АНОТАЦІЯ

Каптьол Є.Ю. Методи оцінки та порівняльного аналізу асиметричних електронних підписів, стійких до класичного та квантового криптоаналізу. – Кваліфікаційна нукова 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.

В умовах стрімкого розвитку квантових технологій на міжнародному та національному рівнях вирішується питання обрання та стандартизації квантовостійких криптографічних перетворень. Це пов’язано зі значним зростанням швидкості обчислень та викликами для безпеки криптографічних перетворень, що прогнозуються за умови використання для криптоаналізу квантового комп’ютера достатньої потужності. Через це з боку NIST було запроваджено конкурс NIST PQC, призначений для обрання кандидатів для стандартизації в сфері квантовостійких криптографічних перетворень. З іншого боку, велику загрозу можуть становити спеціальні атаки, що ґрунтуються на витоках побічними каналами та на основі помилок. Тому як на міжнародному, так і на національному рівнях, важливо зреагувати на можливості криптоаналітиків найвищого рівня та визначити вимоги і розробити перспективні захищені криптоперетворення електронного підпису та стандартизувати їх в тому числі на національному рівні.

Дисертаційна робота присвячена розв’язанню актуальної задачі: аналізу та дослідженню, оцінці та порівнянню існуючих та перспективних квантовостійких електронних підписів по сукупності безумовних, умовних та прагматичних критеріїв.

Мета і завдання дослідження. Обгрунтування вибору, аналіз та дослідження, оцінка та порівняння існуючих та перспективних квантовостійких електронних підписів по сукупності безумовних, умовних та прагматичних критеріїв.

Для досягнення поставленої мети були розв’язані наступні задачі:

1. Аналіз стану безпеки існуючих та обгрунтування вимог до методів перспективних квантовостійких електронних підписів.
2. Обгрунтування моделей порушника та загроз, а також у цілому моделі безпеки перспективних постквантових електронних підписів та множин безумовних, умовних та прагматичних критеріїв їх оцінки та порівняння.
3. Науково-методичні основи розробки, оцінки та порівняння існуючих та перспективних квантовостійких електронних підписів по безумовним, умовним та прагматичним критеріям.
4. Аналіз, оцінка та порівняння існуючих та кандидатів на песпективні квантовостійкі національні та міжнародні електронні підписи по безумовним критеріям (безпеці).
5. Програмне моделювання інструментарію практичної оцінки та порівняння проєктів та стандартизованих міжнародних та національних квантовостійких електронних підписів.

У першому розділі дисертації (*Аналіз стану безпеки існуючих та обгрунтування вимог до методів перспективних квантовостійких електронних підписів*) на основі пошуку джерел, що присвячені обгрунтуванню вимог та моделей безпеки вирішуються наступні задачі:

Проблеми захищеності від нового класу квантових атак виникли декілька десятиліть тому, але відчуття загрози від них було сприйнято тільки після появи в 2015-му році статті професорів Менезис та Кобліц, які по суті заявили про низьку захищеність існуючих асиметричних криптографічних перетворень, в тому числі електронного підпису від квантових атак

реалізованих на квантових комп’ютерах які розробляються. В статті було вказано, що квантовостійкі асиметричні криптоперетворення можуть бути побудовані на основі нових математичних методів: модулярні перетворення (математичні решітки), математичні коди, квадратичні поля, ізогенії еліптичних кривих, геш-функції на основі криптографії. Далі послідувала наукова конференція в Японії, на якій було прийнято позитивне рішення щодо створення квантовостійких криптоперетворень. NIST США на основі рішень оголосив конкурс на розроблення проектів стандартів квантовостійких асиметричних кпритоперетворень, в тому числі, ЕП. В наступні роки відбулось три раунди і в 2022 році на форумі NIST США конференція прийняла рішення про стандартизацію і в NIST 8413 наведено перелік стандартизованих ЕП, таких як ЕП на основі математичних решіток, такі як проекти ЕП Crystall-Delithium та Falcon, а також на основі використання одноразових ключів з використанням геш-функції. Також було прийнято рішення про стандартизацію протоколів інкапсуляції ключів на основі математичного методу Crystal-Kyber. В подальшому після річного дослідження у США були прийняті федеральні стандарти FIPS 203 на основі Crystal-Kyber, FIPS 204 на основі Crystall-Delithium та FIPS 205 на основі геш-функції. Щодо математичного методу Falcon продовжено дослідження його безпечності.

На національному рівні було прийнято рішення взяти за основу математичні методи Crystall-Delithium, Crystal-Kyber, Falcon та ЕП на основі одноразових ключів.

Крім того, було оголошено продовження досліджень на 4-му раунді та було організовано конкурс на розроблення альтернативних варіантів електронного підпису. Серед видів ЕП поданих на розгляд до першого раунду додаткового процесу стандартизації наявні наступні: підписи засновані на кодах, підписи на ізогеніях, мультиваріативні підписи, симетричні підписи, MPC-in-the-head та підписи визначені NIST як "інші".

Аналіз показав, що з’явилось багато пропозицій на переших раундах конкурсів: 69 на першому конкурсі та 40 на конкурсі альтернативних варіантів ЕП. Виникла проблема оцінки та порівняльного аналізу кандидатів. Наші дослідження показали, що на основі моделей порушника, моделей загроз та моделей безпеки оцінювати і порівнювати кандидатів за умови використання криптоаналітиком класичних квантових атак та атак по бічним каналам з використанням системи [] безумовних, умовних та прагматичних критеріїв. Таким чином поряд з розробкою квантовостійких ЕП і виникла проблемна задача розроблення методичних основ оцінки та порівняння асиметричних криптоперетворень, в тому числі ЕП. Вирішення як теоретичної так і практичної задачі дозволило на основі математичних решіток розробити та прийняти квантовостійкі ЕК ДСТУ 9212:2023 та протокол АСШ та інкапсуляції ключів ДСТУ 8961:2019.

Для вирішення проблемних задач в 2-5 розділах вирішуються науково-практичні задачі обгрунтування, аналізу, дослідження, оцінки та порівняння існуючих та перспективних квантовостійких електронних підписів по сукупності безумовних, умовних та прагматичних критеріїв.

У другому розділі дисертації (*Модель безпеки та критерії оцінки і порівняння перспективних постквантових електронних підписів*) обгрунтовано моделі порушника, загроз та безпеки. Показано, що асиметричні електронні підписи мають множину різноманітних застосувань, котрі висувають дещо відмінні один від одного вимоги до криптографічних перетворень типу асиметричний електронний підпис. Наведено переліки безумовних, умовних та прагматичних критеріїв.

У третьому розділі дисертації (*Науково-методичні основи розробки, оцінки та порівняння існуючих та перспективних квантовостійких електронних підписів за безумовними, умовними та прагматичними критеріями*) обгрунтовано комплексну методику оцінки та порівняльного аналізу асиметричних електронних підписів, стійких до класичного та

квантового криптоаналізу. Запропоновано вдосконалення комплексної методики оцінки та порівняльного аналізу в частині врахування в процесі оцінки та порівняння за прагматичними критеріями мети здійснення порівняння та можливих варіантів застосування ЕП, що призодить до збільшення точності та відповідності отриманого результату вихідним вимогам.

У четвертому розділі дисертації (*Аналіз, оцінка та порівняння існуючих та кандидатів на перспективні квантовостійкі національні та міжнародні електронні підписи за безумовними критеріями*) здійснено оцінку та порівняльний аналіз як кандидатів на стандартизацію між собою, так і вже стандартизованих для використання в перехідний та пост-квантовий періоди алгоритми електронного підпису між собою. Проведено порівняння отриманих результатів порівняння вже стандартизованих алгоритмів з міжнародними результатами.

У п’ятому розділі дисертації (*Програмне моделювання та експериментальні дослідження процесів порівняння за безумовними критеріями*) уточнено оцінки та отримано експерементальні результати порівняння електронних підписів за допомогою розробленого програмного забезпечення. Для електронного підпису Falcon запропонована атака відновлення ключів та досліджено вплив використання фіксованої точки замість плаваючої точки в процесі формування підпису на безпеку.

Ключові слова: електронний підпис, шифрування, цілісність, конфіденційність, кібербезпека, інформаційна безпека, система безпеки, криптоаналіз, квантовостійка криптографія, порівняльний аналіз, асиметричні криптосистеми, ізогенія еліптичної кривої

ABSTRACT

Kaptol Ye. Yu. Methods for evaluation and comparative analysis of asymmetric electronic signatures resistant to classical and quantum cryptanalysis. – Qualification scholarly paper: a manuscript.

Thesis submitted for obtaining the Doctor of Philosophy degree in Information Technologies, Speciality 125 – Cyber Security. – V. N. Karazin Kharkiv National University, Ministry of Education and Science of Ukraine, Kharkiv, 2024.

In the conditions of the rapid development of quantum technologies at the international and national levels, the issue of choosing and standardizing quantum-resistant cryptographic transformations is being resolved. This is due to the significant increase in the speed of calculations and challenges to the security of cryptographic transformations, which are predicted if a quantum computer of sufficient power is used for cryptanalysis. Because of this, NIST launched the NIST PQC competition, designed to select candidates for standardization in the field of quantum-resistant cryptographic transformations. On the other hand, ad hoc attacks based on side-channel leaks and errors can pose a major threat. Therefore, both at the international and national levels, it is important to respond to the capabilities of top-level cryptanalysts and determine the requirements and develop promising secure crypto-transformations of electronic signatures and standardize them, including at the national level.

The dissertation work is devoted to the solution of the actual problem: analysis and research, evaluation and comparison of existing and promising quantum-resistant electronic signatures according to a set of unconditional, conditional and pragmatic criteria.

The purpose and tasks of the research. Justification of the choice, analysis and research, evaluation and comparison of existing and prospective quantum-resistant electronic signatures according to a set of unconditional, conditional and pragmatic criteria.

To achieve the goal, the following tasks were solved:

1. Analysis of the current state of security and substantiation of the requirements for methods of promising quantum-resistant electronic signatures.
2. Justification of models of the violator and threats, as well as in general security models of promising post-quantum electronic signatures and sets of unconditional, conditional and pragmatic criteria for their evaluation and comparison.
3. Scientific and methodological bases for the development, assessment and comparison of existing and promising quantum-resistant electronic signatures according to unconditional, conditional and pragmatic criteria.
4. Analysis, assessment and comparison of existing and prospective quantum-resistant national and international electronic signatures according to unconditional criteria (security).
5. Software modeling of practical evaluation tools and comparison of projects and standardized international and national quantum-resistant electronic signatures.

In the first chapter of the dissertation (Analysis of the security status of existing and justification of requirements for methods of promising quantum-resistant electronic signatures) based on the search for sources devoted to the justification of requirements and security models, it was found that the problems of protection against a new class of quantum attacks arose several decades ago, but the feeling of threat it was accepted from them only after the appearance in 2015 of the article by professors Menesis and Koblitz [], who essentially stated the low security of existing asymmetric cryptographic transformations, including electronic signatures against quantum attacks implemented on quantum computers that are being developed. The article indicated that quantum-resistant asymmetric cryptotransformations can be built on the basis of new mathematical methods: modular transformations (mathematical lattices), mathematical codes, quadratic fields, isogenies of elliptic curves, hash functions based on cryptography. This was followed by a scientific conference in Japan, at which a positive decision was made to create quantum-resistant cryptotransformations. The US NIST, based on the

decisions, announced a competition for the development of projects of standards for quantum-resistant asymmetric kpritotransformations, including EP. In the following years, three rounds took place, and in 2022, at the NIST USA forum, the conference decided to standardize and in NIST 8413 [] a list of standardized EP EPs based on mathematical lattices, such as the Crystall-Delithium and Falcon EP projects, as well as based on the use of disposable keys using a hash function. It was also decided to standardize key encapsulation protocols based on the Crystal-Kyber mathematical method. Subsequently, after a year of research, the US federal standards FIPS 203 based on Crystal-Kyber, FIPS 204 based on Crystall-Delithium, and FIPS 205 based on a hash function were adopted. Regarding the Falcon mathematical method, the study of its safety has been continued.

At the national level, it was decided to take as a basis the mathematical methods of Crystall-Delithium, Crystal-Kyber, Falcon and EP based on one-time keys.

In addition, the continuation of research in the 4th round was announced and a competition was organized for the development of alternative options for electronic signature. [] Among the types of EP submitted for consideration to the first round of the additional standardization process are the following [6,7]: signatures based on codes, signatures on isogenies, multivariate signatures, symmetric signatures, MPC-in-the-head, and signatures defined by NIST as "other".

The analysis showed that there were many proposals in the first rounds of tenders: 69 in the first tender and 40 in the tender of alternative EP options. There was a problem of evaluation and comparative analysis of candidates. Our research has shown that based on intruder models, threat models, and security models, candidates can be evaluated and compared under the condition that the cryptanalyst uses classical quantum attacks and side-channel attacks using a system of [] unconditional, conditional, and pragmatic criteria. Thus, along with the development of quantum-resistant EPs, the problematic task of developing methodical bases for evaluating and comparing asymmetric cryptotransformations, including EPs, arose.

The solution of both theoretical and practical problems made it possible to develop and adopt quantum-resistant EC DSTU 9212:2023 and the ASSH protocol and key encapsulation DSTU 8961:2019 on the basis of mathematical lattices.

In order to solve problematic problems, scientific and practical problems of substantiation, analysis, research, evaluation and comparison of existing and promising quantum-resistant electronic signatures are solved in chapters 2-5 according to a set of unconditional, conditional and pragmatic criteria.

In the second chapter of the dissertation (Security model and criteria for evaluating and comparing promising post-quantum electronic signatures), the models of the intruder, threats and security are substantiated. It is shown that asymmetric electronic signatures have a variety of applications, which put forward somewhat different requirements for cryptographic transformations of the asymmetric electronic signature type. Lists of unconditional, conditional and pragmatic criteria are given.

In the third chapter of the dissertation (Scientific and methodological foundations of the development, evaluation and comparison of existing and promising quantum-resistant electronic signatures according to unconditional, conditional and pragmatic criteria), a comprehensive methodology for the evaluation and comparative analysis of asymmetric electronic signatures resistant to classical and quantum cryptanalysis is substantiated. An improvement of the comprehensive methodology for the evaluation and comparative analysis is proposed in terms of taking into account in the process of evaluation and comparison according to pragmatic criteria the purpose of the comparison and possible options for the application of the EP, which will contribute to increasing the accuracy and compliance of the obtained result with the initial requirements.

In the fourth chapter of the dissertation (Analysis, evaluation and comparison of existing and candidates for promising quantum-resistant national and international electronic signatures according to unconditional criteria), an evaluation and comparative analysis of both candidates for standardization among themselves

and already standardized for use in the transitional and post-quantum periods electronic signature algorithms among themselves is carried out. The obtained results of the comparison of already standardized algorithms with international results were compared.

In the fifth chapter of the dissertation (Software modeling and experimental studies of comparison processes by unconditional criteria), the estimates are refined and experimental results of the comparison of electronic signatures are obtained using the developed software. For the Falcon electronic signature, a key recovery attack is proposed and the impact of using a fixed point instead of a floating point in the signature formation process on security is investigated.

Keywords: digital signature, encryption, integrity, sensitivity, cybersecurity, information security, security system, cryptanalysis, quantum-resistant cryptography, comparative analysis, asymmetric cryptosystems, elliptic curve isogeny