі квантових комп'ютерів сприяє розробці та застосуванню постквантових криптосистем, стійкість яких базується на математичних задачах, що є обчислювально складними як до традиційного, так і до квантового криптоаналізу. Як з теоретичного, так і з практичного поглядів, важливий клас серед зазначених криптосистем утворюють решіткові (NTRU-подібні) криптосистеми, до яких відноситься, зокрема, приблизно третина всіх криптосистем і протоколів, поданих до конкурсу NIST, а також новітній національний стандарт асиметричного шифрування [49].

1.2. Обчислювально складні задачі, на яких базується стійкість NTRU-подібних шифросистем

Позначимо $\mathbf{R}^n$ множину n-вимірних векторів з дійсними координатами. Ця множина є евклідовим простором відносно скалярного добутку векторів $xy = x_1y_1 + \cdots + x_ny_n$, де $x = (x_1,...,x_n)$, $y = (y_1,...,y_n)$. Довжина (або евклідова норма) вектора x визначається за формулою $\| x \|_2 = \left(\sum_{i=1}^{n} | x_i |^2 \right)^{1/2}$.

Решіткою у просторі $\mathbf{R}^n$ називається адитивна група, що складається з усіх лінійних комбінацій з цілими коефіцієнтами заздалегідь визначених лінійно незалежних векторів $b_1,...,b_m \in \mathbf{R}^n$. Набір зазначених векторів називається *базисом решітки*. При цьому їхня кількість m залежить тільки

від решітки та називається її *вимірністю*. Решітка максимальної вимірності $m = n$ називається *повною*.

Стійкість сучасних NTRU-подібних (та деяких інших) криптосистем базується на складності розв'язання окремих задач, пов'язаних із решітками. Найважливішими з них є такі (див., наприклад, [50]).

1. Задача про найкоротший вектор з параметром $\gamma \geq 1$ (SVP_γ): для заданого базису $b_1,...,b_n$ повної решітки L знайти ненульовий вектор $b \in L$ такий, що $\| b \|_2 \leq \gamma \lambda_1(L)$, де $\lambda_1(L) = \min\{\| x \|_2 : x \in L \setminus \{0\}\}$.

2. Задача про найближчий вектор з параметром $\gamma \geq 1$ (CVP_γ): для заданого базису $b_1,...,b_n$ повної решітки L та вектора $x \in \mathbf{R}^n$ знайти вектор $b \in L$ такий, що $\| x - b \|_2 \leq \gamma \operatorname{dist}(x, L)$, де $\operatorname{dist}(x, L)$ – відстань від x до L.

3. Задача декодування на обмеженій відстані з параметром $\gamma \geq 1$ (BDD_γ): для заданого базису $b_1,...,b_n$ повної решітки L та вектора $x \in \mathbf{R}^n$ такого, що $\operatorname{dist}(x, L) \leq \gamma^{-1} \lambda_1(L)$, знайти вектор $b \in L$ такий, що $\| x - b \|_2 = \operatorname{dist}(x, L)$,

Зрозуміло, що часова складність цих задач зростає з ростом n та зменшується з ростом γ. Розпізнавальна версія задачі SVP_γ (коли треба вирішити, чи є довжина найкоротшого вектора решітки не вище за 1, чи вона є більше ніж γ за умови, що одна із зазначених альтернатив має місце) є NP-складною (NP-hard) для достатньо малих значень γ [51, 52]. Аналогічний результат має місце і для задачі CVP_γ [53, 54]. Незважаючи на те, що найбільші значення γ, для яких доведено подібні твердження, є малими (меншими за n^c для будь-якого $c > 0$), обидві задачі залишаються на сьогодні обчислювально складними для достатньо великих значень γ. Найкращі з відомих алгоритмів розв'язання цих задач для $\gamma \leq \mathrm{poly}(n)$ мають експоненційні оцінки часової складності та гіпотетично вважаються

експоненційними у найгіршому випадку [55 – 59]. Алгоритм Шнорра [60] із допоміжною процедурою, описаною в [57], надає змогу балансування між складністю розв'язання задачі та якістю результату. На сьогодні цей алгоритм вважається найкращим для проміжних значень $\gamma = k^{O(nk^{-1})}$ та має часову і ємкісну складності вигляду $\mathrm{poly}(n)2^{O(k)}$ (з точністю до співмножника, який поліноміально залежить від довжини вхідних даних). Вважаючи $k = O(\log n)$, отримаємо поліноміальний алгоритм для $\gamma = k^{O\left(n\frac{\log\log n}{\log n}\right)}$. Покращення цих оцінок залишається відкритою проблемою [50].

Зазначимо також, що на сьогодні не відомо як можна покращити класичні алгоритми розв'язання наведених задач за допомогою квантових комп'ютерів. Отже, ці задачі вважаються складними за умови існування останніх [50, 61 – 63].

Усі відомі алгоритми розв'язання задачі SVP_γ базуються на побудові так званих редукованих базисів вхідної решітки, тобто базисів, які складаються з достатньо коротких та майже ортогональних у певному сенсі векторів (при цьому, в ролі розв'язку задачі вибирається найкоротший вектор у редукованому базисі).

Найвідомішим алгоритмом побудови редукованого (а точніше, LLL-редукованого) базису решітки є алгоритм Ленстри-Ленстри-Ловаса [64]. Він має поліноміальну складність, проте є застосовним лише для значень γ, які експоненційно зростають з ростом n. Відомі численні вдосконалення цього алгоритму [60, 65 – 69], проте їхня складність має той самий порядок росту як функція розміру задачі.

Для менших значень γ є застосовними алгоритми, які мають більшу часову складність (табл. 1.1), проте саме вони використовуються для оцінювання стійкості сучасних NTRU-подібних шифросистем [50].

Таблиця 1.1 – Сучасні алгоритми розв'язання задач SVP_γ и CVP_γ

Джерело, де опубліковано алгоритм	Верхня оцінка часової складності алгоритму	Верхня оцінка ємкісної складності алгоритму
[57] для SVP_γ і CVP_γ	$2^{2n+o(n)}$	$2^{n+o(n)}$
[58, 59 ,70 – 72] для SVP_γ [73, 74] для CVP_γ	$2^{2.465n+o(n)}$ $(2+1/(\gamma-1))^{O(n)}$	$2^{1.325n+o(n)}$ $(2+1/(\gamma-1))^{O(n)}$
[56, 75 – 79] для SVP_γ [56, 75 – 79] для CVP_γ	$n^{n/(2e)+o(n)}$ $n^{n/2+o(n)}$	$\mathrm{poly}(n)$ $\mathrm{poly}(n)$

Одним з найшвидших на сьогодні алгоритмів побудови редукованого базису решітки є блоковий алгоритм Коркіна-Золотарьова BKZ 2.0 [80]. Цей алгоритм залежить від натуральних параметрів β і l, що позначають так звані довжину блоку та кількість ітерацій відповідно, і дозволяє будувати редукований за Коркіним-Золотарьовим базис повної решітки вимірності n за $2^{E(\beta, l, n)}$ операцій, де

$$E(\beta, l, n) = 0{,}000784314\,\beta^2 + 0{,}366078\,\beta + \log(nl) + 0{,}875$$

(зауважимо, що наведена формула є емпіричною оцінкою, яка базується на результатах обчислювальних експериментів [81]).

Мірою якості редукованого базису, який будується за допомогою алгоритму BKZ 2.0, є так званий кореневий фактор Ерміта (root Hermire factor): число $\delta > 1$, що визначається за формулою $\| b_1 \|_2 = \delta^n (\det L)^{1/n}$, де b_1 є найкоротшим вектором у побудованому базисі, $\det(L)$ – об'єм решітки L [80]. В [80] описано симулятор алгоритму BKZ 2.0, який надає змогу обчислювати за вхідним параметром $\delta > 1$ такі значення параметрів β і l, що застосування алгоритму BKZ 2.0 з цими параметрами до будь-якого вхідного базису повної решітки вимірності n приводить до її редукованого базису з кореневим фактором Ерміта δ. Такий підхід до оцінювання

складності розв'язання задач SVP_γ і CVP_γ використовується в [81] та [82] при аналізі стійкості алгоритмів NTRUEncrypt та NTRU Prime відповідно. Зауважимо також, що протягом останніх років запропоновано низку алгоритмів розв'язання зазначених задач за допомогою методів просіювання (sieving methods). Найефективніші з відомих сьогодні таких алгоритмів мають евристичну трудомісткість $(3/2)^{n/2+o(1)}$ при $n \to \infty$, де n – вимірність решітки, причому залишковий член $o(1)$ є додатним числом [83, 84].

В цілому, кожна з трьох наведених вище задач вважається сьогодні обчислювально складною, а найкращі з відомих алгоритмів розв'зання цих задач є експоненційними у найгіршому випадку.

Іншою задачею, на якій базується стійкість багатьох решіткових криптосистем (зокрема, схем цифрового підпису та протоколів інкапсуляції ключів [23]) є задача LWE (Learning With Errors) [85, 86].

Ця задача має два варіанти постановки, перший з яких полягає в тому, щоб розв'язати певну систему лінійних рівнянь зі спотвореними правими частинами над скінченним полем або кільцем лишків за натуральним модулем, а другий – в тому, щоб відрізнити послідовність у правій частині такої системи рівнянь від суто випадкової послідовності елементів цього поля або кільця відповідно.

Точна постановка задачі є такою [85 – 87]. Розглядається вектор $b = As + \xi$, де s – невідомий вектор-стовпець довжини n над скінченним комутативним кільцем R, A – $t \times n$-матриця над цим кільцем, вибрана навмання (тобто випадково і рівноймовірно), ξ – вектор з незалежними випадковими координатами, кожна з яких має той самий нерівномірний розподіл на кільці R. Треба відновити вектор s за відомими A, b та законом розподілу координат вектора ξ. Розпізнавальний варіант задачі LWE (Decision LWE) полягає в тому, щоб статистично відрізнити вектор b зазначеного вигляду від випадкової рівноймовірної послідовності довжини m елементів кільця R.

Відомо [86], що обидві варіанти задачі є рівносильними з погляду обчислювальної складності. Класична версія задачі LWE (коли $R = \mathbf{Z}_q$, де q є простим числом, $m = \text{poly}(n)$, $q < 2^{\text{poly}(n)}$, а розподіл спотворень у правих частинах рівнянь є дискретним гаусовим з певними параметрами) є не менш складною, ніж задача SVP_γ для $\gamma = O(n)$, навіть за умови існування квантового комп'ютера [85, 86]. Поряд з тим, обчислювально стійкими є на сьогодні деякі інші версії цієї задачі, наприклад, коли розподіл спотворень є рівномірним на певній невеликій за потужністю підмножині кільця $R = \mathbf{Z}_q$, де q є простим числом [85 – 90].

Складність відомих алгоритмів розв'язання задачі LWE залежить від числа m рівнянь у системі та розподілу координат вектора ξ. У випадку $m = \text{poly}(n)$, який становить найбільший інтерес з погляду побудови асиметричних криптосистем, усі відомі алгоритми базуються на зведенні вхідної задачі до задачі SVP_γ. Таке зведення здійснюється, принаймні, двома способами, у зв'язку з чим говорять про первинну та, відповідно, дуальну атаки на задачу LWE [91 – 95]. Таким чином, у випадку $m = \text{poly}(n)$ розв'язання цієї задачі здійснюється шляхом знаходження коротких векторів у певних решітках. Для оцінювання складності первинної та дуальної атак використовують алгоритми, наведені в [91, 92], які однак не вважаються остаточними, оскільки базуються на низці евристичних припущень.

Якщо кількість рівнянь у системі є необмеженою (що характерно для атак на деякі симетричні криптосистеми [87, 96], то найкращим з відомих сьогодні алгоритмів розв'язання задачі LWE є алгоритм BKW [97 – 106]. Цей алгоритм дозволяє отримувати шуканий вектор s за $q^{O\left(\frac{n}{\log n}\right)}$ операцій над n-вимірними векторами над довільним комутативним кільцем R порядку q за умови, що число m має той самий порядок росту: $m = q^{O\left(\frac{n}{\log n}\right)}$ [107]. Для

випадку $R = \mathbf{Z}_q$ та простого q відомо чимало вдосконалень алгоритму BKW [97 – 106], але їхня часова складність має той самий порядок росту.

Суттєвою перешкодою для практичного застосування криптосистем, стійкість яких базується на складності задачі LWE, є великий розмір відкритих ключів. Тому в [108] запропоновано модифікацію задачі LWE, яка надає змогу зменшити розмір ключів без втрати стійкості. Ця модифікована задача називається Ring-LWE і формулюється таким чином.

Спостерігається послідовність вигляду $(a_i, b_i = a_i s + \xi_i)$, $i \in \overline{1,m}$, де $a_1,...,a_m$ – незалежні випадкові рівноймовірні елементи кільця R, s – невідомий елемент кільця R, $\xi_1,...,\xi_m$ – незалежні випадкові елементи з деяким нерівномірним розподілом на цьому кільці. Треба відновити елемент s за відомою послідовністю (a_i, b_i), $i \in \overline{1,m}$. Розпізнавальна версія задачі Ring-LWE (Decision Ring-LWE) полягає в тому, щоб статистично відрізнити зазначену послідовність від суто випадкової послідовності пар елементів кільця R.

Взаємозв'язок між обома варіантами задачі досліджено в [90]. На сьогодні кожен з цих варіантів вважається обчислювально складним за більш-менш загальних умов (наприклад, коли $R = \mathbf{Z}_q$, де q є простим числом, а закон розподілу випадкових елементів $\xi_1,...,\xi_m$ є дискретним гаусовим або рівномірним на підмножині кільця R, яка має невелику потужність). При цьому, як для задачі LWE, у випадку $m = \mathrm{poly}(n)$ єдиним відомим способом розв'язання задачі Ring-LWE залишається знаходження коротких векторів у певних (так званих ідеальних) решітках [108, 109].

Таким чином, задача (Decision) Ring-LWE є однією з еталонних обчислювально складних задач, на яких базується стійкість багатьох сучасних решіткових криптосистем.

1.3. Аналіз методів побудови, оцінювання та обґрунтування стійкості NTRU-подібних шифросистем

Шифросистема NTRU [110] є однією з найперших асиметричних решіткових криптосистем. На сьогодні запропоновано чимало модифікацій та вдосконалень цієї шифросистеми, серед яких є фіналісти конкурсу NIST, а також постквантовий алгоритм відкритого шифрування, стандартизований в Україні [49] (рис. 1.1).

Для означення шифросистеми введемо низку позначень.

Зафіксуємо взаємно прості натуральні числа, $n, q > 3$, де q не ділиться на 3, та позначимо $\mathbf{Z}_q$ кільце класів лишків за модулем q, елементи якого ототожнимо з цілими числами, що належать інтервалу $[-(q-1)/2, (q-1)/2]$ для непарного q та інтервалу $[-q/2, q/2-1]$ для парного q. Позначимо $R_{n,q} = \mathbf{Z}_q[x]/(x^n - 1)$ кільце зрізаних поліномів степеня не вище $n-1$ над кільцем $\mathbf{Z}_q$. Для будь-якого $u = u_0 + u_1 x + \cdots + u_{n-1} x^{n-1} \in \mathbf{Z}[x]$ позначимо $u \bmod q$ поліном $(u_0 \bmod q) + (u_1 \bmod q)x + \cdots + (u_{n-1} \bmod q)x^{n-1} \in R_{n,q}$. Аналогічний сенс має позначення $u \bmod 3$.

Далі, позначимо $\| u \|_\infty = \max\limits_{0 \le i \le n-1} |u_i|$ та назвемо поліном u малим, якщо $\| u \|_\infty = 1$, $i \in \overline{0, n-1}$.

Для будь-яких натуральних чисел d_1, d_2 позначимо S_{d_1,d_2} множину всіх малих поліномів степеня не вище $n-1$, серед коефіцієнтів яких є точно d_1, що дорівнюють 1, та точно d_2, що дорівнюють -1.

За означенням [81, 111] секретним ключем шифросистеми NTRUEncrypt є будь-яка пара поліномів (F, g), де $F \in S_{d,d}$, $g \in S_{d'+1,d'}$, $d' = \lfloor n/3 \rfloor$ і поліном $f = 1 + 3F$ є оборотним елементом кільця $R_{n,q}$. Відповідним

відкритим ключем є поліном $h = 3g / f$, який обчислюється в кільці $R_{n,q}$ шляхом множення полінома $3g$ на поліном, обернений до f.

Множина відкритих текстів шифросистеми складається з усіх малих поліномів степеня не вище n. Для зашифрування такого полінома m на відкритому ключі h генерується випадковий поліном $r \in S_{d,d}$ та обчислюється шифротекст

$$E_h(m,r) = (m + rh) \bmod q. \tag{1.1}$$

Розшифрування довільного тексту $c \in R_{n,q}$ на секретному ключі (F, g) здійснюється за формулою

$$D_f(c) = cf \,(\bmod q) \bmod 3. \tag{1.2}$$

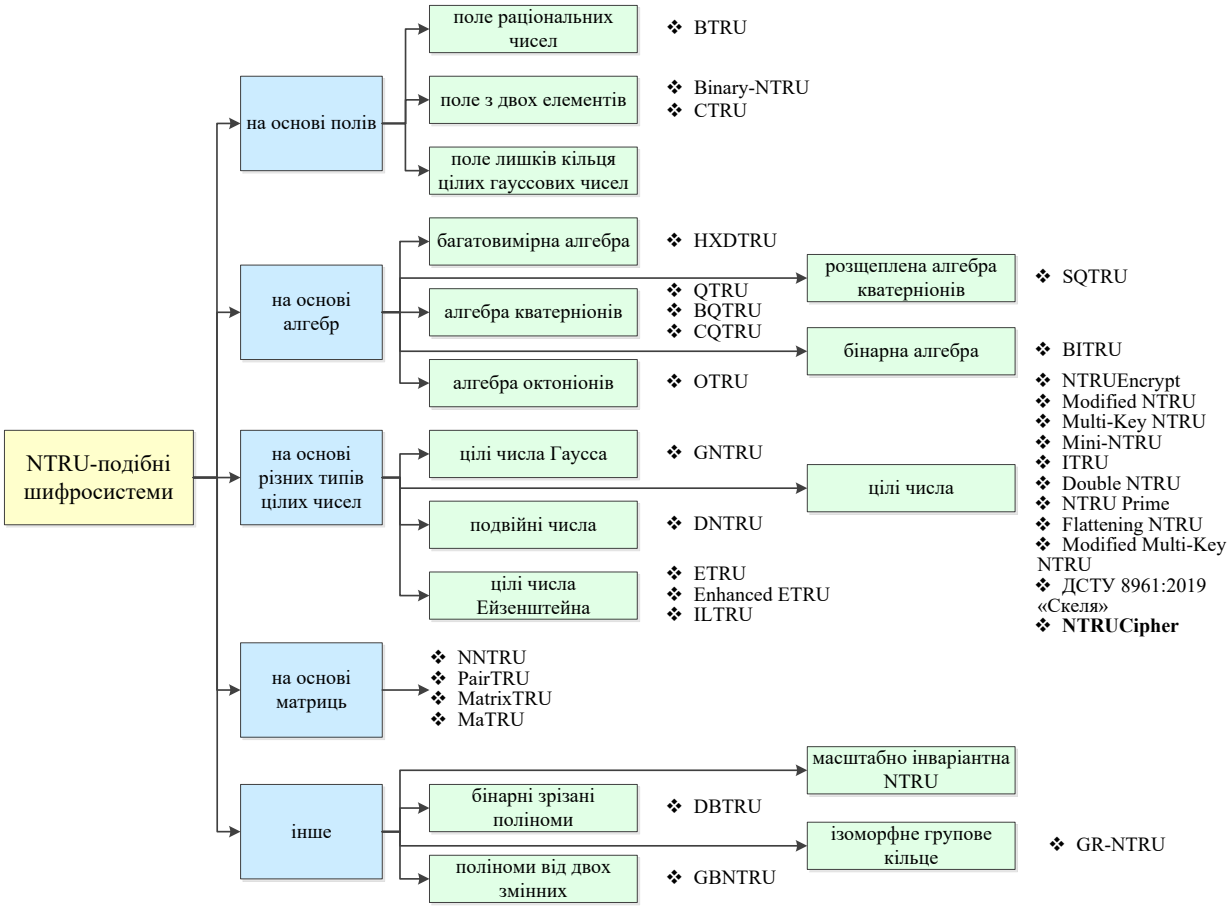

Рис. 1.2. Класифікація NTRU-подібних шифросистем

Зауважимо, що аналогічним чином будуються інші NTRU-подібні шифросистеми, серед яких слід відзначити NTRUEncrypt [110], NTRU Prime [82], LPR [108, 109, 112] та NNTRU [113]. Відмінності між ними полягають у тому, як вибираються кільце, над яким здійснюються криптографічні перетворення, а також числові параметри, що визначають вигляд відкритих та допоміжних повідомлень (m і r відповідно). Наприклад, в алгоритмі NTRU Prime замість кільця $R_{n,q}$ використовується поле $\mathbf{Z}_q[x]/(x^n - x - 1)$, де n і q є простими числами такими, що поліном $x^n - x - 1$ є незвідним над полем $\mathbf{Z}_q$. В алгоритмі LPR використовується кільце $\mathbf{Z}_q[x]/(x^n + 1)$, де n є степенем двійки, що ділить число $q - 1$, а в алгоритмі NNTRU – кільце зрізаних поліномів за модулем полінома $x^n - x^{n/2} + 1$, де n є парним числом. Крім того, замість тернарних (з коефіцієнтами $0, 1, -1$) поліномів m і r можуть використовуватись бінарні (з коефіцієнтами $0, 1$), а замість числа 3 у виразі для відкритого ключа та у рівнянні розшифрування – довільне мале число p, що є взаємно простим з q [112]. Нарешті, є NTRU-подібні шифросистеми, побудовані над кільцями більш складного вигляду (цілих гаусових чисел, цілочисельних кватерніонів тощо; див. рис. 1.2) [114 – 121]. Метою таких модифікацій є збільшенні стійкості або практичності шифросистем.

Показниками практичності NTRU-подібних шифросистем є такі параметри:

1) ймовірність оборотності випадкового полінома f, за допомогою якого обчислюється відкритий ключ h;

2) ймовірність помилки при розшифруванні відкритих повідомлень за формулою (1.2);

3) розмір секретного та відкритого ключів;

4) часова складність процедур зашифрування та розшифрування.

Зауважимо, що ймовірність оборотності полінома f, який генерується за тією чи іншою ймовірнісною схемою, характеризує “швидкість” формування ключів у шифросистемі. Якщо зазначений поліном виявляється не оборотним, відкритий ключ $h = 3g / f$ не може бути обчислений коректно і треба генерувати інший поліном f доти, поки він не виявиться оборотним. Добре відомо, як обчислити оборотність випадкового рівноймовірного полінома у кільці $R_{n,q}$, якщо q простим числом або степенем двійки, а n є взаємно простим з q [111, 122], але задача про ймовірність оборотності випадкових малих поліномів є на сьогодні відкритою. Виходячи з цього, на практиці часто-густо накладають додаткові обмеження стосовно кільця (наприклад, визначають його як поле того чи іншого вигляду) для того, щоб зменшити ймовірність появи необоротних поліномів при випадковій генерації (або виключити їх існування взагалі). Тим не менш, знаходження аналітичних співвідношень чи оцінок ймовірності оборотності випадкових поліномів, що можуть використовуватись для формування ключів NTRU-подібних шифросистем, є актуальною задачею подальших досліджень.

Якщо для повідомлень (1.1) та (1.2) виконується нерівність $D_f(E_h(m,r)) \neq m$, то говорять, що відбувається помилка розшифрування. Наявність таких помилок є характерною рисою багатьох NTRU-подібних шифросистем. Отже, для надійного (з погляду законного отримувача) функціонування шифросистеми треба забезпечити належну малість ймовірності помилки розшифрування. (Зауважимо, що, згідно з [82], така ймовірність повинна бути не вище за 2^{-80}).

Для багатьох сучасних NTRU-подібних шифросистем неважко позбутися помилок розшифрування взагалі шляхом зменшення (або збільшення) тих чи інших параметрів, наприклад, зменшення числа d при фіксованому q. Проте звичайно це призводить до зменшення стійкості (або уповільнення) шифросистеми. Тому розробники деяких алгоритмів,

наприклад, NTRUEncrypt [122, 123], пропонують користувачам набори параметрів (n,q,d), за яких можливі помилки розшифрування, але які надають змогу пришвидшити (при заданій стійкості) зашифрування/розшифрування повідомлень. Інші розробники [82, 112] наполягають на тому, щоб позбутися помилок розшифрування, оскільки вони можуть призводити по побудови певних атак [124].

В [81, 122, 123] отримано аналітичний вираз ймовірності помилки розшифрування в алгоритмі NTRUEncrypt за умови, що всі поліноми m,r,F та g вибираються випадково та незалежно в сукупності за певною ймовірнісною схемою. Зокрема, це означає, що ймовірність помилки розшифрування оцінюється в середньому за ансамблем ключів (F,g), в той час як з практичного погляду більш адекватним показником є набір ймовірностей, обчислених для кожного секретного ключа. До того ж формула для ймовірності помилки, наведена в [81, 122, 123], є евристичною, оскільки базується на заміні певного дограничного розподілу ймовірностей граничним (а саме, нормальним). Отже, є актуальною задача знаходження аналітичних співвідношень для ймовірності помилкового розшифрування повідомлень в NTRU-подібних шифросистемах для фіксованих значень секретних ключів (при цьому бажано охопити усі відомі конструкції шифросистем та позбутися будь-яких евристичних міркувань при обґрунтуванні шуканих співвідношень).

Стандартною вимогою до сучасних шифросистем (як симетричних, так і асиметричних) є їхня стійкість відносно атак на основі підібраних відкритих текстів (CPA-стійкість). Це поняття визначається наступним чином (див., наприклад, [125]).

Розглядається така “гра” між Криптоаналітиком та Дослідником:

1) Дослідник генерує секретний ключ k симетричної шифросистеми;

2) Криптоаналітик може подавати на вхід оракула E_k, що здійснює зашифрування, будь-які відкриті та отримувати відповідні шифровані повідомлення;

3) Криптоаналітик подає Досліднику пару різних повідомлень m_0, m_1 однакової довжини;

4) Дослідник вибирає випадкове рівноймовірне число $b \in \{0,1\}$ та повертає Криптоаналітику шифроване повідомлення $c = E_k(m_b)$;

5) Криптоаналітик може звертатися до оракула E_k (як в п. 2)) і повинен відновити значення b.

Шифросистема називається $(T, \varepsilon) - CPA$*-стійкою*, якщо будь-який алгоритм відновлення значення b з імовірністю $\varepsilon > 1/2$ у наведеній "грі" виконує не менше ніж T операцій.

Для асиметричних шифросистем поняття CPA-стійкості формулюється аналогічно з урахуванням того, що Криптоаналітик має безпосередній доступ до оракула зашифровування з визначеним відкритим ключем [125].

Відомо, що асиметрична шифросистема є CPA-стійкою тоді й тільки тоді, коли вона є семантично стійкою, проте для симетричних шифросистем поняття CPA-стійкості є більш сильним (тягне за собою семантичну стійкість, але не навпаки) [125].

На сьогодні прийнято поділяти обчислювально стійки шифросистеми на *обґрунтовано стійки* (provable secure) та *практично стійки* (practical secure). До перших відносять шифросистеми, для яких є доведення стійкості (security proof): математичне твердження про те, що будь-яку CP-атаку з параметрами (T, ε) на шифросистему можна трансформувати в алгоритм розв'язання певної обчислювально складної задачі так, що трудомісткість та ймовірність успішного завершення цього алгоритму є порівняними зі значеннями T і ε відповідно. Таке твердження є підґрунтям для висновку, що зазначена шифросистема є стійкою відносно будь-якої атаки з підібраним відкритим текстом (вигляд якої описується наведеною вище "грою") за умови, що

відповідна обчислювальна задача є дійсно складною. Якщо для шифросистеми не відомо доведення стійкості, проте вона (за певних умов) виявляється стійкою відносно відомих атак, то її називають практично (або евристично) стійкою [125].

Обґрунтована CPA-стійкість є однією зі стандартних вимог до сучасних шифросистем. Більш того, як правило, висувається сильніша вимога, а саме, стійкості у сенсі IND CCA-2 (тобто до адаптивних атак на основі підібраних шифрованих текстів) [126]. Поряд з тим, є численні схеми доповнення (padding schemes), які надають змогу отримувати з довільної (або довільної CPA-стійкої) CCA-2-стійку шифросистему [126 – 134]. Зауважимо, що такі схеми доповнення застосовуються у всіх асиметричних алгоритмах, представлених на конкурс NIST [23], проте отримані для них доведення стійкості базуються на так званій *моделі з випадковим оракулом*. Кажучи неформально, це означає, що стійкість доводиться не для конкретної схеми шифрування, а "у середньому за ансамблем" подібних схем. Іншими словами, з певною високою (але не стовідсотковою) ймовірністю виявляється стійкою шифросистема, що вибирається навмання з певного широкого класу, якій містить досліджувану схему шифрування [125].

Такі доведення стійкості вважаються сьогодні прийнятними за відсутністю кращих, отриманих для так званої *стандартної моделі*, проте задача побудови шифросистем, для яких є доведення стійкості (принаймні, на рівні CPA) саме для цієї моделі, залишається дуже актуальною.

Як зазначено в [135], існує дві обчислювально складні задачі, пов'язані з NTRU-подібними шифросистемами.

Задача 1 (NTRU Decision Key Craking Problem) полягає у встановленні закону розподілу випадкового елемента h, який з імовірністю $1/2$:

– має рівномірний розподіл на кільці $R_{n,q}$ (гіпотеза H_0);

– є відкритим ключем шифросистеми NTRU, сформованим за обраними належним чином випадковими елементами g та F (гіпотеза H_1).

Задача 2 (NTRU Search Key Craking Problem) полягає у тому, щоби для заданого (обраного навмання) випадкового елемента $h \in R_{n,q}$ встановити закон розподілу випадкового елемента c, який з імовірністю $1/2$:

– має рівномірний розподіл на множині $R_{n,q}$ (гіпотеза H_0);

– формується за правилом

$$c = 3(hr + e), \tag{1.3}$$

де r і e є незалежними випадковими малими поліномами (гіпотеза H_1).

Для шифросистеми NTRUEncrypt відомо [135], що вона є CPA-стійкою лише за умови, що обидві задачі (Задача 1 та Задача 2) є обчислювально складними. При цьому шифросистема може не бути CPA-стійкою, якщо Задача 2 не є обчислювально складною. Саме таким є випадок, коли доданок e у формулі (1.3) дорівнює нулю. Виходячи з цього, Д. Стеле і Р. Штайнфельд [136] запропонували модифікацію алгоритму NTRUEncrypt, який є CPA-стійким за умови обчислювальної складності задачі SVP_γ для певного значення $\gamma \geq 1$. Обґрунтовано стійка версія NTRU Стеле-Штайнфельда вважається помітним досягненням у сучасній решітковій криптографії, проте вона є малопрактичною внаслідок дуже великих довжин ключів, що використовуються (див., наприклад, [82]). Зауважимо, що в алгоритмі NTRUEncrypt [123], а також стандартах [49] для забезпечення обґрунтованої стійкості шифросистем (на рівні IND CCA-2) використовується спеціально розроблена схема доповнення під назвою NAEP [126].

Найвідомішими атаками на NTRU-подібні шифросистеми є атаки узгодження (зустрічі посередині) [137 – 141] та решіткові атаки [91 – 95].

Класична атака зустрічі посередині [137] полягає у розбитті множини секретних ключів шифросистеми на дві підмножини Φ_1, Φ_2 такі, що кожен

ключ F має єдине представлення у вигляді $F = F_1 + F_2$, де $F_1 \in \Phi_1$, $F_2 \in \Phi_2$. Атака полягає у пошуку секретного ключа за відкритим шляхом узгодження пар (F_1, F_2) з використанням спеціально організованої пам'яті, попереднє заповнення якої надає змогу зменшити складність пошуку приблизно до кореня квадратного з величини, що є складністю перебірної атаки. Остання дорівнює $\binom{n}{d}\binom{n-d}{d}$ для алгоритму NTRUEncrypt та $\binom{n}{2d}2^{2d}$ для алгоритму NTRU Prime [82]. Для першого алгоритму атаку зустрічі посередині можна прискорити в $\sqrt{2n}$ разів, якщо скористатися "еквівалентністю" ключів вигляду $(\pm x^i F,\ \pm x^i g)$, де $i \in \overline{0, n-1}$, а множення здійснюється у кільці $R_{n,q}$. Для другого алгоритму декілька більш складні міркування надають змогу прискорити атаку у $\sqrt{2(n-d)}$ разів [82].

У [82, 139 – 141] для низки NTRU-подібних шифросистем наведено оцінки трудомісткості різноманітних модифікацій атаки узгодження, проте їхня складність за порядком величини не надто відрізняється від трудомісткості класичної атаки.

Зауважимо також, що в нещодавніх публікаціях [83, 84] запропоновано вдосконалення алгоритму зустрічі посередині, причому (евристично) стверджується, що часова складність цього удосконаленого алгоритму становить порядку кореня четвертого степеня зі складності перебірної атаки.

Історично першою атакою на шифросистему NTRU є решіткова атака Куперсміта-Шаміра [142]. Для ілюстрації основної ідеї атаки розглянемо, наприклад, шифросистему NTRU Prime, де секретний ключ (g, f) пов'язаний з відкритим ключем h співвідношенням $3h = g/f$ у полі $\mathbf{Z}_q[x]/(x^n - x - 1)$, де n і q є простими числами, а поліном $x^n - x - 1$ є незвідним над полем $\mathbf{Z}_q$. З наведеного співвідношення випливає, що існує

поліном k такий, що в кільці $\mathbf{Z}[x]/(x^n - x - 1)$ виконується рівність $3hf + qk = g$, яку можна записати в еквівалентній формі:

$$(k, f)\begin{pmatrix} qI & 0 \\ H & I \end{pmatrix} = (g, f), \tag{1.4}$$

де множення вектор-рядка на матрицю здійснюється на кільцем цілих чисел, I є одиничною матрицею порядку n, а H – матрицею, i-й рядок якої дорівнює вектору коефіцієнтів залишку від ділення полінома $3x^i h$ на поліном $x^n - x - 1$, $i \in \overline{0, n-1}$.

З формули (1.4) випливає, що секретний ключ (g, f) належить повній решітці вимірності $2n$, породженій рядками матриці $\begin{pmatrix} qI & 0 \\ H & I \end{pmatrix}$, а оскільки g і f є малими поліномами (тобто з коефіцієнтами $0, 1, -1$), то вектор (g, f) є коротким (тобто має малу евклідову норму). Таким чином, шуканий секретний ключ міститься серед достатньо коротких векторів зазначеної решітки, і для його знаходження можна використовувати відомі методи розв'язання задачі SVP_γ, огляд яких наведено у підрозділі 1.2. Неважко також переконатися в тому, що й навпаки, будь-який достатньо короткий вектор, що належить наведеній решітці, може застосовуватися в ролі "еквівалентного" секретного ключа для відкритого ключа h (тобто на ньому можна коректно здійснювати розшифрування отриманих шифрованих повідомлень) [142]. Отже, задача відновлення секретного ключа за відкритим близько пов'язана із задачею знаходження достатньо коротких векторів у решітках наведеного вигляду (які називаються іноді NTRU-решітками).

Аналогічно доводиться, що відновлення відкритого тексту m за шифрованим текстом $c = m + rh$ будь-якої NTRU-подібної шифросистеми

зводиться до знаходження коротких векторів, які належать решітці, породженій рядками матриці

$$\begin{pmatrix} 1 & 0_{1\times n} & c \\ 0_{n\times 1} & I_n & H \\ 0_{n\times 1} & 0_{n\times 1} & qI_n \end{pmatrix}.$$

Таким чином, атака на NTRU за відомим шифротекстом також зводиться до розв'язання задачі SVP_γ.

Прогрес у розвитку асиметричної решіткової криптографії приводить до активізації досліджень, спрямованих на створення симетричних схем шифрування, які будуються на решітках. Слід зазначити, що побудова симетричної шифросистеми, виходячи з асиметричної, шляхом простого "засекречування відкритого ключа" не надає бажаного результату, оскільки отримані таким чином симетричні шифросистеми можуть виявитись не стійкими до атак на основі підібраних відкритих текстів. Дійсно, зашифрування будь-яких повідомлень на відкритому ключі асиметричної шифросистеми не надає криптоаналітику додаткової інформації про відповідний секретний ключ, в той час як для симетричних шифросистем зашифрування кожного нового відкритого повідомлення збільшує інформацію про секретний ключ, що використовується.

З метою створення симетричного NTRU-подібного алгоритму шифрування, в [143] запропоновано шифросистему NTRUCipher. Як і класичну схему шифрування NTRU, цю шифросистему можна визначити над різними кільцями зрізаних поліномів за допомогою різних числових параметрів (на кшталт чисел n, q, d, зазначених вище).

Як приклад, розглянемо кільце $R_{n,q}$ та позначимо символом S множину всіх малих поліномів степеня не вище $n-1$, а символом S_d множину всіх поліномів $u \in S$, серед коефіцієнтів яких є точно d, що дорівнюють 1, та

точно d, що дорівнюють -1. Секретними ключами шифросистеми NTRUCipher є поліноми $F \in S_d$, такі, що $f = 1 + 3F$ є оборотним елементом кільця $R_{n,q}$, а відкритими повідомленнями – довільні малі поліноми.

Для зашифрування повідомлення $m \in S$ на ключі F генеруються незалежні випадкові поліноми r та $e = e_0 + e_1 x + \cdots + e_{n-1} x^{n-1}$, де r має рівномірний розподіл ймовірностей на множині S_d, а $e_0, e_1, \ldots, e_{n-1}$ є незалежними випадковими величинами, які приймають значення $0, 1, -1$ з імовірністю $1/3$. Далі обчислюється шифроване повідомлення $c = (m + 3rf^{-1}) \bmod q$, де f^{-1} – обернений до f елемент кільця $R_{n,q}$. Розшифрування довільного повідомлення $c \in R_{n,q}$ на ключі F здійснюється за формулою $D_f(c) = cf \,(\mathrm{mod}\, q) \bmod 3$.

Як і для асиметричної шифросистеми NTRU, при використанні алгоритму NTRUCipher можливі помилки розшифрування, для оцінювання ймовірності яких в [143] використовується традиційний підхід (тобто в середньому за ансамблем ключів).

В [143] досліджено також стійкість шифросистеми NTRUCipher до решіткових атак та наведено “обґрунтування” її CPA-стійкості за умови обчислювальної складності наведеної вище Задачі 1 (NTRU Decision Key Craking Problem). Зауважимо, що це “обґрунтування” містить помилку, яка полягає у неправильному визначенні задачі розпізнавання, від складності якої залежить стійкість шифросистеми. Міркування, наведені в [143], фактично повторюють ті, що використовуються при обґрунтуванні стійкості асиметричних NTRU-подібних шифросистем [125]. Проте для симетричної шифросистеми стійкість визначається складністю розв’язання задачі, яка є слабше за Задачу 1: треба статистично відрізнити послідовність шифрованих текстів $c_1, \ldots, c_t$, отриманих у серії незалежних випробувань з відкритого тесту

$m = 0$ (при тому ж самому невідомому секретному ключі $F \in S$), від суто випадкової послідовності t елементів кільця $R_{n,q}$.

Зауважимо, що Задача 1 є окремим випадком сформульованої задачі, а саме, при $t = 1$. І хоча Задача 1 вважається на сьогодні обчислювально складною, її послаблена версія (для довільного натурального t) такою може не бути. Наприклад, видається природним дослідити складність вирішення цієї задачі шляхом складання та розв'язання системи лінійних рівнянь зі спотвореними правим частинами відносно невідомого ключа F, наприклад, за допомогою алгоритму BKW [97].

В цілому, твердження про обґрунтовану стійкість шифросистеми NTRUCipher потребує корекції, а сама шифросистема – подальших досліджень, спрямованих на з'ясування її стійкості відносно атак на основі підібраних відкритих текстів.

1.4. Основні напрями та окремі задачі дисертаційного дослідження

Вище показана актуальність *наукової задачі* дисертаційної роботи, яка полягає у розробці методу побудови симетричних NTRU-подібних шифросистем, що є обґрунтовано стійкими відносно атак на основі підібраних відкритих текстів.

Метою дисертаційної роботи є створення обґрунтовано стійких симетричних NTRU-подібних шифросистем для систем захисту інформації в інформаційно-комунікаційних системах.

Об'єктом дослідження у дисертаційній роботі є процес перетворення інформації з використанням сучасних NTRU-подібних шифросистем, а *предметом дослідження* – методи побудови та обґрунтування стійкості зазначених шифросистем відносно атак на основі підібраних відкритих текстів.

Відповідно до поставленої мети, наукова задача дисертаційної роботи включає в себе низку взаємопов'язаних окремих задач, порядок розв'язання яких визначає основні напрями дисертаційних досліджень (рис. 1.3).

Перший напрям полягає в отриманні аналітичних виразів параметрів, що характеризують практичність NTRU-подібних шифросистем (ймовірності оборотності випадкових поліномів та ймовірності помилкового розшифрування повідомлень при фіксованому ключі; див. задачі 2-3 на рис. 1.3). Окремою задачею цього напряму є отримання аналітичних оцінок складності статистичних атак на симетричні шифросистеми NTRUCipher та NTRUCipher+ (задача 4 на рис. 1.3).

Основною задачею *другого напряму* є розробка методу побудови симетричних NTRU-подібних шифросистем, які мають обґрунтовану стійкість відносно атак на основі підібраних відкритих повідомлень. Ця задача охоплює, зокрема, розробку алгоритму вибору параметрів запропонованих шифросистем, що гарантують їхню стійкість відносно відомих атак на заздалегідь визначеному рівні.

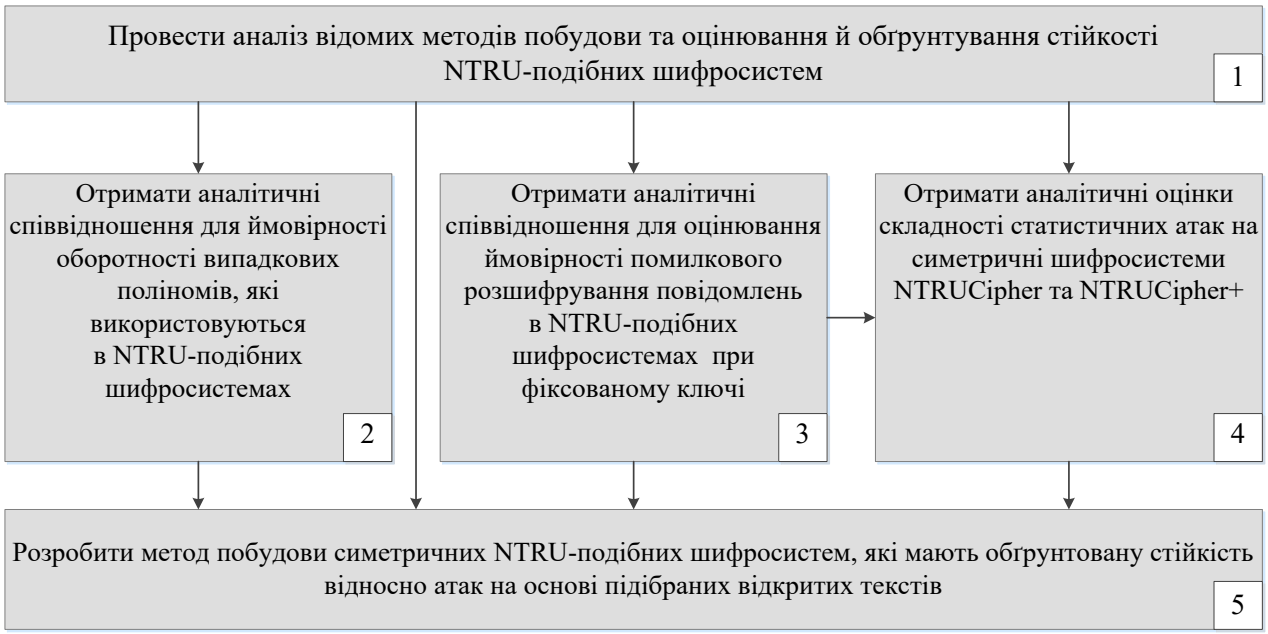

Рис. 1.3. Структурно-логічна схема дисертаційного дослідження

Розв'язання перелічених окремих задач надає змогу вирішити наукову задачу дисертаційної роботи та досягнути поставленої в роботі мети.

Висновки

1. Створення у найближчій перспективі квантових комп'ютерів стимулює розробку та застосування постквантових криптосистем, стійкість яких базується на математичних задачах, що є обчислювально складними як до традиційного, так і до квантового криптоаналізу. Важливий клас серед зазначених криптосистем утворюють NTRU-подібні криптосистеми, до яких відноситься, зокрема, приблизно третина всіх пропозицій, поданих до конкурсу NIST [23], а також новітній національний стандарт України асиметричного шифрування [49].

2. Стійкість NTRU-подібних шифросистем базується на складності розв'язання добре відомих обчислювально складних задач (таких як SVP_γ чи LWE; див. підрозділ 1.2). Ці шифросистеми надають змогу створювати різноманітні криптографічні примітиви (такі як схеми гомоморфного чи функціонального шифрування), забезпечуючи при цьому високу швидкість шифрування поряд з помірними довжинами ключів.

3. Прогрес у розвитку решіткової криптографії приводить до активізації досліджень, спрямованих на створення симетричних NTRU-подібних шифросистем, єдиною відомою з яких на сьогодні є NTRUCipher [143]. При цьому твердження в [143] про обґрунтовану стійкість цієї шифросистеми потребує корекції, а сама шифросистема – подальших досліджень, спрямованих на з'ясування її стійкості відносно атак на основі підібраних відкритих текстів.

4. Дисертаційні дослідження проведено за двома напрямами, перший з яких полягає в отриманні аналітичних виразів параметрів, що характеризують практичність NTRU-подібних шифросистем (ймовірності оборотності випадкових поліномів та ймовірності помилкового розшифрування повідомлень при фіксованому ключі), а також в отриманні аналітичних оцінок складності статистичних атак на симетричні NTRU-подібні шифросистеми. Основною задачею другого напряму є розробка

методу побудови симетричних NTRU-подібних шифросистем, які мають обґрунтовану стійкість відносно атак на основі підібраних відкритих повідомлень.

Список використаних джерел у першому розділі

1. Deutsch D. Quantum theory, the Church–Turing principle and the universal quantum computer. *Proceedings of the Royal Society of London. A. Mathematical and Physical Sciences*. 1985. Vol. 400, no. 1818. P. 97–117. DOI: https://doi.org/10.1098/rspa.1985.0070.

2. Shor P. W. Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer. *SIAM Journal on Computing*. 1997. Vol. 26, no. 5. P. 1484–1509. DOI: https://doi.org/10.1137/s0097539795293172.

3. Post-Quantum Cryptography / ed. by D. J. Bernstein, J. Buchmann, E. Dahmen. Berlin, Heidelberg: Springer Berlin Heidelberg, 2009. DOI: https://doi.org/10.1007/978-3-540-88702-7.

4. Diffie W., Hellman M. New directions in cryptography. *IEEE Transactions on Information Theory*. 1976. Vol. 22, no. 6. P. 644–654. DOI: https://doi.org/10.1109/tit.1976.1055638.

5. Rivest R. L., Adleman L., Dertouzos M. L. On Data Banks and Privacy Homomorphism. *Foundations of Secure Computation*. 1978. P. 169–180.

6. Elgamal T. A public key cryptosystem and a signature scheme based on discrete logarithms. *IEEE Transactions on Information Theory*. 1985. Vol. 31, no. 4. P. 469–472. DOI: https://doi.org/10.1109/tit.1985.1057074.

7. Miller V. S. Use of Elliptic Curves in Cryptography. *In Conference on the Theory and Application of Cryptographic Techniques*: CRYPTO 1985: Advances in Cryptology – CRYPTO ’85 Proceedings, Berlin. 1985. P. 417–426.

8. ДСТУ 7624:2014. Інформаційні технології. Криптографічний захист інформації. Алгоритм симетричного блокового перетворення. Чинний від 2015-07-01. Вид. офіц. 2014. 238 с.

9. DESIGN PRINCIPLES AND MAIN PROPERTIES OF THE NEW UKRAINIAN NATIONAL STANDARD OF BLOCK ENCRYPTION / P. B. Олійников et al. *Ukrainian Information Security Research Journal*. 2015. Vol. 17, no. 2. DOI: https://doi.org/10.18372/2410-7840.17.8789.

10. О криптографических свойствах нового национального стандарта шифрования Украины / А. Н. Алексейчук та ін. *Кибернетика и системный анализ*. 2016. Т. 52, № 3. С. 16–31. URL: http://dspace.nbuv.gov.ua/handle/123456789/133678 (дата звернення: 02.05.2023).

11. Mittal S., Ramkumar K. R. A retrospective study on NTRU cryptosystem. *INTERNATIONAL CONFERENCE ON ADVANCES IN MULTI-DISCIPLINARY SCIENCES AND ENGINEERING RESEARCH: ICAMSER-2021*, Chitkara University, Himachal Pradesh, India. 2022. DOI: https://doi.org/10.1063/5.0095312.

12. Chang K. Quantum Computing Advance Begins New Era, IBM Says. *The New York Times*. URL: https://www.nytimes.com/2023/06/14/science/ibm-quantum-computing.html (дата звернення: 02.05.2023).

13. Mandelbaum R. New IBM, UC Berkeley paper shows path toward useful quantum | IBM Research Blog. *IBM Research Blog*. URL: https://research.ibm.com/blog/utility-toward-useful-quantum (дата звернення: 02.05.2023).

14. Scientific Publications | D-Wave. *D-Wave Systems | The Practical Quantum Computing Company*. URL: https://www.dwavesys.com/learn/publications/ (дата звернення: 02.05.2023).

15. Qubits23 – D-Wave Asserts the Quantum Wait Is Over. *HPCwire*. URL: https://www.hpcwire.com/2023/01/18/qubits23-d-wave-asserts-the-quantum-wait-is-over/ (дата звернення: 02.05.2023).

16. Quantum Computing - Microsoft Research. *Microsoft Research*. URL: https://www.microsoft.com/en-us/research/research-area/quantum-computing/ (дата звернення: 02.05.2023).

17. Chadwick J. Google claims quantum computer breaththrough. *Mail Online*. URL: https://www.dailymail.co.uk/sciencetech/article-12258353/Google-claims-quantum-computer-breaththrough.html (дата звернення: 02.05.2023).

18. Intel's New Chip to Advance Silicon Spin Qubit Research for Quantum. *Intel*. URL: https://www.intel.com/content/www/us/en/newsroom/ news/quantum-computing-chip-to-advance-research.html#gs.2pag4c (дата звернення: 02.05.2023).

19. Announcing the opening of the AWS Center for Quantum Computing | Amazon Web Services. *Amazon Web Services*. URL: https://aws.amazon.com/ru/blogs/quantum-computing/announcing-the-opening-of-the-aws-center-for-quantum-computing/ (дата звернення: 02.05.2023).

20. IonQ Harmony. *IonQ*. URL: https://ionq.com/quantum-systems/harmony (дата звернення: 02.05.2023).

21. Roundy J. 10 companies building quantum computers | TechTarget. *Data Center*. URL: https://www.techtarget.com/searchdatacenter/feature/ Companies-building-quantum-computers (дата звернення: 02.05.2023).

22. Report on Post-Quantum Cryptography. *NIST Technical Series Publications*. URL: http://nvlpubs.nist.gov/nistpubs/ir/2016/NIST.IR.8105.pdf (дата звернення: 03.05.2023).

23. Post-Quantum Cryptography | CSRC. *NIST Computer Security Resource Center | CSRC*. URL: https://csrc.nist.gov/projects/post-quantum-cryptography (дата звернення: 03.05.2023).

24. Post-Quantum and Code-Based Cryptography–Some Prospective Research Directions / C. Balamurugan et al. *Cryptography*. 2021. Vol. 5, no. 4. P. 38. DOI: https://doi.org/10.3390/cryptography5040038.

25. Post-Quantum Cryptography: Current state and quantum mitigation / W. Beullens et al. Publications Office of the European Union, 2022. 46 p. URL: https://data.europa.eu/doi/10.2824/92307 (дата звернення: 03.05.2023).

26. Initial recommendations of long-term secure post-quantum systems / D. Augot et al. URL: http://pqcrypto.eu.org/docs/initial-recommendations.pdf (дата звернення: 03.05.2023).

27. Singh H. Code based Cryptography: Classic McEliece. Delhi, 2020. 45 p. DOI: https://doi.org/10.48550/arXiv.1907.12754.

28. Goppa V. D. A New Class of Linear Correcting Codes. *Probl. Peredachi Inf*. 1970. Vol. 6, no. 3. P. 24–30.

29. Classic McEliece:Intro. *Classic McEliece:Intro*. URL: https://classic.mceliece.org/index.html (дата звернення: 03.05.2023).

30. BIKE - Bit Flipping Key Encapsulation. *BIKE - Bit Flipping Key Encapsulation*. URL: https://bikesuite.org/ (дата звернення: 03.05.2023).

31. HQC. *HQC*. URL: https://pqc-hqc.org/ (дата звернення: 03.05.2023).

32. Merkle R. C. Secrecy, authentication, and public key systems : Ph.D. thesis. Stanford, 1979. URL: https://www.merkle.com/papers/Thesis1979.pdf (дата звернення: 03.05.2023).

33. Grover L. K. A fast quantum mechanical algorithm for database search. *the twenty-eighth annual ACM symposium*, Philadelphia, Pennsylvania, United States, 22–24 May 1996. New York, New York, USA, 1996. P. 212–219. DOI: https://doi.org/10.1145/237814.237866.

34. SPHINCS+. *SPHINCS+*. URL: https://sphincs.org/ (дата звернення: 03.05.2023).

35. Ding J., Petzoldt A. Current State of Multivariate Cryptography. *IEEE Security & Privacy*. 2017. Vol. 15, no. 4. P. 28–36. DOI: https://doi.org/10.1109/msp.2017.3151328.

36. PQCRainbow. *PQCRainbow*. URL: https://www.pqcrainbow.org/ (дата звернення: 03.05.2023).

37. GeMSS: A Great Multivariate Short Signature. *Computer Algebra, Polynomial systems and Mathematical software*. URL: https://www-polsys.lip6.fr/Links/NIST/GeMSS_specification.pdf (дата звернення: 03.05.2023).

38. Rostovtsev A., Stolbunov A. PUBLIC-KEY CRYPTOSYSTEM BASED ON ISOGENIES. *IACR Cryptology ePrint Archive, Report 2006/145*. 2006. URL: https://eprint.iacr.org/2006/145 (дата звернення: 04.05.2023).

39. Shumow D. Isogenies of Elliptic Curves: A Computational Approach. 2009. DOI: https://doi.org/10.48550/arXiv.0910.5370.

40. De Feo L., Jao D., Plût J. Towards quantum-resistant cryptosystems from supersingular elliptic curve isogenies. *Journal of Mathematical Cryptology*. 2014. Vol. 8, no. 3. DOI: https://doi.org/10.1515/jmc-2012-0015.

41. SIKE – Supersingular Isogeny Key Encapsulation. *SIKE – Supersingular Isogeny Key Encapsulation*. URL: https://sike.org/ (дата звернення: 03.05.2023).

42. Lepoint T. Design and Implementation of Lattice-Based Cryptography: Ph.D. thesis. Paris, France, 2014. URL: https://theses.hal.science/tel-01069864/preview/thesis-lepoint-print.pdf (дата звернення: 03.05.2023).

43. Elkabbany G. F., Aslan H. K., Hassan I. Stepping up the NTRU-Post Quantum Algorithm Using Parallel Computing. 2023. (Preprint). DOI: https://doi.org/10.21203/rs.3.rs-2885476/v1.

44. Kyber. *CRYSTALS*. URL: https://pq-crystals.org/kyber/ (дата звернення: 03.05.2023).

45. NTRU. *NTRU*. URL: https://ntru.org/ (дата звернення: 03.05.2023).

46. SABER: LWR-based KEM. *Home - Departement Elektrotechniek (ESAT)*. URL: https://www.esat.kuleuven.be/cosic/pqcrypto/saber/ (дата звернення: 03.05.2023).

47. Dilithium. *CRYSTALS*. URL: https://pq-crystals.org/dilithium/ (дата звернення: 03.05.2023).

48. Falcon. *Falcon*. URL: https://falcon-sign.info/ (дата звернення: 03.05.2023).

49. ДСТУ 8961:2019. Інформаційні технології. Криптографічний захист інформації. Алгоритми асиметричного шифрування та інкапсуляції ключів. Чинний від 21.12.2019. Вид. офіц. Київ: УкрНДНЦ, 2019. 72 с.

50. Stehlé D. Euclidean lattices: algorithms and cryptography. Lyon, 2011. URL: https://theses.hal.science/tel-00645387/file/HDR_full.pdf (дата звернення: 04.05.2023).

51. Ajtai M. The shortest vector problem in L2 is NP-hard for randomized reductions (extended abstract). *The thirtieth annual ACM symposium*, Dallas, Texas, United States, 24–26 May 1998. New York, New York, USA, 1998. DOI: https://doi.org/10.1145/276698.276705.

52. Haviv I., Regev O. Tensor-based hardness of the shortest vector problem to within almost polynomial factors. *The thirty-ninth annual ACM symposium*, San Diego, California, USA, 11–13 June 2007. New York, New York, USA, 2007. DOI: https://doi.org/10.1145/1250790.1250859.

53. Dinur I., Kindler G., Safra S. Approximating-CVP to within almost-polynomial factors is NP-hard. *39th Annual Symposium on Foundations of Computer Science*, Palo Alto, CA, USA. DOI: https://doi.org/10.1109/sfcs.1998.743433.

54. Emde Boas P. Another NP-complete partition problem and the complexity of computing short vectors in a lattice. Technical report 81-04, Mathematisch Instituut, Universiteit van Amsterdam, 1981.

55. Hanrot G., Pujol X., Stehlé D. Algorithms for the Shortest and Closest Lattice Vector Problems. *Lecture Notes in Computer Science*. Berlin, Heidelberg, 2011. P. 159–190. DOI: https://doi.org/10.1007/978-3-642-20901-7_10.

56. Hanrot G., Stehlé D. Improved Analysis of Kannan's Shortest Lattice Vector Algorithm. *Advances in Cryptology - CRYPTO 2007*. Berlin, Heidelberg. P. 170–186. DOI: https://doi.org/10.1007/978-3-540-74143-5_10.

57. Micciancio D., Voulgaris P. A Deterministic Single Exponential Time Algorithm for Most Lattice Problems Based on Voronoi Cell Computations. *SIAM Journal on Computing*. 2013. Vol. 42, no. 3. P. 1364–1391. DOI: https://doi.org/10.1137/100811970.

58. Micciancio D., Voulgaris P. Faster exponential time algorithms for the shortest vector problem. *Proceedings of the Twenty-First Annual ACM-SIAM*

Symposium on Discrete Algorithms. Philadelphia, PA, 2010. DOI: https://doi.org/10.1137/1.9781611973075.119.

59. Pujol X., Stehle D. Solving the Shortest Lattice Vector Problem in Time 2^2.465n. *Cryptology ePrint Archive*. 2009. URL: https://eprint.iacr.org/2009/605.

60. Schnorr C. P. A more efficient algorithm for lattice basis reduction. *Journal of Algorithms*. 1988. Vol. 9, no. 1. P. 47–62. DOI: https://doi.org/10.1016/0196-6774(88)90004-1.

61. Aharonov D., Regev O. A Lattice Problem in Quantum NP. *44th Annual IEEE Symposium on Foundations of Computer Science, 2003. Proceedings.* 2003. P. 210–219. DOI: https://doi.org/10.48550/arXiv.quant-ph/0307220.

62. Ajtai M. The shortest vector problem in L2 is NP-hard for randomized reductions. *in Symposium on the Theory of Computing*. 1998. P. 10–19.

63. Ambainis A. QuaQuantum walk algorithm for element distinctnessntum walk algorithm for element distinctness. *in Foundations of Computer Science*. 2003. P. 22–31. DOI: https://doi.org/10.48550/arXiv.quant-ph/0311001.

64. Lenstra A. K., Lenstra H. W., Lovász L. Factoring polynomials with rational coefficients. *Mathematische Annalen*. 1982. Vol. 261, no. 4. P. 515–534. DOI: https://doi.org/10.1007/bf01457454.

65. Kaltofen E. On the complexity of finding short vectors in integer lattices. *In Proceedings of EUROCAL'83, volume 162 of LNCS, Springer*. 1983. P. 236–244.

66. Nguyen P. Q., Stehle D. Floating-point LLL revisited. *in Proceedings of Eurocrypt, volume 3494 of LNCS, Springer*. 2005. P. 215–233.

67. Nguyen P. Q., Stehlé D. An LLL Algorithm with Quadratic Complexity. *SIAM Journal on Computing*. 2009. Vol. 39, no. 3. P. 874–903. DOI: https://doi.org/10.1137/070705702.

68. Morel I., Stehlé D., Villard G. H-LLL. *The 2009 international symposium*, Seoul, Republic of Korea, 28–31 July 2009. New York, New York, USA, 2009. P. 271–278. DOI: https://doi.org/10.1145/1576702.1576740.

69. Novocin A., Stehlé D., Villard G. An LLL-reduction algorithm with quasi-linear time complexity. *the 43rd annual ACM symposium*, San Jose, California, USA, 6–8 June 2011. New York, New York, USA, 2011. P. 403–412. DOI: https://doi.org/10.1145/1993636.1993691.

70. Ajtai M., Kumar R., Sivakumar D. A sieve algorithm for the shortest lattice vector problem. *The thirty-third annual ACM symposium*, Hersonissos, Greece. New York, New York, USA, 2001. P. 601–610. DOI: https://doi.org/10.1145/380752.380857.

71. Regev O. Lecture notes of lattices in computer science, course taught at the Computer Science Tel Aviv University. URL: https://cims.nyu.edu/~regev/teaching/lattices_fall_2009/ (дата звернення: 04.05.2023).

72. Nguyen P. Q., Vidick T. Sieve algorithms for the shortest vector problem are practical. *Journal of Mathematical Cryptology*. 2008. Vol. 2, no. 2. DOI: https://doi.org/10.1515/jmc.2008.009.

73. Ajtai M., Kumar R., Sivakumar D. Sampling short lattice vectors and the closest lattice vector problem. *17th IEEE Annual Conference on Computational Complexity*, Montreal, Que., Canada. 2002. P. 53–57. DOI: https://doi.org/10.1109/ccc.2002.1004339.

74. Blömer J., Naewe S. Sampling methods for shortest vectors, closest vectors and successive minima. *Theoretical Computer Science*. 2009. Vol. 410, no. 18. P. 1648–1665. DOI: https://doi.org/10.1016/j.tcs.2008.12.045.

75. Fincke U., Pohst M. A procedure for determining algebraic integers of given norm. *Lecture Notes in Computer Science*. Berlin, Heidelberg, 1983. P. 194–202. DOI: https://doi.org/10.1007/3-540-12868-9_103.

76. Fincke U., Pohst M. Improved methods for calculating vectors of short length in a lattice, including a complexity analysis. *Mathematics of Computation*. 1985. Vol. 44, no. 170. P. 463. DOI: https://doi.org/10.1090/s0025-5718-1985-0777278-8.

77. Kannan R. Improved algorithms for integer programming and related lattice problems. *The fifteenth annual ACM symposium*, Not Known. New York, New York, USA, 1983. P. 99–108. DOI: https://doi.org/10.1145/800061.808749.

78. Kannan R. Minkowski's Convex Body Theorem and Integer Programming. *Mathematics of Operations Research*. 1987. Vol. 12, no. 3. P. 415–440. DOI: https://doi.org/10.1287/moor.12.3.415.

79. Helfrich B. Algorithms to construct minkowski reduced and hermite reduced lattice bases. *Theoretical Computer Science*. 1985. Vol. 41. P. 125–139. DOI: https://doi.org/10.1016/0304-3975(85)90067-2.

80. Chen Y., Nguyen P. Q. BKZ 2.0: Better Lattice Security Estimates. *Lecture Notes in Computer Science*. Berlin, Heidelberg, 2011. P. 1–20. DOI: https://doi.org/10.1007/978-3-642-25385-0_1.

81. Choosing Parameters for NTRUEncrypt / J. Hoffstein et al. *Topics in Cryptology – CT-RSA 2017*. Cham, 2017. P. 3–18. DOI: https://doi.org/10.1007/978-3-319-52153-4_1.

82. NTRU Prime: Reducing Attack Surface at Low Cost / D. J. Bernstein et al. *Selected Areas in Cryptography – SAC 2017*. Cham, 2017. P. 235–260. DOI: https://doi.org/10.1007/978-3-319-72565-9_12.

83. New directions in nearest neighbor searching with applications to lattice sieving / A. Becker et al. *Proceedings of the Twenty-Seventh Annual ACM-SIAM Symposium on Discrete Algorithms*. Philadelphia, PA, 2015. DOI: https://doi.org/10.1137/1.9781611974331.ch2.

84. Laarhoven T. Sieving for Closest Lattice Vectors (with Preprocessing). *Lecture Notes in Computer Science*. Cham, 2017. P. 523–542. DOI: https://doi.org/10.1007/978-3-319-69453-5_28.

85. Regev O. On lattices, learning with errors, random linear codes, and cryptography. *the thirty-seventh annual ACM symposium*, Baltimore, MD, USA, 22–24 May 2005. New York, New York, USA, 2005. DOI: https://doi.org/10.1145/1060590.1060603.

86. Regev O. On lattices, learning with errors, random linear codes, and cryptography. *Journal of the ACM*. 2009. Vol. 56, no. 6. P. 1–40. DOI: https://doi.org/10.1145/1568318.1568324.

87. Ігнатенко С. М. Методи розв'язання задачі LPN над скінченними кільцями для оцінювання стійкості симетричних постквантових шифроситем : дис. канд. техн. наук : 05.13.21. Харків, 2021. 179 с.

88. Classical Hardness of Learning with Errors / Z. Brakerski et al. *45th ACM STOC, Palo Alto, CA, USA*. 2013. P. 575–584.

89. Peikert C. Public-key cryptosystems from the worst-case shortest vector problem: extended abstract. *Proceedings of the 41st annual ACM symposium on theory of computing, STOC 2009, Bethesda, MD, USA*. 2009. P. 333–342.

90. Lyubashevsky V. Search to decision reduction for the learning with errors over rings problem. *2011 IEEE Information Theory Workshop (ITW)*, Paraty, Brazil, 16–20 October 2011. 2011. DOI: https://doi.org/10.1109/itw.2011.6089491.

91. Post-quantum key exchange - a new hope / E. Alkim et al. *Cryptology ePrint Archive*. URL: https://eprint.iacr.org/2015/1092 (дата звернення: 04.05.2023).

92. Frodo: Take off the ring! Practical, Quantum-Secure Key Exchange from LWE / J. Bos et al. *Cryptology ePrint Archive*. URL: https://eprint.iacr.org/2016/659 (дата звернення: 04.05.2023).

93. Zhang X., Zheng Z., Wang X. A detailed analysis of primal attack and its variants. *Science China Information Sciences*. 2021. Vol. 65, no. 3. DOI: https://doi.org/10.1007/s11432-020-2958-9.

94. Revisiting the Expected Cost of Solving uSVP and Applications to LWE / M. R. Albrecht et al. *Advances in Cryptology – ASIACRYPT 2017*. Cham, 2017. P. 297–322. DOI: https://doi.org/10.1007/978-3-319-70694-8_11.

95. Guo Q., Johansson T. Faster Dual Lattice Attacks for Solving LWE with Applications to CRYSTALS. *Lecture Notes in Computer Science*. Cham, 2021. P. 33–62. DOI: https://doi.org/10.1007/978-3-030-92068-5_2.

96. Ігнатенко С. М. Application of sequential method for constructing a statistical attack on the LPN-C cipher system over residue ring modulo 2N. *Ukrainian Information Security Research Journal*. 2018. Vol. 20, no. 3. DOI: https://doi.org/10.18372/2410-7840.20.12956.

97. Blum A., Kalai A., Wasserman H. Noise-tolerant learning, the parity problem, and the statistical query model. *Journal of the ACM*. 2003. Vol. 50, no. 4. P. 506–519. DOI: https://doi.org/10.1145/792538.792543.

98. On the complexity of the BKW algorithm on LWE / M. R. Albrecht et al. *Designs, Codes and Cryptography*. 2013. Vol. 74, no. 2. P. 325–354. DOI: https://doi.org/10.1007/s10623-013-9864-x.

99. Duc A., Tramèr F., Vaudenay S. Better Algorithms for LWE and LWR. *Advances in Cryptology - EUROCRYPT 2015 - 34th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Sofia, Bulgaria, April 26-30, 2015, Proceedings, Part I*. 2015. P. 173–202. DOI: https://doi.org/10.1007/978-3-662-46800-5_8.

100. Kirchner P., Fouque P.-A. An Improved BKW Algorithm for LWE with Applications to Cryptography and Lattices. *Lecture Notes in Computer Science*. Berlin, Heidelberg, 2015. P. 43–62. DOI: https://doi.org/10.1007/978-3-662-47989-6_3.

101. Zhang B., Jiao L., Wang M. Faster Algorithms for Solving LPN. *35th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Vienna, Austria, May 8-12, 2016,*. Proceedings, Part I, 2016. P. 168–195. DOI: https://doi.org/10.1007/978-3-662-49890-3_7.

102. An Algorithm for Solving the LPN Problem and Its Application to Security Evaluation of the HB Protocols for RFID Authentication / M. P. C. Fossorier et al. *Progress in Cryptology - INDOCRYPT 2006*. Berlin, Heidelberg, 2006. P. 48–62. DOI: https://doi.org/10.1007/11941378_5.

103. Bogos S., Vaudenay S. Optimization of LPN Solving Algorithms. *Advances in Cryptology – ASIACRYPT 2016*. Berlin, Heidelberg, 2016. P. 703–728. DOI: https://doi.org/10.1007/978-3-662-53887-6_26.

104. Guo Q., Johansson T., Löndahl C. Solving LPN Using Covering Codes. *Journal of Cryptology*. 2019. Vol. 33, no. 1. P. 1–33. DOI: https://doi.org/10.1007/s00145-019-09338-8.

105. Guo Q., Johansson T., Stankovski P. Coded-BKW: Solving LWE Using Lattice Codes. *Lecture Notes in Computer Science*. Berlin, Heidelberg, 2015. P. 23–42. DOI: https://doi.org/10.1007/978-3-662-47989-6_2.

106. Levieil É., Fouque P.-A. An Improved LPN Algorithm. *Lecture Notes in Computer Science*. Berlin, Heidelberg, 2006. P. 348–359. DOI: https://doi.org/10.1007/11832072_24.

107. Олексійчук А. М., Ігнатенко С. М., Поремський М. В. Системи лінійних рівнянь зі спотвореними правими частинами над скінченними кільцями. *Математичне та комп'ютерне моделювання. Серія: Технічні науки*. 2017. № 15. С. 150–155. URL: http://dspace.nbuv.gov.ua/handle/123456789/133807 (дата звернення: 04.05.2023).

108. Lyubashevsky V., Peikert C., Regev O. On Ideal Lattices and Learning with Errors over Rings. *Journal of the ACM*. 2013. Vol. 60, no. 6. P. 1–35. DOI: https://doi.org/10.1145/2535925.

109. Lyubashevsky V., Peikert C., Regev O. A Toolkit for Ring-LWE Cryptography. *Advances in Cryptology – EUROCRYPT 2013*. Berlin, Heidelberg, 2013. P. 35–54. DOI: https://doi.org/10.1007/978-3-642-38348-9_3.

110. Hoffstein J., Pipher J., Silverman J. H. NTRU: A new high speed public key cryptosystem. Preprint, presented at the rump session of Crypto’96, 1996. (Preprint).

111. American National Standard X9.98-2010. Lattice-based polynomial public key encryption algorithm, Part 1: key establishment, Part 2: data encryption. Official edition. 2010.

112. NTRU-LPR IND-CPA: A New Ideal Lattices-based Scheme / S. Diop et al. *Cryptology ePrint Archive, Report 2018/109*. 2018. URL: https://eprint.iacr.org/2018/109.pdf (дата звернення: 04.05.2023).

113. Lyubashevsky V., Seiler G. NTTRU: Truly Fast NTRU Using NTT. *IACR Transactions on Cryptographic Hardware and Embedded Systems*. 2019. P. 180–201. DOI: https://doi.org/10.46586/tches.v2019.i3.180-201.

114. Nevins M., KarimianPour C., Miri A. NTRU over rings beyond Z. *Designs, Codes and Cryptography*. 2009. Vol. 56, no. 1. P. 65–78. DOI: https://doi.org/10.1007/s10623-009-9342-7.

115. Kouzmenko R. Generalizations of the NTRU Cryptosystem. *Security Comm. Networks*. 2006. Vol. 9 (1). P. 6315–6334.

116. Juraphanthong W., Jitprapaikulsarn S. An asymmetric cryptography using Gaussian integers. *Engineering and Applied Science Research*. 2020. Vol. 47 (2). P. 153–160. URL: https://www.thaiscience.info/Journals/Article/EASR/10991028.pdf (дата звернення: 04.05.2023).

117. Camara M. G., Sow D., Sow D. DTRU1: first generalization of NTRU using dual integers. *International Journal of Algebra*. 2018. Vol. 12, no. 7. P. 257–271. DOI: https://doi.org/10.12988/ija.2018.311115.

118. Malekian E., Zakerolhosseini A., Mashatan A. QTRU: A Lattice Attack Resistant Version of NTRU PKCS Based on Quaternion Algebra. *Cryptology ePrint Archive*. 2009. P. 1–25. URL: https://eprint.iacr.org/2009/386.pdf (дата звернення: 04.05.2023).

119. M.G. Alsaidi N., T. Sadiq A., A. Majid A. CQTRU: A Commutative Quaternions Rings Based Public Key Cryptosystem. *Engineering and Technology Journal*. 2016. Vol. 34, no. 6B. P. 901–911. DOI: https://doi.org/10.30684/etj.34.6b.19.

120. Thakur K., Tripathi B. A Variant of NTRU with split quaternions algebra. *Palestine Journal of Mathematics*. 2017. Vol. 6 (2). P. 598–610. URL: https://pjm.ppu.edu/sites/default/files/papers/PJM_April_2017_28.pdf (дата звернення: 05.05.2023).

121. Bagheri K., Sadeghi M.-R., Panario D. A non-commutative cryptosystem based on quaternion algebras. *Designs, Codes and Cryptography*.

2017. Vol. 86, no. 10. P. 2345–2377. DOI: https://doi.org/10.1007/s10623-017-0451-4.

122. Choosing NTRUEncrypt Parameters in Light of Combined Lattice Reduction and MITM Approaches / P. S. Hirschhorn et al. *Applied Cryptography and Network Security*. Berlin, Heidelberg, 2009. P. 437–455. DOI: https://doi.org/10.1007/978-3-642-01957-9_27.

123. NIST PQ Submission: NTRUEncrypt A lattice based encryption algorithm / Z. Zhang et al. 2017.

124. Proos J. Imperfect decryption and an attack on the NTRU encryption scheme. *Cryptology ePrint Archive*. 2003. URL: https://eprint.iacr.org/2003/002 (дата звернення: 05.05.2023).

125. Lindell Y., Katz J. Introduction to Modern Cryptography. Taylor & Francis Group, 2020. 628 p.

126. NAEP: provable security in the presence of decryption failures / N. Howgrave-Graham et al. *Cryptology ePrint Archive*. 2013. URL: https://eprint.iacr.org/2003/172 (дата звернення: 05.05.2023).

127. Hoffstein J., Silverman J. Optimizations for NTRU. *Public-Key Cryptography and Computational Number Theory*. Berlin, New York. DOI: https://doi.org/10.1515/9783110881035.77.

128. Hoffstein J., Silverman J. H. Protecting NTRU Against Chosen Ciphertext and Reaction Attacks. *Technical report*. 2000. URL: https://www.ntru.org/f/tr/tr016v1.pdf (дата звернення: 05.05.2023).

129. EESS #1. Implementation Aspects of NTRUEncrypt and NTRUSign. Official edition. URL: https://messagevortex.net/devel/repo/thesis/src/main/latex/inc/bib/ntru_implementation.pdf (дата звернення: 05.05.2023).

130. Nguyen P. Q., Pointcheval D. Analysis and Improvements of NTRU Encryption Paddings. *Advances in Cryptology – CRYPTO 2002*. Berlin, Heidelberg, 2002. P. 210–225. DOI: https://doi.org/10.1007/3-540-45708-9_14.

131. Bellare M., Rogaway P. Optimal asymmetric encryption. *Advances in Cryptology – EUROCRYPT'94*. Berlin, Heidelberg, 1995. P. 92–111. DOI: https://doi.org/10.1007/bfb0053428.

132. Boneh D. Simplified OAEP for the RSA and Rabin Functions. *Advances in Cryptology – CRYPTO 2001*. Berlin, Heidelberg, 2001. P. 275–291. DOI: https://doi.org/10.1007/3-540-44647-8_17.

133. Universal Padding Schemes for RSA / J.-S. Coron et al. *Advances in Cryptology – CRYPTO 2002*. Berlin, Heidelberg, 2002. P. 226–241. DOI: https://doi.org/10.1007/3-540-45708-9_15.

134. Fujisaki E., Okamoto T. How to Enhance the Security of Public-Key Encryption at Minimum Cost. *Public Key Cryptography*. Berlin, Heidelberg, 1999. P. 53–68. DOI: https://doi.org/10.1007/3-540-49162-7_5.

135. Steinfeld R. NTRU cryptosystem: Recent developments and emerging mathematical problems in finite polynomial rings. *Algebraic Curves and Finite Fields*. 2014. P. 179–212. DOI: https://doi.org/10.1515/9783110317916.179

136. Stehlé D., Steinfeld R. Making NTRU as Secure as Worst-Case Problems over Ideal Lattices. *Advances in Cryptology – EUROCRYPT 2011*. Berlin, 82, 2011. P. 27–47. DOI: https://doi.org/10.1007/978-3-642-20465-4_4.

137. May A. How to Meet Ternary LWE Keys. *Advances in Cryptology – CRYPTO 2021*. Cham, 2021. P. 701–731. DOI: https://doi.org/10.1007/978-3-030-84245-1_24.

138. Kirshanova E., May A. How to Find Ternary LWE Keys Using Locality Sensitive Hashing. *Cryptography and Coding*. Cham, 2021. P. 247–264. DOI: https://doi.org/10.1007/978-3-030-92641-0_12.

139. Hoffstein J., Pipher J., Silverman J. H. NTRU: A ring-based public key cryptosystem. *Lecture Notes in Computer Science*. Berlin, Heidelberg, 1998. P. 267–288. DOI: https://doi.org/10.1007/bfb0054868.

140. Howgrave-Graham N. A Hybrid Lattice-Reduction and Meet-in-the-Middle Attack Against NTRU. *Advances in Cryptology - CRYPTO 2007*. Berlin, Heidelberg. P. 150–169. DOI: https://doi.org/10.1007/978-3-540-74143-5_9.

141. Howgrave-Graham N., Silverman J., Whyte W. A meet-in-the-midle attack on an NTRU private key. *Technical report*. 2003. URL: https://ntru.org/f/tr/tr004v2.pdf (дата звернення: 05.05.2023).

142. Coppersmith D., Shamir A. Lattice Attacks on NTRU. *Advances in Cryptology – EUROCRYPT '97*. Berlin, Heidelberg, 1997. P. 52–61. DOI: https://doi.org/10.1007/3-540-69053-0_5.

143. Valluri M. R. NTRUCipher-lattice based secret key encryption. 2017. DOI: https://doi.org/10.48550/arXiv.1710.01928.

РОЗДІЛ 2

АНАЛІТИЧНІ СПІВВІДНОШЕННЯ ДЛЯ ОЦІНЮВАННЯ ПАРАМЕТРІВ, ЩО ХАРАКТЕРИЗУЮТЬ ПРАКТИЧНІСТЬ NTRU-ПОДІБНИХ ШИФРОСИСТЕМ

Як зазначено в попередньому розділі, важливою окремою задачею дослідження NTRU-подібних шифросистем є отримання аналітичних співвідношень для параметрів, що характеризують їхню практичність. Це, насамперед, ймовірність оборотності випадкових поліномів, які використовуються в ролі компонентів секретних ключів шифросистем, та ймовірність помилкового розшифрування шифрованих повідомлень законним користувачем.

Для означення асиметричних NTRU-подібних шифросистем найчастіше використовують кільце зрізаних поліномів $R_{n,q} = \mathbf{Z}_q[x]/(x^n - 1)$, де n і q – взаємно прості натуральні числа, а також натуральне число p, взаємно просте з q. Секретним ключем шифросистеми є пара поліномів $F(x), g(x) \in R_{n,q}$ таких, що поліном $f(x) = 1 + pF(x)$ є оборотним у кільці $R_{n,q}$, а відкритим ключем – поліном $h = pg(x)(f(x))^{-1} \in R_{n,q}$. У випадку симетричної NTRU-подібної шифросистеми [1] секретний ключ визначається аналогічно.

В п. 2.1 наведено аналітичні співвідношення для оцінювання ймовірності оборотності полінома $f(x)$ у припущенні, що коефіцієнти полінома $F(x)$ є незалежними випадковими величинами, які приймають значення ± 1 і 0 з ймовірностями θ і $1 - 2\theta$ відповідно, де $\theta \in (0, 1/2)$. Зазначені співвідношення отримано вперше. Показано, що вони надають змогу оцінювати (а окремих практично важливих випадках – обчислювати)

значення ймовірності оборотності випадкових поліномів, що використовуються в NTRU-подібних шифросистемах.

В п. 2.2 наведено аналітичні співвідношення для оцінювання ймовірності помилкового розшифрування повідомлень при фіксованому ключі у шифросистемі NTRUEncrypt [2, 3]. Перша з двох отриманих аналітичних оцінок доводиться аналогічно оцінці з [3] та є наближеною в тому сенсі, що при її доведенні (саме так, як і в [3]) здійснюється заміна дограничного розподілу ймовірностей суми певних незалежних випадкових величин граничним (нормальним) розподілом. Друга отримана аналітична оцінка доводиться за допомогою нерівності Гефдінга [4] та не базується на жодних припущеннях евристичного характеру. В цілому, отримані співвідношення надають більш адекватну інформацію про частоту виникнення помилок при розшифруванні для розглянутої шифросистеми та можуть бути використані в подальшому при виборі параметрів цієї шифросистеми для її оптимізації за стійкістю або практичністю.

Нарешті, в п. 2.3 наведено узагальнення основного результату п. 2.2 на випадок довільних NTRU-подібних шифросистем, які будуються над кільцем R_f зрізаних поліномів за модулем унітарного полінома $f(x)$ з дійсними коефіцієнтами. Науковою основою для цього узагальнення є твердження, що надає змогу обчислювати на практиці значення параметра $\theta(f)$, який характеризує величину sup-норми добутку елементів кільця R_f. Зокрема, отримано (позитивну) відповідь на важливе запитання, поставлене в 2008 р. В. Любашевським [5], про існування ефективного алгоритму обчислення параметра $\theta(f)$.

2.1. Аналітичні співвідношення для ймовірності оборотності випадкових поліномів, які використовуються в NTRU-подібних шифросистемах

Нехай n і q – різні прості числа, p – натуральне число, взаємно просте з q, $p < q-1$, $\mathbf{Z}_q$ – кільце класів лишків за модулем q, $R_{n,q} = \mathbf{Z}_q[x]/(x^n - 1)$ – кільце зрізаних поліномів степеня не вище $n-1$ над кільцем $\mathbf{Z}_q$. Нехай, далі, $\xi_0, \xi_1, \ldots, \xi_{n-1}$ – незалежні випадкові величини, розподілені за законом

$$\mathbf{P}\{\xi_i = 1\} = \mathbf{P}\{\xi_i = -1\} = \theta,\ \mathbf{P}\{\xi_i = 0\} = 1 - 2\theta,\ i \in \overline{0, n-1}, \qquad (2.1)$$

де $\theta \in (0, 1/2)$. Необхідно отримати аналітичні співвідношення для оцінювання ймовірності $\pi_{n,q}$ події, яка полягає в тому, що елемент кільця $R_{n.q}$, який відповідає поліному $f(x) = 1 + pF(x)$, де $F(x) = \xi_0 + \xi_1 x + \ldots + \xi_{n-1} x^{n-1}$, є оборотним в цьому кільці.

Зауважимо, що у випадку, коли q є степенем простого числа $\bar{q}$, то оборотність полінома $f(x)$ в кільці $R_{n.q}$ є рівносильною його оборотності в кільці $R_{n,\bar{q}}$. Тому результати, наведені нижче для простого q, є справедливими також у випадку, коли q є степенем простого числа.

Для знаходження оцінок ймовірності $\pi_{n,q}$ розглянемо канонічний розклад полінома $x^n - 1$ над полем $\mathbf{Z}_q$. Нехай m – показник, якому належить q за модулем n (тобто найменше натуральне число, для якого $q^m \equiv 1 \bmod n$). Тоді $x^n - 1 = (x-1) f_1(x) \cdots f_t(x)$, де $f_1(x), \ldots, f_t(x)$ – різні незвідні поліноми степені m над полем $\mathbf{Z}_q$, $t = (n-1)/m$ [6], теор. 2.47. Позначимо α_j довільний корінь полінома $f_j(x)$ в полі $\mathbf{GF}(q^m)$, $j \in \overline{1,t}$. Покладемо $\alpha_0 = 1$,

$$\pi_{n,q}(\alpha_j) = \mathbf{P}\{f(\alpha_j) = 0\},\ j \in \overline{0,t}. \qquad (2.2)$$

Зрозуміло, що поліном $f(x)$ не є оборотним в кільці $R_{n.q}$ тоді й тільки

тоді, коли існує $j \in \overline{0,t}$ таке, що $f(\alpha_j) = 0$. Звідси випливають такі нерівності:

$$\max_{0 \le j \le t} \pi_{n,q}(\alpha_j) \le \pi_{n,q} \le \pi_{n,q}(\alpha_0) + t \max_{1 \le j \le t} \pi_{n,q}(\alpha_j) \qquad (2.3)$$

Наступне твердження встановлює явні вирази параметрів (2.2).

Твердження 2.1. Для будь-якого $j \in \overline{0,t}$ справедлива рівність

$$\pi_{n,q}(\alpha_j) = q^{-m} \sum_{x \in \mathbf{GF}(q^m)} \cos\left(\frac{2\pi \operatorname{Tr}(x)}{q}\right) \prod_{k=0}^{n-1} \left(1 - 2\theta\left(1 - \cos\left(\frac{2\pi p \operatorname{Tr}(\alpha_j^{\,k} x)}{q}\right)\right)\right), \quad (2.4)$$

де $\operatorname{Tr}(z) = z + z^q + \cdots + z^{q^{m-1}}$ – абсолютний слід елементу $z \in \mathbf{GF}(q^m)$.

Доведення. За означенням

$$\pi_{n,q}(\alpha_j) = \mathbf{P}\{f(\alpha_j) = 0\} = \mathbf{P}\{p\xi_0 + p\xi_1 \alpha_j + \ldots + p\xi_{n-1} \alpha_j^{\,n-1} = -1\},$$

де $\xi_0, \xi_1, \ldots, \xi_{n-1}$ – незалежні випадкові величини, що розподілені за законом (2.1).

Позначимо $\chi(z) = \exp\left\{\frac{2\pi i \operatorname{Tr}(z)}{q}\right\}$, $z \in \mathbf{GF}(q^m)$ нетривіальний адитивний характер поля $\mathbf{GF}(q^m)$ (де $i^2 = -1$; див., наприклад, [7]). Перетворення Фур'є розподілу випадкової величини $\eta_k = p\xi_k \alpha_j^{\,k}$ має такий вигляд:

$$\psi_k(x) = \sum_{a \in \mathbf{GF}(q^m)} \mathbf{P}\{\eta_k = a\}\chi(ax) = 1 - 2\theta + \theta(\chi(\alpha_j^{\,k} px) + \chi(-\alpha_j^{\,k} px)) =$$

$$= 1 - 2\theta + \theta(\chi(\alpha_j^{\,k} px) + \overline{\chi(\alpha_j^{\,k} px)}) = 1 - 2\theta(1 - \operatorname{Re}(\chi(\alpha_j^{\,k} px))) =$$

$$= 1 - 2\theta\left(1 - \cos\left(\frac{2\pi p \mathrm{Tr}(\alpha_j{}^k x)}{q}\right)\right),\ x \in \mathbf{GF}(q^m),\ k \in \overline{0, n-1}.$$

Звідси, використовуючи теорему про згортку і формулу обернення для перетворення Фур'є (див., наприклад, [7]), отримаємо, що

$$\pi_{n,q}(\alpha_j) = q^{-m} \sum_{x \in \mathbf{GF}(q^m)} \overline{\chi(-x)}\, \psi_0(x) \cdots \psi_{n-1}(x) =$$

$$= q^{-m} \sum_{x \in \mathbf{GF}(q^m)} \exp\left\{\frac{2\pi i\, \mathrm{Tr}(x)}{q}\right\} \prod_{k=0}^{n-1}\left(1 - 2\theta\left(1 - \cos\left(\frac{2\pi p \mathrm{Tr}(\alpha_j^k x)}{q}\right)\right)\right).$$

Оскільки $\pi_{n,q}(\alpha_j)$ – дійсне число, то отримана рівність є рівносильною формулі (2.4). Твердження доведено.

Вважаючи у формулі (2.4) $j = 0$, отримаємо такий результат.

Наслідок 2.1. Має місце рівність

$$\pi_{n,q}(1) = q^{-1} \sum_{k=0}^{q-1} \cos\left(\frac{2\pi k}{q}\right)\left(1 - 2\theta\left(1 - \cos\left(\frac{2\pi p k}{q}\right)\right)\right)^n. \qquad (2.5)$$

Зокрема, якщо $q = 2$, то

$$\pi_{n,2}(1) = 2^{-1}(1 - (1 - 4\theta)^n) \qquad (2.6)$$

Наступне твердження є основним в цьому підрозділі та надає аналітичний вираз ймовірності $\pi_{n,q}$ у випадку, коли m приймає найбільше можливе значення, що дорівнює $n-1$.

Твердження 2.2. Нехай $m = n-1$. Тоді, якщо q є непарним, то

$$\pi_{n,q} = q^{-1}\sum_{k=0}^{q-1}\cos\left(\frac{2\pi k}{q}\right)\left(1-2\theta\left(1-\cos\left(\frac{2\pi pk}{q}\right)\right)\right)^n. \qquad (2.7)$$

Якщо ж $q = 2$, то

$$\pi_{n,2} = 2^{-1}(1-(1-4\theta)^n) + (1-2\theta)\theta^{n-1}. \qquad (2.8)$$

Крім того, якщо p' є елементом, оберненим до p за модулем q, $p' \in \overline{0, q-1}$ і $n < \min\{p', q-p'\}$, то $\pi_{n,q} = 0$.

Доведення. Якщо $m = n-1$, то $t = 1$, і поліном $x^n - 1$ над полем $\mathbf{Z}_q$ розкладається у добуток двох різних незвідних множників: $x-1$ і $\Phi_n(x) = x^{n-1} + x^{n-2} + \cdots + 1$. Тому елемент $f(x)$ кільця $R_{n,q}$ є необоротним тоді й тільки тоді, коли має місце одна з двох взаємовиключних умов: $f(1) = 0$; $f(x) = \Phi_n(x)$.

Нехай $f(x) = 1 + pF(x)$, де $F(x) = \xi_0 + \xi_1 x + \ldots + \xi_{n-1}x^{n-1}$, а $\xi_0, \xi_1, \ldots, \xi_{n-1}$ – незалежні випадкові величини, розподілені за законом (2.1). Тоді при непарному q в силу нерівності $p < q-1$ маємо

$$\mathbf{P}\{f(x) = \Phi_n(x)\} = \mathbf{P}\{1 + p\xi_0 = 1,\ p\xi_1 = \ \ldots\ = p\xi_{n-1} = 1\} = 0,$$

$\pi_{n,q} = \pi_{n,q}(1)$, звідки на підставі формули (2.5) випливає рівність (2.7).

Якщо ж $q = 2$, то

$$\mathbf{P}\{f(x) = \Phi_n(x)\} = \mathbf{P}\{\xi_0 = 0,\ \xi_1 = \ \ldots\ = \xi_{n-1} = 1\} = (1-2\theta)\theta^{n-1},$$

$\pi_{n,2} = \pi_{n,2}(1) + (1-2\theta)\theta^{n-1}$, звідки на підставі формули (2.6) випливає рівність (2.8).

Покажемо, нарешті, що з умови $n < \min\{p', q-p'\}$ випливає рівність $\pi_{n,q} = 0$. Зауважимо, що $p' > 1$, оскільки $n > 1$; отже, q є непарним простим числом і згідно з доведеним

$$\pi_{n,q} = \pi_{n,q}(1) = \mathbf{P}\{\xi_0 + \xi_1 + \cdots + \xi_{n-1} \equiv (q-p') \bmod q\}.$$

Позначимо $\eta = \xi_0 + \xi_1 + \cdots + \xi_{n-1}$. Оскільки випадкові величини $\xi_0, \xi_1, \ldots, \xi_{n-1}$ приймають значення $0, \pm 1$, то $|\eta| \le n$. Якщо $\eta \ge 0$, то в силу співвідношення $0 \le \eta \le n < \min\{p', q-p'\} < q$ отримаємо, що $\eta \bmod q = \eta < q - p'$ і порівняння $\eta \equiv (q-p') \bmod q$ не виконується. Якщо $\eta \le 0$, то в силу тих самих співвідношень отримаємо, що $-\eta \bmod q = -\eta < p'$, і порівняння $\eta \equiv (q-p') \bmod q$ також не виконується. Таким чином, подія $\{\eta \equiv (q-p') \bmod q\}$ є неможливою і $\pi_{n,q} = \mathbf{P}\{\eta \equiv (q-p') \bmod q\} = 0$.

Твердження доведено.

Наслідок 2.2. Нехай виконується умова твердження 2.2, $p = 3$ і $q > 3n+1$. Тоді $\pi_{n,q} = 0$.

Доведення. Достатньо зазначити, що $p' = \dfrac{q+1}{3}$, якщо $q \equiv -1 \bmod 3$ і $p' = \dfrac{2q+1}{3}$, якщо $q \equiv 1 \bmod 3$.

Співвідношення (2.7), (2.8) надають змогу дослідити поведінку ймовірності $\pi_{n,q}$ як функції параметра θ у найбільш цікавих з практичної точки зору випадках:

а) $q = 2^l$, n – непарне просте число, 2 – примітивний елемент поля $\mathbf{Z}_n$;

б) q і n – різні непарні прості числа, $p = 3 < q-1$, і показник, якому

належить q за модулем n, дорівнює $n-1$.

Як зазначено вище, у випадку (а) виконується рівність $\pi_{n,q}=\pi_{n,2}$. При цьому ймовірність $\pi_{n,q}$ практично не відрізняється від 0,5 при всіх розумних, з практичної точки зору, значеннях n і θ (іншими словами, в середньому кожен другий випадково згенерований за наведеним вище законом поліном є необоротним у кільці $R_{n.q}$; рис. 2.1, 2.2).

У випадку (б) ймовірність $\pi_{n,q}$ швидко зменшується з ростом q при фіксованих n і θ, обертаючись в нуль при $q>3n+1$. Аналогічна поведінка ймовірності спостерігається зі зменшенням параметра θ при фіксованих n і q, див. табл. 2.1, 2.2. При цьому ймовірність необоротності випадкового полінома у кільці $R_{n.q}$ не перевищує $1{,}5\cdot10^{-2}$, що суттєво менше 0,5.

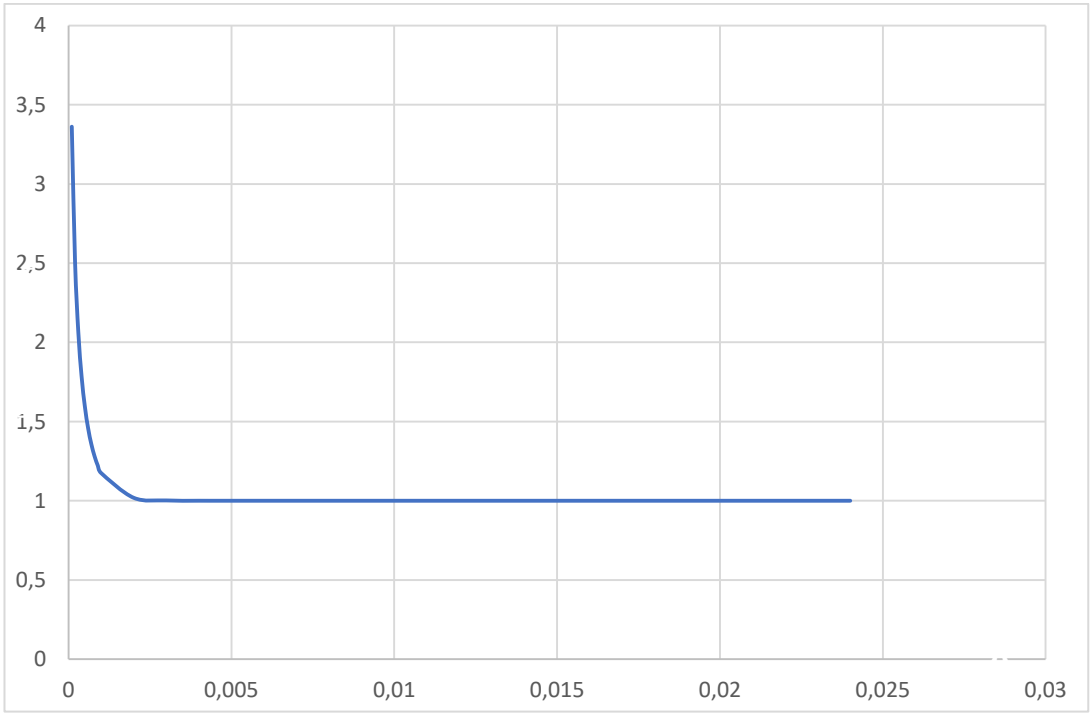

Рисунок 2.1 – Залежність (взятого зі знаком мінус) двійкового логарифма ймовірності (2.8) від параметра θ при $n=541$

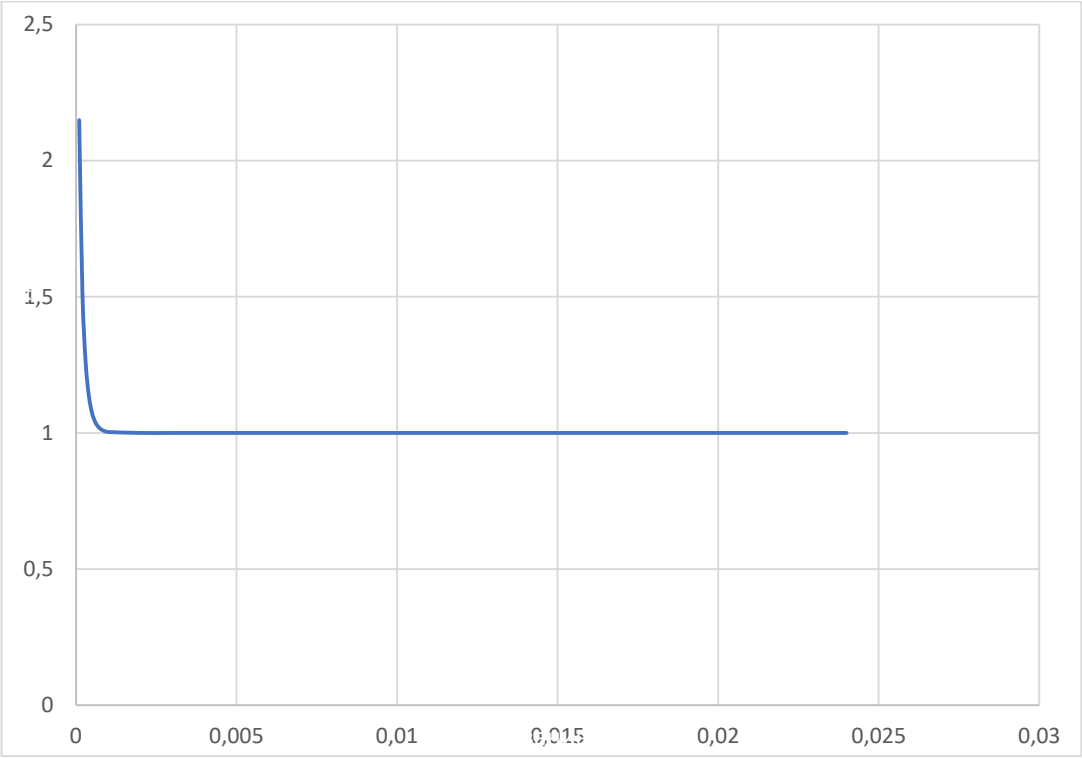

Рисунок 2.2 – Залежність (взятого зі знаком мінус) двійкового логарифма ймовірності (2.8) від параметра θ при $n=1499$

Таблиця 2.1 – Чисельні значення ймовірності (2.7) при $n=541,\ p=3$

q θ	0,0001	0,001	0,01	0,1	0,2	0,3	0,4
59	$1{,}2\cdot10^{-44}$	$4{,}7\cdot10^{-25}$	$1{,}3\cdot10^{-8}$	$6{,}1\cdot10^{-3}$	$1{,}2\cdot10^{-2}$	$1{,}4\cdot10^{-2}$	$1{,}5\cdot10^{-2}$
73	$3{,}4\cdot10^{-55}$	$1{,}4\cdot10^{-31}$	$3{,}3\cdot10^{-11}$	$2{,}7\cdot10^{-3}$	$7{,}3\cdot10^{-3}$	$9{,}7\cdot10^{-3}$	$1{,}1\cdot10^{-2}$
257	$3{,}4\cdot10^{-243}$	$1{,}5\cdot10^{-157}$	$4{,}8\cdot10^{-75}$	$9{,}9\cdot10^{-17}$	$9{,}9\cdot10^{-10}$	$3{,}6\cdot10^{-6}$	$8{,}9\cdot10^{-6}$
331	$1{,}0\cdot10^{-323}$	$8{,}0\cdot10^{-214}$	$3{,}7\cdot10^{-107}$	$9{,}3\cdot10^{-26}$	$1{,}8\cdot10^{-14}$	$1{,}5\cdot10^{-8}$	$6{,}8\cdot10^{-8}$
383	0	$6{,}3\cdot10^{-258}$	$3{,}9\cdot10^{-133}$	$7{,}6\cdot10^{-34}$	$8{,}0\cdot10^{-19}$	$9{,}8\cdot10^{-11}$	$7{,}8\cdot10^{-10}$
487	0	0	$5{,}0\cdot10^{-186}$	$4{,}6\cdot10^{-52}$	$7{,}1\cdot10^{-29}$	$8{,}2\cdot10^{-16}$	$2{,}4\cdot10^{-14}$

Таблиця 2.2 – Чисельні значення ймовірності (2.7) при $n=1499,\ p=3$

q θ	0,0001	0,001	0,01	0,1	0,2	0,3	0,4
463	0	$7{,}6\cdot10^{-250}$	$5{,}9\cdot10^{-106}$	$2{,}1\cdot10^{-19}$	$4{,}1\cdot10^{-11}$	$2{,}5\cdot10^{-8}$	$5{,}8\cdot10^{-7}$
659	0	0	$1{,}2\cdot10^{-181}$	$7{,}2\cdot10^{-37}$	$4{,}4\cdot10^{-20}$	$2{,}5\cdot10^{-14}$	$1{,}9\cdot10^{-11}$
787	0	0	$3{,}3\cdot10^{-235}$	$5{,}3\cdot10^{-51}$	$1{,}9\cdot10^{-27}$	$2{,}9\cdot10^{-19}$	$3{,}7\cdot10^{-15}$

827	0	0	$7{,}1\cdot10^{-254}$	$3{,}2\cdot10^{-56}$	$3{,}4\cdot10^{-30}$	$4{,}2\cdot10^{-21}$	$1{,}6\cdot10^{-16}$
1151	0	0	0	$9{,}9\cdot10^{-105}$	$2{,}8\cdot10^{-56}$	$1{,}2\cdot10^{-38}$	$1{,}1\cdot10^{-29}$
1289	0	0	0	$1{,}2\cdot10^{-129}$	$4{,}6\cdot10^{-70}$	$6{,}3\cdot10^{-48}$	$1{,}2\cdot10^{-36}$

Отримані аналітичні співвідношення надають змогу оцінювати (а в окремих практично важливих випадках – обчислювати) значення ймовірності оборотності випадкових поліномів, які використовуються як секретні ключі відповідних NTRU-подібних шифросистем. Ці співвідношення можуть бути використані також для вибору параметрів n, q і θ цих шифросистем.

2.2. Аналітичні співвідношення для оцінювання ймовірності помилкового розшифрування повідомлень у шифросистемі NTRUEncrypt при фіксованому ключі

Нехай n і q – взаємно прості натуральні числа, $n,q>3$, q не ділиться на 3. Як і раніше, позначимо $\mathbf{Z}_q$ кільце класів лишків за модулем q, елементи якого ототожнимо з цілими числами, що належать інтервалу $[-(q-1)/2,(q-1)/2]$ для непарного q та інтервалу $[-q/2,q/2-1]$ для парного q. Позначимо $R_{n,q}=\mathbf{Z}_q[x]/(x^n-1)$ кільце зрізаних многочленів степеня не вище $n-1$ над кільцем $\mathbf{Z}_q$. Для будь-якого $u=u_0+u_1x+\cdots+u_{n-1}x^{n-1}\in\mathbf{Z}[x]$ позначимо $u \bmod q$ поліном $(u_0 \bmod q)+(u_1 \bmod q)x+\cdots+(u_{n-1} \bmod q)x^{n-1}\in R_{n,q}$. Аналогічний сенс має позначення $u \bmod 3$.

Позначимо також $\|u\|_\infty=\max\limits_{0\le i\le n-1}|u_i|$, $\|u\|_1=\sum\limits_{i=0}^{n-1}|u_i|$. Поліном u називається малим, якщо $\|u\|_\infty=1$, $i\in\overline{0,n-1}$.

Для будь-яких натуральних чисел d_1,d_2 позначимо S_{d_1,d_2} множину всіх

малих поліномів степеня не вище $n-1$, серед коефіцієнтів яких є точно d_1, що дорівнюють 1, та точно d_2, що дорівнюють -1.

Нагадаємо, що секретним ключем шифросистеми NTRUEncrypt є будь-яка пара поліномів (F, g), де $F \in S_{d,d}$, $g \in S_{d'+1,d'}$, $d' = \lfloor n/3 \rfloor$ і поліном $f = 1 + 3F$ є оборотним елементом кільця $R_{n,q}$. Відповідним відкритим ключем є поліном $h = 3g / f$, який обчислюється в кільці $R_{n,q}$ шляхом множення полінома $3g$ на поліном, обернений до f.

Множина відкритих текстів шифросистеми NTRUEncrypt складається з усіх малих поліномів степеня не вище n. Для зашифрування такого полінома m на відкритому ключі h генерується випадковий поліном $r \in S_{d,d}$ та обчислюється шифротекст $E_h(m,r) = (m + rh) \bmod q$. Розшифрування довільного тексту $c \in R_{n,q}$ на секретному ключі (F, g) здійснюється за формулою $D_f(c) = cf \pmod q \bmod 3$. Якщо при цьому $D_f(E_h(m,r)) \neq m$, то говорять, що відбувається помилка розшифрування.

Як випливає з наведених означень, за умови помилки розшифрування принаймні один з коефіцієнтів полінома $mf + 3rg \in \mathbf{Z}[x]$ є за модулем не менше ніж $q/2$. Отже, справедлива імплікація

$$D_f(E_h(m,r)) \neq m \;\Rightarrow \| mf + 3rg \|_\infty \geq q/2. \qquad (2.9)$$

Зауважимо, що на підставі рівностей $f = 1 + 3F$, $\| F \|_1 = \| r \|_1 = 2d$ мають місце такі співвідношення:

$$\| mf + 3rg \|_\infty = \| m + 3(mF + rg) \|_\infty \leq 1 + 3(\| m \|_\infty \| F \|_1 + \| r \|_1 \| g \|_\infty) = 1 + 12d.$$

Таким чином, за умови

$$d < (q-2)/24 \tag{2.10}$$

помилки розшифрування є неможливими. Якщо ж нерівність (2.10) не виконується, то помилки можливі, і постає задача оцінювання ймовірності помилкового розшифрування повідомлень при тих чи інших припущеннях відносно елементів F, g, m та r.

В [3] отримано наближену верхню оцінку ймовірності $p_{er} = \mathbf{P}_{F,g,m,r}\{D_f(E_h(m,r)) \neq m\}$ за умови, що коефіцієнти поліномів F, g, m і r є незалежними випадковими величинами, розподіленими за законами

$$\mathbf{P}(F_i = 1) = \mathbf{P}(F_i = -1) = dn^{-1},\ \mathbf{P}(F_i = 0) = 1 - 2dn^{-1},$$

$$\mathbf{P}(g_i = 1) = \mathbf{P}(g_i = -1) = d'n^{-1},\ \mathbf{P}(g_i = 0) = 1 - 2d'n^{-1},$$

$$\mathbf{P}(m_i = 1) = \mathbf{P}(m_i = -1) = \mathbf{P}(m_i = 0) = 1/3, \tag{2.11}$$

$$\mathbf{P}(r_i = 1) = \mathbf{P}(r_i = -1) = dn^{-1}, \mathbf{P}(r_i = 0) = 1 - 2dn^{-1}: \tag{2.12}$$

$$p_{er} \leq 2n\ \Phi\left(-\frac{q-2}{6} \Big/ \sqrt{\frac{4d}{3}\left(1 + \frac{d'}{n}\right)} \right), \tag{2.13}$$

де $\Phi(x) = \dfrac{1}{\sqrt{2\pi}} \int\limits_{-\infty}^{x} e^{-\frac{t^2}{2}} dt$ є функція розподілу стандартного нормального закону. Зауважимо, що наближений характер оцінки (2.13) обумовлений заміною догранічного розподілу суми певних незалежних випадкових величин її граничним (нормальним) розподілом ймовірностей.

У даному підрозділі розв'язується задача отримання оцінок ймовірності $p_{er}(F,g) = \mathbf{P}_{m,r}\{D_f(E_h(m,r)) \neq m\}$ за умови, що поліноми F і g є

фіксованими, а коефіцієнти поліномів m і r є незалежними випадковими величинами, розподіленими за законами (2.11) і (2.12) відповідно.

Підкреслимо, що набір ймовірностей $(p_{er}(F,g): F \in S_{d,d}, g \in S_{d'+1,d'})$ є суттєво більш точним показником частоти виникнення помилок розшифрування у шифросистемі NTRUEncrypt в порівнянні з єдиним параметром $p_{er}(F,g)$ (який є усередненим значенням ймовірностей $p_{er}(F,g)$ за всіма $F \in S_{d,d}$, $g \in S_{d'+1,d'}$).

Справедливо таке твердження.

Твердження 2.3. Нехай $F \in S_{d,d}$, $g \in S_{d'+1,d'}$, а коефіцієнти поліномів m і r є незалежними випадковими величинами, розподіленими за законами (2.11) і (2.12) відповідно. Для будь-якого $i \in \overline{0,n-1}$ позначимо $p(i,F,g)$ ймовірність того, що модуль i-го коефіцієнту випадкового полінома $mf+3rg$ є не менше ніж $q/2$. Тоді справедливі (наближені) нерівності

$$2\,\Phi\left(-\frac{q+2}{6}\Bigg/\sqrt{\frac{4d}{3}\left(1+\frac{3(2d'+1)}{2n}\right)}\right) \le p(i,F,g) \le$$

$$\le 2\,\Phi\left(-\frac{q-2}{6}\Bigg/\sqrt{\frac{4d}{3}\left(1+\frac{3(2d'+1)}{2n}\right)}\right). \qquad (2.14)$$

Крім того, справедлива (наближена) нерівність

$$p_{er}(F,g) \le 2n\,\Phi\left(-\frac{q-2}{6}\Bigg/\sqrt{\frac{4d}{3}\left(1+\frac{3(2d'+1)}{2n}\right)}\right), \qquad (2.15)$$

а також нерівність

$$p_{er}(F,g) \le 2n \exp\left\{ - \frac{(q-2)^2}{72(2d+2d'+1)} \right\}, \qquad (2.16)$$

Доведення. На підставі наведених означень

$$p(i,F,g) = \mathbf{P}\{|\, m_i + 3(mF)_i + 3(rg)_i \,| \ge q/2\} \le \mathbf{P}\{|\, (mF)_i + (rg)_i \,| \ge (q-2)/6\} =$$

$$= \mathbf{P}\left\{ \left| \sum_{j=0}^{n-1} F_j m_{i-j} + \sum_{j=0}^{n-1} g_j r_{i-j} \right| \ge (q-2)/6 \right\}. \qquad (2.17)$$

Позначимо

$$I' = \{ j \in \overline{0,n-1} : F_j = 1 \},\ I'' = \{ j \in \overline{0,n-1} : F_j = -1 \},$$

$$J' = \{ j \in \overline{0,n-1} : g_j = 1 \},\ J'' = \{ j \in \overline{0,n-1} : g_j = -1 \}.$$

Тоді, враховуючи формули (2.11), (2.12), можна записати нерівність (2.17) у вигляді

$$p(i,F,g) \le \mathbf{P}\left\{ \left| \sum_{j \in I'} m_{i-j} - \sum_{j \in I''} m_{i-j} + \sum_{j \in J'} r_{i-j} - \sum_{j \in J''} r_{i-j} \right| \ge (q-2)/6 \right\} =$$

$$= \mathbf{P}\left\{ \left| \sum_{k=1}^{2d} \xi_k + \sum_{l=1}^{2d'+1} \eta_l \right| \ge (q-2)/6 \right\}, \qquad (2.18)$$

де ξ_k, η_l є незалежними випадковими величинами, розподіленими за законами

$$\mathbf{P}(\xi_k = 1) = \mathbf{P}(\xi_k = -1) = \mathbf{P}(\xi_k = 0) = 1/3\,,\ k \in \overline{1,2d}\,,$$

$$\mathbf{P}(\eta_l = 1) = \mathbf{P}(\eta_l = -1) = dn^{-1},\ \mathbf{P}(\eta_l = 0) = 1 - 2dn^{-1},\ l \in \overline{1,2d'+1}.$$

Позначимо $\varsigma = \sum_{k=1}^{2d} \xi_j + \sum_{l=1}^{2d'+1} \eta_l$. Тоді

$$\mathbf{E}\varsigma = 0\,,\ \mathbf{D}\varsigma = \sum_{k=1}^{2d} \mathbf{D}\xi_j + \sum_{l=1}^{2d'+1} \mathbf{D}\eta_l = 2d \cdot \frac{2}{3} + (2d'+1) \cdot \frac{2d}{n}\,.$$

Отже, підставі центральної граничної теореми справедлива (наближена) рівність

$$\mathbf{P}\{|\,\varsigma\,| \ge (q-2)/6\} = \mathbf{P}\left\{ \left| \frac{\varsigma - \mathbf{E}\varsigma}{\sqrt{\mathbf{D}\varsigma}} \right| \ge \frac{q-2}{6\sqrt{\mathbf{D}\varsigma}} \right\} = 2\Phi\left(-\frac{q-2}{6\sqrt{\mathbf{D}\varsigma}} \right). \qquad (2.19)$$

Безпосередньо з формул (2.18), (2.19) випливає верхня оцінка (2.14).

Нижня оцінка (2.14) доводиться аналогічно, виходячи з нерівностей

$$p(i,F,g) = \mathbf{P}\{|\,m_i + 3(mF)_i + 3(rg)_i\,| \ge q/2\} \ge \mathbf{P}\{3\,|\,(mF)_i + (rg)_i\,| - 1 \ge q/2\} =$$

$$= \mathbf{P}\{|\,(mF)_i + (rg)_i\,| \ge (q+2)/6\} = \mathbf{P}\left\{ \left| \sum_{j=0}^{n-1} F_j m_{i-j} + \sum_{j=0}^{n-1} g_j r_{i-j} \right| \ge (q+2)/6 \right\}.$$

Далі, формула (2.15) випливає з верхньої оцінки (2.14) та нерівності

$$p_{er}(F,g) \le n \cdot \max_{0 \le i \le n-1} p(i,F,g)\,, \qquad (2.20)$$

яка є наслідком співвідношення (2.9).

Для доведення формули (2.16) скористаємося нерівністю Гефдінга [4]: якщо $\zeta_1, \ldots, \zeta_m$ є незалежними випадковими величинами такими, що $\alpha_i \le \zeta_i \le \beta_i$, де $\alpha_i, \beta_i \in \mathbf{R}$, $i \in \overline{1,m}$, то для будь-якого $u > 0$ має місце нерівність

$$\mathbf{P}\left\{\left|\sum_{i=1}^{m}(\xi_i - \mathbf{E}\xi_i)\right| \ge mu\right\} \le 2\exp\left\{-\frac{2m^2u^2}{\sum\limits_{i=1}^{m}(\beta_i - \alpha_i)^2}\right\}. \qquad (2.21)$$

Застосовуючи оцінку (2.21) до $m = 2d + 2d' + 1$ випадкових величин у правій частині нерівності (2.18), на підставі формули (2.20) отримаємо, що

$$p_{er}(F,g) \le n \cdot \max_{0 \le i \le n-1} p(i,F,g) \le 2n\exp\left\{-\frac{(q-2)^2}{72(2d+2d'+1)}\right\}.$$

Таким чином, твердження повністю доведено.

В табл. 2.3 для низки пар (n, d), перші п’ять з яких рекомендовано в [3], а дві останні – в [8], наведені значення $-\log_2 p$, де p визначається за однією з формул (2.13) – (2.17); при цьому $q = 2048$, $d' = \lfloor n/3 \rfloor$.

Таблиця 2.3 – Результати оцінювання параметрів, що характеризують частоту виникнення помилок розшифрування у шифросистемі NTRUEncrypt

(n, d)	Нижня оцінка (2.14)	Верхня оцінка (2.14)	Оцінка (2.15)	Оцінка (2.16)	Оцінка (2.13)
(401, 113)	284,26	283,15	274,51	160,49	414,33
(449, 134)	240,31	239,36	230,55	138,12	348,49
(677, 157)	205,59	204,82	195,42	99,24	296,03
(1087, 120)	267,69	266,64	256,55	75,84	388,05
(1171, 106)	302,52	301,35	291,15	73,28	439,97

(443, 143)	225,40	224,54	215,75	134,58	326,28
(743, 247)	131,96	131,45	121,92	74,28	185,96

Як видно з табл. 2.3, значення верхньої та нижньої оцінок (2.14) практично співпадають за порядком величини. При цьому значення верхньої оцінки (2.16) є суттєво більше в порівнянні зі значеннями (наближеної) верхньої оцінки (2.15). Наприклад, при $(n,d)=(401,113)$ ймовірність події, яка полягає в тому, що (для фіксованого $i \in \overline{0,n-1}$) модуль i-го коефіцієнту випадкового полінома $mf+3rg$ є не менше ніж $q/2$, знаходиться в межах від $2^{-284,26}$ до $2^{-283,15}$, а ймовірність помилкового розшифрування повідомлення при будь-якому фіксованому ключі (F,g) не перевищує $2^{-160,49}$. Проте за умови справедливості рівності (2.19) можна стверджувати, що ця ймовірність не перевищує $2^{-274,51}$.

В табл. 2.4, 2.5 показано, як змінюються значення отриманих оцінок з ростом параметра d при фіксованих q і n.

Таблиця 2.4 – Значення верхніх меж ймовірності помилкового розшифрування у шифросистемі NTRUEncrypt при $q=2048, n=443$

d	86	90	100	105	110	120	130	140	147
Оцінка (2.15)	361,99	345,69	310,65	295,62	281,97	258,06	237,83	220,48	209,74
Оцінка (2.16)	169,82	166,80	159,66	156,31	153,08	146,99	141,34	136,09	132,62

Таблиця 2.5 – Значення верхніх меж ймовірності помилкового розшифрування у ш'ифросистемі NTRUEncrypt при $q=2048, n=743$

d	86	100	120	145	165	190	210	230	247
Оцінка (2.15)	361,16	309,83	257,26	211,91	185,52	160,32	144,48	131,38	121,92
Оцінка (2.16)	115,22	110,15	103,58	96,315	91,13	85,32	81,13	77,29	74,27

Зауважимо, що на сьогодні вважається прийнятним такий вибір параметрів шифросистеми NTRUEncrypt, для яких ймовірність помилкового розшифрування $p_{er} = \mathbf{P}_{F,g,m,r}\{D_f(E_h(m,r)) \neq m\}$ не перевищує 2^{-80} (див., наприклад, [9], с. 13). Отримані результати показують, що параметри, рекомендовані в [3, 8], задовольняють навіть більш жорсткому критерію, згідно з яким ймовірність $p_{er}(F,g) = \mathbf{P}_{m,r}\{D_f(E_h(m,r)) \neq m\}$ обмежена зверху величиною такого ж порядку для будь-якого фіксованого ключа (F,g).

2.3. Досяжна верхня межа sup-норми добутку елементів кільця зрізаних поліномів та її застосування до аналізу ймовірності помилкового розшифрування повідомлень в NTRU-подібних шифросистемах

Нехай $f(x) = x^n - c_{n-1}x^{n-1} - \cdots - c_0$ – унітарний поліном степеня $n > 1$ над полем $\mathbf{R}$ дійсних чисел. Позначимо $R_f = \mathbf{R}[x]/(f(x))$ кільце зрізаних поліномів, яке складається з усіх дійсних поліномів степеня не вище $n-1$ з операціями додавання та множення за модулем $f(x)$. Як і вище, ототожнимо довільний поліном $a(x) = a_0 + a_1x + \cdots + a_{n-1}x^{n-1} \in R_f$ з вектором його коефіцієнтів $a = (a_0, a_1, ..., a_{n-1})$. Поліном, що дорівнює добутку елементів $a(x), b(x) \in R_f$ в кільці R_f, позначимо символом $a(x) \cdot^f b(x)$, а вектор коефіцієнтів цього полінома – символом $a \cdot^f b$. Нарешті, визначимо sup-норму та l_1-норму полінома $a(x) \in R_f$ (вектора a), вважаючи $\| a \|_\infty = \max\limits_{0 \le i \le n-1} | a_i |$ і $\| a \|_1 = | a_0 | + \cdots + | a_{n-1} |$ відповідно.

В розділі 1 зазначено, що кільця вигляду R_f широко використовуються при побудові криптосистем, які базуються на решітках, зокрема, NTRU-подібних. При цьому питання про коректність роботи таких криптосистем (а

саме, малість імовірності помилкового розшифрування повідомлень законним одержувачем) приводить до задачі знаходження верхніх оцінок sup-норми полінома $a(x) \cdot^f b(x)$ в термінах норм поліномів-співмножників. Вирішенню цієї задачі присвячена робота [5], де введено параметр, що дорівнює найменшому числу $\theta(f)$ з властивістю

$$\forall a(x) \in R_f : \max_{0 \le i \le n-1} \| a(x) \cdot^f x^i \|_\infty \le \theta(f) \| a \|_\infty \tag{2.25}$$

і показано, що

$$\| a(x) \cdot^f b(x) \|_\infty \le n\theta(f) \| a \|_\infty \| b \|_\infty, \; a(x), b(x) \in R_f . \tag{2.26}$$

В [5] отримано також верхню межу $\theta(f) \le \max_{0 \le i,j \le n-1} \| x^i \cdot^f x^j \|_\infty$ і знайдено точні значення параметра $\theta(f)$ для поліномів $f(x) = x^n - 1$, $f(x) = x^n + 1$ та $f(x) = x^n + x^{n-1} + \cdots + 1$. Разом з тим, є відкритим питання про існування алгоритму, який дозволяє обчислювати значення $\theta(f)$ для будь-якого унітарного полінома $f(x)$.

Один з основних наукових результатів цього підрозділу полягає в тому, що $\theta(f)$ співпадає з нормою білінійного відображення $(a, b) \mapsto a \cdot^f b$, яке задано на добутку нормованих векторних просторів $(\mathbf{R}^n, \| \cdot \|_\infty) \times (\mathbf{R}^n, \| \cdot \|_1)$ та приймає значення в нормованому векторному просторі $(\mathbf{R}^n, \| \cdot \|_\infty)$. Це дозволяє запропонувати алгоритм обчислення значення $\theta(f)$ для будь-якого заздалегідь визначеного унітарного полінома $f(x)$ степеня n за $O(n^2)$ операцій над n-вимірними векторами, а також отримати більш точну в порівнянні з (2.26) (досяжну) верхню межу: $\| a(x) \cdot^f b(x) \|_\infty \le \theta(f) \| a \|_\infty \| b \|_1$,

$a(x), b(x) \in R_f$. Крім того, отримано підсилення леми 2.11 з [5], яка стверджує, що якщо $b(x)$ – випадковий поліном з R_f із незалежними коефіцієнтами, що розподілені в інтервалі $[-B, B]$ за довільним законом з математичним сподіванням 0, то для будь-якого $a(x) \in R_f$ справедлива нерівність

$$\mathbf{P}(\| a \cdot^f b \|_\infty \geq \theta(f) B \| a \|_\infty \sqrt{n} \log n) \leq 4ne^{-\frac{\log^2 n}{8}}. \qquad (2.27)$$

Отримана нижче нова оцінка стверджує, що ймовірність у лівій частині нерівності (2.27) обмежена зверху значенням $2ne^{-\frac{\log^2 n}{2}}$. Нарешті, розглянуто застосування отриманих результатів до оцінювання ймовірності помилкового розшифрування повідомлень в NTRU-подібних шифросистемах.

Наведемо явний вираз та алгоритм обчислення параметра $\theta(f)$.

Нехай E_1, E_2 та E_3 – нормовані векторні простори з нормами $\|\cdot\|'$, $\|\cdot\|''$ та $\|\cdot\|'''$ відповідно, $B : E_1 \times E_2 \to E_3$ – білінійне відображення. Згідно із відомим означенням (див., наприклад, [10], п. 1.8), норма відображення B визначається як найменше число $\| B \|$ таке, що $\| B(a,b) \|''' \leq \| B \| \| a \|' \| b \|''$ для будь-яких $a \in E_1$, $b \in E_2$.

Розглянемо в ролі B білінійне відображення $B_f(a, b) = a \cdot^f b$, вважаючи $(E_1, \|\cdot\|') = (E_3, \|\cdot\|''') = (\mathbf{R}^n, \|\cdot\|_\infty)$, $(E_2, \|\cdot\|'') = (\mathbf{R}^n, \|\cdot\|_1)$.

Лема 2.1. Справедлива рівність $\theta(f) = \| B_f \|$.

Доведення. З визначення норми випливає, що

$$\| a(x) \cdot^f x^i \|_\infty \leq \| B_f \| \| a(x) \|_\infty \| x^i \|_1 = \| B_f \| \| a(x) \|_\infty, \; a(x) \in R_f, \; 0 \leq i \leq n-1.$$

Отже, згідно з означенням параметра $\theta(f)$ виконується нерівність $\theta(f) \le \| B_f \|$.

Далі, для будь-яких $a(x), b(x) \in R_f$ маємо:

$$\| a(x) \cdot^f b(x) \|_\infty = \left\| \sum_{i=0}^{n-1} b_i (a(x) \cdot^f x^i) \right\|_\infty \le \sum_{i=0}^{n-1} | b_i | \| a(x) \cdot^f x^i \|_\infty \le$$

$$\le \sum_{i=0}^{n-1} | b_i | \theta(f) \| a(x) \|_\infty = \theta(f) \| a(x) \|_\infty \| b(x) \|_1,$$

звідки випливає, що $\| B_f \| \le \theta(f)$. Лему доведено.

Позначимо $S = \begin{pmatrix} 0\,1\,0 \ldots\ 0 \\ 0\,0\,1 \ldots\ 0 \\ \ldots\ \ldots\ \ldots \\ 0\,0\,0 \ldots\ 1 \\ c_0\, c_1 \ldots c_{n-1} \end{pmatrix}$ супровідну матрицю полінома $f(x) = x^n - c_{n-1} x^{n-1} - \cdots - c_0$.

Лема 2.2. Для будь-яких $a(x), b(x) \in R_f$ справедлива рівність $a \cdot^f b = a\, b(S)$. Іншими словами, вектор коефіцієнтів добутку поліномів $a(x)$ та $b(x)$ в кільці R_f дорівнює добутку вектора-рядка a на матрицю $b(S)$.

Доведення. Позначимо e_i вектор коефіцієнтів полінома x^i, $0 \le i \le n-1$.

Перш за все, переконаємося в справедливості рівності

$$e_0 a(S) = a. \qquad (2.28)$$

Дійсно, використовуючи індукцію по i, неважко перевірити, що $e_0 S^i = e_i$, $0 \le i \le n-1$. Отже, $e_0 a(S) = \sum_{i=0}^{n-1} a_i e_0 S^i = \sum_{i=0}^{n-1} a_i e_i = a$, що й треба було довести.

Зауважимо тепер, що оскільки $f(x)$ є мінімальним поліномом матриці S, то відображення $a(x) \mapsto a(S)$ є ізоморфізмом кільця R_f на кільце, яке складається з усіх квадратних матриць вигляду $b(S)$, де $b(x) \in R_f$. При цьому ізоморфізмі поліному $a(x) \cdot^f b(x)$ відповідає матриця $a(S)b(S)$ і на підставі формули (2.28), яка послідовно застосовується до поліномів $a(x) \cdot^f b(x)$ та $a(x)$, справедливі рівності $a \cdot^f b = e_0 a(S)\, b(S) = a\, b(S)$. Лему доведено.

Задамо звичайним чином sup-норму дійсної $n \times n$-матриці A, вважаючи $\| A \|_\infty = \max\{\| Ax^T \|_\infty : \| x \|_\infty = 1\}$, де максимум береться за всіма векторами $x = (x_1, ..., x_n) \in \mathbf{R}^n$ такими, що $\| x \|_\infty = 1$. Неважко бачити, що

$$\| A \|_\infty = \max\{\| A_1 \|_1, \| A_2 \|_1, \dots, \| A_n \|_1\}, \tag{2.29}$$

де $A_1, A_2, \dots, A_n$ – рядки матриці A.

Для будь-яких $i, j, k \in \{0, 1, ..., n-1\}$ позначимо $(x^i \cdot^f x^j)_k$ k-й коефіцієнт полінома $x^i \cdot^f x^j$. Розглянемо $n \times n$-матрицю B_k з елементами $B_k(i, j) = (x^i \cdot^f x^j)_k$.

Лема 2.3. Справедлива рівність $\theta(f) = \max\limits_{0 \le k \le n-1} \| B_k \|_\infty$.

Доведення. З означення матриці B_k випливає, що для будь-яких $a(x), b(x) \in R_f$ k-й коефіцієнт полінома $a(x) \cdot^f b(x)$ дорівнює $(a(x) \cdot^f b(x))_k = bB_k a^T$. Отже,

$$|(a(x) \cdot^f b(x))_k| \le \| b \|_1 \| B_k a^T \|_\infty \le \| b \|_1 \| B_k \|_\infty \| a \|_\infty,\ 0 \le k \le n-1$$

і

$$\| a \cdot^f b \|_\infty \le (\max_{0 \le k \le n-1} \| B_k \|_\infty) \| a \|_\infty \| b \|_1. \tag{2.30}$$

Звідси на підставі леми 2.1 випливає, що $\theta(f) \le \max\limits_{0\le k\le n-1} \| B_k \|_\infty$.

Для доведення рівності $\theta(f) = \max\limits_{0\le k\le n-1} \| B_k \|_\infty$ достатньо переконатися в тому, що існує пара поліномів $a(x), b(x) \in R_f$, для яких нерівність (2.30) перетворюється на рівність.

Дійсно, виберемо число $l \in \{0, 1, ..., n-1\}$ і вектор $a \in \mathbf{R}^n$ такі, що $\| B_l \|_\infty = \max\limits_{0\le k\le n-1} \| B_k \|_\infty$, $\| B_l a^T \|_\infty = \| B_l \|_\infty \| a \|_\infty$. Нехай $b = e_i$, де i – номер найбільшої за модулем координати вектора $B_l a^T$. Для зазначених a і b виконуються рівності

$$| (a(x) \cdot^f b(x))_l | = | bB_l a^T | = \| B_l a^T \|_\infty = \| B_l \|_\infty \| a \|_\infty = \| B_l \|_\infty \| a \|_\infty \| b \|_1 .$$

При цьому за доведеним для будь-якого $0 \le k \le n-1$ мають місце нерівності

$$| (a(x) \cdot^f b(x))_k | \le \| B_k \|_\infty \| a \|_\infty \| b \|_1 \le \| B_l \|_\infty \| a \|_\infty \| b \|_1 .$$

Отже, $\| a \cdot^f b \|_\infty = \max\limits_{0\le k\le n-1} | (a(x) \cdot^f b(x))_k | = \| B_l \|_\infty \| a \|_\infty \| b \|_1$ і нерівність (2.30) перетворюється на рівність.

Лему доведено.

Спираючись на лему 2.3 і формулу (2.29), можна запропонувати наступний алгоритм обчислення параметра $\theta(f)$.

Алгоритм 2.1.

Вхідні дані: поліном $f(x) = x^n - c_{n-1}x^{n-1} - \cdots - c_0$

Для кожного $k = 0, 1, ..., n-1$:

1) покласти $(x(0), x(1), ..., x(n-1)) = e_k$;

2) обчислити $x(i+n) = c_0 x(i) + \cdots + c_{n-1} x(i+n-1))$ для $i = 0, 1, ..., n-1$;

3) покласти $B_k(i, j) = x(i + j)$, $i, j = 0, 1, ..., n-1$;

4) покласти $\theta_k = \max\limits_{0 \le i \le n-1} \{ | B_k(i,0) | + | B_k(i,1) | + \cdots + | B_k(i,n-1) | \}$.

Покласти $\theta(f) = \max\limits_{0 \le k \le n-1} \theta_k$.

Твердження 2.4. Наведений алгоритм коректно обчислює значення $\theta(f)$ за $O(n^2)$ операцій над n-вимірними векторами. Крім того, $\theta(f)$ дорівнює найбільшому елементу матриці $U = \sum\limits_{j=0}^{n-1} \mathrm{abs}(S^j)$, де $\mathrm{abs}(S^j)$ – матриця, яка складається з модулів елементів матриці S^j, $0 \le j \le n-1$.

Доведення. Перша частина твердження випливає безпосередньо з леми 2.3 і формули (2.29), застосованої до матриці $A = B_k$ при $k = 0, 1, ..., n-1$.

Для доведення другої частини твердження зауважимо, що на підставі леми 2.2 (i,j)-й елемент матриці B_k дорівнює $(x^i \cdot^f x^j)_k = e_i S^j e_k^T$, $i, j, k \in \{0, 1, ..., n-1\}$. Тому l_1-норма i-го рядка матриці B_k дорівнює значенню $\sum\limits_{j=0}^{n-1} | e_i S^j e_k^T | = \sum\limits_{j=0}^{n-1} e_i \mathrm{abs}(S^j) e_k^T$, яке співпадає з (i,k)-м елементом матриці U. Для завершення доведення залишається застосувати лему 2.3 і формулу (2.29).

Твердження доведено.

Нижче, у табл. 2.6 – 2.9 наведено результати застосування алгоритму 2.1 до низки трьохчленів з коефіцієнтами ± 1. Зауважимо, що окремі з таких трьохчленів (наприклад, $f(x) = x^n - x^{n/2} + 1$ та $f(x) = x^n - x - 1$ для певних значень n) використовуються в сучасних NTRU-подібних криптосистемах [11 – 13] і характеризуються малим значенням $\theta(f) = 2$.

Таблиця 2.6 – Значення параметра $\theta(f)$ для поліномів $f(x) = x^n + x^k + 1$ при $n = 100$

Значення k	Параметр $\theta(f)$	Значення k	Параметр $\theta(f)$
1, 50	2	91	12

$2 \div 49$	3	92	14
$51 \div 67, 75$	4	93	16
$68 \div 74$	5	94	18
$76 \div 80$	6	95	20
$81 \div 83$	7	96	26
$84 \div 85$	8	97	34
$86 \div 87$	9	98	50
$88 \div 90$	10	99	100

Таблиця 2.7 – Значення параметра $\theta(f)$ для поліномів $f(x) = x^n + x^k - 1$ при $n = 100$

Значення k	Параметр $\theta(f)$	Значення k	Параметр $\theta(f)$
1	2	91	12
$2 \div 50$	3	92	14
$51 \div 67$	4	93	16
$68 \div 75, 80$	5	94	18
$76 \div 79$	6	95	21
$81 \div 83$	7	96	25
$84 \div 85$	8	97	34
$86 \div 87$	9	98	51
$88 \div 89$	10	99	100
90	11		

Таблиця 2.8 – Значення параметра $\theta(f)$ для поліномів $f(x) = x^n - x^k + 1$ при $n = 100$

Значення k	Параметр $\theta(f)$	Значення k	Параметр $\theta(f)$
$1, 50$	2	91	12
$2 \div 49$	3	92	14
$51 \div 67, 75$	4	93	16
$68 \div 74, 80$	5	94	18
$76 \div 79$	6	95	20
$81 \div 83$	7	96	25
$84 \div 85$	8	97	34
$86 \div 87$	9	98	50
$88 \div 90$	10	99	100

Таблиця 2.9 – Значення параметра $\theta(f)$ для поліномів $f(x) = x^n - x^k - 1$ при $n = 100$

Значення k	Параметр $\theta(f)$	Значення k	Параметр $\theta(f)$
1	2	91	12
$2 \div 50$	3	92	14
$51 \div 67$	4	93	16
$68 \div 75$	5	94	18
$76 \div 80$	6	95	21
$81 \div 83$	7	96	26
$84 \div 85$	8	97	34
$86 \div 87$	9	98	51
$88 \div 89$	10	99	100
90	11		

Доведемо зараз наступне твердження, яке підсилює оцінку, наведену в [5], лема 2.11.

Твердження 2.5. Нехай $b(x)$ – випадковий поліном з R_f із незалежними коефіцієнтами, розподіленими в інтервалі $[-B, B]$ за довільним законом із математичним сподіванням 0. Тоді для будь-якого $a(x) \in R_f$ справедлива нерівність

$$\mathbf{P}(\| a \cdot^f b \|_\infty \geq \theta(f) B \| a \|_\infty \sqrt{n} \log n) \leq 2ne^{-\frac{\log^2 n}{2}}. \qquad (2.31)$$

Доведення. Позначимо $c(n) = \theta(f) B \| a \|_\infty \sqrt{n} \log n$. Оцінимо зверху ймовірність $p_k = \mathbf{P}(|(a(x) \cdot^f b(x))_k| \geq c(n))$, $0 \leq k \leq n-1$.

На підставі леми 2.2 справедлива рівність

$$(a(x) \cdot^f b(x))_k = ba(S)e_k^T = \sum_{i=0}^{n-1} b_i m_i \text{, де } b = (b_0, ..., b_{n-1}),\ m_i = e_i a(S) e_k^T,$$

$$0 \leq i \leq n-1.$$

Помітимо, що

$$|m_i| = \left| \sum_{j=0}^{n-1} a_j (e_i S^j e_k^T) \right| \le \sum_{j=0}^{n-1} |a_j| \, \| e_i S^j e_k^T | \le \| a \|_\infty \sum_{j=0}^{n-1} | e_i S^j e_k^T | \le \| a \|_\infty \, \theta(f),$$

де остання нерівність випливає з твердження 2.4.

Таким чином, випадкова величина $(a(x) \cdot^f b(x))_k$ є сумою незалежних випадкових величин $b_i m_i$, розподілених в інтервалі $[-B \| a \|_\infty \theta(f), B \| a \|_\infty \theta(f)]$ із математичним сподіванням 0. Звідси на підставі нерівності Гефдінга [4] випливає, що

$$p_k \le 2 \exp\left\{ - \frac{2c(n)^2}{n(2B \| a \|_\infty \theta(f))^2} \right\} = 2 \exp\left\{ - \frac{\log^2 n}{2} \right\}.$$

Нарешті, формула (2.31) випливає з оцінки $\mathbf{P}(\| a \cdot^f b \|_\infty \ge c(n)) \le n \max\limits_{0 \le k \le n-1} p_k$.

Твердження доведено.

Застосуємо отримані результати до знаходження верхньої межі ймовірності помилкового розшифрування повідомлень в NTRU-подібній шифросистеми над кільцем $R_{f,q} = \mathbf{Z}_q[x]/(f(x))$, де $\mathbf{Z}_q$ – кільце класів лишків за модулем q, а $f(x)$ – унітарний поліном степеня n з цілими коефіцієнтами. Як звичайно, припустимо, що q не ділиться на 3, а елементи кільця $\mathbf{Z}_q$ ототожнюються з цілими числами в інтервалі $[-(q-1)/2, (q-1)/2]$ для непарного q і $[-q/2, q/2-1]$ для парного q.

Секретним ключем NTRU-подібної шифросистеми, що розглядається, є пара поліномів (F, g) таких, що $F, g \in R_{f,q}$, $\| F \|_\infty = \| g \|_\infty = 1$ і поліном $\varphi = 1 + 3F$ є оборотним в кільці $R_{f,q}$, а відповідним відкритим ключем є елемент кільця $R_{f,q}$, що дорівнює $h = 3g\varphi^{-1}$.

Множина відкритих текстів шифросистеми складається з усіх поліномів

$m \in R_{f,q}$ таких, що $\| m \|_\infty = 1$. Для зашифрування відкритого тексту m на відкритому ключі h генерується випадковий поліном $r \in R_{f,q}$ такий, що $\| r \|_\infty = 1$, і обчислюється шифрований текст $E_h(m,r) = (m + rh) \bmod q$. Розшифрування довільного тексту $c \in R_{f,q}$ на секретному ключі (F, g) виконується за формулою $D_\varphi(c) = c\varphi (\bmod q) \bmod 3$. Якщо при цьому $D_\varphi(E_h(m,r)) \neq m$, то відбувається помилка розшифрування.

Твердження 2.6. Нехай $F, g \in R_{f,q}$, $\| F \|_\infty = \| g \|_\infty = 1$, поліном $\varphi = 1 + 3F$ є оборотним в кільці $R_{f,q}$ і $h = 3g\varphi^{-1}$. Нехай, далі, m та r є випадковими поліномами із $R_{f,q}$ з незалежними в сукупності коефіцієнтами, розподіленими на множині $\{-1, 0, 1\}$ за довільним законом з математичним сподіванням 0. Тоді справедлива нерівність

$$\mathbf{P}(D_\varphi(E_h(m,r)) \neq m) \leq 2n \exp\left\{ - \frac{(q-2)^2}{144\, n\, \theta(f)^2} \right\}. \qquad (2.32)$$

Доведення. З наведених вище означень випливає, що у випадку помилки розшифрування модуль принаймні одного з коефіцієнтів полінома $m\varphi + 3rg \in \mathbf{Z}[x]$ є не менше ніж $q/2$. Отже, справедливі співвідношення

$$D_\varphi(E_h(m,r)) \neq m \;\Rightarrow \| m(1+3F) + 3rg \|_\infty \geq q/2 \Rightarrow \| mF + rg \|_\infty \geq (q-2)/6.$$

Для будь-якого $k \in \overline{0, n-1}$ позначимо $p_k(F,g)$ ймовірність того, що модуль k-го коефіцієнта випадкового полінома $mF + rg$ є більше або дорівнює $q/2$. Повторюючи міркування, наведені в доведенні твердження 2.5, з урахуванням рівностей $\| F \|_\infty = \| g \|_\infty = 1$, $\| m \|_\infty = \| r \|_\infty = 1$ отримаємо, що k-й коефіцієнт кожного з поліномів mF і rg є сумою не більше ніж n

незалежних випадкових величин, розподілених в інтервалі $[-\theta(f), \theta(f)]$, математичне сподівання кожної з яких дорівнює 0. Звідси на підставі нерівності Гефдінга випливає, що $p_k(F,g) \le 2\exp\left\{-\dfrac{(q-2)^2}{144\,n\,\theta(f)^2}\right\}$. Нарешті, формула (2.32) випливає з оцінки $\mathbf{P}(D_\varphi(E_h(m,r)) \ne m) \le n \max\limits_{0\le k\le n-1} p_k(F,g)$.

Твердження доведено.

У табл. 2.10 наведено результати розрахунків, отримані за допомогою алгоритму 2.1 та формули (2.32), для низки значень параметрів, що використовуються у деяких сучасних NTRU-подібних криптосистемах [11, 13].

Таблиця 2.10 – Верхні межі ймовірності помилкового розшифрування повідомлень в NTRU-подібних криптосистемах

Криптосистема	n	q	$f(x)$	$\theta(f)$	Верхня оцінка (2.32)
NTRUEncrypt	443	2048	$x^n - 1$	1	$2^{-84,88}$
Falcon	512	12289	$x^n + 1$	1	$2^{-2944,16}$
Falcon	768	18433	$x^n - x^{n/2} + 1$	2	$2^{-1097,28}$
NNTRU	768	7681	$x^n - x^{n/2} + 1$	2	$2^{-181,72}$
SNTRUPrime	761	4591	$x^n - x - 1$	2	$2^{-58,74}$

Відзначимо, що ці результати мають місце при дуже слабких (зазначених у твердженні 2.6) припущеннях щодо поліномів F, g, m і r. Разом з тим, у багатьох випадках вони дозволяють отримати змістовну інформацію про величину ймовірності помилкового розшифрування повідомлень при будь-якому фіксованому секретному ключі.

Висновки

1. Першим науковим результатом, представленим у розділі, є

аналітичні співвідношення для оцінювання ймовірності оборотності випадкових поліномів, які використовуються в NTRU-подібних шифросистемах. Зазначені співвідношення отримано вперше. 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. Ці співвідношення можуть бути використані також для вибору параметрів n, q і θ зазначених шифросистем (див. твердження 2.1, 2.2).

2. Вибір в якості q великого простого числа є доцільнішим (за критерієм высокої ймовірності оборотності полінома) в порівнянні з розповсюдженим варіантом $q = 2^l$. Так, в останньому випадку ймовірність $\pi_{n,q}$ практично не відрізняється від $0{,}5$ при всіх розумних, з практичної точки зору, значеннях n і θ (іншими словами, в середньому кожен другий випадково згенерований за наведеним законом поліном є необоротним). В той же час, у першому випадку ймовірність $\pi_{n,q}$ швидко зменшується з ростом q при фіксованих n і θ, обертаючись в нуль при $q > 3n+1$. При цьому ймовірність необоротності випадкового полінома не перевищує $1{,}5 \cdot 10^{-2}$, що суттєво менше $0{,}5$ (див. рис. 2.1, 2.2 і табл. 2.1, 2.2).

3. Другим науковим результатом, викладеним в цьому розділі, є аналітичні співвідношення для оцінювання ймовірності помилкового розшифрування повідомлень в NTRU-подібних шифросистемах при фіксованому секретному ключі.

Для шифросистеми NTRUEncrypt отримані аналітичні співвідношення вдосконалюють раніше відомі [3, 8, 14], надаючи більш адекватну інформацію про частоту виникнення помилок при розшифруванні. При цьому результати чисельних розрахунків (табл. 2.4, 2.5) показують, що

параметри шифросистеми NTRUEncrypt, рекомендовані в [3, 8], задовольняють більш жорсткому критерію малості ймовірності помилкового розшифрування для будь-якого фіксованого секретного ключа (а не тільки критерію малості середнього значення цієї ймовірності за всіма секретними ключами).

4. Результати, отримані для шифросистеми NTRUEncrypt, узагальнено на випадок довільних NTRU-подібних шифросистем (див. твердження 2.6). Науковою основою для цього узагальнення є твердження 2.4, яке надає змогу обчислювати на практиці значення параметра $\theta(f)$, що характеризує величину sup-норми добутку елементів кільця зрізаних поліномів за модулем заданого унітарного полінома $f(x)$ з дійсними коефіцієнтами. Вперше розроблено алгоритм обчислення цього параметра, який базується на його інтерпретації як норми деякого білінійного відображення на добутку певних нормованих векторних просторів. Це надає змогу отримати більш точну порівняно з відомою [5] верхню межу sup-норми добутку елементів кільця R_f, підсилити лему 2.11 з [5], а також встановити оцінки ймовірності помилкового розшифрування повідомлень в NTRU-подібних шифросистемах над кільцем R_f при фіксованому ключі.

Список використаних джерел у другому розділі

1. Valluri M. R. NTRUCipher-lattice based secret key encryption. 2017. DOI: https://doi.org/10.48550/arXiv.1710.01928.

2. American National Standard X9.98-2010. Lattice-based polynomial public key encryption algorithm, Part 1: key establishment, Part 2: data encryption. Official edition. 2010.

3. Choosing NTRUEncrypt Parameters in Light of Combined Lattice Reduction and MITM Approaches / P. S. Hirschhorn et al. *Applied Cryptography and Network Security*. Berlin, Heidelberg, 2009. P. 437–455. DOI: https://doi.org/10.1007/978-3-642-01957-9_27.

4. Hoeffding W. Probability Inequalities for Sums of Bounded Random Variables. *Journal of the American Statistical Association*. 1963. Vol. 58, no. 301. P. 13–30. DOI: https://doi.org/10.1080/01621459.1963.10500830.

5. Lyubashevsky V., Towards Practical Lattice-Based Cryptography, Ph.D. Theses, Univ. of California, San Diego. 2008.

6. Лидл Р., Нидеррайтер Г. Конечные поля: В 2-х т. Т. 2 : монографія. Москва : Мир, 1988. 818 с.

7. Babai L. The Fourier transform and equations over finite abelian groups. 2002. URL: https://people.cs.uchicago.edu/~laci/reu02/fourier.pdf (дата звернення: 05.05.2023).

8. NIST PQ Submission: NTRUEncrypt. A lattice based algorithm / Z. Zhang et al. *NIST Computer Security Resource Center | CSRC*. URL: https://csrc.nist.gov/Projects/post-quantum-cryptography/post-quantum-cryptography-standardization/round-1-submissions (дата звернення: 02.05.2023).

9. NTRU Prime: Reducing Attack Surface at Low Cost / D. J. Bernstein et al. *Selected Areas in Cryptography – SAC 2017*. Cham, 2017. P. 235–260. DOI: https://doi.org/10.1007/978-3-319-72565-9_12.

10. Картан А. Дифференциальное исчисление. Дифференциальные формы. Москва : Мир, 1971. 392 с.

11. Estimate All the {LWE, NTRU} Schemes! / M. R. Albrecht et al. *Lecture Notes in Computer Science*. Cham, 2018. P. 351–367. DOI: https://doi.org/10.1007/978-3-319-98113-0_19.

12. NTRU-LPR IND-CPA: A New Ideal Lattices-based Scheme / S. Diop et al. *Cryptology ePrint Archive*. URL: https://eprint.iacr.org/2018/109 (дата звернення: 05.05.2023).

13. Lyubashevsky V., Seiler G. NTTRU: Truly Fast NTRU Using NTT. *IACR Transactions on Cryptographic Hardware and Embedded Systems*. 2019. P. 180–201. DOI: https://doi.org/10.46586/tches.v2019.i3.180-201.

14. Choosing Parameters for NTRUEncrypt / J. Hoffstein et al. *Topics in Cryptology – CT-RSA 2017*. Cham, 2017. P. 3–18. DOI: https://doi.org/10.1007/978-3-319-52153-4_1.

РОЗДІЛ 3

АНАЛІТИЧНІ ОЦІНКИ СКЛАДНОСТІ СТАТИСТИЧНИХ АТАК НА ШИФРОСИСТЕМИ NTRUCIPHER ТА NTRUCIPHER+

В першому розділі відзначено актуальність задачі створення обґрунтовано стійких симетричних NTRU-подібних шифросистем. Єдиною такою шифросистемою, відомою на сьогодні, є NTRUCipher [1]. Зауважимо, що в зазначеній публікації проаналізовано стійкість цієї шифросистеми відносно окремих атак, проте деякі інші можливі атаки не розглянуто.

Даний розділ присвячено дослідженню стійкості шифросистеми NTRUCipher, а також її природного узагальнення – NTRUCipher+, відносно двох статистичних атак: BKW-атаки та певної розрізнювальної атаки. (Зауважимо, що введення до розгляду шифросистеми NTRUCipher+ пов’язано з необхідністю підсилити оригінальну шифросистему NTRUCipher, яка не є семантично стійкою, як і її асиметричний аналог – алгоритм NTRUEncrypt; див., наприклад, [2]).

У п. 3.1 наведено означення шифросистеми NTRUCipher+ та (з використанням результатів підрозділу 2.2) отримано аналітичні співвідношення для ймовірності безпомилкового розшифрування шифрованих повідомлень у цій шифросистемі.

У п. 3.2 отримано аналітичні оцінки складності BKW-атаки на шифросистеми NTRUCipher та NTRUCipher+. Сутність цієї атаки полягає у складанні певної системи лінійних рівнянь зі спотвореними правими частинами над скінченним полем простого порядку та у розв’язанні цієї системи рівнянь за допомогою узагальненого алгоритму BKW [3, 4]. Зауважимо, що ця атака є можливою саме для симетричних NTRU-подібних шифросистем, проте вона не розглядається у доступних публікаціях. Отримано аналітичні (нижню та верхню) оцінки складності BKW-атаки на

NTRUCipher та NTRUCipher+ відповідно, що надає змогу порівняти ці шифросистеми за стійкістю та практичністю. Декілька несподіваним виявляється кінцевий висновок про недоцільність використання NTRUCipher+ для підвищення стійкості шифросистеми NTRUCipher відносно BKW-атаки.

У п. 3.3 наведено швидку розрізнювальну атаку на шифросистему NTRUCipher+ над кільцем зрізаних поліномів за модулем полінома $x^n - 1$ та (для окремого випадку) ще більш швидку модифікацію цієї атаки. Отримано аналітичні оцінки трудомісткості наведеної атаки та її модифікації. Показано, що шифросистема NTRUCipher+ над зазначеним кільцем є вразливою до наведеної атаки, яка може бути реалізована в режимі реального часу, хоча й не дозволяє відновлювати ключі шифросистеми, а тільки відрізняти послідовність її шифрованих повідомлень від суто випадкової послідовності.

3.1. Означення та первісні властивості шифросистеми NTRUCipher+

Нехай n і q – різні прості числа, $n, q > 3$, причому q є примітивним елементом за модулем n (тобто найменше натуральне l таке, що $q^l \equiv 1 \bmod n$, дорівнює $n-1$). Як і вище, позначимо $\mathbf{Z}_q$ кільце класів лишків за модулем q, елементи якого ототожнимо з цілими числами, що належать інтервалу $[-(q-1)/2, (q-1)/2]$. Позначимо $R_{n,q} = \mathbf{Z}_q[x]/(x^n - 1)$ кільце зрізаних поліномів степеня не вище $n-1$ над кільцем $\mathbf{Z}_q$. Нагадаємо, що це кільце складається з q^n поліномів вигляду $u = u_0 + u_1 x + \cdots + u_{n-1} x^{n-1}$, де $u_i \in \mathbf{Z}_q$, $i \in \overline{0, n-1}$, які додаються та перемножуються за модулем полінома $x^n - 1$. Позначимо $R_{n,q}^*$ групу оборотних елементів кільця $R_{n,q}$.

Для будь-якого $u = u_0 + u_1 x + \cdots + u_{n-1} x^{n-1} \in \mathbf{Z}[x]$ позначимо $u \bmod q$

поліном $(u_0 \bmod q) + (u_1 \bmod q)x + \cdots + (u_{n-1} \bmod q)x^{n-1} \in R_{n,q}$. Аналогічний сенс має позначення $u \bmod 3$.

Позначимо також $\| u \|_\infty = \max\limits_{0 \le i \le n-1} | u_i |$, $\| u \|_1 = \sum\limits_{i=0}^{n-1} | u_i |$. Поліном u називається малим, якщо $\| u \|_\infty = 1$.

Позначимо символом S множину всіх малих поліномів степеня не вище $n-1$, а символом S_d множину всіх поліномів $u \in S$, серед коефіцієнтів яких є точно d, що дорівнюють 1, та точно d, що дорівнюють -1, $1 \le d \le n-2$.

Для зазначених вище чисел n, q і d *шифросистема NTRUCipher+ визначається таким чином*.

Секретними ключами цієї шифросистеми є довільні поліноми $F \in S_d$, а відкритими повідомленнями – довільні малі поліноми. Зауважимо, що на підставі результатів підрозділу 2.1 виконується умова $f \overset{\text{def}}{=} 1 + 3F \in R_{n,q}^*$.

Для зашифрування повідомлення $m \in S$ на ключі F генеруються незалежні випадкові поліноми r та $e = e_0 + e_1 x + \cdots + e_{n-1} x^{n-1}$, де r має рівномірний розподіл ймовірностей на множині S_d, а $e_0, e_1, \ldots, e_{n-1}$ є незалежними випадковими величинами, які приймають значення $0, 1, -1$ з імовірністю $1/3$. Далі обчислюється шифроване повідомлення

$$E_f(m, r, e) = (m + 3(rf^{-1} + e)) \bmod q, \tag{3.1}$$

де f^{-1} – обернений до f елемент кільця $R_{n,q}$.

Розшифрування довільного повідомлення $c \in R_{n,q}$ на ключі F здійснюється за формулою

$$D_f(c) = cf \,(\bmod q) \bmod 3, \tag{3.2}$$

де $f = 1 + 3F$.

З наведених означень випливає, що $D_f(E_f(m,r,e)) = m$, якщо $\| mf + 3(r + ef) \|_\infty < q/2$. При цьому, оскільки $\| F \|_1 = 2d$, $\| e \|_\infty = \| r \|_\infty = 1$, то

$$\| mf + 3(r + ef) \|_\infty = \| m + 3(mF + r + e + 3eF) \|_\infty \le$$

$$\le 1 + 3(\| m \|_\infty \| F \|_1 + \| r \|_\infty + \| e \|_\infty + 3 \| e \|_\infty \| F \|_1) = 7 + 24d .$$

Таким чином, за умови

$$d < (q - 14)/48 \tag{3.3}$$

розшифрування отриманих повідомлень відбувається коректно.

Зауважимо, що головною відмінністю шифросистеми NTRUCipher+ від NTRUCipher [1] є використання додаткового випадкового полінома e при зашифруванні (для NTRUCipher доданок e у формулі (3.1) дорівнює нулю). Використовувати такий доданок в одній з асиметричних версій криптосистеми NTRU запропоновано в [2] для забезпечення семантичної стійкості криптосистеми.

Базуючись на результатах підрозділу 2.2, отримаємо верхню оцінку ймовірності $p_{er}(F) = \mathbf{P}_{m,r,e}\{D_f(E_f(m,r,e)) \ne m\}$ за умови, що поліном F є фіксованим, а поліноми m, r і e вибираються випадково та незалежно один від одного, причому m має рівномірний розподіл ймовірностей на множині S, а r і e – розподіли, зазначені вище.

Твердження 3.1. Справедлива нерівність

$$p_{er}(F) \le 2n \exp\left\{ - \frac{(q-8)^2}{72(20d+1)} \right\}. \tag{3.4}$$

Доведення. Скористаємося міркуваннями, які використовуються для доведення формули (2.16). Для будь-якого $i \in \overline{0,n-1}$ позначимо $p(i,F)$ ймовірність того, що модуль i-го коефіцієнту випадкового полінома $mf + 3(r + ef) = m + 3(mF + r + e + 3eF)$ є не менше ніж $q/2$.

На підставі наведених означень

$$p(i,F) = \mathbf{P}\{|\, m_i + 3(mF)_i + 3r_i + 3e_i + 9(eF)_i \,| \geq q/2\} \leq$$

$$\leq \mathbf{P}\{4 + |\, 3(mF)_i + 3r_i + 9(eF)_i \,| \geq q/2\} =$$

$$= \mathbf{P}\left\{\left| r_i + \sum_{j=0}^{n-1} F_j m_{i-j} + 3\sum_{j=0}^{n-1} F_j e_{i-j} \right| \geq (q-8)/6 \right\}. \qquad (3.5)$$

Позначимо

$$I' = \{j \in \overline{0,n-1} : F_j = 1\},\ I'' = \{j \in \overline{0,n-1} : F_j = -1\}.$$

На підставі формули (3.5) справедливі такі співвідношення:

$$p(i,F) \leq \mathbf{P}\left\{\left| r_i + \sum_{j\in I'} m_{i-j} - \sum_{j\in I''} m_{i-j} + 3\sum_{j\in J'} e_{i-j} - 3\sum_{j\in J''} e_{i-j} \right| \geq (q-8)/6 \right\} =$$

$$= \mathbf{P}\left\{\left| r_i + \sum_{k=1}^{2d} \xi_k + 3\sum_{l=1}^{2d} \eta_l \right| \geq (q-8)/6 \right\}, \qquad (3.6)$$

де r_i, ξ_k, η_l є незалежними випадковими величинами, розподіленими за законами

$$\mathbf{P}(r_i = 1) = \mathbf{P}(r_i = -1) = dn^{-1},\ \mathbf{P}(r_i = 0) = 1 - 2dn^{-1},$$

$$\mathbf{P}(\xi_k = 1) = \mathbf{P}(\xi_k = -1) = \mathbf{P}(\xi_k = 0) = 1/3,\ k \in \overline{1,2d},$$
$$\mathbf{P}(\eta_l = 1) = \mathbf{P}(\eta_l = -1) = \mathbf{P}(\eta_l = 0) = 1/3,\ l \in \overline{1,2d}.$$

Застосовуючи до виразу у правій частині формули (3.6) нерівність Гефдінга [5], отримаємо, що

$$p(i,F) \le 2\exp\left\{-\frac{2\left(\frac{q-8}{6}\right)^2}{4(2d+1)+36\cdot 2d}\right\} = 2\exp\left\{-\frac{(q-8)^2}{72(20d+1)}\right\}.$$

Звідси на підставі нерівності $p_{er}(F) \le n \cdot \max\limits_{0\le i\le n-1} p(i,F)$ випливає формула (3.4). Твердження доведено.

Зауважимо, що у випадку $e = 0$ має місце оцінка ймовірності помилкового розшифрування повідомлень, аналогічна формулі (3.4).

Наслідок 3.1. Припустимо, що у формулі (3.1) $e = 0$. Тоді за умови твердження 3.1 справедлива нерівність

$$p_{er}(F) \le 2n\exp\left\{-\frac{(q-8)^2}{72(2d+1)}\right\}. \tag{3.7}$$

Крім того, за умови

$$d < (q-8)/12 \tag{3.8}$$

виконується рівність $p_{er}(F) = 0$, тобто розшифрування отриманих повідомлень відбувається коректно.

В табл. 3.1 для низки пар (n,d), перші п’ять з яких рекомендовано в [6], а дві останні – в [7], наведені верхні оцінки значень $-\log_2 p_{er}(F)$ для шифросистем NTRUCipher та NTRUCipher+; при цьому q змінюється в межах $1500 < q < 3000$ та $4500 < q < 10000$ відповідно. Символом * у таблиці позначені числа q, для яких при зазначених n і d виконується рівність $p_{er}(F) = 0$ (згідно з формулами (3.3) та (3.8) для шифросистем NTRUCipher+ та NTRUCipher відповідно).

Таблиця 3.1 – Результати оцінювання помилки розшифрування у криптосистемах NTRUCipher та NTRUCipher+

(n,d)	q	$-\log p_{er}(F)$ (формула (3.4), NTRUCipher+)	q	$-\log p_{er}(F)$ (формула (3.7), NTRUCipher)
(401,113)	4871	199,93	1543*	198,34
	5237	232,67	1663*	232,13
	5701*	277,58	1811*	277,30
	6763*	394,73	2141*	391,96
	7499*	487,66	2383*	488,25
	8161*	579,44	2591*	579,28
	8681*	656,98	2573*	655,47
	9439*	778,59	2999*	780,03
(449,134)	4877	167,37	1553	167,99
	5701	232,42	1811*	232,34
	6577*	312,69	2087*	312,15
	7681*	430,21	2437*	429,68
	8167*	487,72	2591*	487,17
	8837*	572,79	2803*	572,09
	9463*	658,33	3001*	657,46
(677,157)	4831	137,99	1531	137,14
	5867	208,59	1861	208,01
	6703	275,54	2129*	275,75
	7417	339,78	2375*	340,59
	8059*	403,09	2557*	402,90
	8677*	469,01	2753*	468,91
	9461*	559,65	2999*	558,67
(1091,120)	4831	183,03	1543*	184,81
	5867*	275,39	1861*	274,39
	6659*	358,08	2113*	357,32
	7537*	461,98	2393*	461,84
	8237*	554,03	2617*	554,85
	8779*	630,93	2789*	631,93

	9439*	731,18	2999*	732,71
(1171,106)	4871	212,22	1549*	212,19
	5927*	319,78	1879*	318,12
	6733*	416,06	2137*	415,20
	7561*	527,75	2399*	526,61
	8243*	629,47	2617*	629,15
	8807*	720,23	2801*	722,65
	9241*	794,16	2939*	796,96
(443,143)	4861	155,16	1543	154,71
	5981	240,08	1901*	240,39
	6781	311,49	2153*	311,44
	7681*	402,55	2437*	402,13
	8387*	481,92	2663*	482,35
	8821*	534,17	2801*	534,84
	9377*	604,98	2971*	603,16
(743,247)	4817	83,25	1531	83,36
	5903	130,39	1877	130,86
	6959	185,40	2207	185,21
	7681	228,22	2437	228,29
	8387	274,18	2663	274,80
	8831	305,15	2801	305,24
	9371	344,98	2969	344,37

Як видно з табл. 3.1, зі збільшенням значення q в NTRUCipher+ у порівнянні з NTRUCipher приблизно втричі верхні межі ймовірності помилкового розшифрування повідомлень у зазначених шифросистемах досягають майже однакових значень. При фіксованих значеннях n, d зі збільшенням q верхня межа ймовірності помилкового розшифрування повідомлень стрімко зменшується і досягає найменшого (з наведених в таблиці) значення 2^{-796} при $(n,d)=(1171,106)$, $q=2939$ для NTRUCipher та $(n,d)=(1171,106)$, $q=9241$ для NTRUCipher+. Крім того, для переважної більшості значень q у табл. 3.1 ймовірність помилкового розшифрування повідомлень фактично дорівнює нулю.

3.2. BKW-атака на шифросистеми NTRUCipher+ та NTRUCipher

Отримаємо аналітичні співвідношення, що надають змогу оцінювати стійкість шифросистеми NTRUCipher+ відносно атаки, при проведенні якої супротивник зашифровує N разів на тому ж самому (невідомому) ключі F відкрите повідомлення $m = 0$.

В результаті супротивник отримає систему рівнянь над кільцем $R_{n,q}$: $3(r^{(i)} f^{-1} + e^{(i)}) = c^{(i)}$, $i \in \overline{1,N}$, де $c^{(1)}, \ldots, c^{(N)}$ – шифровані повідомлення, $r^{(1)}, \ldots, r^{(N)}$, $e^{(1)}, \ldots, e^{(N)}$ – незалежні випадкові поліноми, що використовуються при зашифруванні (див. формулу (3.1)). Цю систему рівнянь можна записати у вигляді

$$3^{-1} c^{(i)} = -c^{(i)} F + (r^{(i)} + e^{(i)} f),\ i \in \overline{1,N},$$

де 3^{-1} є оберненим до 3 елементом поля $\mathbf{Z}_q$. Позначаючи $c^{(i)} = \sum_{j=0}^{n-1} c_{i,j} x^j$, $e^{(i)} = \sum_{j=0}^{n-1} e_{i,j} x^j$, $r^{(i)} = \sum_{j=0}^{n-1} r_{i,j} x^j$ та прирівнюючи вільні члени поліномів у обох частинах наведеної СР, отримаємо таку систему рівнянь зі спотвореними правими частинами відносно коефіцієнтів $F_0, F_1, \ldots, F_{n-1}$ невідомого полінома F:

$$3^{-1} c_{i,0} = -\sum_{j=0}^{n-1} c_{i,n-j} F_j + (r_{i,0} + e_{i,0}(1 + 3F_0) + 3\sum_{j=1}^{n-1} e_{i,n-j} F_j),\ i \in \overline{1,N}. \qquad (3.9)$$

Для отримання оцінки складності розв'язання СР (3.9) за допомогою одного з найбільш ефективних на сьогодні алгоритмів (а саме, узагальненого алгоритму BKW [3, 4]) скористаємося наступним твердженням.

Твердження 3.2 [4]. Нехай n_1 –натуральне число, $1 \le n_1 \le n-3$, $\delta \in (0,1)$,

$$u = \left\lceil \frac{\log(n-n_1)}{2} \right\rceil,\ v = \left\lceil \frac{2(n-n_1)}{\log(n-n_1)} \right\rceil,$$

$$k = 2^{u-1},\ l = (u\ +\ \left|\ln(2t\delta^{-1})\right|\ -\ 1)q^v,$$

$$N(n_1) = lt, \tag{3.10}$$

де

$$t = \frac{(1-\delta/2)n_1 \log 3 + \delta/2 \log \delta/2 + (1-\delta/2)\log(1-\delta/2)}{\Delta(p^{(k)})},$$

$$\Delta(p^{(k)}) = q^{-1} \sum_{z \in \mathbf{Z}_q} (qp^{(k)}(z) - 1)^2, \tag{3.11}$$

$p^{(k)} = (p^{(k)}(z) : z \in \mathbf{Z}_q)$ – розподіл ймовірностей випадкової величини $\eta_k = \xi_1 + \cdots + \xi_{k/2} - (\xi_{k/2+1} + \cdots + \xi_k)$, де $\xi_1, \ldots, \xi_{k/2}, \xi_{k/2+1}, \ldots, \xi_k$ – незалежні випадкові величини, розподілені за тим самим законом, що й спотворення $r_{i,0} + e_{i,0}(1+3F_0) + 3\sum_{j=1}^{n-1} e_{i,n-j}F_j$ у правій частині СР (3.9). Тоді, для відновлення з цієї СР за допомогою узагальненого алгоритму BKW довільних n_1 коефіцієнтів шуканого полінома F з ймовірністю не менше ніж $1-\delta$ необхідно виконати принаймні

$$T(n_1) = 2n_1 t 3^{n_1} + ult \tag{3.12}$$

операцій над n-вимірними векторами над полем $\mathbf{Z}_q$.

Для того, щоб скористатися твердженням 3.2, доведемо наступне твердження, яке встановлює аналітичний вираз параметра (3.11).

Твердження 3.3. Справедлива рівність

$$\Delta(p^{(k)}) = \sum_{\alpha \in \mathbf{Z}_q \setminus \{0\}} |\pi(\alpha)|^{2k}, \tag{3.13}$$

де

$$\pi(\alpha) = \begin{cases} \theta(dn^{-1}, \alpha)\theta(1/3, \alpha)\theta(1/3, 3\alpha)^{2d}, \text{ якщо } F_0 = 0; \\ \theta(dn^{-1}, \alpha)\theta(1/3, 2\alpha)\theta(1/3, 3\alpha)^{2d-1}, \text{ якщо } F_0 = 1; \\ \theta(dn^{-1}, \alpha)\theta(1/3, 4\alpha)\theta(1/3, 3\alpha)^{2d-1}, \text{ якщо } F_0 = -1, \end{cases} \tag{3.14}$$

і для будь-яких $p \in [0,1]$, $x \in \mathbf{Z}_q$

$$\theta(p, x) = 1 - 2p\left(1 - \cos\left(\frac{2\pi x}{q}\right)\right).$$

Доведення. Позначимо $\omega = \exp\{2\pi i q^{-1}\}$, де $i^2 = -1$ та розглянемо перетворення Фур'є $\hat{p}^{(k)}(\alpha) = \sum_{z \in \mathbf{Z}_q} p^{(k)}(z)\omega^{-\alpha z}$ розподілу ймовірностей випадкової величини $\eta_k = \xi_1 + \cdots + \xi_{k/2} - (\xi_{k/2+1} + \cdots + \xi_k)$. З формули (3.11) та рівності Парсеваля (див., наприклад, [8]) випливає, що

$$\Delta(p^{(k)}) = \sum_{\alpha \in \mathbf{Z}_q \setminus \{0\}} |\hat{p}^{(k)}(\alpha)|^2.$$

При цьому на підставі теореми про згортку [8]

$$\hat{p}^{(k)}(\alpha) = \pi(\alpha)^{k/2}\,\overline{\pi(\alpha)}^{\,k/2} = |\pi(\alpha)|^k,$$

де $\pi(\alpha) = \sum_{z \in \mathbf{Z}_q} p_{\xi_1}(z)\omega^{-\alpha z}$ є перетворенням Фур'є розподілу випадкової величини ξ_1, а $\overline{\pi(\alpha)}$ позначає число, комплексно спряжене до $\pi(\alpha)$, $\alpha \in \mathbf{Z}_q$.

Отже, для завершення доведення залишається переконатися в тому, що перетворення Фур'є випадкової величини ξ_1 має вигляд (3.14).

З формули $\xi_1 = r_{i,0} + e_{i,0}(1+3F_0) + 3\sum_{j=1}^{n-1} e_{i,n-j}F_j$ та умови $F \in S_d$ випливає, що випадкова величина ξ_1 має той самий закон розподілу, що і сума

$$\zeta_0 = r_0 + e_0 + 3\sum_{j=1}^{2d} e_j \text{, якщо } F_0 = 0; \tag{3.15}$$

$$\zeta_1 = r_0 + 4e_0 + 3\sum_{j=1}^{2d-1} e_j \text{, якщо } F_0 = 1; \tag{3.16}$$

$$\zeta_{-1} = r_0 - 2e_0 + 3\sum_{j=1}^{2d-1} e_j \text{, якщо } F_0 = -1, \tag{3.17}$$

де r_0, e_j – незалежні випадкові величини, розподілені за законами

$$\mathbf{P}(r_0 = 1) = \mathbf{P}(r_0 = -1) = dn^{-1},\ \mathbf{P}(r_0 = 0) = 1 - 2dn^{-1}, \tag{3.18}$$

$$\mathbf{P}(e_j = 1) = \mathbf{P}(e_j = -1) = \mathbf{P}(e_j = 0) = 1/3,\ j \in \overline{0,2d}.$$

Далі, перетворення Фур'є випадкової величини r_0 дорівнює

$$\hat{r}_0(\alpha) = \sum_{z \in \mathbf{Z}_q} \mathbf{P}(r_0 = z)\omega^{-\alpha z} = \mathbf{P}(r_0 = 0) + \mathbf{P}(r_0 = 1)\omega^{-\alpha} + \mathbf{P}(r_0 = -1)\omega^{\alpha} =$$

$$= 1 - 2dn^{-1} + dn^{-1}(\omega^{-\alpha} + \omega^{\alpha}) = 1 - 2dn^{-1}\left(1 - \cos\left(\frac{2\pi\alpha}{q}\right)\right) = \theta(dn^{-1}, \alpha),\ \alpha \in \mathbf{Z}_q, \tag{3.19}$$

і для будь-якого $c \in \mathbf{Z}_q \setminus \{0\}$ перетворення Фур'є випадкової величини ce_j дорівнює $1 - \frac{2}{3}\left(1 - \cos\left(\frac{2\pi c\alpha}{q}\right)\right) = \theta(1/3, c\alpha)$. Звідси на підставі теореми про згортку та формул (3.15) – (3.17) безпосередньо випливає, що перетворення Фур'є випадкової величини ξ_1 визначається за формулою (3.14).

Твердження доведено.

Описана BKW-атака є застосовною і до криптосистеми NTRUCipher: достатньо побудувати та розв'язати СР (3.9), вважаючи $e_{i,0} = ... = e_{i,n-1} = 0$, $i \in \overline{1, N}$. Складність розв'язання цієї СР у зазначеному випадку можна оцінити за допомогою твердження, яке доводиться аналогічно двом попереднім.

Твердження 3.4. Нехай у системі рівнянь (3.9) $e_{i,0} = ... = e_{i,n-1} = 0$, $i \in \overline{1, N}$, причому кількість рівнянь у системі дорівнює

$$N_0 = lt_0, \tag{3.20}$$

де параметри l, u, v, k, δ, n_1 визначаються так саме як у формулюванні твердження 3.2,

$$t_0 = \frac{2n_1 \ln(6\delta^{-1})(\log p_{\max}^{(k)} - \log p_{\min}^{(k)})^2}{(D(p^{(k)} \parallel \omega) + D(\omega \parallel p^{(k)}))^2},$$

$$p_{\max}^{(k)} = \max_{z \in \mathbf{Z}_q} p^{(k)}(z),\ p_{\min}^{(k)} = \min_{z \in \{\mathbf{Z}_q : p^{(k)}(z) \neq 0\}} p^{(k)}(z),$$

$$D(p^{(k)} \parallel \omega) = \sum_{z \in \{\mathbf{Z}_q : p^{(k)}(z) \neq 0\}} p^{(k)}(z) \log qp^{(k)}(z),\ D(\omega \parallel p) = -q^{-1} \sum_{z \in \{\mathbf{Z}_q : p^{(k)}(z) \neq 0\}} \log qp^{(k)}(z),$$

а $p^{(k)} = (p^{(k)}(z) : z \in \mathbf{Z}_q)$ – розподіл ймовірностей випадкової величини $\eta_k = \xi_1 + \cdots + \xi_{k/2} - (\xi_{k/2+1} + \cdots + \xi_k)$, де $\xi_1, \ldots, \xi_{k/2}, \xi_{k/2+1}, \ldots, \xi_k$ – незалежні випадкові величини, розподілені за законом (3.18). Тоді для відновлення з СР (3.9) за допомогою узагальненого алгоритму BKW довільних n_1 коефіцієнтів шуканого полінома F з ймовірністю не менше ніж $1-\delta$ достатньо виконати

$$T_0 = 2n_1 t_0 3^{n_1} + ult_0 \tag{3.21}$$

операцій над n-вимірними векторами над полем $\mathbf{Z}_q$.

При проведенні чисельних розрахунків за формулами (3.20), (3.21) можна скористатися такою формулою, що випливає з теореми про згортку, рівності (3.19) та формули для оберненого перетворення Фур'є:

$$p^{(k)}(z) = q^{-1} \sum_{\alpha \in \mathbf{Z}_q} \cos\left(\frac{2\pi\alpha z}{q}\right) |\, \theta(dn^{-1}, \alpha)\,|^k \quad z \in \mathbf{Z}_q .$$

Зауважимо, що твердження 3.2, 3.3 надають нижню оцінку трудомісткості BKW-атаки на шифросистему NTRUCipher+, в той час як твердження 3.4 – верхню оцінку трудомісткості цієї атаки на шифросистему NTRUCipher. Для отримання нижньої оцінки трудомісткості BKW-атаки на NTRUCipher можна використовувати твердження 3.2, 3.3, вважаючи у формулі (3.14) $\pi(\alpha) = \theta(dn^{-1}, \alpha)$.

В табл. 3.2 для низки значень n, d, q з табл. 3.1 наведені чисельні оцінки трудомісткості BKW-атаки на шифросистему NTRUCipher+. Символом $n_{1,\min}$ в табл. 3.2 позначено значення параметра n_1, для якого досягається мінімум значень (3.12). В табл. 3.3 наведені чисельні (верхня та нижня) оцінки трудомісткості BKW-атаки на шифросистему NTRUCipher, а також верхня оцінка трудомісткості тривіальної атаки, яка полягає у розв'язанні СР (3.9)

(при $e_{i,0} = ... = e_{i,n-1} = 0$, $i \in \overline{1,N}$) методом максимуму правдоподібності. Для обчислення останньої використано формулу, що випливає з результатів роботи [4]:

$$\log T_{\text{MMP}} = \log\left(\binom{n}{d}\binom{n-d}{d}\right) + \log(t_{\text{MMP}}\, n) + 1,$$

де t_{MMP} обчислюється за такою ж формулою, що й t_0 (див. твердження 3.4), в якій треба покласти $k = 1, n_1 = n$ та замінити 6 на 3:

$$t_{\text{MMP}} = \frac{2n\ln(3\delta^{-1})(\log p_{\max}^{(1)} - \log p_{\min}^{(1)})^2}{(D(p^{(1)} \parallel \omega) + D(\omega \parallel p^{(1)}))^2}.$$

Символом $n_{1,\min}$ в табл. 3.3 позначено значення параметра n_1, для якого досягається мінімум значень (3.21). Нарешті, для обчислення значень $\log T(n_{1,\min})$ та $\log N(n_{1,\min})$ у табл. 3.3 використано формули (3.12) та (3.10) відповідно, при застосуванні яких параметр $\pi(\alpha)$ у формулі (3.13) вважається рівним $\theta(dn^{-1}, \alpha)$ (див. твердження 3.5).

Таблиця 3.2 – Оцінки ефективності BKW-атаки на шифросистему NTRUCipher+ ($\delta = 0{,}01$)

(n, d)	q	$n_{1,\min}$	$\log T(n_{1,\min})$ (формула (3.12))	$\log N(n_{1,\min})$ (формула (3.10))
(401, 113)	4871	276	455,83	452,23
	5237	277	457,26	453,17
	5701	278	458,84	454,69
	6763	280	461,98	457,61
	7499	281	463,71	459,88
	8161	282	465,23	461,15
	8681	282	466,56	464,22
	9439	283	467,86	465,37
(449,134)	4877	306	504,64	502,15
	5701	308	507,98	505,57
	6577	310	510,73	508,05

	7681	312	513,79	511,01
	8167	313	514,92	511,51
	8837	314	516,46	512,93
	9463	315	517,85	513,73
(677, 157)	4831	448	730,95	728,39
	5867	452	737,04	734,33
	6703	455	741,05	737,43
	7417	457	744,15	740,38
	8059	458	746,93	744,43
	8677	460	748,87	744,95
	9461	461	751,67	749,16
(1091,120)	4831	700	1130,31	1125,49
	5867	706	1140,15	1136,42
	6659	710	1146,56	1142,95
	7537	714	1152,77	1148,83
	8237	717	1157,30	1152,53
	8779	719	1160,45	1155,48
	9439	721	1163,76	1159,46
(1171, 106)	4871	748	1206,63	1202,07
	5927	755	1217,67	1212,72
	6733	759	1224,34	1220,55
	7561	763	1230,58	1226,53
	8243	766	1235,22	1230,75
	8807	768	1238,57	1234,63
	9241	769	1241,26	1238,56
(443, 143)	4861	303	498,59	493,74
	5981	305	502,64	499,86
	6781	307	505,15	501,19
	7681	308	507,72	505,18
	8387	309	509,51	507,09
	8821	310	510,19	506,90
	9377	311	511,46	507,25
(743, 247)	4817	489	795,17	791,51
	5903	493	802,48	799,86
	6959	497	807,88	804,25
	7681	499	811,17	807,75
	8387	501	814,11	810,18
	8831	502	815,77	812,02
	9371	503	817,69	814,51

Таблиця 3.3 – Оцінки ефективності атак на шифросистему NTRUCipher ($\delta = 0{,}01$)

(n, d)	q	$n_{1,\min}$	$\log T_0(n_{1,\min})$ (формула (3.21))	$\log N_0(n_{1,\min})$ (формула (3.20))	$\log T(n_{1,\min})$ (формула (3.12))	$\log N(n_{1,\min})$ (формула (3.10))	$\log T_{\text{ММР}}$
(401, 113)	1543	261	437,46	434,11	431,94	428,46	637,29
	1663	262	439,98	436,79	433,62	430,21	637,41

	1811	263	442,57	439,81	435,55	432,69	637,46
	2141	266	446,51	441,76	439,47	437,11	637,18
	2383	267	447,09	443,72	441,50	438,01	637,33
	2591	268	450,27	447,17	443,25	440,03	637,22
	2753	269	450,41	446,74	444,57	440,76	637,17
	2999	270	452,46	449,09	446,28	442,78	637,38
(449,134)	1553	290	483,98	479,82	477,95	473,63	719,89
	1811	292	487,74	484,74	481,64	478,52	719,95
	2087	294	491,06	488,43	485,20	482,49	719,87
	2437	297	495,65	491,32	489,07	484,58	719,79
	2591	298	496,36	491,70	490,61	485,79	719,96
	2803	299	498,53	494,38	492,29	487,99	719,81
	3001	300	500,24	496,04	493,88	489,52	719,94
(677, 157)	1531	423	693,84	690,06	689,99	686,07	1004,45
	1861	427	702,01	699,53	697,59	695,06	1004,22
	2129	431	706,95	702,66	702,58	698,16	1004,30
	2375	433	710,52	707,54	706,38	703,31	1004,39
	2557	435	713,41	709,65	709,09	705,19	1004,32
	2753	436	716,29	713,82	711,89	709,35	1004,28
	2999	438	718,80	716,19	714,79	712,11	1004,30
(1091,120)	1543	658	1065,75	1062,75	1064,34	1061,26	1086,78
	1861	665	1078,10	1075,51	1076,13	1073,48	1086,56
	2113	670	1085,59	1082,79	1083,67	1080,00	1086,54
	2393	675	1092,93	1089,48	1090,97	1087,40	1086,73
	2617	678	1098,17	1095,25	1096,21	1093,22	1086,74
	2789	681	1102,07	1097,48	1100,09	1095,35	1086,80
	2999	683	1105,28	1102,21	1103,98	1100,82	1086,66
(1171, 106)	1549	703	1137,13	1133,89	1135,63	1132,29	1028,61
	1879	711	1148,97	1145,87	1148,46	1145,27	1028,93
	2137	716	1158,48	1155,74	1156,91	1154,11	1028,67
	2399	721	1165,19	1161,83	1164,14	1160,67	1028,92
	2617	724	1171,38	1168,71	1169,75	1167,02	1028,76
	2801	727	1175,42	1172,19	1173,77	1170,46	1028,70
	2939	729	1177,43	1173,89	1176,74	1173,08	1028,71
(443, 143)	1543	286	477,34	474,10	471,91	468,55	716,62
	1901	289	483,97	481,26	477,12	474,32	716,66
	2153	291	486,13	483,19	480,09	477,05	716,72
	2437	293	489,29	485,98	483,02	479,58	716,51
	2663	294	491,04	488,37	485,13	482,38	716,58
	2801	295	492,35	489,08	486,24	482,85	716,64
	2971	296	493,86	490,15	487,64	483,78	716,59
(743, 247)	1531	461	757,05	753,26	750,47	746,53	1193,69
	1877	466	765,42	762,47	758,95	755,91	1193,53
	2207	470	772,58	769,88	765,63	762,86	1193,61
	2437	473	776,79	773,01	769,57	765,66	1193,55
	2663	475	779,72	776,43	772,99	769,59	1193,43
	2801	476	782,23	779,41	775,00	772,10	1193,46
	2969	478	784,05	779,79	777,38	772,97	1193,49

Як видно з табл. 3.2 і 3.3, при фіксованих значеннях n, d зі збільшенням q трудомісткість BKW-атаки на кожну шифросистему повільно зростає. Зокрема, при $(n,d)=(1171,106)$ нижня оцінка трудомісткості BKW-атаки на NTRUCipher змінюється від 2^{1135} до 2^{1176} операцій, в той час як нижня оцінка трудомісткості цієї атаки на NTRUCipher+ змінюється від 2^{1206} до 2^{1241} операцій (в залежності від значення q, яке для криптосистеми NTRUCipher+ є майже у 3 рази більше). Крім того, для n, d і q, зазначених в табл. 3.2 і 3.3, трудомісткість BKW-атаки на NTRUCipher+ є від 2^{15} до 2^{69} разів більше, ніж для NTRUCipher (при цьому обидві шифросистеми характеризуються майже одноковими верхніми межами ймовірності помилки розшифрування; див. табл. 3.1). Нарешті, як видно з табл. 3.3, для кожної пари (n, d), за винятком (1091,120) та (1171, 106), складність BKW-атаки на NTRUCipher є на декілька порядків нижче, ніж складність тривіальної атаки. Поряд з тим, BKW-атака потребує набагато більшої кількості рівнянь (див. значення $\log N_0(n_{1,\min})$ в табл. 3.3) в порівнянні з тривіальною атакою.

В табл. 3.4 наведено результати порівняння шифросистем NTRUCipher та NTRUCipher+ за довжиною шифрованих повідомлень при заданій множині ключів (параметрах n і d), заданому рівні стійкості L відносно BKW-атаки та заданій верхній межі ймовірністю помилки розшифрування.

Для шифросистеми NTRUCipher+ символом $q_{\min}$ в табл. 3.4 позначено найменше просте число q (що є примітивним елементом за модулем n), для якого нижня межа $T(q_{\min})$ складності BKW-атаки на шифросистему (згідно з твердженням 3.3) є не менше ніж 2^L операцій, і верхня межа p_{er} ймовірності помилки розшифрування (згідно з формулою (3.4)) є не більше ніж 2^{-80}. В таблиці наведені також фактичні значення двійкових логарифмів параметрів $T(q_{\min})$ і p_{er} та відповідні значення довжини шифрованих повідомлень

$n\log q_{\min}$. Для шифросистеми NTRUCipher параметри в табл. 3.4 мають той самий сенс.

Таблиця 3.4 – Оцінки практичності шифросистем NTRUCipher та NTRUCipher+ ($\delta = 0{,}01$)

(n,d)	L	NTRUCipher				NTRUCipher +			
		$q_{\min}$	$\log T(q_{\min})$	$-\log p_{er}$	$n\log q_{\min}$	$q_{\min}$	$\log T(q_{\min})$	$-\log p_{er}$	$n\log q_{\min}$
(401, 113)	256	1019	422,20	80,58	4007,17	3191	447,70	80,14	4667,56
(449, 134)	256	1109	468,88	80,48	4541,65	3517	497,36	82,22	5289,28
	512	7079	512,14	3714,55	5742,41	7039	512,01	359,66	5738,74
(677, 157)	256, 512	1201	680,39	80,13	6925,72	3793	722,96	80,99	8048,94
(1091, 120)	512, 1024	1087	1041,70	85,71	11003,97	3313	1109,79	80,07	12758,07
(1171, 106)	512, 1024	1039	1108,06	85,91	11710	3119	1180,44	80,24	13591,64
(443, 143)	256	1163	464,70	83,35	4511,35	3613	492,26	81,23	5235,81
	512	9697	512,02	6544,38	5866,79	9697	512,02	647,69	5866,79
(743, 247)	256, 512	1531	750,47	83,36	7861,13	4751	794,88	80,69	9075,01

Як видно з табл. 3.4, при заданих нижній межі стійкості та верхній межі ймовірності помилкового розшифрування шифровані повідомлення у шифросистемі NTRUCipher+ мають більшу довжину в порівнянні із системою NTRUCipher. Виключення спостерігаються лише для трійок $(n, d, L) = (449, 134, 512)$ та $(n, d, L) = (443, 143, 512)$, коли ці довжини майже співпадають. Такий ефект пояснюється необхідністю збільшення значення $q_{\min}$ у шифросистемі NTRUCipher+ в порівнянні з NTRUCipher для забезпечення належної малості ймовірності помилки розшифрування (див. твердження 3.1 та наслідок 3.1).

Таким чином, підвищення стійкості шифросистеми NTRUCipher відносно BKW-атаки за рахунок використання додаткового доданку e у формулі (3.1), що збільшує рівень спотворень у правих частинах рівнянь системи (3.9), майже повністю нівелюється збільшенням верхньої межі ймовірності помилки розшифрування. Це має негативний вплив на практичність шифросистеми NTRUCipher+ в порівнянні з NTRUCipher. В цілому, отримані результати свідчать про недоцільність використовувати

NTRUCipher+ для підвищення стійкості шифросистеми NTRUCipher відносно BKW-атаки.

3.3. Розрізнювальна атака на шифросистему NTRUCipher+

Розглянемо зараз атаку, мета якої полягає в тому, щоб відрізнити послідовність шифрованих повідомлень шифросистеми NTRUCipher+ від суто випадкової послідовності елементів кільця $R_{n,q}$.

Точна постановка задачі має такий вигляд. Спостерігається послідовність незалежних випадкових величин $c^{(1)}, \dots, c^{(t)}$, які з ймовірністю $1/2$ мають рівномірний розподіл на множині $R_{n,q}$ (гіпотеза H_0) та з імовірністю $1/2$ отримуються за формулою

$$c^{(i)} = (m^{(i)} + 3(r^{(i)}(1+3F)^{-1} + e^{(i)})) \bmod q,\ i \in \overline{1,t}, \qquad (3.22)$$

де $m^{(i)}, r^{(i)}$ та $e^{(i)}$ є незалежними поліномами, що мають рівномірні розподіли ймовірностей на множинах S, S_d та S відповідно, $i \in \overline{1,t}$, а $F \in S_d$ є невідомим ключем шифросистеми NTRUCipher+ (гіпотеза H_1).

Для побудови критерію перевірки гіпотез H_0 та H_1 розглянемо значення поліномів $c^{(1)}, \dots, c^{(t)}$ в точці, що дорівнює одиниці поля $\mathbf{Z}_q$. Зрозуміло, що за умови гіпотези H_0 елементи $c^{(1)}(1), \dots, c^{(t)}(1)$ є незалежними в сукупності та мають рівномірний розподіл на цьому полі. Поряд з тим, на підставі формули (3.22) та рівностей $R_{n,q} = \mathbf{Z}_q[x]/(x^n - 1)$, $F(1) = r^{(i)}(1) = 0$ за умови гіпотези H_1 справедливе співвідношення

$$c^{(i)}(1) = (m^{(i)}(1) + 3e^{(i)}(1)) \bmod q\,,\ i \in \overline{1,t}\,. \qquad (3.23)$$

Твердження 3.5. Розподіл ймовірностей випадкової величини (3.23) визначається за формулою

$$p(z) \stackrel{\text{def}}{=} \mathbf{P}(c^{(i)}(1) = z) = q^{-1} \sum_{\alpha \in \mathbf{Z}_q} \cos\left(\frac{2\pi\alpha z}{q}\right) \theta(1/3, \alpha)^n \theta(1/3, 3\alpha)^n\,,\ z \in \mathbf{Z}_q\,, \qquad (3.24)$$

де для будь-яких $p \in [0,1]$, $x \in \mathbf{Z}_q$

$$\theta(p, x) = 1 - 2p\left(1 - \cos\left(\frac{2\pi x}{q}\right)\right).$$

Доведення. Оскільки випадкові поліноми $m^{(i)}, e^{(i)}$ є незалежними та мають рівномірний розподіл ймовірностей на множині S, то їхні коефіцієнти є незалежними випадковими величинами, що приймають кожне значення $0, 1, -1$ з ймовірністю $1/3$. Звідси за допомогою міркувань, використаних при доведенні твердження 3.3, отримаємо, що перетворення Фур'є над полем $\mathbf{Z}_q$ довільного коефіцієнта полінома $m^{(i)}$ дорівнює $\theta(1/3, \alpha)$, а перетворення Фур'є довільного коефіцієнта полінома $3e^{(i)}$ дорівнює $\theta(1/3, 3\alpha)$. Звідси на підставі теореми про згортку та формули оберненого перетворення Фур'є випливає рівність (3.24).

Твердження доведено.

Позначимо

$$M = \{z \in \mathbf{Z}_q : p(z) > q^{-1}\}\,,\ C = \frac{1}{2} \sum_{z \in M} \left(p(z) + q^{-1}\right),$$

$$\Delta = \sum_{\alpha \in \mathbf{Z}_q \setminus \{0\}} \theta(1/3, \alpha)^{2n} \theta(1/3, 3\alpha)^{2n}$$

та опишемо алгоритм, що дозволяє перевіряти справедливість однієї з гіпотез H_0, H_1 із (середньою) ймовірністю помилки, яка не перевищує заданого порогу.

Алгоритм 3.1.

Вхідні дані: вибірка $c^{(1)}, \ldots, c^{(t)}$, члени якої розподілені відповідно до однієї з гіпотез H_0, H_1.

Обчислити послідовність $c^{(1)}(1), \ldots, c^{(t)}(1)$ та підрахувати значення $N = |\{i \in \overline{1,t} : c^{(i)}(1) \in M\}|$.

Результат: якщо $N \le Ct$, прийняти гіпотезу H_0; інакше – прийняти гіпотезу H_1.

Твердження 3.6. Нехай $\delta \in (0, 1/2)$,

$$t = \left\lceil \frac{8q \ln(\delta^{-1})}{\Delta} \right\rceil. \qquad (3.25)$$

Тоді алгоритм 3.1 дозволяє розрізнити гіпотези H_0 і H_1 із середньою ймовірністю помилки не вище ніж δ, використовуючи $O(nt)$ операцій над елементами поля $\mathbf{Z}_q$.

Доведення. Позначимо ξ_i індикатор події $\{c^{(i)}(1) \in M\}$, $i \in \overline{1,t}$. Справедлива рівність $N = \xi_1 + \cdots + \xi_t$.

Якщо справедлива гіпотеза H_0, то ймовірність помилки алгоритму 3.1 дорівнює $\mathbf{P}(\xi_1 + \cdots + \xi_t > Ct)$, і випадкові величини $\xi_1, \ldots, \xi_t$ є незалежними та рівномірно розподіленими на полі $\mathbf{Z}_q$. Отже, на підставі нерівності Гефдінга та означення параметра C

$$\mathbf{P}(\xi_1 + \cdots + \xi_t > Ct) = \mathbf{P}\left(\sum_{i=1}^{t} \xi_i - tq^{-1} \mid M \mid > t(C - q^{-1} \mid M \mid) \right) \leq$$

$$\leq \exp\left\{ -2t(C - q^{-1} \mid M \mid)^2 \right\} = \exp\left\{ -1/2 \cdot td^2 \right\},$$

де $d = \sum_{z \in M} \left(p(z) - q^{-1} \right)$.

Якщо справедлива гіпотеза H_1, то ймовірність помилки алгоритму 3.1 дорівнює $\mathbf{P}(\xi_1 + \cdots + \xi_t \leq Ct)$, і випадкові величини $\xi_1, \ldots, \xi_t$ є незалежними та мають математичні сподівання, що дорівнюють $p(M) \stackrel{\text{def}}{=} \sum_{z \in M} p(z)$. Отже, згідно з нерівністю Гефдінга

$$\mathbf{P}(\xi_1 + \cdots + \xi_t \leq Ct) = \mathbf{P}\left(\sum_{i=1}^{t} \xi_i - tp(M) \leq t(C - p(M)) \right) \leq$$

$$\leq \exp\left\{ -2t(C - p(M))^2 \right\} = \exp\left\{ -1/2 \cdot td^2 \right\}.$$

Таким чином, середня ймовірність помилки алгоритму 3.1 не перевищує $\exp\left\{ -1/2 \cdot td^2 \right\}$. Звідси, використовуючи співвідношення

$$d^2 = \left(\sum_{z \in M} \left(p(z) - q^{-1} \right) \right)^2 = \left(\frac{1}{2q} \sum_{z \in \mathbf{Z}_q} \mid qp(z) - 1 \mid \right)^2 \geq$$

$$\geq \frac{1}{4q^2} \sum_{z \in \mathbf{Z}_q} \mid qp(z) - 1 \mid^2 = \frac{1}{4q} \sum_{\alpha \in \mathbf{Z}_q \setminus \{0\}} \hat{p}(\alpha)^2 = \frac{\Delta}{4q},$$

передостаннє з яких є наслідком рівності Парсеваля (див., наприклад, [8]), а останнє випливає з формули (3.24), отримаємо, що середня ймовірність помилки алгоритму 3.1 не перевищує $\exp\left\{-\frac{\Delta\cdot t}{8q}\right\}$, що, у свою чергу, є не вище ніж δ згідно з формулою (3.25).

Твердження доведено.

В табл. 3.5 наведено результати розрахунків інформаційної складності алгоритму 3.1 (тобто параметра (3.25)) для низки значень параметрів n і q шифросистеми NTRUCipher+ (зауважимо, що трудомісткість алгоритму 3.1 не залежить від параметра d).

Таблиця 3.5 – Оцінки інформаційної складності розрізнювальної атаки на шифросистему NTRUCipher+ ($\delta = 0{,}01$)

n	q	$\log t$	Δ
401	139	19,22	0,01
	1051	13,00	4,73
	2393	12,84	12,05
449	389	13,80	1,01
	2207	12,94	10,38
	3449	12,89	16,78
677	409	14,36	0,72
	2423	13,25	9,17
	5171	13,17	20,71
1091	457	15,00	0,51
	4217	13,55	12,95
	8581	13,49	27,38
1171	443	15,25	0,42
	3851	13,62	11,29
	8009	13,56	24,57

Як видно з табл. 3.5, із збільшенням параметра q збільшується значення параметра Δ та зменшується інформаційна (а, отже, і часова) складність алгоритму 3.1. При $n = 401$, $q = 139$ спостерігається найбільше значення обсягу матеріалу $t = 2^{19}$, потрібного для реалізації атаки із середньою

ймовірністю помилки не вище ніж δ.

Покажемо зараз, що у випадку, коли

$$8n+1<q, \tag{3.26}$$

для надійного розрізнення гіпотез H_0 і H_1 можна використовувати більш простий (та більш ефективний з погляду трудомісткості) алгоритм.

Алгоритм 3.2.

Вхідні дані: вибірка $c^{(1)},\dots,c^{(t)}$, члени якої розподілені відповідно до однієї з гіпотез H_0, H_1.

Обчислити послідовність $c^{(1)}(1),\dots,c^{(t)}(1)$.

Результат: якщо існує $i\in\overline{1,t}$ таке, що $|c^{(i)}(1)|>4n$, прийняти гіпотезу H_0 ; інакше – прийняти гіпотезу H_1.

Твердження 3.7. Нехай виконується умова (3.26), $\delta\in(0,1/2)$,

$$t=\left|\frac{\log\left((2\delta)^{-1}\right)}{\log\left(\frac{q}{8n+1}\right)}\right|. \tag{3.27}$$

Тоді алгоритм 3.2 дозволяє розрізнити гіпотези H_0 і H_1 із середньою ймовірністю помилки не вище ніж δ, використовуючи $O(nt)$ операцій над елементами поля $\mathbf{Z}_q$.

Доведення. Якщо справедлива гіпотеза H_0, то $c^{(1)}(1),\dots,c^{(t)}(1)$ є незалежними випадковими величинами з рівномірним розподілом ймовірностей на полі $\mathbf{Z}_q$, і алгоритм 3.2 припускається помилки тоді й тільки тоді, коли усі ці величини приймають значення в інтервалі $[-4n,4n]$. Отже,

ймовірність помилки алгоритму 3.2 в цьому випадку дорівнює $\left(\frac{8n+1}{q}\right)^t$.

Якщо справедлива гіпотеза H_1, то ймовірність помилки алгоритму дорівнює нулю. Дійсно, внаслідок умови $m^{(i)}, e^{(i)} \in S$ модуль суми коефіцієнтів полінома $m^{(i)} + 3e^{(i)}$ в кільці цілих чисел не перевищує $4n$, що є менше ніж $(q-1)/2$ на підставі нерівності (3.26). Отже, зазначений модуль співпадає зі значенням $|(m^{(i)}(1) + 3e^{(i)}(1)) \bmod q|$, яке дорівнює $|c^{(i)}(1)|$ згідно з формулою (3.23), $i \in \overline{1,t}$.

Таким чином, середня ймовірність помилки алгоритму 3.2 дорівнює $\frac{1}{2}\left(\frac{8n+1}{q}\right)^t$, що не перевищує δ на підставі рівності (3.27). Твердження доведено.

Отримані результати показують, що шифросистема NTRUCipher+ є вразливою до наведеної розрізнювальної атаки. Ця атака може бути реалізована в режимі реального часу, хоча й не дозволяє відновлювати ключ шифросистеми, а тільки відрізняти послідовність її шифрованих повідомлень від суто випадкової послідовності елементів кільця $R_{n,q}$. Зауважимо, що жодна з наведених вище атак не розглянута в роботі [1], де запропоновано шифросистему NTRUCipher.

Висновки

1. У розділі викладено результати дослідження стійкості шифросистеми NTRUCipher та її природного узагальнення NTRUCipher+ відносно двох статистичних атак. Основним науковим результатом розділу є аналітичні оцінки часової складності цих атак. Отримані оцінки надають змогу порівняти між собою шифросистеми NTRUCipher та NTRUCipher+ за

стійкістю та практичністю, а також визначити умови, за яких зазначені шифросистеми мають потрібну стійкості відносно розглянутих атак.

2. Перша з двох атак на шифросистеми NTRUCipher та NTRUCipher+ (BKW-атака) проводиться на основі підібраного відкритого тексту і полягає у складанні системи лінійних рівнянь зі спотвореними правими частинами вигляду (3.9) та її розв'язанні за допомогою узагальненого алгоритму BKW. Ця атака є можливою саме для симетричних NTRU-подібних шифросистем, проте вона не розглядається у доступних публікаціях. Отримані аналітичні оцінки (твердження 3.2 – 3.4) свідчать про те, що трудомісткість BKW-атаки на шифросистему NTRUCipher+ є в $2^{15} \div 2^{69}$ разів вище в порівнянні з трудомісткістю цієї атаки на шифросистему NTRUCipher.

3. При фіксованих значеннях параметрів n, d шифросистеми зі збільшенням значення q трудомісткість BKW-атаки повільно зростає. Зокрема, при $(n,d) = (1171,106)$ нижня оцінка трудомісткості BKW-атаки на NTRUCipher змінюється від 2^{1135} до 2^{1176} операцій, в той час як нижня оцінка трудомісткості цієї атаки на NTRUCipher+ змінюється від 2^{1206} до 2^{1241} операцій (в залежності від значення q, яке для шифросистеми NTRUCipher+ є майже у 3 рази більше). При цьому обидві шифросистеми характеризуються майже одноковими верхніми межами ймовірності помилки розшифрування (табл. 3.1 – 3.3).

4. Підвищення стійкості шифросистеми NTRUCipher відносно BKW-атаки за рахунок використання додаткового доданку e у формулі (3.1), що збільшує рівень спотворень у правих частинах рівнянь системи (3.9), майже повністю нівелюється збільшенням верхньої межі ймовірності помилки розшифрування. Це має негативний вплив на практичність шифросистеми NTRUCipher+ в порівнянні з NTRUCipher (табл. 3.4) та свідчить про недоцільність використовувати NTRUCipher+ для підвищення стійкості шифросистеми NTRUCipher відносно BKW-атаки.

5. Друга з двох розглянутих атак (див. алгоритми 3.1 та 3.2) полягає в

тому, щоб відрізнити послідовність шифрованих повідомлень шифросистеми NTRUCipher+ від суто випадкової послідовності елементів кільця $R_{n,q}$. Показано (твердження 3.6, 3.7), що шифросистема NTRUCipher+ над зазначеним кільцем є цілком вразливою до наведеної атаки, яка може бути реалізована в режимі реального часу. Зокрема, найбільше (з розрахованих; див. табл. 3.5) значення складності атаки досягається при $n = 401$, $q = 139$ і становить порядку $t = 2^{19}$ двійкових операцій.

Список використаних джерел у третьому розділі

1. Valluri M. R. NTRUCipher-lattice based secret key encryption. 2017. DOI: https://doi.org/10.48550/arXiv.1710.01928.

2. Stehlé D., Steinfeld R. Making NTRU as secure as worst-case problems over ideal lattices. *Advances in Cryptology – EUROCRYPT 2011*. Berlin, Heidelberg, 2011. P. 27–47. DOI: https://doi.org/10.1007/978-3-642-20465-4_4.

3. Blum A., Kalai A., Wasserman H. Noise-tolerant learning, the parity problem, and the statistical query model. *Journal of the ACM*. 2003. Vol. 50, no. 4. P. 506–519. DOI: https://doi.org/10.1145/792538.792543.

4. Олексійчук А. М., Ігнатенко С. М., Поремський М. В. Системи лінійних рівнянь зі спотвореними правими частинами над скінченними кільцями. *Математичне та комп'ютерне моделювання. Серія: технічні науки.* 2017. № 15. С. 150–155. DOI: https://doi.org/10.32626/2308-5916.2017-15.150-155.

5. Hoeffding W. Probability inequalities for sums of bounded random variables. *Journal of the American Statistical Association*. 1963. Vol. 58, no. 301. P. 13–30. DOI: https://doi.org/10.1080/01621459.1963.10500830.

6. Choosing NTRUEncrypt Parameters in Light of Combined Lattice Reduction and MITM Approaches / P. S. Hirschhorn et al. *Applied Cryptography and Network Security*. Berlin, Heidelberg, 2009. P. 437–455. DOI: https://doi.org/10.1007/978-3-642-01957-9_27.

7. NIST PQ Submission: NTRUEncrypt. A lattice based algorithm / Z. Zhang et al. *NIST Computer Security Resource Center | CSRC*. URL: https://csrc.nist.gov/Projects/post-quantum-cryptography/post-quantum-cryptography-standardization/round-1-submissions (дата звернення: 02.05.2023)

8. Babai L. The Fourier transform and equations over finite abelian groups. 2002. URL: https://people.cs.uchicago.edu/~laci/reu02/fourier.pdf (дата звернення: 05.05.2023).

РОЗДІЛ 4

МЕТОД ПОБУДОВИ СИМЕТРИЧНИХ NTRU-ПОБІДНИХ ШИФРОСИСТЕМ, ЩО Є ОБҐРУНТОВАНО СТІЙКИМИ ВІДНОСНО АТАК НА ОСНОВІ ПІДІБРАНИХ ВІДКРИТИХ ТЕКСТІВ

В попередньому розділі досліджено стійкість шифросистем NTRUCipher та NTRUCipher+, визначених над кільцем зрізаних поліномів за модулем полінома $x^n - 1$, відносно певних статистичних атак. Показано, що обидві шифросистеми є вразливими до природної розрізнювальної атаки, яка може бути реалізована в режимі реального часу. В даному розділі продовжено дослідження стійкості шифросистеми NTRUCipher, яка зараз розглядається над круговим кільцем (тобто кільцем зрізаних поліномів за модулем полінома $x^n + 1$, де n – степінь двійки). Зауважимо, що це кільце часто використовується для побудови асиметричних NTRU-подібних та близьких до них шифросистем (див., підрозділ 1.3). Крім того, саме над ним визначається оригінальна версія шифросистеми NTRUCipher [1].

В п. 4.1 отримано аналітичну оцінку складності розрізнювальної атаки, з якої випливає, що шифросистема NTRUCipher над круговим кільцем є вразливою до неї. Цей факт, поряд з результатами підрозділу 3.3, свідчить про необхідність створення методу побудови обґрунтовано стійких симетричних NTRU-подібних шифросистем, що відрізняються за сутністю від NTRUCipher або NTRUCipher+. Зазначений метод є основним науковим результатом цього розділу.

В п. 4.2 викладено наукові основи методу, зокрема, означення запропонованих шифросистем та обґрунтування їх CPA-стійкості, яка (на відміну від стійкості шифросистем NTRUCipher та NTRUCipher+) базується

на складності еталонної обчислювально складної задачі Decision-Ring-LWE [2].

В п. 4.3 наведено алгоритм вибору параметрів запропонованих шифросистем, які забезпечують їхню стійкість на заздалегідь визначеному рівні. Зазначено, що час зашифрування чи розшифрування повідомлень у запропонованих шифросистемах є порівняним з відповідним часом у криптосистемі NTRU Prime [3], яка є одним з фіналістів конкурсу NIST зі створення нових постквантових криптографічних стандартів.

4.1. Розрізнювальна атака на шифросистему NTRUCipher над круговим кільцем

Розглянемо шифросистему NTRUCipher, визначену над кільцем $R(n,q)=\mathbf{Z}_q[x]/(x^n+1)$, де $n\geq 2$ є степенем двійки, а q – простим числом таким, що $q\equiv 1 \bmod 2n$ [1]. З останньої умови випливає, що мультиплікативна група поля $\mathbf{Z}_q$ містить циклічну підгрупу порядку $2n$, і якщо β є твірним елементом цієї групи, то поліном x^n+1 розкладається над полем $\mathbf{Z}_q$ на лінійні множники: $x^n+1=(x-\beta)(x-\beta^3)\cdots(x-\beta^{2n-1})$, а отже, співпадає з $2n$-круговим (або циклотомічним) поліномом $\Phi_{2n}(x)$ над цим полем (див., наприклад, [4]).

Зауважимо, що кільце $R(n,q)$ часто використовується для побудови асиметричних NTRU-подібних та близьких до них) шифросистем, що пояснюється можливістю застосування швидкого перетворення Фур'є над полем $\mathbf{Z}_q$ для множення елементів кільця $R(n,q)$, а також відомим результатом [2] про складнісну еквівалентність двох версій задачі Ring-LWE над цим кільцем (див. підрозділ 1.3).

Шифросистема NTRUCipher над $R(n,q)$ визначається так само, як і над

кільцем $R_{n,q}$ (див. підрозділ 3.3). Для зашифрування відкритого тексту $m \in R(n,q)$, що є малим поліномом (тобто з коефіцієнтами $0, 1, -1$) на секретному ключі f, який вибирається певним чином з групи $R(n,q)^*$ оборотних елементів кільця $R(n,q)$, генерується випадковий поліном $r \in R(n,q)$ та обчислюється шифротекст $c = (m + 3rf^{-1}) \bmod q$.

Надалі не накладатимемо жодних обмежень щодо способу формування секретного ключа f. Стосовно розподілу випадкового полінома r вважатимемо, що цей розподіл задовольняє такій *умові* β*-інваріантності*:

$$\forall z \in \mathbf{Z}_q : p(z) \stackrel{\text{def}}{=} \mathbf{P}(r(\beta) = z) = \mathbf{P}(\beta r(\beta) = z), \qquad (4.1)$$

де β – зазначений вище корінь полінома $x^n + 1$. Крім того, вважатимемо, що розподіл ймовірностей (4.1) є відмінним від рівномірного на полі $\mathbf{Z}_q$.

Важливі приклади β-інваріантних законів розподілу надає наступне твердження.

Твердження 4.1. Нехай виконується одна з таких умов:

1) коефіцієнти $r_0, r_1, \ldots, r_{n-1}$ полінома r є незалежними випадковими величинами, розподіленими за законом $\mathbf{P}(r_i = 1) = \mathbf{P}(r_i = -1) = dn^{-1}$, $\mathbf{P}(r_i = 0) = 1 - 2dn^{-1}$, де $1 \le d \le n - 2$;

2) поліном r формується за правилом $r = r_1 r_2 + r_3$, де r_1, r_2, r_3 – незалежні випадкові поліноми, розподілені за законом 1), а обчислення виконуються в кільці $R(n,q)$.

Тоді розподіл ймовірностей випадкового полінома r є β-інваріантним.

Доведення. Нехай $r(x) = r_0 + r_1 x + \cdots + r_{n-1} x^{n-1}$. Оскільки $\beta^n = -1$, то

$$r(\beta) = r_0 + r_1\beta + \cdots + r_{n-1}\beta^{n-1},\ \beta r(\beta) = -r_{n-1} + r_0\beta + \cdots + r_{n-2}\beta^{n-1}.$$

Звідси, використовуючи заміну змінних $b_0 = -a_{n-1}$, $b_1 = a_0$, …, $b_{n-1} = a_{n-2}$, отримаємо, що за умови 1) для будь-якого $z \in \mathbf{Z}_q$ виконуються рівності

$$\mathbf{P}(\beta r(\beta) = z) = \sum_{b_0 + b_1\beta + \cdots + b_{n-1}\beta^{n-1} = z} \mathbf{P}(r_{n-1} = -b_0)\mathbf{P}(r_0 = b_1)\cdots\mathbf{P}(r_{n-2} = b_{n-1}) =$$

$$= \sum_{-a_{n-1} + a_0\beta + \cdots + a_{n-2}\beta^{n-1} = z} \mathbf{P}(r_{n-1} = a_{n-1})\mathbf{P}(r_0 = a_0)\cdots\mathbf{P}(r_{n-2} = a_{n-2}) =$$

$$= \sum_{-a_{n-1} + a_0\beta + \cdots + a_{n-2}\beta^{n-1} = z} \mathbf{P}(r_0 = -a_{n-1})\mathbf{P}(r_1 = a_0)\cdots\mathbf{P}(r_{n-1} = a_{n-2}) = \mathbf{P}(r(\beta) = z).$$

Далі, за умови 2) з рівності $r(x) = r_1(x)r_2(x) + r_3(x)$ в кільці $R(n,q)$ випливає рівність $r(\beta) = r_1(\beta)r_2(\beta) + r_3(\beta)$ в полі $\mathbf{Z}_q$, яка, у свою чергу, тягне рівність $\beta r(\beta) = (\beta r_1(\beta))r_2(\beta) + \beta r_3(\beta)$, де випадкові елементи $\beta r_1(\beta), r_2(\beta), \beta r_3(\beta)$ є незалежними в сукупності та (на підставі доведеного) мають той самий закон розподілу, що і випадкові елементи $r_1(\beta), r_2(\beta), r_3(\beta)$. Звідси випливає, що розподіли ймовірностей випадкових елементів $r(\beta)$ та $\beta r(\beta)$ співпадають.

Твердження доведено.

Зауважимо, що спосіб, визначений умовою 2) твердження 4.1, використовується в [1] для формування випадкових поліномів r у шифросистемі NTRUCipher.

Розрізнювальна атака на цю шифросистему має за мету розв’язання такої задачі, відомої під назвою Decision NTRUCipher Ciphertext Cracking Problem [1].

Спостерігається послідовність $\gamma^{(1)}, \ldots, \gamma^{(t)}$ незалежних випадкових

елементів кільця $R(n,q)$, які з імовірністю $1/2$ мають рівномірний розподіл на цьому кільці (гіпотеза H_0) та з імовірністю $1/2$ розподілені за законом

$$\gamma^{(i)} = 3r^{(i)} f^{-1}, \ \ i \in \overline{1,t}, \tag{4.2}$$

де $r^{(1)}, \ldots, r^{(t)}$ – незалежні випадкові елементи кільця $R(n,q)$, що мають однаковий розподіл ймовірностей (гіпотеза H_1). Треба побудувати критерій для розрізнення зазначених гіпотез. Іншими словами, мета розрізнювальної атаки – відрізнити "гаму" (4.2), що виробляється за допомогою шифросистеми NTRUCipher від суто випадкової послідовності елементів кільця $R(n,q)$.

За допомогою міркувань, аналогічних наведеним у доведенні теореми 3.26 в [5], неважко переконатися, що у випадку, коли задача Decision NTRUCipher Ciphertext Cracking Problem є обчислювально складною, шифросистема NTRUCipher є CPA-стійкою. Звідси постає природне запитання про оцінки складності розв'зання цієї задачі, які можна використовувати для вибору параметрів шифросистеми NTRUCipher, запропонованій в [1].

Для викладення алгоритму, що пропонується, введемо додаткові позначення.

Зафіксуємо довільну множину A представників усіх суміжних класів групи $R(n,q)^*$ по підгрупі, породженій елементом β. Для заданого розподілу ймовірностей (4.1) (що відрізняється від рівномірного розподілу на полі $\mathbf{Z}_q$) позначимо

$$M = \{z \in \mathbf{Z}_q : p(z) > q^{-1}\}, \ p(M) = \sum_{z \in M} p(z),$$

$$C = 1/2 \cdot (p(M) + |M| q^{-1}), \ D = p(M) - |M| q^{-1}.$$

Алгоритм 4.1.

Вхідні дані: вибірка $\gamma^{(1)},\dots,\gamma^{(t)}$, члени якої розподілені відповідно до однієї з зазначених вище гіпотез H_0, H_1.

1. Обчислити $\xi^{(i)}=\gamma^{(i)}(\beta)$ для кожного $i\in\overline{1,t}$.

2. Для кожного $a\in A$ підрахувати значення $n_a=|\{i\in\overline{1,t}:a\xi^{(i)}\in M\}|$.

Результат: якщо $n_a<Ct$ для кожного $a\in A$, прийняти гіпотезу H_0; інакше – прийняти гіпотезу H_1.

Твердження 4.2. Нехай $\delta\in(0,1/2)$,

$$t=\left\lceil 2D^{-2}\ln\left(\frac{\delta^{-1}(q-1+2n)}{2n}\right)\right\rceil. \tag{4.3}$$

Тоді алгоритм 4.1 дозволяє розрізнити гіпотези H_0 і H_1 із середньою ймовірністю помилки не вище ніж δ, використовуючи $O\left(\left(\frac{q-1}{n}+n\right)t\right)$ операцій над елементами поля $\mathbf{Z}_q$.

Доведення. Позначимо $\eta_{i,a}$ індикатор події $\{a\xi^{(i)}\in M\}$, $i\in\overline{1,t}$. Справедлива рівність $n_a=\eta_{1,a}+\dots+\eta_{t,a}$, $a\in A$.

Нехай є справжньою гіпотеза H_0 і алгоритм 4.1 припускається помилки. Тоді існує елемент $a\in A$ такий, що $\eta_{1,a}+\dots+\eta_{t,a}\ge Ct$. При цьому випадкові величини $\eta_{1,a},\dots,\eta_{t,a}$ є незалежними в сукупності та мають математичне сподівання, що дорівнює $\mathbf{P}(a\gamma^{(i)}(\beta)\in M)=|M|q^{-1}$, $i\in\overline{1,t}$. Отже, на підставі нерівності Гефдінга та означення параметрів C і D

$$\mathbf{P}(\eta_{1,a}+\dots+\eta_{t,a}\ge Ct)=\mathbf{P}\left(\sum_{i=1}^{t}\eta_{i,a}-tq^{-1}|M|\ge t(C-q^{-1}|M|)\right)\le$$

$$\le \exp\left\{-2t(C-q^{-1}\,|\,M\,|)^2\right\}=\exp\left\{-1/2\cdot tD^2\right\}.$$

Таким чином, ймовірність помилки алгоритму 4.1 за умови справедливості гіпотези H_0 не перевищує

$$p_0=|\,A\,|\exp\left\{-1/2\cdot tD^2\right\}=\frac{q-1}{2n}\exp\left\{-1/2\cdot tD^2\right\}. \qquad (4.4)$$

Нехай є справжньою гіпотеза H_1, тобто випадкові величини $\gamma^{(1)},\ldots,\gamma^{(t)}$ розподілені за законом (4.2).

Позначимо g обернений елемент до полінома $f\in R(n,q)^*$ та покладемо $a_0=3g(\beta)$. На підставі формули (4.2) справедлива рівність $\xi^{(i)}=a_0 r^{(i)}(\beta)$, $i\in\overline{1,t}$, де $a_0\neq 0$. При цьому, згідно з означенням множини A існує число $j\in\overline{0,2n-1}$ таке, що $a\overset{\text{def}}{=}(a_0)^{-1}\beta^j\in A$.

Якщо алгоритм 4.1 припускається помилки, то для кожного, а, отже, й для зазначеного вище елемента a виконується нерівність $\eta_{1,a}+\cdots+\eta_{t,a}<Ct$. При цьому випадкові величини $\eta_{1,a},\ldots,\eta_{t,a}$ є незалежними в сукупності та мають математичне сподівання, що дорівнює

$$\mathbf{P}(a\xi^{(i)}\in M)=\mathbf{P}((a_0)^{-1}\beta^j a_0 r^{(i)}(\beta)\in M)=\mathbf{P}(r^{(i)}(\beta)\in M)=p(M),\ i\in\overline{1,t},$$

де передостання рівність випливає з формули (4.1). Звідси на підставі нерівності Гефдінга отримаємо такі нерівності:

$$\mathbf{P}(\eta_{1,a}+\cdots+\eta_{t,a}<Ct)=\mathbf{P}\left(\sum_{i=1}^{t}\eta_{i,a}-tp(M)<t(C-p(M))\right)\le$$

$$\le \exp\left\{-2t(C-p(M))^2\right\} = \exp\left\{-1/2\cdot tD^2\right\}.$$

Таким чином, ймовірність помилки алгоритму 4.1 за умови справедливості гіпотези H_1 не перевищує

$$p_1 = \exp\left\{-1/2\cdot tD^2\right\}. \tag{4.5}$$

З формул (4.4), (4.5) випливає, що середня ймовірність помилки алгоритму 4.1 не перевищує $1/2\cdot(p_0+p_1) = \left(\frac{q-1}{2n}+1\right)\exp\left\{-1/2\cdot tD^2\right\}$, що, в свою чергу, на підставі формули (4.3) є не вище ніж δ.

Нарешті, складність обчислення усіх значень $\xi^{(i)}$, $i\in\overline{1,t}$, за допомогою схеми Руффіні-Горнера на кроці 1 алгоритму 4.1 складає $O(nt)$ арифметичних операцій в полі $\mathbf{Z}_q$ (див., наприклад, [6]), а обчислення усіх значень n_a, $a\in A$, на кроці 2 потребує $O(|A|t) = O\left(\frac{q-1}{2n}t\right)$ операцій. Звідси безпосередньо випливає, що часова складність алгоритму 4.1 дорівнює $O\left(\left(\frac{q-1}{n}+n\right)t\right)$.

Твердження доведено.

В табл. 4.1 наведено оцінки інформаційної складності (4.3) розрізнювальної атаки на шифросистему NTRUCipher для низки значень n і q у випадку, коли розподіл ймовірностей випадкового полінома r визначається згідно з умовою 1) твердження 4.1 (при $dn^{-1} = 1/3$). Для проведення розрахунків використано наступну формулу для розподілу (4.1), яка доводиться аналогічно рівності (3.19):

$$p(z) = q^{-1} \sum_{\alpha \in \mathbf{Z}_q} \cos\left(\frac{2\pi\alpha z}{q}\right) \prod_{i=0}^{n-1} \theta(dn^{-1}, \alpha\beta^i),\ z \in \mathbf{Z}_q, \qquad (4.6)$$

де $\theta(p, x) = 1 - 2p\left(1 - \cos\left(\frac{2\pi x}{q}\right)\right)$ для будь-яких $p \in [0,1],\ x \in \mathbf{Z}_q$.

Таблиця 4.1 – Оцінки інформаційної складності розрізнювальної атаки на шифросистему NTRUCipher ($\delta = 0{,}01$)

$n = 256$				$n = 512$			
q	β	$-\log_2 D$	$\log_2 t$	q	β	$-\log_2 D$	$\log_2 t$
7681	17	33,95	71,79	12289	11	56,09	116,03
10753	11	31,82	67,59	13313	3	56,46	116,77
11777	3	33,88	71,71	15361	7	57,93	119,75
12289	11	33,33	70,62	18433	5	55,35	114,61
13313	3	33,02	70,03	19457	3	59,91	123,75

Як видно з таблиці, при $n = 256$ інформаційна складність атаки змінюється в межах від $2^{67,59}$ до $2^{71,79}$ (при цьому часова складність перевищує інформаційну приблизно в $\frac{q-1}{n} + n$ разів). Зауважимо, що сучасні асиметричні NTRU-подібні шифросистеми [3, 7] характеризуються помітно більшою стійкістю (порядку 2^{-128}) при аналогічних значеннях параметрів q і n. Зазначений факт свідчить про недоцільність використання шифросистеми NTRUCipher для забезпечення конфіденційності інформації в інформаційно-телекомунікаційних системах.

4.2. Наукові основи методу, що пропонується

Нехай n і q – цілі числа такі, що $n, q \geq 2$ і q не ділиться на 3. Як і вище, позначимо $\mathbf{Z}_q$ кільце класів лишків за модулем q, елементи якого

ототожнимо з цілими числами, що належать інтервалу $[-(q-1)/2, (q-1)/2]$ для непарного q та інтервалу $[-q/2, q/2-1]$ для парного q.

Зафіксуємо поліном $f(x) = x^n - c_{n-1}x^{n-1} - \cdots - c_0$ над кільцем $\mathbf{Z}_q$ та позначимо $R_{f,q} = \mathbf{Z}_q[x]/(f(x))$ кільце зрізаних поліномів степеня не вище $n-1$, що складається з q^n поліномів вигляду $u = u_0 + u_1x + \cdots + u_{n-1}x^{n-1}$, де $u_i \in \mathbf{Z}_q$, $i \in \overline{0, n-1}$, які додаються та перемножуються за модулем полінома $f(x)$.

Ототожнимо довільний поліном $u = u_0 + u_1x + \cdots + u_{n-1}x^{n-1} \in \mathbf{R}[x]$ з вектором його коефіцієнтів та позначимо $\| u \|_\infty = \max\limits_{0 \le i \le n-1} | u_i |$, $\| u \|_1 = \sum\limits_{i=0}^{n-1} | u_i |$. Для будь-якого $u = u_0 + u_1x + \cdots + u_{n-1}x^{n-1} \in \mathbf{Z}[x]$ позначимо $u \bmod q$ поліном $(u_0 \bmod q) + (u_1 \bmod q)x + \ldots + (u_{n-1} \bmod q)x^{n-1} \in R_{f,q}$. Аналогічний сенс має позначення $u \bmod 3$.

Зафіксуємо натуральне число d таке, що $2d < n$.

Для заданих чисел n, q, d і полінома $f(x)$ *симетрична NTRU-подібна шифросистема, що пропонується,* визначається таким чином.

Секретними ключами шифросистеми є довільні поліноми $h \in R_{f,q}$ такі, що $\| h \|_\infty = 1$, $\| h \|_1 = 2d$, а відкритими текстами – поліноми $m \in R_{f,q}$ такі, що $\| h \|_\infty = 1$.

Для зашифрування тексту $m \in S$ на ключі h генеруються незалежні випадкові поліноми r, $e_1 = e_{1,0} + e_{1,1}x + \cdots + e_{1,\,n-1}x^{n-1}$ та $e_2 = e_{2,0} + e_{2,1}x + \cdots + e_{2,\,n-1}x^{n-1}$, де r має рівномірний розподіл ймовірностей на кільці $R_{f,q}$, а $e_{1,0}, e_{1,1}, \ldots, e_{1,n-1}, e_{2,0}, e_{2,1}, \ldots, e_{2,n-1}$ є незалежними випадковими величинами, які приймають кожне значення $0, 1, -1$ з імовірністю $1/3$. Далі обчислюється шифрований текст

$$E_h(m,r,e_1,e_2)=(c_1,c_2)=((r-e_1)\bmod q,(m+3(rh+e_2))\bmod q) \qquad (4.7)$$

Розшифрування довільного тексту $c=(c_1,c_2)\in R_{f,q}\times R_{f,q}$ на ключі h здійснюється за формулою

$$D_h(c)=((c_2-3hc_1)\bmod q)\bmod 3. \qquad (4.8)$$

Зауважимо, що у формулах (4.7), (4.8) і далі додавання та множення поліномів здійснюється за модулем полінома $f(x)$.

Отримаємо умову, за якою розшифрування повідомлення (4.7) за формулою (4.8) є коректним.

Позначимо $\theta(f)$ найменше додатне число таке, що $\| ab \|_\infty \le \theta(f) \| a \|_1 \| b \|_\infty$ для будь-яких поліномів $a,b\in \mathbf{R}[x]$ степеня не вище $n-1$, де (згідно з прийнятою вище домовленістю) ab позначає добуток поліномів a і b за модулем полінома $f(x)$ [8].

Помітимо, що на підставі формули (4.7)

$$(c_2-3hc_1)\bmod q=(m+3he_1+3e_2)\bmod q.$$

Звідси випливає, що $D_h(E_h(m,r,e_1,e_2))=m$, якщо $\| m+3he_1+3e_2 \|_\infty < q/2$. При цьому, оскільки

$$\| h \|_1 = 2d,\ \| m \|_\infty = \| e_1 \|_\infty = \| e_2 \|_\infty = 1,$$

то

$$\| m+3he_1+3e_2 \|_\infty \le \| m \|_\infty + 3\theta(f) \| h \|_1 \| e_1 \|_\infty + 3 \| e_2 \|_\infty = 4+6d\cdot\theta(f).$$

Таким чином, за умови

$$d < \frac{q-8}{6 \cdot \theta(f)} \tag{4.9}$$

розшифрування отриманих повідомлень відбувається коректно.

Обґрунтування CPA-стійкості запропонованої шифросистеми.

Нагадаємо означення CPA-стійкості симетричної шифросистеми (див. підрозділ 1.3 або [5]). Розглядається така "гра" між супротивником і дослідником:

1) дослідник генерує секретний ключ k;

2) супротивник може подавати на вхід оракула E_k, що здійснює зашифрування, будь-які відкриті та отримувати відповідні шифровані тексти;

3) супротивник подає досліднику пару різних текстів m_0 та m_1 однакової довжини;

4) дослідник вибирає випадкове рівноймовірне число $b \in \{0,1\}$ та повертає супротивнику шифрований текст $c = E_k(m_b)$;

5) супротивник може звертатися до оракула E_k (як в п. 2)) і повинен відновити значення b.

Шифросистема називається (T, ε)-*CPA-стійкою*, якщо будь-який алгоритм відновлення значення b з імовірністю $\varepsilon > 1/2$ у наведеній "грі" виконує не менше ніж T операцій.

Сформулюємо допоміжне твердження, яке використовується далі для обґрунтування CPA-стійкості запропонованої NTRU-подібної шифросистеми.

Розглянемо довільну симетричну шифросистему з множиною відкритих текстів M, множиною шифрованих текстів C, множиною ключів K, множиною секретних параметрів S та оракулом зашифрування вигляду

$$E_k(m) = G(m) + F_k(s),\ m \in M,\ k \in K, \tag{4.10}$$

де $G: M \to C$ – загальновідома функція; $F_k: S \to C$ – функція, що залежить від секретного ключа k; $+$ позначає комутативну групову операцію на множині C; (невідомий) елемент s вибирається з множини S випадково згідно з певним законом розподілу Γ.

Задача про розрізнення полягає в наступному. Розглядається оракул, який з імовірністю $1/2$ виробляє незалежні випадкові рівноймовірні елементи множини C (гіпотеза H_0) та з такою ж ймовірністю – випадкові елементи вигляду $F_k(s_1), F_k(s_2), \ldots$ для заздалегідь вибраного з множини K (невідомого) випадкового рівноймовірного елемента k та незалежних випадкових елементів $s_1, s_2, \ldots$, розподілених на множині S за законом Γ (гіпотеза H_1). Маючи доступ до зазначеного оракула, треба з'ясувати, яка з двох гіпотез має місце.

Наступна лема доводиться аналогічно теоремі 3.18 в [5].

Лема 4.1. Нехай існує СР-атака, яка використовує t звернень до оракула (4.10), має часову складність T і ймовірність успіху $1/2 + \varepsilon$, де $\varepsilon > 0$. Тоді існує алгоритм, який розв'язує задачу про розрізнення зі складністю не вище ніж $T + \nu t$ та ймовірністю успіху $1/2 \cdot (1 + \varepsilon)$, де ν – максимальна часова складність обчислення одного значення вигляду $G(m) + c$ для будь-яких $m \in M$, $c \in C$.

Важливим окремим випадком задачі про розрізнення є відома *задача Decision-Ring-LWE*, на складності якої базується стійкість багатьох сучасних решіткових криптосистем [2]. В цьому випадку $C = R_{f,q} \times R_{f,q}$, $K = R_{f,q}$, а значення $F_k(s_1), F_k(s_2), \ldots$ формуються за правилом

$$F_k(s_i) = (s_{1,i},\ s_{1,i}k + s_{2,i}), \tag{4.11}$$

де обчислення виконуються в кільці $R_{f,q}$, $s_i = (s_{1,i}, s_{2,i})$ і $s_{1,i}, s_{2,i}$ є незалежними випадковими елементами, першій з яких має рівномірний розподіл ймовірностей на кільці $R_{f,q}$, а другий – певний (відмінний від рівномірного) розподіл на цьому кільці, $i = 1, 2, \ldots$.

Таким чином, задача Decision-Ring-LWE над кільцем $R_{f,q}$ полягає в тому, щоб відрізнити послідовність незалежних випадкових елементів вигляду (4.11) із зазначеним законом розподілу від суто випадкової послідовності елементів множини $C = R_{f,q} \times R_{f,q}$. Зрозуміло, що складність розв'язання цієї задачі залежить від самого кільця, закону розподілу випадкових поліномів $s_{2,i}$, $i = 1, 2, \ldots$, а також від того, який обсяг даних є доступним для аналізу (у випадку, що розглядається, зазначений обсяг вважається потенційно не обмеженим).

Наступне твердження показує, що означена вище симетрична NTRU-подібна шифросистема є CPA-стійкою, якщо є обчислювально складною задача Decision-Ring-LWE для наступних вхідних даних: у формулі (4.11) $k = 3h$, де h є секретним ключем криптосистеми; $s_{2,i} = 3(he_{1,i} + e_{2,i})$ в кільці $R_{f,q}$, де $e_{1,i}, e_{2,i}$ – випадкові поліноми степеня не вище $n-1$ з незалежними в сукупності коефіцієнтами, які приймають кожне значення $0, 1, -1$ з імовірністю $1/3$.

Твердження 4.3. Нехай існує CP-атака, яка використовує t звернень до оракула (4.7), має часову складність T і ймовірність успіху $1/2 + \varepsilon$, де $\varepsilon > 0$. Тоді існує алгоритм, який розв'язує зазначену вище задачу Decision-Ring-LWE зі складністю не вище ніж $T + O(nt \log q)$ та ймовірністю успіху $1/2 \cdot (1 + \varepsilon)$.

Доведення. Помітимо, що шифросистема, що описується рівнянням (4.7), є окремим випадком шифросистеми, яка описується рівнянням (4.10):

треба покласти

$$G(m) = (0, m),\ \ k = 3h,\ s = (r, e_1, e_2),\ F_k(s) = (r - e_1, 3rh + 3e_2),$$

де обчислення виконуються в кільці $R_{f,q}$.

Отже, на підставі леми з існування СР-атаки, зазначеної у формулюванні твердження, випливає існування алгоритму, який розв'язує відповідну задачу про розрізнення зі складністю не вище ніж $T + \nu t$ та ймовірністю успіху $1/2 \cdot (1 + \varepsilon)$, де ν – максимальна часова складність обчислення одного значення вигляду $m + r$ для будь-яких $m, r \in R_{f,q}$. Звідси випливає, що $\nu = O(n \log q)$.

Далі, значення $F_k(s_i) = F_k(r_i, e_{1,i}, e_{2,i})$ має вигляд (4.11), якщо покласти $s_{1,i} = r_i - e_{1,i}$, $s_{2,i} = 3(he_{1,i} + e_{2,i})$, де обчислення виконуються в кільці $R_{f,q}$. Оскільки за означенням шифросистеми r_i є випадковим елементом з рівномірним розподілом ймовірностей на кільці $R_{f,q}$, а $e_{1,i}$ не залежить від r_i, то випадковий елемент $s_{1,i}$ має рівномірний закон розподілу на кільці $R_{f,q}$, і для завершення доведення залишається переконатися в тому, що випадкові елементи $s_{1,i}$, $s_{2,i}$ є незалежними.

Дійсно, позначаючи 3^{-1} обернений до 3 елемент кільця $\mathbf{Z}_q$ (який існує, оскільки q не ділиться на 3) та використовуючи означення випадкових елементів $r_i, e_{1,i}, e_{2,i}$, отримаємо, що для будь-яких $u, v \in R_{f,q}$ справедливі такі рівності:

$$\mathbf{P}(s_{1,i} = u,\ s_{2,i} = v) = \mathbf{P}(r_i - e_{i,1} = u, 3he_{i,1} + 3e_{2,i} = v) =$$

$$= \sum_{w \in R_{f,q}} \mathbf{P}(e_{i,1} = w)\mathbf{P}(r_i = u + w)\mathbf{P}(e_{i,2} = 3^{-1}(v - 3hw)) =$$

$$= \frac{1}{|R_{f,q}|} \sum_{w \in R_{f,q}} \mathbf{P}(e_{i,1} = w)\mathbf{P}(e_{i,2} = 3^{-1}(v - 3hw)),$$

$$\mathbf{P}(s_{1,i} = u)\mathbf{P}(s_{2,i} = v) = \mathbf{P}(r_i - e_{i,1} = u)\mathbf{P}(3he_{i,1} + 3e_{2,i} = v) =$$

$$= \frac{1}{|R_{f,q}|} \sum_{w \in R_{f,q}} \mathbf{P}(e_{i,1} = w)\mathbf{P}(e_{i,2} = 3^{-1}(v - 3hw)) .$$

Таким чином, $\mathbf{P}(s_{1,i} = u,\ s_{2,i} = v) = \mathbf{P}(s_{1,i} = u)\mathbf{P}(s_{2,i} = v)$, що і треба було довести.

Твердження доведено.

4.3. Вибір параметрів запропонованої шифросистеми для забезпечення її стійкості відносно відомих атак

На підставі твердження 4.3 CPA-стійкість запропонованої шифросистеми визначається складністю розв'язання зазначеної вище задачі Decision-Ring-LWE над кільцем $R_{f,q}$, яку (враховуючи оберненість числа 3 за модулем q) можна сформулювати таким чином.

Спостерігається послідовність незалежних випадкових елементів, кожен з яких або є рівномірно розподіленим на множині $R_{f,q} \times R_{f,q}$ (гіпотеза H_0), або має вигляд $(3^{-1}a_i,\ a_i h + (he_{1,i} + e_{2,i}))$, $i = 1, 2, \ldots$, де обчислення виконуються в кільці $R_{f,q}$, h є невідомим фіксованим елементом цього кільця, $\| h \|_\infty = 1$, $\| h \|_1 = 2d$, $a_i, e_{1,i}, e_{2,i}$ є незалежними випадковими елементами, причому a_i має рівномірний розподіл ймовірностей на кільці

$R_{f,q}$, $e_{1,i}, e_{2,i}$ є випадковими поліномами степеня не вище $n-1$ з незалежними в сукупності коефіцієнтами, які приймають кожне значення $0, 1, -1$ з імовірністю $1/3$ (гіпотеза H_1). Треба з'ясувати, яка з двох гіпотез має місце.

Визначимо, як вибирати параметри шифросистеми (числа n, q, d та поліном $f(x)$) для забезпечення належної складності відомих алгоритмів розв'язання наведеної задачі.

Перш за все, зауважимо, що у випадку коли число q має власний дільник $q' > 1$, для розв'язання цієї задачі можна скористатися гомоморфізмом кільця $R_{f,q}$ в кільце $R_{f,q'}$. Останнє має менший порядок, що, в принципі, надає можливість спростити будь-який алгоритм розв'язання поставленої задачі шляхом зведення її до аналогічної задачі меншого розміру над гомоморфним образом вхідного кільця. Аналогічно, якщо у полінома $f(x)$ є нетривіальний дільник $f'(x)$, можна скористатися гомоморфізмом кільця $R_{f,q}$ в кільце $R_{f',q}$ для зведення вхідної задачі до аналогічної задачі меншого розміру. Зауважимо, що при такому зведенні "рівень" спотворення (тобто випадкового елемента $he_{1,i} + e_{2,i}$) збільшиться, але зменшиться розмір вхідної задачі, що може в цілому зменшити складність її розв'язання (див. роботу [9], де наведено приклад суттєвого зменшення складності розв'язання подібної задачі). Для того, щоб в принципі запобігти можливості застосування методу гомоморфізмів, вважатимемо, що q є простим числом, а поліном $f(x)$ є незвідним над полем $\mathbf{Z}_q$. Крім того, якщо число n не є простим, то поле $R_{f,q}$ (для простого q та незвідного $f(x)$) має власне підполе, відмінне від поля $\mathbf{Z}_q$, що також надає можливість застосувати метод гомоморфізмів до розв'язання поставленої задачі (на кшталт того, як це робиться в [10] із застосування функції сліду).

Таким чином, для протидії методу гомоморфізмів, вважатимемо далі, що n і q є різними простими числами, а $f(x)$ – незвідним над полем $\mathbf{Z}_q$ поліномом. Більш того, виходячи з вимоги практичності шифросистеми (можливості швидкого множення елементів поля $R_{f,q}$), вважатимемо, що $f(x)$ має такий саме вигляд, як і в криптосистемі NTRU Prime: $f(x) = x^n - x - 1$ [3].

На сьогодні єдиним відомим методом розв'язання зазначеної вище задачі Decision-Ring-LWE є її зведення до задачі LWE (див., наприклад, [2], п. 5.3). Сутність цього методу полягає в наступному.

По-перше, розглянемо довільні поліноми $u(x) = \sum_{i \geq 0} u_i x^i$, $v(x) = \sum_{i \geq 0} v_i x^i \in R_{f,q}$ та позначимо $w(x) = \sum_{i=0}^{2n-2} w_i x^i$ їхній добуток в кільці $\mathbf{Z}[x]$, $w_i = \sum_{j=0}^{i} u_j v_{i-j}$, $i \in \overline{0,2n-2}$. Тоді, як показує безпосередня перевірка, добуток цих поліномів за модулем полінома $f(x) = x^n - x - 1$ дорівнює $u(x)v(x) = (w_0 + w_n)x^0 + \ + \sum_{i=1}^{n-2}(w_i + w_{i+n} + w_{i+n-1})x^i + (w_{n-1} + w_{2n-2})x^{n-1}$. Отже, вільний член добутку поліномів $u(x)$ та $v(x)$ в полі $R_{f,q}$ дорівнює $(w_0 + w_n) \bmod q = (u_0 v_0 + u_1 v_{n-1} + \cdots + u_{n-1} v_1) \bmod q$.

По-друге, розглянемо послідовність випадкових елементів $(3^{-1} a_i, b_i)$, які є вхідними даними для задачі Decision-Ring-LWE, тобто розподілені відповідно до однієї з двох зазначених вище гіпотез H_0, H_1. Обчислимо вільні члени $b_{i,0}$ поліномів b_i, $i = 1,2,\ldots$. Якщо має місце гіпотеза H_0, тобто b_i є випадковим рівноймовірним елементом поля $R_{f,q}$, що не залежить від a_i, то $b_{i,0}$ є випадковим рівноймовірним елементом поля $\mathbf{Z}_q$, який також не

залежить від a_i. Якщо ж справедлива гіпотеза H_1, тобто $b_i = a_i h + (he_{1,i} + e_{2,i})$, то на підставі зазначеної вище формули для вільного члена добутку двох поліномів у полі $R_{f,q}$, а також рівностей $\| h \|_\infty = 1$, $\| h \|_1 = 2d$ має місце таке співвідношення над полем $\mathbf{Z}_q$:

$$b_{i,0} = a_{i,0}h_0 + a_{i,1}h_{n-1} + \cdots + a_{i,n-1}h_1 + \xi_i, \qquad (4.12)$$

де $\sum_{j=0}^{n-1} a_{i,j}x^j = a_i$, $\sum_{j=0}^{n-1} h_j x^j = h$, ξ_i є сумою $2d+1$ незалежних випадкових величин, які приймають кожне значення $0, 1, -1$ з імовірністю $1/3$ та не залежать від a_i.

Таким чином, за умови гіпотези H_1 вектор коефіцієнтів полінома h є істинним розв'язком системи лінійних рівнянь зі спотвореними правими частинами вигляду (4.12). Отже, для перевірки гіпотез H_0, H_1 достатньо відновити вектор $(h_0, h_{n-1}, \ldots, h_1)$ із зазначеної системи рівнянь за відомими векторами $(a_{i,0}, a_{i,1}, \ldots, a_{i,n-1})$ та значеннями $b_{i,0}$, $i = 1, 2, \ldots$. В цьому полягає один з варіантів задачі LWE над полем $\mathbf{Z}_q$ [11].

На сьогодні відомі такі методи розв'язання зазначеної задачі: метод максимальної правдоподібності [12], метод зустрічі посередині та його вдосконалення [13], [14], метод BKW [15], а також решіткові методи (так звані первинна та дуальна атаки) [16], [17]. Використовуючи відомі алгоритми оцінювання трудомісткості цих методів, що базуються на результатах відзначених робіт, можна обчислити для заздалегідь вибраного рівня стійкості λ значення параметрів n, q, d запропонованої шифросистеми, для яких трудомісткість найкращого із зазначених методів (яка визначає CPA-стійкість цієї шифросистеми) є не менше ніж λ.

Нижче в табл. 4.2 представлено результати чисельних розрахунків, проведених для низки значень n, q і d. Підкреслимо, що за означенням

шифросистеми n і q є різними простими числами такими, що поліном $f(x) = x^n - x - 1$ є незвідним над полем $\mathbf{Z}_q$; d є натуральним числом таким, що $n > 2d$ і $q > 12d + 8$. При цьому стійкість шифросистеми базується на складності задачі LWE, яка полягає у розв'язанні системи лінійних рівнянь зі спотвореними правими частинами від n невідомих над полем $\mathbf{Z}_q$, де істинний розв'язок системи є $(0, 1, -1)$-вектором, який містить точно $2d$ ненульових координат, а спотворення в правій частині кожного рівняння є сумою $2d + 1$ незалежних випадкових величин, які приймають кожне значення $0, 1, -1$ з імовірністю $1/3$.

Нижні оцінки складності алгоритмів розв'язання задачі LWE визначаються таким чином.

1. Метод максимуму правдоподібності (повний перебір): $T_1 = 2^{2d}\binom{n}{2d}$ [12].
2. Удосконалений алгоритм зустрічі посередині: $T_2 = \sqrt[4]{T_1}$ [13, 14].
3. Решіткові алгоритми.

Первинна атака: виконати наступний алгоритм [16, 17].

Алгоритм 4.2: для кожного $m = 1, 2, \ldots$ виконати такі дії:

1) покласти $t = n + m + 1$;
2) знайти найменше $b = b^{(1)}(m) \in \{200, 201, \ldots, t\}$ таке, що

$$(2d+1)\sqrt{\frac{b}{3}} \le \delta^{2b-t} q^{\frac{m}{t}}, \text{ де } \delta = \left((\pi b)^{\frac{1}{b}} \frac{b}{2\pi e}\right)^{\frac{1}{2(b-1)}}$$

та завершити обчислення.

Нижня оцінка складності атаки: $T_3 = 2^{0,292b}$.

Дуальна атака: виконати наступний алгоритм [16, 17].

Алгоритм 4.3: для кожного $m = 1, 2, \ldots$ виконати такі дії:

1) покласти $t = n + m$;

2) знайти найменше число $b = b^{(2)}(m) \in \{200, 201, \ldots, t\}$ таке, що

$$\delta^t q^{\frac{n}{t}} \le \frac{q}{\pi\sqrt{2d+1}} \sqrt{\frac{(c+2)\ln 2}{2}}, \text{ де } \delta = \left((\pi b)^{\frac{1}{b}} \frac{b}{2\pi e} \right)^{\frac{1}{2(b-1)}}, \; c = 8$$

та завершити обчислення.

Нижня оцінка складності атаки: $T_4 = 2^{0,292b + 2c}$.

4. BKW-атака. Розрахунки проводяться згідно з твердженнями 3.2, 3.3 (див. підрозділ 3.2), де у формулі (3.14) слід покласти $\pi(\alpha) = \theta(1/3, \alpha)^{2d+1}$.

Таблиця 4.2 – Двійкові логарифми нижніх оцінок складності відомих атак на запропоновану шифросистему

Параметри			ММП	Зустріч посередині	Первинна атака	Дуальна атака	BKW-атака
n	q	d					
439	6833	142	690,6	172,7	490,9	329,0	501,3
503	2879	59	508,8	127,2	505,5	419,8	545,6
503	8663	67	549,9	137,5	388,1	309,5	571,9
569	3929	81	647,6	161,9	594,8	476,2	618,5
607	6317	131	855,9	213,9	672,2	495,2	669,4
631	2081	43	444,0	111,0	610,9	573,7	658,3
631	2693	56	533,1	133,3	632,8	560,9	667,2
677	3251	67	615,2	153,8	691,7	599,9	717,5
727	5827	121	904,27	226,1	798,1	623,1	786,1
787	4243	88	774,6	193,6	832,2	705,7	833,1
829	1657	34	402,9	100,7	777,3	821,6	832,5
883	8089	168	1177,1	294,3	1005,4	768,5	952,2
947	3917	81	782,3	195,6	990,8	890,2	982,75
991	9349	194	1339,8	334,9	1145,8	873,9	1064,9
1019	6691	139	1134,4	283,6	1136,2	929,9	1077,1
1021	5393	112	993,9	248,5	1110,8	949,5	1068,7
1021	8819	183	1321,9	330,5	1172,9	910,4	1091,9

Як видно з табл. 4.2, для забезпечення стійкості на рівні $\lambda = 2^{128}$ достатньо вважати $n = 631,\ q = 2693,\ d = 56$, а для забезпечення стійкості на

рівні $\lambda = 2^{256}$ достатньо вважати $n = 883$, $q = 8089$, $d = 168$. При таких значеннях вхідних параметрів час зашифрування чи розшифрування повідомлень у запропонованих шифросистемах є порівняним з відповідним часом у криптосистемі NTRU Prime [3], яка є одним з фіналістів конкурсу NIST зі створення нових постквантових криптографічних стандартів.

Висновки

1. Першим науковим результатом розділу є аналітична оцінка складності розрізнювальної атаки на шифросистему NTRUCipher над круговим кільцем за модулем полінома $x^n + 1$, де n – степінь двійки. З отриманої оцінки випливає, зокрема, що при $n = 256$ інформаційна складність атаки змінюється в межах від $2^{67,59}$ до $2^{71,79}$ (при цьому часова складність перевищує інформаційну приблизно в $\frac{q-1}{n} + n$ разів; див. табл. 4.1). Оскільки сучасні асиметричні NTRU-подібні шифросистеми [3, 7] характеризуються помітно більшою стійкістю (порядку 2^{128}) при аналогічних значеннях параметрів q і n, то отриманий результат свідчить про недоцільність застосування шифросистеми NTRUCipher на практиці.

2. Другим (та основним) науковим результатом цього розділу є метод побудови обґрунтовано стійких симетричних NTRU-подібних шифросистем. Цей метод запропоновано вперше. Його сутність полягає у використанні для зашифрування і розшифрування перетворень, що визначаються за формулами (4.7) і (4.8) відповідно. Показано, що на відміну від NTRUCipher та NTRUCipher+, запропоновані шифросистеми мають обґрунтовану стійкість відносно атак на основі підібраних відкритих повідомлень, яка базується на складності еталонної обчислювально складної задачі Decision-Ring-LWE.

3. Для вибору параметрів n, q і d, що забезпечують стійкість запропонованих шифросистем на заздалегідь вибраному рівні λ, можна використовувати відомі методи оцінювання складності зазначеної задачі. Результати чисельних розрахунків свідчать про те, що для забезпечення стійкості на рівні $\lambda = 2^{128}$ достатньо вважати $n = 631,\ q = 2693,\ d = 56$, а для забезпечення стійкості на рівні $\lambda = 2^{256}$ достатньо вважати $n = 883$, $q = 8089$, $d = 168$. При таких значеннях вхідних параметрів час зашифрування чи розшифрування повідомлень у запропонованих шифросистемах є порівняним з відповідним часом у криптосистемі NTRU Prime, яка є одним з фіналістів конкурсу NIST зі створення нових постквантових криптографічних стандартів.

Список використаних джерел у четвертому розділі

1. Valluri M. R. NTRUCipher-lattice based secret key encryption. 2017. DOI: https://doi.org/10.48550/arXiv.1710.01928.

2. Lyubashevsky V., Peikert C., Regev O. On Ideal Lattices and Learning with Errors over Rings. *Journal of the ACM*. 2013. Vol. 60, no. 6. P. 1–35. DOI: https://doi.org/10.1145/2535925.

3. NTRU Prime: Reducing Attack Surface at Low Cost / D. J. Bernstein et al. *Selected Areas in Cryptography – SAC 2017*. Cham, 2017. P. 235–260. DOI: https://doi.org/10.1007/978-3-319-72565-9_12.

4. Лидл Р., Нидеррайтер Г. Конечные поля: В 2-х т. Т. 2 : монографія. Москва : Мир, 1988. 818 с.

5. Lindell Y., Katz J. Introduction to Modern Cryptography. Taylor & Francis Group, 2020. 628 p.

6. Черемушкин А. В. Лекции по арифметическим алгоритмам в криптографии. Москва : МЦНМО, 2002. 104 с.

7. Lyubashevsky V., Seiler G. NTTRU: Truly Fast NTRU Using NTT. *IACR Transactions on Cryptographic Hardware and Embedded Systems*. 2019. P. 180–201. DOI: https://doi.org/10.46586/tches.v2019.i3.180-201.

8. Lyubashevsky V., Towards Practical Lattice-Based Cryptography, Ph.D. Theses, Univ. of California, San Diego. 2008.

9. Ihnatenko S. M. Security Estimates of a Ring-Lwe Symmetric Cryptosystem Against Chosen Plaintext Attack. *Cybernetics and Systems Analysis*. 2020. DOI: https://doi.org/10.1007/s10559-020-00248-3.

10. Alekseychuk A. N., Poremskyi M. V. A general scheme for design of correlation attacks on SNOW 2.0-like stream ciphers. *Legal, regulatory and metrological support of information security system in Ukraine*. 2018. No. 1 (32). P. 70–79.

11. Regev O. On lattices, learning with errors, random linear codes, and cryptography. *Proc. the 37th Annual ACM Symposium on Theory of Computing,* Baltimore, USA. 2005. P. 84–93.

12. Олексійчук А. М., Ігнатенко С. М., Поремський М. В. Системи лінійних рівнянь зі спотвореними правими частинами над скінченними кільцями. *Математичне та комп'ютерне моделювання. Серія: технічні науки.* 2017. № 15. С. 150–155. DOI: https://doi.org/10.32626/2308-5916.2017-15.150-155.

13. May A. How to Meet Ternary LWE Keys. *Advances in Cryptology – CRYPTO 2021*. Cham, 2021. P. 701–731. DOI: https://doi.org/10.1007/978-3-030-84245-1_24.

14. Kirshanova E., May A. How to Find Ternary LWE Keys Using Locality Sensitive Hashing. *Cryptography and Coding*. Cham, 2021. P. 247–264. DOI: https://doi.org/10.1007/978-3-030-92641-0_12.

15. Blum A., Kalai A., Wasserman H. Noise-tolerant learning, the parity problem, and the statistical query model. *Journal of the ACM*. 2003. Vol. 50, no. 4. P. 506–519. DOI: https://doi.org/10.1145/792538.792543.

16. Post-quantum key exchange - a new hope / E. Alkim et al. *Cryptology ePrint Archive*. URL: https://eprint.iacr.org/2015/1092 (дата звернення: 05.05.2023).

17. Frodo: Take off the ring! Practical, Quantum-Secure Key Exchange from LWE / J. Bos et al. *Cryptology ePrint Archive*. URL: https://eprint.iacr.org/2016/659 (дата звернення: 05.05.2023).

ВИСНОВКИ

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.

Аналіз існуючих публікацій показує, що 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 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 дисертаційній роботі розв'язано **актуальну наукову задачу** розробки методу побудови симетричних NTRU-подібних шифросистем, що є обґрунтовано стійкими відносно атак на основі підібраних відкритих текстів.

Для розв'язання поставленої наукової задачі **використано методи** теорії скінченних полів, теорії дискретного перетворення Фур'є на скінченних абелевих групах, лінійної алгебри, теорії ймовірностей та кореляційного

криптоаналізу. Чисельні розрахунки на обчислювальній системі виконувалися з використанням інтегроване середовище розробки PyCharm (мова програмування Python) з процесором 12th Gen Intel(R) Core(TM) i5-1235U 1.30 GHz та обсягом оперативної пам'яті 16 ГБ.

Основні наукові та практичні результати, отримані в дисертації.

1. *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.

2. *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.

3. *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).

4. *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.

Достовірність результатів дисертаційної роботи забезпечується адекватністю припущень, які лежать в основі проведених наукових досліджень, а також коректним застосуванням відомих математичних методів. Результати проведених чисельних розрахунків узгоджуються з отриманими теоретичними висновками.

Значення наукових результатів дисертації для теорії полягає в тому, що вони утворюють наукову основу для вирішення задачі побудови симетричних NTRU-подібних шифросистем, які є обґрунтовано стійкими відносно атак на основі підібраних відкритих текстів.

Практичне значення роботи. 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 $R_{n.q}$ (з 0,5 до $1{,}5\cdot 10^{-2}$) 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 $2^{15} \div 2^{69}$ 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 λ (зокрема $n = 631$, $q = 2693$, $d = 56$ при $\lambda = 2^{128}$, $n = 883$, $q = 8089$, $d = 168$ при $\lambda = 2^{256}$).

Висновки та рекомендації по науковому та практичному використанню наукових результатів.

1. Для підвищення ймовірності оборотності випадкового полінома, що використовується в ролі (частини) секретного ключа NTRU-подібної шифросистеми, доцільно вибирати параметр q, який є великим простим числом, на відміну від розповсюдженого варіанту $q = 2^l$. Зокрема, при $q = 2^l$ ймовірність необоротності випадкового полінома не перевищує $1{,}5 \cdot 10^{-2}$, що суттєво менше ніж значення ймовірності 0,5 при виборі в якості q великого простого числа.

2. Отримані аналітичні оцінки ймовірності помилкового розшифрування повідомлень для шифросистеми NTRUEncrypt надають більш адекватну інформацію про частоту виникнення помилок. Зі збільшенням параметра d спостерігається збільшення ймовірності помилкового розшифрування повідомлень, проте для рекомендованих значень вхідних параметрів шифросистеми ця ймовірність не перевищує 2^{-80} для будь-якого фіксованого ключа.

3. Розроблений алгоритм обчислення значень параметра $\theta(f)$ (що характеризує величину sup-норми добутку елементів кільця зрізаних

поліномів за модулем заданого унітарного полінома $f(x)$) надає змогу на практиці оцінювати ймовірність помилкового розшифрування повідомлень для довільної NTRU-подібної шифросистеми над кільцем R_f при фіксованому ключі.

4. Трудомісткість BKW-атаки на шифросистему NTRUCipher+ є в $2^{15} \div 2^{69}$ разів вище ніж на шифросистему NTRUCipher. При фіксованих значеннях параметрів n, d шифросистеми зі збільшенням значення q трудомісткість BKW-атаки повільно зростає. Зокрема, при $(n,d) = (1171,106)$ нижня оцінка трудомісткості BKW-атаки на NTRUCipher змінюється від 2^{1135} до 2^{1176} операцій, в той час як нижня оцінка трудомісткості цієї атаки на NTRUCipher+ змінюється від 2^{1206} до 2^{1241} операцій (в залежності від значення q, яке для шифросистеми NTRUCipher+ є майже у 3 рази більше). При цьому обидві шифросистеми характеризуються майже однаковими верхніми межами ймовірності помилки розшифрування.

5. Для підвищення стійкості шифросистеми NTRUCipher відносно BKW-атаки недоцільно використовувати доданок e у формулі (3.1), оскільки це збільшує рівень спотворень у правих частинах рівнянь системи (3.9), що призводить до збільшення верхньої межі ймовірності помилки розшифрування. Це має негативний вплив на практичність шифросистеми NTRUCipher+ в порівнянні з NTRUCipher та свідчить про недоцільність використовувати NTRUCipher+ для підвищення стійкості шифросистеми NTRUCipher відносно BKW-атаки.

6. Шифросистема NTRUCipher+ над кільцем $R_{n,q}$ є вразливою до розрізнювальної атаки, спрямованої на те, щоб відрізнити послідовність шифрованих повідомлень шифросистеми від суто випадкової послідовності елементів цього кільця. Зазначена атака може бути реалізована в режимі реального часу. Зокрема, найбільше (з розрахованих; див. табл. 3.5) значення складності атаки досягається при $n = 401,\ q = 139$ і становить порядку $t = 2^{19}$

двійкових операцій.

7. Аналітичні оцінки складності розрізнювальної атаки на шифросистему NTRUCipher над круговим кільцем за модулем полінома x^n+1, де n – степінь двійки, демонструють недоцільність застосування цієї шифросистеми на практиці. При $n=256$ інформаційна складність атаки змінюється в межах від $2^{67,59}$ до $2^{71,79}$, в той час як сучасні асиметричні NTRU-подібні шифросистеми характеризуються помітно більшою стійкістю (порядку 2^{128}) при аналогічних значеннях параметрів q і n.

8. Для забезпечення стійкості запропонованих шифросистем на рівні $\lambda=2^{128}$ достатньо вважати $n=631,\ q=2693,\ d=56$, а для забезпечення їхньої стійкості на рівні $\lambda=2^{256}$ достатньо вважати $n=883,\ q=8089,\ d=168$. При таких значеннях вхідних параметрів час зашифрування чи розшифрування повідомлень у запропонованих шифросистемах є порівняним з відповідним часом у криптосистемі NTRU Prime, яка є одним з фіналістів конкурсу NIST зі створення нових постквантових криптографічних стандартів.

9. Написані здобувачкою комп'ютерні програми надають змогу в режимі реального часу обчислювати значення параметрів для побудови запропонованих обґрунтовано стійких NTRU-подібних шифросистем. Ці програми можуть бути використані у подальших дослідженнях зазначених шифросистем як розробниками, так і фахівцями в галузі криптоаналізу.

10. Основні наукові та практичні результати дисертаційної роботи реалізовані в НДР "Дорадо" та НДР "Сарган", що виконувалися на замовлення Служби зовнішньої розвідки України, а також у науково-технічних розробках АТ "Інститут інформаційних технологій". Подальший розвиток наукових ідей та методів, які лежать в основі дисертаційного дослідження, є актуальним напрямом в галузі кібербезпеки та захисту інформації.

ДОДАТКИ

ДОДАТОК А

Програмний код алгоритму знаходження параметру $\theta(f)$

Програмна реалізація виконана на комп'ютері 12th Gen Intel(R) Core(TM) i5-1235U 1.30 GHz та обсягом оперативної пам'яті 16 ГБ. Мова програмування – Python. Середовище розробки – PyCharm.

```
# Значення параметра θ(f) для поліномів f(x) = x^n ± x^k ±1 при n = 100
import numpy as np
n=100

for k in range(n):
    def pidf(x):
        x[n-1][0] = 1
        x[n-1][k]= 1
        #x[n - 1][1] = -1
    zeors_array = np.zeros( (n, n) )

    #print(zeors_array)

    for i in range(n-1):
        zeors_array[i][i+1]=1
    #print(zeors_array)
    pidf(zeors_array)
    #print(zeors_array)
    a = np.zeros( (n, n) )
    for i in range(n):
        a+= abs(np.linalg.matrix_power(zeors_array,i))
    k1=a
    #print(k)
    print(k1.max(),f'k={k}')

# Алгоритм обчислення параметру θ(f) та чисельні оцінки верхніх меж ймовірності помилкового розшифрування повідомлень в NTRU-подібних криптосистемах
import numpy as np
n=int(100)
def pidf(x):
    x[0] = 1
    x[int(90)] = -1
al=[]
for k in range(n):
    zeors_array = np.zeros((n * 2, n))
    for i in range(n):
        zeors_array[(i+k)%n][i] = 1
    koev = np.zeros(n)
    pidf(koev)
    print(f'Коефициенты:\n{koev}')
```

```
    print(f'Значення що вийшли x: \n {zeors_array}' )

    for i in range(n):
        k=np.zeros(n)
        for j in range(n):
            k+=zeors_array[j+i]*koev[j]
        #k=koev*zeors_array[i]
        zeors_array[i+n, :]=k
    print(zeors_array)
    zeors_array=abs(zeors_array)

    g=[]
    for i in range(n*2):
        g.append(np.sum(zeors_array[i]))
    print(f'Сума стр{g}')
    print(f'Максимальне значення{max(g)}')

    al.append(max(g))
print(f'Відповідь{max(al)}')

# Чисельні оцінки верхніх меж ймовірності помилкового розшифрування повідомлень в NTRU-подібних криптосистемах через параметр θ(f)
import math
from decimal import Decimal
n=761
q=4591
f=2
n=Decimal(n)
q=Decimal(q)
f=Decimal(f)
p=Decimal(2)*Decimal(n)*Decimal.exp(-(Decimal(q-
2)**2)/Decimal(144)/Decimal(n)/(f**2))
plog=Decimal.log10(Decimal(p))/Decimal.log10(Decimal(2))
print(p)
print(-plog)
```

ДОДАТОК Б

Програмний код алгоритму дослідження стійкості шифросистем NTRUCipher та NTRUCipher+ відносно певних статистичних атак

Програмна реалізація виконана на комп'ютері 12th Gen Intel(R) Core(TM) i5-1235U 1.30 GHz та обсягом оперативної пам'яті 16 ГБ. Мова програмування – Python. Середовище розробки – PyCharm.

```
# Ймовірність помилки розшифрування NTRUCipher+
import math
from math import sqrt

n = int(input('Введіть ваше просте число n'))
a1 = int(input('Введіть проміжок от '))
a2 = int(input('Введіть проміжок до '))
answer=[]#відповідь
a=[]#прості числа
kp=[]
def prostie(a1,a2):  #заповнення масиву простими числами
    for k in range(a1, a2):
        prime = True
        for i in range(2, k):
            if k % i == 0:
                prime = False
                break
        if prime:
            a.append(k)
def nearest(lst, target):#наближений елемент
  return min(lst, key=lambda x: abs(x-target))
def proga(n):
    Ans = []
    a= []
    Z=n-1;
    k21= []
    vid= []
    ki=[]
    def is_prime(n): #перевірка на простоту
        if n < 2:
            quit(2)
        if n == 2:
            print()
        limit = sqrt(n)
        i = 2
        while i <= limit:
            if n % i == 0:
                quit(2)
            i += 1
    def prostie(N): #заповнення масиву простими числами
        for k in range(2, N + 1):
            prime = True
            for i in range(2, k):
                if k % i == 0:
```

```
                prime = False
                break
        if prime:
            a.append(k)

def gcd(a, b): #перевірка на кратність
    while a != b:
        if a > b:
            a = a - b
        else:
            b = b - a
    return a;

def Factor(n):#розклад числа
    d = 2
    while d * d <= n:
        if n % d == 0:
            Ans.append(d)
            n //= d
        else:
            d += 1
    if n > 1:
        Ans.append(n)


is_prime(n)
Factor(Z)
#print(Ans)#масив дільників
prostie(n)
#print(a)#масив простих
gg=[]#масив для створення елементів

for k1 in range(len(a)):
    for k2 in range(len(Ans)):
        k123 = Z/Ans[k2]
        k123=int(k123)
        el=a[k1] ** k123
        k21.append(el)
    #print(k21)-масив числа в степені для перевірки
    for i in range(0,len(k21)):
        if k21[i]%n == 1:
            gg=[]
            k21=[]
            break
        else:
            gg.append(a[k1])
    #print(gg)
    if gg != []:
        break

k211=int(gg[0])#
#print(k211)

for i in range(1,Z):
    n=int(n)
    i=int(i)
    e=int(gcd(Z,i))
    if e == 1:
        ki.append(i)
#print(ki)
```

```
    for i in range(len(ki)):
       answer.append((k211 ** ki[i])%n)
    answer.sort()
    #print(answer)
    return answer

prostie(a1,a2)
proga(n)
print(a)
print(answer)
for i in range(len(a)):
    e=0
    e= int(int(a[i])%n)
    for i2 in range(len(answer)):
        if e == answer[i2]:
            kp.append(a[i])
            break
print(kp)
d=int(input('Введіть d'))
for i in range(len(kp)):
    p=2*n*math.exp(-((kp[i]-8)**2)/(72*(2*d+1)))
    pn = 2 * n * math.exp(-((kp[i] - 8) ** 2) / (72 * (20 * d + 1)))
    p1 = -math.log2(pn)
    print('q=', kp[i], '1=', p1)

# Оцінки ефективності BKW-атаки на шифросистему NTRUCipher+
import math
from math import sqrt
from decimal import Decimal
for safas in range(10000):
    delta=float(0.01)
    F=1
    n=449
    d=134
    q=int(input('Введіть q '))
    n1=[]
    u=[]
    v=[]
    k1=[]
    l=[]
    t=[]
    delpk1=0
    N=[]
    T=[]

    def is_prime(n):  # перевірка на простоту
        if n < 2:
            quit(2)
        if n == 2:
            print()
        limit = sqrt(n)
        i = 2
        while i <= limit:
            if n % i == 0:
                quit(2)
            i += 1
    is_prime(n)

    for i in range (1,n-2):
        n1.append(i)
```

```
    for i in range(len(n1)):
        k=math.log2(n-n1[i])/2
        u.append(k)

    for i in range(len(n1)):
        kg=(2*(n-n1[i])/math.log2(n-n1[i]))
        v.append(kg)

    for i in range(len(u)):
        k1.append(pow(2,u[i]-1))

    def teta(p,x):
        return 1-2*p*(1-math.cos(2*math.pi*x/q))
    pa=[]
    if F == 0:
        for a in range(q):
            pa.append(teta(d/n,a)*teta(1/3,a)*(teta(1/3,3*a)**(2*d)))

    elif F ==1:
        for a in range(q):
            pa.append(teta(d/n,a)*teta(1/3,2*a)*(teta(1/3,3*a)**(2*d-1)))

    elif F==-1:
        for a in range(q):
            pa.append(teta(d/n,a)*teta(1/3,4*a)*(teta(1/3,3*a)**(2*d-1)))

    prov=[]
    for i in range(len(k1)):
        for i2 in range(len(pa)):
            delpk1=+ math.fabs(pa[i2])**(2*k1[i])
        prov.append(delpk1)
        delpk1=0

    for i in range(len(n1)):
        t.append(float(((1-
delta/2)*n1[i]*math.log2(3)+((delta/2)*math.log2(delta/2))+((1-delta/2)*math.log2(1-
delta/2)))/prov[i]))
    #print('t:',t)

    for i in range(len(n1)):
        t[i]=Decimal(t[i])
        q=Decimal(q)
        u[i]=Decimal(u[i])
        delta=Decimal(delta)
        v[i]=Decimal(v[i])
        l.append(((u[i] + Decimal(math.log1p(Decimal(2) * t[i] / delta)) -
Decimal(1)) * (q ** v[i])))

    for i in range(len(n1)):
        N.append(l[i]*t[i])
    #print('N:',N)

    for i in range(len(n1)):
        n1[i]=Decimal(n1[i])
        t[i]=Decimal(t[i])
        q=Decimal(q)
        l[i]=Decimal(l[i])
        t[i]=Decimal(t[i])
        u[i]=Decimal(u[i])
        T.append((2*n1[i]*t[i]*3**(n1[i]))+u[i]*l[i]*t[i])
    print('T:',T)
```

```
    Nlog=[]
    Tlog=[]
    for i in range(len(n1)):
        Nlog.append(Decimal.log10(N[i])/Decimal.log10(Decimal(2)))
        Tlog.append(Decimal.log10(T[i])/Decimal.log10(Decimal(2)))
    print('log(T):',Tlog)
    #print('log(N):',Nlog)

    print('Minimalnoe T is :',min(Tlog))
    print('Minimalnoe N is :',Nlog[Tlog.index((min(Tlog)))])
    print(('N1 is: '),n1[Tlog.index(min(Tlog))])
# Оцінки ефективності BKW-атаки на шифросистему NTRUCipher
import math
from math import sqrt
from decimal import Decimal
import numpy as np
kp = []

def zapq():
    n=401
    a1 = int(input('Введите промежуток от '))
    a2 = int(input('Введите промежуток до '))
    answer = []  # відповідь
    a = []  # прості числа


    def prostie(a1, a2):  #заповнення масиву простими числами
        for k in range(a1, a2):
            prime = True
            for i in range(2, k):
                if k % i == 0:
                    prime = False
                    break
            if prime:
                a.append(k)

    def nearest(lst, target):
        return min(lst, key=lambda x: abs(x - target))

    def proga(n):
        Ans = []
        a = []
        Z = n - 1;
        k21 = []
        vid = []
        ki = []

        def is_prime(n):  #перевірка на простоту
            if n < 2:
                quit(2)
            if n == 2:
                print()
            limit = sqrt(n)
            i = 2
            while i <= limit:
                if n % i == 0:
                    quit(2)
                i += 1

        def prostie(N):  #заповнення масиву простими числами
            for k in range(2, N + 1):
```

```
        prime = True
        for i in range(2, k):
            if k % i == 0:
                prime = False
                break
        if prime:
            a.append(k)

def gcd(a, b):  #перевірка на кратність
    while a != b:
        if a > b:
            a = a - b
        else:
            b = b - a
    return a;

def Factor(n):  #розклад числа
    d = 2
    while d * d <= n:
        if n % d == 0:
            Ans.append(d)
            n //= d
        else:
            d += 1
    if n > 1:
        Ans.append(n)

is_prime(n)
Factor(Z)
prostie(n)
gg = []  #масив для створюваних елементів

for k1 in range(len(a)):
    for k2 in range(len(Ans)):
        k123 = Z / Ans[k2]
        k123 = int(k123)
        el = a[k1] ** k123
        k21.append(el)
    # print(k21)-масив числа в степені для перевірки
    for i in range(0, len(k21)):
        if k21[i] % n == 1:
            gg = []
            k21 = []
            break
        else:
            gg.append(a[k1])
    # print(gg)
    if gg != []:
        break

k211 = int(gg[0])

for i in range(1, Z):
    n = int(n)
    i = int(i)
    e = int(gcd(Z, i))
    if e == 1:
        ki.append(i)

for i in range(len(ki)):
    answer.append((k211 ** ki[i]) % n)
```

```
        answer.sort()
        return answer

    prostie(a1, a2)
    proga(n)
    print(a)
    print(answer)
    for i in range(len(a)):
        e = 0
        e = int(int(a[i]) % n)
        for i2 in range(len(answer)):
            if e == answer[i2]:
                kp.append(a[i])
                break
    print(kp)
zapq()
print(kp)

for i in range(len(kp)):
    print('q is',kp[i])
    q=kp[i]
    n=401
    d=113
    #q=1543
    n1=[]
    u=[]
    v=[]
    k1=[]
    delta=0.01
    F=1
    l=[]
    def is_prime(n):  # перевірка на простоту
        if n < 2:
            quit(2)
        if n == 2:
            print()
        limit = sqrt(n)
        i = 2
        while i <= limit:
            if n % i == 0:
                quit(2)
            i += 1
    is_prime(n)

    for i in range (1,n-2):
        n1.append(i)
    for i in range(len(n1)):
        k=math.log2(n-n1[i])/2
        u.append(k)
    for i in range(len(n1)):
        kg=(2*(n-n1[i])/math.log2(n-n1[i]))
        v.append(kg)
    for i in range(len(u)):
        k1.append(pow(2,u[i]-1))

    def teta(p,x,q):
        p=float(p)
        x=float(x)
        q=float(q)
        return 1-2*p*(1-math.cos(2*math.pi*x/q))
    pa=[]#F=0
```

```
    if F == 0:
        for a in range(q):
            pa.append(teta(d/n,a,q)*teta(1/3,a,q)*(teta(1/3,3*a,q)**(2*d)))

    elif F ==1:
        for a in range(q):
            pa.append(teta(d/n,a,q)*teta(1/3,2*a,q)*(teta(1/3,3*a,q)**(2*d-1)))

    elif F==-1:
        for a in range(q):
            pa3.append(teta(d/n,a,q)*teta(1/3,4*a,q)*(teta(1/3,3*a,q)**(2*d-1)))
#    print('p(a):',pa)
    prov=[]
    for i in range(len(k1)):
        for i2 in range(len(pa)):
            delpk1=+ math.fabs(pa[i2])**(2*k1[i])
        prov.append(delpk1)
        delpk1=0
#    print("delta p v ster k:",prov)
    t=[]
    for i in range(len(n1)):
        t.append(float(((1-
delta/2)*n1[i]*math.log2(q)+((delta/2)*math.log2(delta/2))+((1-delta/2)*math.log2(1-
delta/2)))/prov[i]))

    for i in range(len(n1)):
        t[i]=Decimal(t[i])
        q=Decimal(q)
        u[i]=Decimal(u[i])
        delta=Decimal(delta)
        v[i]=Decimal(v[i])
        l.append(((u[i] + Decimal(math.log1p(Decimal(2) * t[i] / delta)) -
Decimal(1)) * (q ** v[i])))

    q=int(q)

    k1=np.array(k1)

    def f(x, y):
        i = np.arange(0, q).reshape((1, 1, q))
        a=np.sum((np.cos(2*np.pi*i*x/q)*(np.fabs((1 - 2 * d/n * (1 - np.cos(2 * np.pi
* i / q))))**y)),axis=0)
        return a/q
    X = np.arange(0, q)
    Y = k1
    plane = np.array(np.meshgrid(X, Y))

    g=f(*plane)
    ge=g*q
    ge[ge<=0]=0.000000000000000001
    g1=np.log2(ge)
    g12=g1*g
    dpw=np.sum(g12,axis=1,dtype=float)
    dwp=-1/q*np.sum(g1,axis=1)

    ksa=g[g>0]
    pkmax=g.max()
    pkmin=ksa.min()

    list(dpw)
    list(dwp)
```

```
    t0=[]
    for i in range(len(dpw)):
        t0.append(((2*n1[i]*math.log1p(6/delta)*(math.log2(pkmax)-
math.log2(pkmin))**2))/((dpw[i]+dwp[i])**2))
    n0=[]
    for i in range(len(t0)):
        t0[i]=Decimal(t0[i])
        n0.append(l[i]*t0[i])
    T0=[]

    for i in range(len(t0)):
        q = Decimal(q)
        u[i] = Decimal(u[i])
        T0.append((2*n1[i]*t0[i]*3**(n1[i]))+u[i]*l[i]*t0[i])
    Nlog=[]
    Tlog=[]
    for i in range(len(n1)):
        Nlog.append(Decimal.log10(n0[i])/Decimal.log10(Decimal(2)))
        Tlog.append(Decimal.log10(T0[i])/Decimal.log10(Decimal(2)))


    print('Minimalnoe T is :',min(Tlog))
    print('Minimalnoe N is :',Nlog[Tlog.index((min(Tlog)))])
    print(('N1 is: '),n1[Tlog.index(min(Tlog))])
    if min(Tlog) < 512:
        print()
    else:
        break

# Оцінки тривіальної атаки на шифросистему NTRUCipher
import math
from math import sqrt
from decimal import Decimal
import numpy as np
n=743
d=247
q=2969
delta=0.01
a=[]
def factorial(n):
    factorial = 1
    for i in range(2, n + 1):
        factorial *= i
    return factorial

for z in range(q):
    i = np.arange(0, q)
    p1z=1/q*np.sum(np.cos(2*np.pi*z*i/q)*(1 - 2 * d/n *(1 - np.cos(2 * np.pi * i /
q))))
    a.append(float(p1z))
#print(a)

dpw=0
for i in range(len(a)):
    if a[i]>0:
        dpw=dpw+math.log2(a[i]*q)*a[i]
#print(dpw)
dwp=0
perem=0
for i in range(len(a)):
    if a[i]>0:
```

```
        perem=perem+math.log2(a[i]*q)
dwp=-perem/q
#print(dwp)
k1min=(min([i for i in a if i > 0]))
k1max=(max(a))
t0=(((2*n*math.log1p(3/delta)*(math.log2(k1max)-
math.log2(k1min))**2))/((dwp+dpw)**2))
comb=Decimal(Decimal(factorial(n))/Decimal(factorial(d))/Decimal(factorial(n-
d))*Decimal(factorial(n-d))/Decimal(factorial(d))/(Decimal(factorial(n-2*d))))
#print(comb)
logTTm=comb=Decimal.log10(comb)/Decimal.log10(Decimal(2))+Decimal.log10(Decimal(t0*n)
)/Decimal.log10(Decimal(2))+Decimal(1)
print(logTTm)

# Оцінки складності розрізнювальної атаки на шифросистему NTRUCipher+
import math
import numpy
import numpy as np
from math import sqrt
from decimal import Decimal
for safas in range(10000):
    delta=float(0.01)
    n=401
    q=int(input('Введите q '))
    delt1=0

    def is_prime(n):  # перевірка на простоту
        if n < 2:
            quit(2)
        if n == 2:
            print()
        limit = sqrt(n)
        i = 2
        while i <= limit:
            if n % i == 0:
                quit(2)
            i += 1
    is_prime(n)

    def teta(p,x):
        return 1-2*p*(1-math.cos(2*math.pi*x/q))
    pa=[]

    for i in range(1,q):
        pa.append(((teta(1/3,i))**(2*n))*((teta(1/3,3*i))**(2*n)))
    print('p(a):',pa)

    pa=numpy.array(pa)
    delt1=numpy.sum(pa)
    print('delt1:', delt1)

    t=((8*q*math.log1p(1/delta))/(delt1))
    t=math.ceil(t)
    print('t:', math.log2(t))

# Оцінки інформаційної складності розрізнювальної атаки на шифросистему NTRUCipher
import numpy as np
from decimal import Decimal
import math
from math import sqrt
n=256
```

```
d=n/3
q1=[7681,10753,11777,12289,13313]
ke1=[17,11,3,11,3]
for i in range(len(q1)):
    q=q1[i]
    b=[]
    #g=primi(q)
    #ke=int(g[0])
    ke=ke1[i]
    k=pow(ke,((q-1)/(2*n)))
    beta=k%q
    p=1/3
    e=[]
    for ge in range(n):
        x = pow(int(beta), int(ge), int(q))
        e.append(x)
    a=[]
    e=np.array(e)
    for al in range(q):
        k = 1 - 2 * p * (1 - np.cos((2 * np.pi * ((e * al)%q)%q)/q))
        a.append(k.prod())

    z=np.arange(0,q)

    pz1=[]

    for z in range(q):
        g = []
        for al in range(q):
            k=np.cos(2 * np.pi * ((al * z) % q)/q)*a[al]
            g.append(k)
        k=np.array(g)
        pz1.append(np.sum(k)/q)
    D=np.sum(abs(np.array(pz1)-1/q))/2
    beta=0.01
    t=2/pow(D,2)*math.log1p((q-1+2*n)/(2*n*beta))
    t=math.ceil(t)
    print(f'log2(t)={math.log2(t)}')
```

ДОДАТОК В

Програмний код отримання нижніх оцінок складності алгоритмів розв'язання задачі LWE

Програмна реалізація виконана на комп'ютері 12th Gen Intel(R) Core(TM) i5-1235U 1.30 GHz та обсягом оперативної пам'яті 16 ГБ. Мова програмування – Python. Середовище розробки – PyCharm.

```
# Метод максимуму правдоподібності та удосконалений алгоритм зустрічі посередині
import math
from decimal import Decimal
n=int(input("Enter n:"))
d=int(input("Enter d:"))

def factorial(n):
    factorial = 1
    for i in range(2, n + 1):
        factorial *= i
    return factorial
#print(factorial(2))
comb=Decimal(Decimal(factorial(n))/Decimal(factorial(2*d))/Decimal(factorial(n-2*d)))
#print(comb)
#comb=Decimal.log10(comb)/Decimal.log10(Decimal(2))
#print(comb)
T1=Decimal((2**(2*d))*comb)
T2=T1**Decimal(1/4)
T1=Decimal.log10(T1)/Decimal.log10(Decimal(2))
T2=Decimal.log10(T2)/Decimal.log10(Decimal(2))
print(f'T1={T1}')
print(f'T2={T2}')

# Первинна атака
import math
from decimal import Decimal

def teta(b):
    return ((math.pi*b)**(1/b)*b/(2*math.pi*math.e))**(1/(2*(b-1)))
def main(n,d,q):
    b_w=[]
    for m in range(1,10000):
        t=n+m+1
        #print(t)
        if t>200:
            for b in range(200,t):
                print((2*d+1)*math.sqrt(b/3))
                print(teta(b)**(2*b-t)*q**(m/t))
                if ((2*d+1)*math.sqrt(b/3))<=(teta(b)**(2*b-t)*q**(m/t)):
                    b_w.append(b)
                    break
    print(b_w)
    b_w_z=min(b_w)
    print(f'Результат = {b_w_z}')
```

```
    print(f'Результат = {2**(0.292*b_w_z)}')
    T = 2 ** (0.292 * b_w_z)
    T = Decimal(T)
    T = Decimal(Decimal.log10(T) / Decimal.log10(Decimal(2)))
    print(f'Результат = {T}')

if __name__ == '__main__':
    n=int(input('Enter n:'))
    q=int(input('Enter q:'))
    d=int(input('Enter d:'))
    main(n,d,q)

# Дуальна атака
import math
from decimal import Decimal

def teta(b):
    return ((math.pi*b)**(1/b)*b/(2*math.pi*math.e))**(1/(2*(b-1)))
def main(n,d,q):
    c=8
    b_w=[]
    for m in range(1,10000):
        t=n+m
        if t>200:
            for b in range(200,t):
                if
(teta(b)**t*q**(n/t))<=(q/(math.pi*(2*d+1))*math.sqrt(((c+2)*math.log(2))/2)):
                    b_w.append(b)
                    break
    print(b_w)
    b_w_z=min(b_w)
    print(f'Результат = {b_w_z}')
    print(f'Результат = {2**(0.292*b_w_z+2*c)}')
    T = 2**(0.292*b_w_z+2*c)
    T = Decimal(T)
    T = Decimal(Decimal.log10(T) / Decimal.log10(Decimal(2)))
    print(f'Результат = {T}')

if __name__ == '__main__':
    n = int(input('Enter n:'))
    q = int(input('Enter q:'))
    d = int(input('Enter d:'))
    main(n,d,q)

# BKW-атака
import math
from math import sqrt
from decimal import Decimal
for safas in range(10000):
    delta=float(0.01)
    n=int(input('Введите n:'))
    q=int(input('Введите q:'))
    d=int(input('Введите d:'))
    n1=[]
    u=[]
    v=[]
    k1=[]
    l=[]
    t=[]
    delpk1=0
    N=[]
```

```
    T=[]

    def is_prime(n):  # перевірка на простоту
        if n < 2:
            quit(2)
        if n == 2:
            print()
        limit = sqrt(n)
        i = 2
        while i <= limit:
            if n % i == 0:
                quit(2)
            i += 1
    is_prime(n)

    for i in range (1,n-2):
        n1.append(i)

    for i in range(len(n1)):
        k=math.log2(n-n1[i])/2
        u.append(k)

    for i in range(len(n1)):
        kg=(2*(n-n1[i])/math.log2(n-n1[i]))
        v.append(kg)

    for i in range(len(u)):
        k1.append(pow(2,u[i]-1))

    def teta(p,x):
        return 1-2*p*(1-math.cos(2*math.pi*x/q))
    pa=[]
    for a in range(q):
        pa.append(teta(1/3,a))

    prov=[]
    for i in range(len(k1)):
        for i2 in range(len(pa)):
            delpk1=+ math.fabs(pa[i2])**(2*k1[i])
        prov.append(delpk1)
        delpk1=0

    for i in range(len(n1)):
        t.append(float(((1-
delta/2)*n1[i]*math.log2(3)+((delta/2)*math.log2(delta/2))+((1-delta/2)*math.log2(1-
delta/2)))/prov[i]))

    for i in range(len(n1)):
        t[i]=Decimal(t[i])
        q=Decimal(q)
        u[i]=Decimal(u[i])
        delta=Decimal(delta)
        v[i]=Decimal(v[i])
        l.append(((u[i] + Decimal(math.log1p(Decimal(2) * t[i] / delta)) -
Decimal(1)) * (q ** v[i])))

    for i in range(len(n1)):
        N.append(l[i]*t[i])
 #print('N:',N)

    for i in range(len(n1)):
```

```
    n1[i]=Decimal(n1[i])
    t[i]=Decimal(t[i])
    q=Decimal(q)
    l[i]=Decimal(l[i])
    t[i]=Decimal(t[i])
    u[i]=Decimal(u[i])
    T.append((2*n1[i]*t[i]*3**(n1[i]))+u[i]*l[i]*t[i])
Nlog=[]
Tlog=[]
for i in range(len(n1)):
    Nlog.append(Decimal.log10(N[i])/Decimal.log10(Decimal(2)))
    Tlog.append(Decimal.log10(T[i])/Decimal.log10(Decimal(2)))

print('Minimalnoe T is :',min(Tlog))
print('Minimalnoe N is :',Nlog[Tlog.index((min(Tlog)))])
print(('N1 is: '),n1[Tlog.index(min(Tlog))])
```

ДОДАТОК Г

Список основних публікацій здобувачки за темою дисертації

1. Алексейчук А. Н., Матийко А. А. Оценки вероятности обратимости случайных многочленов, используемых в модифицированной версии криптосистемы NTRU. Радиотехника. 2017. № 189. С. 38–46.

2. Олексійчук А. М., Матійко А. А. Bounds of decryption failure probability in NTRUEncrypt encryption scheme for a fixed key. Ukrainian Information Security Research Journal. 2018. Vol. 20, no. 2. DOI: https://doi.org/10.18372/2410-7840.20.12276.

3. Matiyko A. A. The Comparative Analysis of NTRUCipher and NTRUEncrypt Encryption Schemes. Mathematical and computer modelling. Series: Technical sciences. 2019. No. 19. P. 81–87. DOI: https://doi.org/10.32626/2308-5916.2019-19.81-87.

4. Matiyko A. BKW-attack on NTRUCIPHER and NTRUCIPHER+ enctyption schemes. Collection "Information Technology and Security". 2020. Vol. 8, no. 2. P. 164–176. DOI: https://doi.org/10.20535/2411-1031.2020.8.2.222599.

5. Олексійчук А. М., Матійко А. А. ШВИДКА РОЗРІЗНЮВАЛЬНА АТАКА НА ШИФРОСИСТЕМУ NTRUCipher+. Ukrainian Information Security Research Journal. 2020. Т. 22, № 3. С. 183–189. DOI: https://doi.org/10.18372/2410-7840.22.14981.

6. Matiyko A. Security estimates of the NTRUCipher and NTRUCipher+ encryption schemes against BKW-attack. Physico-mathematical modelling and informational technologies. 2021. No. 33. P. 28–32. DOI: https://doi.org/10.15407/fmmit2021.33.028.

7. Matiyko A., Alekseychuk A. Method for design secure symmetric NTRU-like encryption schemes. Collection "Information Technology and Security". 2022.

Vol. 10, no. 2. P. 165–176. DOI: https://doi.org/10.20535/2411-1031.2022.10.2.270406.

8. 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, no. 2. P. 190–195. DOI: https://doi.org/10.1007/s10559-021-00343-z.

9. Alekseychuk A. N., Matiyko A. A. Distinguishing Attack on the NTRUCipher Encryption Scheme. Cybernetics and Systems Analysis. 2022. Vol. 58, no. 2. P. 186-190. DOI: https://doi.org/10.1007/s10559-022-00449-y.

10. Олексійчук А. М., Матійко А. А. Оцінки ймовірності оборотності випадкових многочленів, що використовуються в модифікованій версії криптосистеми NTRU. Безпека інформації в інформаційно-телекомунікаційних системах : XIX Міжнар. науково-практ. конф., м. Буча, 25–26 трав. 2017 р. С. 82.

11. Олексійчук А. М., Матійко А. А. Оцінки ймовірності помилкового розшифрування повідомлень у шифросистеми NTRUEncrypt при фіксованому ключі. Безпека інформації в інформаційно-телекомунікаційних системах: XX Міжнар. науково-практ. конф., м. Буча, 22–24 трав. 2018 р. С. 37.

12. Олексійчук А. М., Матійко А. А., Грицай В. А. Оцінка трудомісткості BKW-атаки на симетричну криптосистему NTRUCipher. Актуальні питання застосування спеціальних інформаційно-телекомунікаційних систем: Наукова-практ. конф. курсантів (студентів), аспірантів, докторантів та молодих уч., м. Київ, 23–24 черв. 2020 р. С. 80.

13. Олексійчук А. М., Матійко А. А. Швидка розрізнювальна атака на шифросистему NTRUCIPHER+. Інформаційно-телекомунікаційні системи і технології та кібербезпека: нові виклики, нові завдання: Наукова-практ. конф., м. Київ, 18–19 листоп. 2020 р. С. 31.

14. Олексійчук А. М., Матійко А. А., Грицай В. А. Дослідження стійкості симетричних NTRU-подібних шифросистем відносно атак на основі підібраних відкритих текстів. Інформаційно–телекомунікаційні системи і технології та кібербезпека: нові виклики, нові завдання : Наукова-практ. конф., м. Київ, 24 листоп. 2020 р. – 25 листоп. 2021 р. С. 47.

15. Олексійчук А. М., Матійко А. А. Метод побудови обґрунтовано стійких симетричних NTRU-подібних шифросистем. Актуальні питання застосування спеціальних інформаційно-комунікаційних систем : V науково-практ. конф. курсантів (студентів), аспірантів, докторантів та молодих уч., м. Київ, 29 листоп. 2022 р. С. 33.

Прим. № 1

"ЗАТВЕРДЖУЮ"
Начальник управління Служби зовнішньої розвідки України

Седінкін С.К.

"27" 09 2022 року

АКТ
впровадження результатів дисертаційної роботи
Матійко Александри Андріївни
у науково-дослідній роботі "Дослідження, розроблення та застосування новітніх методів криптографічного аналізу систем захисту інформації в різних моделях обчислень з урахуванням їх функціонування"
(шифр "Дорадо")

Комісія у складі голови комісії Армана Р.С. та членів комісії: Гудзенка С.В., Гришакова С.В. з'ясувала, що в Службі зовнішньої розвідки України в результаті виконання науково-дослідної роботи "Дослідження, розроблення та застосування новітніх методів криптографічного аналізу систем захисту інформації в різних моделях обчислень з урахуванням їх функціонування " (шифр "Дорадо") вперше впроваджено отримані Матійко Александрою Андріївною **такі наукові результати**:

1. Аналітичні співвідношення для оцінювання ймовірності оборотності випадкових поліномів, що використовуються в ролі секретних ключів NTRU-подібних шифросистем.
2. Аналітичні співвідношення для оцінювання ймовірності помилкового розшифрування повідомлень в NTRU-подібних шифросистемах при фіксованому секретному ключі.

Ефект від впровадження зазначених наукових результатів полягає в тому, що вони дозволяють:

– зменшити ймовірність необоротності випадкового полінома в кільці $R_{n.q}$ (з 0,5 до $1{,}5 \cdot 10^{-2}$) 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 верхня межа ймовірності помилкового розшифрування повідомлень шифросистеми NTRUCipher змінюється в

межах від 2^{-357} до 2^{-157}, в той час як верхня межа цієї ймовірності для шифросистеми NTRUEncrypt змінюється в межах від 2^{-160} до 2^{-74};

– отримувати більш адекватну інформацію про частоту виникнення помилок при розшифруванні для шифросистеми NTRUEncrypt та використовувати цю інформацію для оптимізації шифросистеми за стійкістю або практичністю.

Голова комісії: _____ Арман Р.С.

Члени комісії:
к.ф-м.н. _____ Гудзенко С.В.

к.т.н. _____ Гришаков С.В.

"27" 09 2022 року

Прим. № 1

"ЗАТВЕРДЖУЮ"
Начальник управління Служби зовнішньої розвідки України

Сединкін С.К.

"27" 09 2022 року

АКТ
впровадження результатів дисертаційної роботи
Матійко Александри Андріївни
у науково-дослідній роботі "Дослідження методів аналізу криптографічного захисту сучасних інформаційних систем" (шифр "Сарган")

Комісія у складі голови комісії Армана Р.С. та членів комісії: Гудзенка С.В., Гришакова С.В. з'ясувала, що в Службі зовнішньої розвідки України в результаті виконання науково-дослідної роботи "Дослідження методів аналізу криптографічного захисту сучасних інформаційних систем" (шифр "Сарган") вперше впроваджено отримані Матійко Александрою Андріївною **такі наукові результати**:

1. Алгоритм обчислення значень параметра, який характеризує величину sup-норми добутку елементів кільця зрізаних поліномів за модулем заданого унітарного полінома з дійсними коефіцієнтами.
2. Аналітичні оцінки трудомісткості атак (BKW та розрізнювальної) на симетричні шифросистеми NTRUCipher та NTRUCipher+.

Ефект від впровадження зазначених наукових результатів полягає в тому, що вони дозволяють:

– отримати більш точну в порівнянні з відомою верхню межу sup-норми добутку елементів кільця зрізаних поліномів та встановити оцінки ймовірності помилкового розшифрування повідомлень в NTRU-подібних шифросистемах при фіксованому ключі;

– встановити, що трудомісткість BKW-атаки на шифросистему NTRUCipher+ є в $2^{15} \div 2^{69}$ разів вище в порівнянні з трудомісткістю аналогічної атаки на шифросистему NTRUCipher;

– встановити, що підвищення стійкості шифросистеми NTRUCipher відносно BKW-атаки за рахунок використання додаткового доданку у формулі зашифрування майже повністю нівелюється збільшенням верхньої межі ймовірності помилки розшифрування, що негативно впливає на практичність шифросистеми NTRUCipher+ в порівнянні з 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 $t = 2^{19}$);

– встановити, що інформаційна складність розрізнювальної атаки на шифросистему NTRUCipher змінюється в межах від $2^{67,59}$ до $2^{71,79}$, що свідчить про необхідність враховувати наведену атаку при виборі параметрів шифросистеми NTRUCipher для забезпечення її належної стійкості.

Голова комісії: _____ Арман Р.С.

Члени комісії:
к.ф-м.н. _____ Гудзенко С.В.

к.т.н. _____ Гришаков С.В.

"27" 09 2022 року

"ЗАТВЕРДЖУЮ"
Генеральний директор АТ "ІІТ"
_____ В.В. Онопрієнко
"__" _____2022 року

АКТ
впровадження результатів досліджень дисертаційної роботи
Матійко Александри Андріївни в приватному акціонерному товаристві
"Інститут Інформаційних технологій" м. Харків

Комісія у складі голови комісії головного конструктора АТ "ІІТ" Горбенка Івана Дмитровича та членів комісії начальників відділів Бобуха Всеволода Анатолійовича та Тоцького Олександра Сергійовича з'ясували, що в АТ "ІІТ" вперше впроваджено отриманий Матійко Александрою Андріївною **такий науковий результат**:

Метод побудови обґрунтовано стійких симетричних NTRU-подібних шифросистем.

Ефект від впровадження зазначеного наукового результату полягає в тому, що він надає змогу вибирати параметри n,q,d NTRU-подібних шифросистем, що забезпечують їхню стійкість на заздалегідь визначеному рівні. Зокрема, для забезпечення стійкості на рівні 2^{128} можна вважати $n=631$, $q=2693$, $d=56$, а для забезпечення стійкості на рівні 2^{256} можна вважати $n=883$, $q=8089$, $d=168$. При цьому час зашифрування/розшифрування повідомлень у запропонованих шифросистемах є порівняним з відповідним часом у криптосистемі NTRU Prime.

Голова комісії: _____ І.Д. Горбенко

Члени комісії: _____ В.А. Бобух

_____ О.С. Тоцький

"24" 11 2022 року