АНОТАЦІЯ

Кандій С.О. Методи та моделі оцінки захищеності асиметричних криптографічних перетворень на решітках від існуючих та потенційних атак – Кваліфікаційна наукова праця на правах рукопису

Дисертація на здобуття ступеня доктора філософії за спеціальністю 125 Кібербезпека та захист інформації (Галузь знань 12 Інформаційні технології). – Харківський національний університет імені В. Н. Каразіна Міністерства освіти і науки України, Харків, 2025.

Дисертаційна робота присвячена розв'язанню актуальної задачі: аналізу та розробці методів та моделей для підвищення захищеності асиметричних криптографічних систем на решітках.

Задача є актуальною, оскільки захист інформації стає одним з ключових викликів у сучасному цифровому світі, де загрози інформаційній безпеці постійно зростають. Криптографічні методи є основою для забезпечення конфіденційності, цілісності та автентичності даних. Сьогоднішня реальність відзначається активним впровадженням криптографічних рішень у різних секторах – від фінансових та урядових структур до промислових і комерційних організацій.

На міжнародній арені спостерігається прагнення до стандартизації криптографічних засобів, що сприяє сумісності систем безпеки різних країн. Такі організації, як Міжнародна організація зі стандартизації (ISO) та Національний інститут стандартів і технологій США (NIST), активно працюють над створенням нових стандартів, які враховують сучасні загрози, зокрема потенційну небезпеку квантових обчислень.

Національний розвиток криптографії також набирає обертів. В Україні активізуються зусилля щодо створення власних стандартів та нормативних документів для регулювання використання криптографічних засобів.

Мета і завдання дослідження. Метою дослідження є аналіз та розробка методів та моделей для підвищення захищеності асиметричних криптографічних систем на решітках від існуючих та потенційних атак.

Для досягнення поставленої мети були розв’язані такі основні задачі:

1. Вибір та обґрунтування моделей редукції решіток, які враховують усі існуючі відомості щодо поведінки базисів під час редукції. Ця задача включала всебічний огляд і порівняння різних моделей редукції решіток, які використовуються для оптимізації базисів решіток, що є ключовим елементом у багатьох криптографічних схемах. Особливо було акцентовано увагу на таких алгоритмах, як BKZ (Block Korkine–Zolotarev), які широко застосовуються для редукції базисів. Проведений аналіз дозволив обґрунтувати вибір найбільш придатних моделей редукції для різних типів задач на решітках та виявити їхні сильні та слабкі сторони. Крім того, були розглянуті аспекти, що впливають на точність і ефективність редукції базисів.

2. Дослідження впливу моделей редукції решіток на складність атак на криптографічні перетворення на решітках та удосконалення методики оцінювання криптографічних перетворень на решітках. Особлива увага приділялась проблемам, які лежать в основі постквантових криптографічних схем: NTRU, LWE, SIS. Проблеми навчання з помилками (LWE) та NTRU є основою багатьох сучасних криптографічних схем. Досліджено, як різні моделі редукції решіток впливають на складність їх розв’язання, а також проаналізовано стійкість криптографічних схем, що базуються на цих задачах. Проблема малого цілочисельного рішення (SIS) є критичною для стійкості багатьох криптографічних протоколів. Досліджено, як зміна параметрів редукції решіток впливає на складність розв’язання SIS, і запропоновано удосконалення для оцінки її криптографічної стійкості. Удосконалена методика оцінювання криптографічних перетворень на решітках враховує особливості цих задач, а також вплив редукції на ключові параметри стійкості криптографічних схем. Це дозволило підвищити точність прогнозування стійкості криптографічних систем

у контексті їх потенційної вразливості до атак квантових і класичних обчислювальних методів.

3. Аналіз криптографічних перетворень на решітках в формальних моделях безпеки, що враховують можливість застосування класичних та квантових атак. У межах цього дослідження був проведений детальний аналіз механізму інкапсуляції ключів, визначеного в стандарті ДСТУ 8961:2019, з урахуванням сучасних викликів у криптографії, пов'язаних із квантовими обчисленнями. Основну увагу було приділено отриманню формального доказу безпеки схеми інкапсуляції ключів у моделі квантового випадкового оракула (QROM).

4. Дослідження впливу обчислень з плаваючою точкою на безпеку криптографічних перетворень на решітках. У рамках цього дослідження особлива увага приділялася аналізу криптографічної стійкості схем електронного підпису, зокрема Falcon — одного з провідних кандидатів для стандартизації постквантової криптографії. Основна мета дослідження полягала в аналізі потенційних атак на основі обчислень з плаваючою точкою, які можуть бути використані для відновлення приватних ключів.

У першому розділі дисертації (*Аналіз сучасних тенденцій у квантово–стійкій криптографії*) на основі проведеного аналізу показано, що розвиток квантових алгоритмів обумовлений двома техніками – квантовим пошуком та квантовою вибіркою Фур'є. Обґрунтовано, що криптографія на решітках є стійкою до застосування цих технік. Розкриті вимоги до квантово–стійкої криптографії. Розкрита сутність доказової безпеки та моделей безпеки IND–CCA (Indistinguishability under Adaptive Chosen Chiphertext Attack) для механізмів інкапсуляції ключів та EUF–CMA (Existentially unforgeable under adaptive chosen message attacks) для електронних підписів. Наведено відомості з теорії решіток та теорії квантових обчислень.

У другому розділі дисертації (*Аналіз та порівняння моделей редукції решіток*) обґрунтовано, що фактор Ерміта відіграє важливу роль при аналізі моделей редукції решіток. Проведено серію експериментів, що направлені на

визначення точності існуючих асимптотичних оцінок фактору Ерміта на криптографічно значущих розмірностях решіток. Показано, що істинне значення фактору Ерміта швидко наближається до асимптотичних оцінок і на криптографічно значущих розмірностях можливо вважати помилку апроксимації фактору Ерміта незначною. Проведено порівняльний аналіз існуючих симуляторів редукції решіток. Для порівняння симуляторів проведено ряд експериментів на решітках малої розмірності. Показано, що симулятор Альбрехта–Лі дає найменшу середньоквадратичну помилку серед усіх симуляторів. Для NTRU решіток розкрито сутність розрідженої підрешітки. Отримано перший науковий результат: Вперше виконано кількісне порівняння точності моделей редукції решіток із застосуванням метрики середньоквадратичної помилки для моделі GSA (Geometric Series Assumption) та симуляторів редукції решіток. Попередні дослідження фокусувалися на якісних або суто теоретичних оцінках якості роботи моделей. Отримані оцінки дозволяють кількісно оцінювати якість роботи симуляторів в залежності від параметрів решіток для оцінки захищеності від класичних та квантових атак.

У третьому розділі дисертації (Методи оцінки складності криптографічних задач з теорії решіток) наведено класифікацію існуючих атак на криптографічні перетворення на решітках. Для атак вкладення та декодування запропонована удосконалена модель оцінки складності атаки, що базується на проведеному у другому розділі аналізі. Для атак декодування запропонований метод визначення оптимальних параметрів атаки. Удосконалено методику оцінювання складності криптографічної задачі SIS (Shortest Integer Solution), що відрізняється від існуючих тим, що у даній методиці враховується алгебраїчна структура решіток під час аналізу процесів редукції для оцінки параметрів та характеристик атак на їх основі.

У четвертому розділі дисертації (Оцінка захищеності механізмів інкапсуляції ключів на алгебраїчних решітках) уточнено оцінки захищеності механізмів інкапсуляції ключів ДСТУ 8961:2019 та Crystals–Kyber. Показано, що врахування структури алгебраїчних решіток, згідно до методу, що був

розроблений в розділі 3, дає більші оцінки безпеки, ніж класична модель GSA. Вперше було отримано узагальнений доказ IND–CCA безпеки перетворень, що використовуються в стандарті ДСТУ 8961:2019, у моделі квантового випадкового оракула. Попередні дослідження не вивчали IND–CCA безпеку перетворень ДСТУ 8961:2019 у моделі квантового випадкового оракула.

У п’ятому розділі дисертації (Оцінка захищеності електронних підписів на алгебраїчних решітках) уточнено оцінки захищеності електронних підписів Falcon та Crystals–Dilithium. Показано, що врахування структури алгебраїчних решіток, згідно до методу, що був розроблений в розділі 3, дає більші оцінки безпеки, ніж класична модель GSA. Для електронного підпису Falcon отримали подальший розвиток обґрунтування оцінки атаки відновлення ключів, що використовує обчислення з плаваючою крапкою, для алгоритмів електронного підпису на основі решіток, що дало змогу підвищити безпеку електронних підписів на решітках.

Практичне значення отриманих результатів полягає у тому, що було уточнено оцінки безпеки криптографічних перетворень на решітках, які підтверджують рівні стійкості квантово–стійких стандартів електронного підпису (ДСТУ 9212:2023) та механізмів інкапсуляції ключів (ДСТУ 8961:2019), що обґрунтовує їх застосування як національних стандартів. Розроблено програмне забезпечення, яке дозволяє оцінювати складність атак вкладення та декодування для проблем LWE та NTRU при процесі практичного оцінювання безпеки криптографічних перетворень на решітках, оцінювати складність проблеми SIS з врахуванням структури решіток та проводити моделювання редукції решіток.

Ключові слова: постквантова криптографія, електронний підпис, механізми інкапсуляції ключів, алгебраїчні решітки, доказова безпека, асиметричні криптосистеми, шифрування, моделі, криптографічні примітиви, конфіденційність, цілісність, аналіз атак, кібербезпека, квантові обчислення.

ABSTRACT

Kandii S.O. Methods and models for evaluating the security of lattice–based asymmetric cryptographic transformations against existing and potential attacks – Qualification scholarly paper: a manuscript.

Thesis submitted for obtaining the Doctor of Philosophy degree in Information Technologies, Speciality 125 Computer Science. – V. N. Karazin Kharkiv National University, Ministry of Education and Science of Ukraine, Kharkiv, 2025.

The dissertation is devoted to solving a relevant problem: the analysis and development of methods and models to enhance the security of lattice–based asymmetric cryptographic systems.

The problem is relevant because information security has become one of the key challenges in the modern digital world, where threats to information security are constantly increasing. Cryptographic methods form the foundation for ensuring data confidentiality, integrity, and authenticity. Today's reality is marked by the active implementation of cryptographic solutions across various sectors, ranging from financial and governmental institutions to industrial and commercial organizations.

On the international stage, there is a growing effort to standardize cryptographic tools, which facilitates the interoperability of security systems across different countries. Organizations such as the International Organization for Standardization (ISO) and the U.S. National Institute of Standards and Technology (NIST) are actively working on developing new standards that address modern threats, including the potential risks posed by quantum computing.

The national development of cryptography is also gaining momentum. In Ukraine, efforts are being intensified to establish national standards and regulatory documents for governing the use of cryptographic tools.

Research Objective and Tasks. The objective of the research is to analyze and develop methods and models to enhance the security of lattice–based asymmetric cryptographic systems against existing and potential attacks.

To achieve the stated objective, the following key tasks were addressed:

1. Selection and justification of lattice reduction models that account for all known aspects of basis behavior during reduction. This task involved a comprehensive review and comparison of various lattice reduction models used for optimizing lattice bases, which are a crucial element in many cryptographic schemes. Special emphasis was placed on algorithms such as BKZ (Block Korkine–Zolotarev), which are widely applied for basis reduction. The conducted analysis enabled the justification of the most suitable reduction models for different types of lattice problems and the identification of their strengths and weaknesses. Additionally, factors influencing the accuracy and efficiency of basis reduction were examined.

2. Investigation of the impact of lattice reduction models on the complexity of attacks against lattice–based cryptographic transformations and enhancement of evaluation methodologies for such transformations. Special attention was given to fundamental problems underlying post–quantum cryptographic schemes, including NTRU, LWE, and SIS. The Learning With Errors (LWE) problem and the NTRU problem form the foundation of many modern cryptographic schemes. The study examined how different lattice reduction models influence the complexity of solving these problems and analyzed the resilience of cryptographic schemes based on them. The Small Integer Solution (SIS) problem is critical to the security of many cryptographic protocols. The research investigated how changes in lattice reduction parameters affect the complexity of solving SIS and proposed improvements for assessing its cryptographic security. The enhanced evaluation methodology for lattice–based cryptographic transformations takes into account the specific characteristics of these problems, as well as the influence of reduction on key security parameters of cryptographic schemes. This advancement has improved the accuracy of predicting the resilience of cryptographic systems concerning their potential vulnerabilities to both quantum and classical computational attack methods.

3. Analysis of lattice–based cryptographic transformations within formal security models that consider the feasibility of classical and quantum attacks. As part of this study, a detailed analysis was conducted on the key encapsulation mechanism specified in the DSTU 8961:2019 standard, taking into account contemporary

cryptographic challenges related to quantum computing. Special attention was given to obtaining a formal security proof for the key encapsulation scheme within the Quantum Random Oracle Model (QROM).

4. Investigation of the impact of floating–point computations on the security of lattice–based cryptographic transformations. This study focused on analyzing the cryptographic resilience of digital signature schemes, particularly Falcon, one of the leading candidates for post–quantum cryptography standardization. The primary objective was to examine potential floating–point–based attacks that could be exploited to recover private keys.

In the first chapter of the dissertation (Analysis of Modern Trends in Quantum–Resistant Cryptography), the conducted analysis demonstrates that the advancement of quantum algorithms is driven by two key techniques: quantum search and quantum Fourier sampling. It is substantiated that lattice–based cryptography remains resistant to these techniques.

The chapter outlines the requirements for quantum–resistant cryptography and explores the concept of provable security, along with security models such as IND–CCA (Indistinguishability under Adaptive Chosen Ciphertext Attack) for key encapsulation mechanisms and EUF–CMA (Existential Unforgeability under Adaptive Chosen Message Attack) for digital signatures. Additionally, fundamental concepts from lattice theory and quantum computing theory are presented.

In the second chapter of the dissertation (Analysis and Comparison of Lattice Reduction Models), it is substantiated that the Hermite factor plays a crucial role in analyzing lattice reduction models. A series of experiments was conducted to assess the accuracy of existing asymptotic estimates of the Hermite factor for cryptographically significant lattice dimensions. The results demonstrate that the true value of the Hermite factor quickly converges to its asymptotic estimates, and for cryptographically relevant dimensions, the approximation error can be considered negligible.

A comparative analysis of existing lattice reduction simulators was performed. To evaluate these simulators, several experiments were conducted on low–dimensional

lattices. The findings indicate that the Albrecht–Lee simulator produces the lowest root–mean–square error among all tested simulators. For NTRU lattices, the concept of a sparse sublattice is explored in detail.

First Scientific Contribution: For the first time, a quantitative comparison of the accuracy of lattice reduction models was performed using the root–mean–square error metric for both the Geometric Series Assumption (GSA) model and lattice reduction simulators. Previous studies primarily focused on qualitative or purely theoretical assessments of model accuracy. The obtained estimates enable a quantitative evaluation of simulator performance based on lattice parameters, contributing to the assessment of security against both classical and quantum attacks.

In the third chapter of the dissertation (Methods for Assessing the Complexity of Cryptographic Problems in Lattice Theory), a classification of existing attacks on lattice–based cryptographic transformations is provided. For embedding and decoding attacks, an enhanced complexity assessment model is proposed, based on the analysis conducted in the second chapter. For decoding attacks, a method for determining optimal attack parameters is introduced.

Additionally, the evaluation methodology for the complexity of the Shortest Integer Solution (SIS) problem has been improved. Unlike existing methods, this approach incorporates the algebraic structure of lattices when analyzing the reduction processes used to estimate the parameters and characteristics of attacks based on SIS.

In the fourth chapter of the dissertation (Security Assessment of Key Encapsulation Mechanisms on Algebraic Lattices), the security estimates of the DSTU 8961:2019 and CRYSTALS–Kyber key encapsulation mechanisms were refined.

The findings demonstrate that considering the structure of algebraic lattices, according to the method developed in Chapter 3, results in higher security estimates compared to the classical Geometric Series Assumption (GSA) model. First Scientific Contribution: For the first time, a generalized IND–CCA security proof for transformations used in DSTU 8961:2019 was obtained within the Quantum Random Oracle Model (QROM). Previous studies had not explored the IND–CCA security of DSTU 8961:2019 transformations in the QROM framework.

In the fifth chapter of the dissertation (Security Assessment of Digital Signatures on Algebraic Lattices), the security estimates of the Falcon and CRYSTALS–Dilithium digital signature schemes were refined.

The findings demonstrate that considering the structure of algebraic lattices, according to the method developed in Chapter 3, results in higher security estimates compared to the classical Geometric Series Assumption (GSA) model.

For the Falcon digital signature scheme, further development was made in justifying the evaluation of key recovery attacks that utilize floating–point computations for lattice–based signature algorithms. This advancement has contributed to enhancing the security of lattice–based digital signatures.

The practical significance of the obtained results lies in the refinement of security estimates for lattice–based cryptographic transformations, which confirm the security levels of quantum–resistant digital signature standards (DSTU 9212:2023) and key encapsulation mechanisms (DSTU 8961:2019), thereby justifying their adoption as national standards.

Additionally, software was developed to: assess the complexity of embedding and decoding attacks for the LWE and NTRU problems in the context of practical security evaluation of lattice–based cryptographic transformations, evaluate the complexity of the SIS problem, taking into account lattice structure and simulate lattice reduction processes for security analysis.

Keywords: post–quantum cryptography, digital signature, key encapsulation mechanisms, algebraic lattices, provable security, asymmetric cryptosystems, encryption, models, cryptographic primitives, confidentiality, integrity, attack analysis, cybersecurity, quantum computing.