Харківський національний університет імені В.Н. Каразіна
Міністерство освіти і науки України

Кваліфікаційна наукова
праця на правах рукопису

Каптьол Євгеній Юрійович

УДК 004.056.5

ДИСЕРТАЦІЯ

МЕТОДИ ОЦІНКИ ТА ПОРІВНЯЛЬНОГО АНАЛІЗУ АСИМЕТРИЧНИХ ЕЛЕКТРОННИХ ПІДПИСІВ, СТІЙКИХ ДО КЛАСИЧНОГО ТА КВАНТОВОГО КРИПТОАНАЛІЗУ

Спеціальність 125 Кібербезпека та захист інформації
(Галузь знань 12 Інформаційні технології)

Подається на здобуття ступеня доктора філософії

Дисертація містить результати власних досліджень. Використання ідей, результатів і текстів інших авторів мають посилання на відповідне джерело.
_____ Є.Ю. Каптьол

Науковий керівник: Горбенко Іван Дмитрович, доктор технічних наук, професор

Харків – 2025

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 [1],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 [2] 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.[3] Серед видів ЕП поданих на розгляд до першого раунду додаткового процесу стандартизації наявні наступні [3, 4]: 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 [5] 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 ЕП 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 for the degree of Doctor of Philosophy in speciality 125 Cyber Security and information protection (Field of knowledge 12 Information Technology). – V. N. Karazin Kharkiv National University, Ministry of Education and Science of Ukraine, Kharkiv, 2025.

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 [1], 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 [2] 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. [3] Among the types of EP submitted for consideration to the first round of the additional standardization process are the following [3, 4]: 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 [5] 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

СПИСОК ПУБЛІКАЦІЙ ЗДОБУВАЧА ЗА ТЕМОЮ ДИСЕРТАЦІЇ

Наукові публікації у наукових виданнях, включених до наукометричної бази Scopus

1. Potii, O., Kachko, Potii, O., Kachko, O., Kandii, S., & Kaptol, Y. (2024). Determining the effect of a floating point on the Falcon digital signature algorithm security. Eastern-European Journal of Enterprise Technologies, 1(9 (127), 52–59.

DOI: 10.15587/1729-4061.2024.295160.

URL: https://journals.uran.ua/eejet/article/view/295160/291714

2. Kachko O.G., Gorbenko Y.I., Kandii S.O., Kaptol Y.Y. Improving protection of falcon electronic signature software implementations against attacks based on Floating Point Noise // Eastern-European Journal of Enterprise Technologies. 2024. Vol. 4, Is. 9, P. 6–17.

DOI:10.15587/1729-4061.2024.310521

URL: https://journals.uran.ua/eejet/article/view/310521/302039

Наукові публікації у фахових виданнях України

3. Kaptiol, Y. Y. (2022). Analysis of the RAINBOW post-quantum electronic signature algorithm state and attacks on it for the period of the NIST PQC third round completion. // Каптьол, Є. Ю. Аналіз стану постквантового алгоритму електронного підпису RAINBOW та атак на нього на період завершення третього раунду NIST PQC. Radiotekhnika, 2(209), 87–92.

DOI: 10.30837/rt.2022.2.209.09

URL: http://rt.nure.ua/article/view/262495/258911

4. Yu.I. Gorbenko, M.V. Yesina, V.A. Ponomar, I.D. Gorbenko, E.Yu. Kapt'ol Scientific and methodological bases of analysis, evaluation and results of comparison of existing and promising (post-quantum) asymmetric cryptographic primitives of electronic signature, protocols of asymmetric encryption and key encapsulation protocols // Ю.І. Горбенко, М.В. Єсіна, В.А. Пономар, І.Д. Горбенко, Є.Ю.

Каптьол. Науково-методичні основи аналізу, оцінки та результати порівняння існуючих та перспективних (постквантових) асиметричних криптографічних примітивів електронного підпису, протоколів асиметричного шифрування та протоколів інкапсуляції ключів. Radiotekhnika, 212, 42-66.

DOI: 10.30837/rt.2023.1.212.05

URL: http://rt.nure.ua/article/view/286512/280398

(Особистий внесок здобувача: Формування безумовних критеріїв оцінки та порівняння із врахуванням моделей порушника, загроз та безпеки, що базуються на міжнародних вимогах дотримання моделей EUF-CMA для ЕП та IND-CCA2 для АСШ. Аналіз та оцінка за критеріями безумовної стійкості, програмне моделювання процесів оцінки за безумовними критеріями. Особистий внесок Ю.І. Горбенко: Дослідження та вирішення питань впровадження методики оцінки та порівняння квантовостійких криптографічних перетворень за сукупностями безумовних, умовних та прагматичних критеріїв. Особистий внесок М.В. Єсіна: Пошук та формування сукупностей безумовних, умовних та прагматичних критеріїв для процесу оцінки та порівняння. Формування критеріїв вимог у відповідності до міжнародних та національних нормативних документів, таких як NIST.IR 8413 та IT Grundschutz Compedium. Особистий внесок В.А. Пономар: програмне моделювання процесів оцінки за сукупностями умовних та прагматичних критеріїв. Особистий внесок І.Д. Горбенко: постановка проблеми дослідження, перевірка наукової достовірності отримуваних результатів, перевірка тексту роботи, вибір методів та проведення порівняння за методами експертних оцінок).

5. Є. Ю. Каптьол, І. Д. Горбенко. Аналіз можливостей та особливості програмування задач криптології на квантовому комп’ютері. Radiotekhnika, 202, 37-48.

DOI: 10.30837/rt.2020.3.202.03

URL: http://rt.nure.ua/article/view/215822/215989

(Особистий внесок здобувача: Дослідження стану побудови квантових комп'ютерів на предмет оцінки можливості створення криптоаналітично значущого квантового комп'ютера. Виділення математичних методів квантового криптоаналізу для оцінки властивостей існуючих квантових комп'ютерів. Реалізація масштабованого методу квантового криптоаналізу на квантовому комп'ютері. Порівняння теоретичних розрахунків застосування обраного методу з результатами практичного застосування. Особистий внесок І.Д. Горбенко: постановка проблеми дослідження, перевірка наукової достовірності отримуваних результатів, перевірка тексту роботи).

6. Gorbenko, I., & Kaptol, Y. (2023). Analysis and comparison of the security of electronic signatures based on new quantum-resistant problems. Radiotekhnika, 4(215), 31–45.

DOI: 10.30837/rt.2023.4.215.04

URL: http://rt.nure.ua/article/view/299724/292240

(Особистий внесок здобувача: Дослідження кандидатів стандартизацію в якості квантовостійкого стандарту електронного підпису на конкурсі NIST зі стандартизації додаткових електронних підписів. Виділення безумовних критеріїв для оцінки та порівняння кандидатів на стандартизацію, що базуються на нових квантовостійких проблемах. Оцінка та порівняння обраних кандидатів на стандартизацію за безумовними критеріями. Особистий внесок Gorbenko, I.: постановка проблеми дослідження, перевірка наукової достовірностіотримуваних результатів, перевірка тексту роботи).

Наукові праці, які засвідчують апробацію матеріалів дисертації

7. Євгеній Каптьол. Key encapsulation mechanisms security in the random oracle model / Безпека механізмів інкапсуляції ключів у моделі випадкового оракула // "Захист інформації і безпека інформаційних систем" збірник

матеріалів IX Міжнародної науково-технічної конференції. Львів – 2023. pp. 67 – 68.

8. Каптьол Є.Ю. Аналіз квантових методів криптоаналізу постквантового електронного підпису Rainbow // “Системи і технології зв’язку, інформатизації та кібербезпеки: актуальні питання і тенденції розвитку” збірник матеріалів I Міжнародної науково-технічної конференції. Київ – 2021. pp. 146 – 147.

9. Yevhenii Kaptol. Analysis of quantum attacks against rainbow post-quantum electronic signature // Information protection and information systems security proceedings of VIIIth International Scientific and Technical Conference November 11–12, 2021. Lviv Polytechnic Publishing House 2021. pp. 77-78.

10. Каптьол. Є.Ю. Порівняння електронних підписів, що грунтуються на нових постквантових проблемах // Системи і технології зв’язку, інформатизації та кібербезпеки: актуальні питання і тенденції розвитку: збірник матеріалів III Міжнародної науково-технічної конференції. - Київ: Військовий інститут телекомунікацій та інформатизації імені Героїв Крут, 2023, pp. 166-167 DOI: https://doi.org/10.61929/viti.mntk.3.2023

11. Потій О. В., Качко О. Г., Кандій С. О., Каптьол Є. Ю. Дослідження впливу плаваючої точки на безпеку алгоритму електронного підпису Falcon // Кіберборотьба: розвідка, захист та протидія: тези доповідей II Міжнародної науково-практичної конференції. - Київ: Військовий інститут телекомунікацій та інформатизації імені Героїв Крут, 2024.-57с.

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ 19
ВСТУП 21
РОЗДІЛ 1. АНАЛІЗ СТАНУ БЕЗПЕКИ ІСНУЮЧИХ ЕЛЕКТРОННИХ ПІДПИСІВ ТА ОБГРУНТУВАННЯ ВИМОГ ДО МЕТОДІВ ПЕРСПЕКТИВНИХ (ПОСТКВАНТОВИХ) ЕЛЕКТРОННИХ ПІДПИСІВ 28
1.1. Обгрунтування та аналіз безпеки існуючих електронних підписів при застосуванні в перехідний та постквантовий періоди 28
1.2. Аналіз вимог до методів, алгоритмів та засобів електронних підписів у постквантовий період 36
1.3. Стан розробки квантовостійких електронних підписів на міжнародному та національному рівнях 40
1.3.1. Роботи зі стандартизації на міжнародному рівні. 40
1.3.2. Роботи зі стандартизації на національному рівні. 43
1.4. Постановка задач щодо методичних основ аналізу, оцінки та порівняння асиметричних квантовостійких криптоперетворень електронного підпису та протоколів інкапсуляції ключів 45
1.5. Висновки до розділу 1 46
РОЗДІЛ 2. МОДЕЛЬ БЕЗПЕКИ ТА КРИТЕРІЇ ОЦІНКИ І ПОРІВНЯННЯ ПЕРСПЕКТИВНИХ ПОСТКВАНТОВИХ ЕЛЕКТРОННИХ ПІДПИСІВ 48
2.1. Особливості застосування електронних підписів на практиці 48
2.2. Аналіз особливостей моделей порушника та загроз щодо безпеки постквантових електронних підписів 55
2.2.1. Модель порушника 55
2.2.2. Модель загроз 58
2.3. Модель безпеки щодо постквантових електронних підписів 60
2.4. Опис безумовних критеріїв 61
2.5. Опис умовних критеріїв 65

2.6. Опис прагматичних критеріїв 67

2.7. Особливості процесу оцінки та порівняння..... 70

2.8. Висновки до розділу 2..... 72

РОЗДІЛ 3. НАУКОВО-МЕТОДИЧНІ ОСНОВИ РОЗРОБКИ, ОЦІНКИ ТА ПОРІВНЯННЯ ІСНУЮЧИХ ТА ПЕРСПЕКТИВНИХ КВАНТОВОСТІЙКИХ ЕЛЕКТРОННИХ ПІДПИСІВ ЗА БЕЗУМОВНИМИ, УМОВНИМИ ТА ПРАГМАТИЧНИМИ КРИТЕРІЯМИ 74

3.1. Обґрунтування, опис, призначення та застосування комплексної методики оцінки, аналізу та порівняння 74

3.1.1. Обґрунтування поняття комплексної методики оцінки та порівняння 74

3.1.2. Обґрунтування, призначення та застосування комплексної методики оцінки, аналізу та порівняння 78

3.2. Обґрунтування та вибір критеріїв та показників оцінки та порівняння 82

3.3. Опис комплексної методики оцінки та порівняння 84

3.3.1. Загальний зміст та опис комплексної методики 84

3.3.2. Результати використання методики та практичні рекомендації 86

3.4. Обґрунтування особливостей застосування методів експертних оцінок 89

3.5. Обґрунтування вдосконалення точності комплексної методики оцінки та порівняльного аналізу 91

3.6. Висновки до розділу 3..... 92

РОЗДІЛ 4. АНАЛІЗ, ОЦІНКА ТА ПОРІВНЯННЯ ІСНУЮЧИХ ТА КАНДИДАТІВ НА ПЕРСПЕКТИВНІ КВАНТОВОСТІЙКІ НАЦІОНАЛЬНІ ТА МІЖНАРОДНІ ЕЛЕКТРОННІ ПІДПИСИ ЗА БЕЗУМОВНИМИ КРИТЕРІЯМИ..... 95

4.1. Аналіз кандидатів додаткового конкурсу на квантово-стійкий електронний підпис 95

4.2. Порівняння кандидатів додаткового конкурсу на квантово-стійкий електронний підпис 112

4.3. Порівняння перспективних механізмів ЕП..... 115

4.4. Порівняння отриманих результатів з міжнародними оцінками перспективних механізмів ЕП..... 120

4.5. Висновки до розділу 4..... 124

РОЗДІЛ 5. МОДЕЛЮВАННЯ ТА ЕКСПЕРИМЕНТАЛЬНІ ДОСЛІДЖЕННЯ ПРОЦЕСІВ ПОРІВНЯННЯ ТА ЇХ МОДИФІКАЦІЇ 126

5.1. Постановка задач експериментальних досліджень з порівняння існуючих та перспективних електронних підписів..... 126

5.2. Логіка побудови модифікованої моделі для проведення порівняння 127

5.3. Результати експериментальних досліджень оцінки та порівняння методів електронного підпису 133

5.4. Виявлені в ході дослідження недоліки в безпеці методів електронного підпису..... 146

5.5. Пропозиції з усунення виявлених недоліків в безпеці методів електроннного підпису..... 152

5.6. Рекомендації із застосування комплексної методики оцінки та порівняння постквантових електронних підписів..... 155

5.7. Висновки до розділу 5..... 157

ВИСНОВКИ..... 159

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ..... 163

Додаток А..... 173

Додаток Б 178

Додаток В 179

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ

АСШ – Асиметричні шифри

ЕП – Електронний підпис

ІВК – інфраструктура відкритих ключів

КЗІ – Криптографічний захист інформації

КЗКК – Криптоаналітично значущий квантовий комп’ютер

КСЗІ – комплексна система захисту інформації

ПІК – Протоколи інкапсуляції ключів

СУІБ – система управління інформаційною безпекою

EUF-CMA – existentially unforgeable under adaptive chosen message attacks, забезпечення захисту від екзістенціональної підробки в умовах адаптивного вибору повідомлення; модель безпеки для електронних підписів

IND-CCA – indistinguishability under chosen-ciphertext attack, нерозрізнювальність для атак з адаптивно обраним шифротекстом; модель безпеки для механізмів інкапсуляції ключів

IND-CPA – indistinguishability under chosen-plaintext attack, атака з адаптивно обраним повідомленням; модель безпеки для механізмів інкапсуляції ключів

IPSec – набір протоколів для забезпечення захисту даних, що передаються за допомогою протоколу IP

KEM – key encapsulation mechanism, механізм інкапсуляції ключів

NIST – національний орган зі стандартизації у США

NIST PQC – NIST Post-Quantum Cryptography Standardization конкурс з відбору для сандартизації квантовостійких алгоритмів від NIST

PKE – public key encryption, шифрування з відкритим ключем

SA – Безпечний зв’язок («Security Association»)

SADB – База даних безпечних зв'язків (Security Associations Database)

SSH – secure shell, протокол захищеної передачі команд через незахищену мережу

SUF-CMA –Strong Existential Unforgeability under Chosen Message Attack, Сильна екзистенційна непідроблюваність при атаці на основі адаптивно вибраних повідомлень; модель безпеки для електронних підписів

TLS – Transport Layer Security, криптографічний протокол захисту транспортного рівня

ВСТУП

Обґрунтування вибору теми дослідження.

Нині на міжнародному та національному рівні є актуальним питання забезпечення криптографічної стійкості стандартизованих асиметричних криптографічних перетворень, обгрунтування та стандартизації електронних підписів, які б забезпечували безумовну стійкість до класичних та квантових атак та атак сторонніми каналами (спеціальними каналами). Вказане пов’язано з тим, що для них розроблено математичні методи для реалізації атак, як на основі класичного, так і квантового криптоаналізу. Також важливу роль відіграє те, що за прогнозами в найближчі роки можливо буде розроблений надпотужний квантовий комп’ютер, який зможе зламувати існуючі криптосистеми орієнтуючись на використання вже існуючих квантових математичних методів [1, 2, 6-8]. Також велику загрозу можуть становити спеціальні атаки, що ґрунтуються на витоках побічними каналами та на основі помилок [6, 8, 9]. Тому важливо, як в теоретичному, так і в практичному змісті, зреагувати на можливості криптоаналітиків найвищого рівня та визначити вимоги та розробити методи оцінки іпорівняння за відповідністю до цих вимог перспективних захищених асиметричних криптографічних перетворень як серед вже стандартизованих так і кандидатів на стандартизацію.

До основних методів і задач криптоаналізу, що можуть бути вирішені за допомогою квантового комп’ютера та становлять загрозу для сучасних криптоперетворень можна віднести наступні [6-8]:

1. алгоритм Гровера для пошуку в несортованій базі;
2. алгоритм факторизації Шора;
3. алгоритм Шора для розв’язку дискретного логарифму в скінченному полі;
4. алгоритм Шора для розв’язку дискретного логарифму в групі точок еліптичної кривої.

Саме через загрозу з боку квантових технологій NIST США було організовано конкурс NIST PQC [2, 10-12], де було проведено три раунди

відбору кандидатів на стандартизацію, розроблено проекти стандартів та продовжено дослідження в четвертому раунді. Після проведення трьох раундів NIST PQC для стандартизації було обрано 4 кандидати (електронні підписи (ЕП) CRYSTALS-Dilithium, Falcon та SPHINCS+ та механізм інкапсуляції ключа CRYSTALS-Kyber). Також було визначено кандидатів для участі в четвертому раунді (криптографічні перетворення механізмів інкапсуляції ключів BIKE, Classic McEliece, HQC та SIKE), один з яких його розробники визнали ненадійним для використання (SIKE) [2, 13, 14].

Специфіка обраних завдяки трьом раундам конкурсу NIST алгоритмів призвела до потреби у пошуку для стандартизації додаткових кандидатів з числа електронних підписів загального призначення. Для цього було розпочато окремий процес стандартизації схем електронного підпису (також відомий як «процес стандартизації додаткових підписів»). Одним з критеріїв, що призвели до цього є потреба у ЕП, що не базуються на використанні решіток (хоча слід зауважити, що попри це у додатковому раунді все одно беруть участь схеми ЕП, що базуються на решітках) [4]. Серед видів ЕП поданих на розгляд до першого раунду додаткового процесу стандартизації наявні наступні [3,4]: підписи засновані на кодах, підписи на ізогеніях, мультиваріативні підписи, симетричні підписи, MPC-in-the-head та підписи визначені NIST як "інші".

Таким чином, можна зробити висновок, що сучасний стан забезпечення безпеки електронними підписами потребує розробки та покращення засобів та методів оцінки захищеності асиметричних криптографічних примітивів та порівняння їх з метою виділення кращих по множині безумовних, умовних та прагматичних критеріїв, що обгрунтовується задачею розробки методичних основ оцінки та порівняння. В таких методичних основах повинні бути обгрунтовані безумовні критерії оцінки безпечності електронних підписів від класичних, квантових атак та атак бічними каналами та на основі помилок. По суті ці задачі зводяться до теоретичного доведення стійкості електронних підписів по моделі безпеки EUF-CMA (existentially unforgeable under adaptive chosen message attacks), тобто забезпечення захисту від екзістенціональної

підробки в умовах адаптивного вибору повідомлення [15]. Під квантовостійкими будемо розуміти електронні підписи, що є стійкими як до класичних так і до квантових атак. Проблеми захищеності від атак бічними каналами у зв’язку зі складністю в цій роботі не розглядаються.

Зв'язок роботи з науковими програмами, планами, темами.

Дослідження, результати яких знайшли відображення в дисертаційній роботі, виконані на кафедрі безпеки інформаційних систем і технологій Харківського національного університету імені В. Н. Каразіна та у приватному акціонерному товаристві «Інститут інформаційних технологій». Результати дисертаційних досліджень використані при розробці та прийнятті в якості національних стандартів ДСТУ 8961:2019 "Інформаційні технології. Криптографічний захист інформації. Алгоритми асиметричного шифрування та інкапсуляції ключів" [16] та ДСТУ 9212:2023 "Інформаційні технології. Криптографічний захист інформації. Алгоритм електронного підпису на алгебраїчних решітках із відхилами" [17] (акт від 06.12.2023 р.).

Результати дисертаційних досліджень були використані при підготовці та проведенні лабораторних робіт по дисципліні «Прикладна Криптологія» для спеціальності «Кібербезпека».

Мета і завдання дослідження.

Мета 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 такі задачі:

- Аналіз стану безпеки існуючих та обгрунтування вимог до методів перспективних квантовостійких електронних підписів.
- Розробка удосконаленої методології оцінки та порівняння існуючих та перспективних квантовостійких електронних підписів по безумовним, умовним та прагматичним критеріям, яка дозволила б

оцінити, порівняти і обрати найбільш перспективні ЕП, і в тому числі виявити вразливості в них.

- Аналіз, оцінка та порівняння існуючих та кандидатів на песпективні квантовостійкі національні та міжнародні електронні підписи.
- Аналіз безпеки математики Falcon і Сокіл, реалізація атаки на відновлення таємних ключів та розробка пропозицій щодо захисту від неї.
- Застосування методології для отримання практичної оцінки та порівняння проєктів та стандартизованих міжнародних та національних квантовостійких електронних підписів.

Об'єкт дослідження: процеси вибору, аналізу та дослідження, оцінки та порівняння існуючих та перспективних квантовостійких електронних підписів по сукупності безумовних, умовних та прагматичних критеріїв.

Предмет дослідження: методи аналізу та дослідження, оцінки та порівняння існуючих та перспективних квантовостійких електронних підписів по сукупності безумовних, умовних та прагматичних критеріїв.

Методи дослідження: методи системного аналізу та прийняття рішень, методи прикладної криптології, методи класичного та квантового криптоаналізу, методи оцінки та порівяння асиметричних електронних підписів, що відповідають сучасним вимогам до національних та міжнародних стандартів, методи математичного моделювання, методи захищеності від квантового криптоаналізу на основі масштабування.

Наукова новизна отриманих результатів.

1. Вперше отримано оцінки порівняльного аналізу вже стандартизованих та кандидатів на стандартизацію квантовостійких ЕП із математичною адаптацією вимог, викликаних особливостями різних варіантів застосування. Попередні дослідження фокусувалися на безпекових вимогах,

котрі входять до першого та частково другого етапів комплексної методики оцінки та порівняльного аналізу квантовостійких та перспективних асиметричних криптоперетворень. Отримані оцінки дозволяють більш точно оцінити придатність до використання оцінюваних криптоперетворень в перехідний та пост-квантовий періоди.

2. Удосконалено комплексну методику оцінки та порівняльного аналізу асиметричних ЕП, стійких до класичного та квантового криптоаналізу, що відрізняється від існуючих тим, що враховує спрямованість та мету здійснення оцінки та порівняльного аналізу та вводить коефіцієнти значущості, котрі збільшують точність визначення найбільш відповідного переможця.

3. Вперше отримано оцінку ймовірності реалізації атаки та впливу виявлених недоліків методу та потенційних векторів атак на захищеність Falcon із врахуванням релевантних моделей безпеки.

4. Обгрунтовано особливостей заміни плаваючої точки на фіксовану точку з метою усунення загрози атаки на відновлення ключів на алгоритм з переліку порівнюваних.

Практичне значення отриманих результатів.

1. Математичні моделі та аналітичні співвідношення знайшли практичне застосування в ХНУ імені В. Н. Каразіна на кафедрі БІСТ в дисциплінах першого рівня вищої освіти “Прикладна криптологія” при проведенні лабораторних робіт.

2. Розроблено програмне забезпечення, яке дозволяє:

- Проведення оцінки існуючих та перспективних методів електронного підпису.
- Проведення покращеного оцінювання та порівняння ЕП із врахуванням мети здійснення оцінювання та спрямованості варіанту застосування ЕП
- Моделювання комплексної методики оцінки та порівняння існуючих та перспективних методів електронного підпису

3. Результати дисертаційних досліджень впровадженні у Приватному акціонерному товаристві «Інститут інформаційних технологій», м. Харків (акт від 06.12.2023 р.) та були використані при розробці стандартів ДСТУ 8961:2019, ДСТУ 9212:2023.

Особистий внесок здобувача.

У наукових статтях, опублікованих у співавторстві, автору належать наступні результати:

- Порівняння наборів параметрів фіналісту третього раунду NIST PQC алгоритму Rainbow за критеріями захищеності та порівняння методів атак на алгоритм Rainbow за критеріями складності [18];

- Верифікація та аналіз результатів здійснення атаки на алгоритм Falcon, оцінка ймовірності її реалізації та впливу виявлених недоліків методу та потенційних векторів атак на захищеність ЕП Falcon із врахуванням релевантних моделей безпеки [19, 20];

- Оцінка впливу на безпеку електронного підпису Falcon застосування фіксованої точки замість плаваючої точки на етапі генерації підпису [21];

- Формування безумовних критеріїв оцінки та порівняння із врахуванням моделей порушника, загроз та безпеки, проведення аналізу та оцінки криптографічних перетворень за безумовними критеріями та програмне моделювання процесів оцінки за безумовними критеріями [5];

- Дослідження кандидатів на стандартизацію в якості квантовостійкого стандарту електронного підпису на конкурсі NIST зі стандартизації додаткових електронних підписів, що базуються на нових квантовостійких проблемах, за безумовними критеріями [22].

Апробація результатів дисертації здійснювалася на I Міжнародній науково-технічній конференції “Системи і технології зв’язку, інформатизації та кібербезпеки: актуальні питання і тенденції розвитку” 25 – 26 листопада 2021 року, м. Київ; на VIIIth International Scientific and Technical Conference «Information protection and information systems security proceedings» November

11–12, 2021, м. Львів; на III Міжнародній науково-технічній конференції «Системи і технології зв'язку, інформатизації та кібербезпеки: актуальні питання і тенденції розвитку», Військовий інститут телекомунікацій та інформатизації імені Героїв Крут. 30 листопада 2023 року, м. Київ; на Міжнародному науковому симпозіумі “Питання оптимізації обчислень (ПОО-XLVIII)”, присвяченому 100-річчю від дня народження академіка В.М. Глушкова 19–22 вересня 2023 р. м. Львів; на IX Міжнародній науково-технічній конференції “Захист інформації і безпека інформаційних систем” 25–26 травня, 2023 року, Львів; на II Міжнародній науково-практичній конференції «Кіберборотьба: розвідка, захист та протидія», Військовий інститут телекомунікацій та інформатизації імені Героїв Крут, 23-24 квітня 2024, м. Київ.

Публікації. Основні наукові результати за темою дисертації опубліковані у 6 статтях, із яких 4 статті у фахових наукових журналах, які входять до переліку МОН України, та 2 статті в науковому зарубіжному виданні, включеному до наукометричної бази Scopus.

Структура та обсяг дисертації. Дисертація містить вступ, п’ять розділів, висновки, три додатки, список використаних джерел. Загальний обсяг дисертації складає 180 сторінок, у тому числі 10 таблиць на окремих сторінках, 8 сторінок додатків, 10 сторінок списку використаних джерел в кількості 73 найменувань.

РОЗДІЛ 1. АНАЛІЗ СТАНУ БЕЗПЕКИ ІСНУЮЧИХ ЕЛЕКТРОННИХ ПІДПИСІВ ТА ОБГРУНТУВАННЯ ВИМОГ ДО МЕТОДІВ ПЕРСПЕКТИВНИХ (ПОСТКВАНТОВИХ) ЕЛЕКТРОННИХ ПІДПИСІВ

1.1. Обгрунтування та аналіз безпеки існуючих електронних підписів при застосуванні в перехідний та постквантовий періоди

Наразі на міжнародному та національному рівнях наявна важлива проблема аналізу шляхів зниження ризиків для криптографічних систем (особливо тих, які є вразливими для класичного чи квантового криптоаналізу). Ще однією проблемо на тому ж рівні є питання стану розробки, прийняття та впровадження в якості стандартів як на національному, так і на міжнародному рівнях постквантових криптоперетворень, особливо електронних підписів, протоколів інкапсуляції ключів та асиметричних шифрів. Тому суттєве значення для зниження ризиків для вразливих стандартизованих криптографічних систем має визначення напрямків розвитку математичних методів. На додаток до цього також варто оцінювати і досліджувати перспективи їх застосування при створенні стандартів ЕП, АШ та ПІК. Це важливо через те, що такі стандарти можуть бути зведені до обгрунтування та визначення саме математичних методів та механізмів, що лежать в їх основі та котрі надають можливість для створення квантово-стійких стандартів ЕП, АШ та ПІК. [5]

В якості підтвердження наявності ризиків для існуючих криптосистем пов’язаних із застосуванням квантових комп’ютерів та обчислень з метою злому стандартів криптографічного захисту інформації можна сприймати прийняття закону США у формі «Меморандуму про національну безпеку з просування лідерства США в галузі квантових обчислень при одночасному зниженні ризиків для вразливих криптографічних систем» від 04 травня 2022 року. Так, разом із можливими перевагами від досягнення та реалізації квантових обчислень, квантові комп’ютери здатні на реалізацію квантових обчислень будуть створювати значні ризики як для економічної так і для

національної безпеки взагалі. Конкретно це буде виражено тим, що, за достатньої розмірності квантового регістру (в кубітах) та достатньої надійності обчислень, квантовий комп'ютер буде здатний зламати більшість систем, що використовують стандартизовану асиметричну криптографію з відкритим ключем [7, 16, 17]. Таким чином, при появі такого квантового комп'ютера, він поставить під загрозу як цивільні так і військові комунікації, протоколи безпеки фінансових операцій (особливо в Інтернеті) та навіть системи нагляду та контролю критичної інфраструктури як у перехідний так і у постквантовий періоди.

Під перехідним періодом [5] розуміється проміжок часу у майбутньому, коли будуть створені та у використанні квантові комп'ютери обмежених потужностей (не достатніх для повноцінного квантового криптоаналізу) та коли класичні методи та засоби криптоаналізу будуть суттєво вдосконалені. Також в цей період можуть застосовуватись вже існуючі стандарти криптографічних перетворень, але за умови використання максимально можливих або збільшених загальносистемних параметрів та ключових даних, надійність функціонування котрих буде вважатись обмеженою.

Під постквантовим періодом [5] розуміється проміжок часу в майбутньому, коли будуть створені та у використанні квантові комп'ютери з достатніми (необхідними для успішного криптоаналізу) довжинами квантових регістрів (в кубітах) та реалізоване необхідне для їх реалізації математичне та програмне забезпечення. До реалізації математичного та програмного забезпечення входить збільшення надійності функціонування, в тому числі за рахунок виправлення помилок. Також в цей період будуть суттєво вдосконалені класичні та квантові методи.

Наразі світ та цивілізація загалом та особливо технологічна спільнота роблять значні успіхи в наукових дослідженнях та практичній реалізації та застосуванні методів та технологій, пов'язаних із квантовими обчисленнями. Також можна помітити суттєві кроки з боку керівництв держав для досягнення конкурентної переваги в тому, що стосується квантової інформаційної науки та

впровадження технологій з цієї галузі на практиці. Як вже було зазначено, значний вплив квантовий комп'ютер справить на кібербезпеку, економічну та національну безпеку. Саме через це дослідження спрямовані в першу чергу на зменшення ризиків, що виникають в наведених галузях у зв'язку з розробкою квантового комп'ютера. З боку технологічно розвинених держав визначаються конкретні дії та для зниження ризиків та кроки для переведення потенційно вразливих комп'ютерних систем на квантово-стійку криптографію, що передбачає багаторічний ретельний процес [2, 10, 11, 12, 23-26]. З метою пришвидшення отримання результатів здійснюються економічні спроби стимулювати інновації в різноманітних сферах (зокрема в першу чергу в сфері кібербезпеки). Не зважаючи на те, що спектр застосування квантового комп'ютера ще не було конкретно визначено, зрозуміло, що лідерство держав в технологічному та науковому плані значною мірою залежатиме від їх здатності зберігати конкурентну перевагу в галузі квантових обчислень та інформаційних технологій [2, 24-28]. Проте слід також зауважити, що разом з перевагами від розвитку квантових технологій, ризики для економічної та національної безпеки будуть тільки збільшуватись.

Як вже було зазначено, у відповідь на існування ризиків, що виникають від розвитку квантових обчислень та можливості їх застосування для криптоаналізу існуючих систем в США було прийнято Меморандум в галузі квантових обчислень, згідно з яким президент США встановив шестимісячний термін для переходу всіх державних установ на постквантову криптографію, що є прямим підтвердженням наявності цих ризиків. Однак, не зважаючи на цю підготовку, вважається, що квантові обчислення все одно становитимуть значні загрози для економічної та національної безпеки навіть такої держави як США. Зокрема, квантовий комп'ютер достатнього розміру та складності, що також може бути відомий як «криптоаналітично значущий квантовий комп'ютер» (далі - КЗКК), буде спроможний на криптоаналіз більшості існуючих стандартизованих криптографічних алгоритмів з відкритим ключем, що використовуються в цифрових системах США та світу. Поява такого

комп’ютера поставить під загрозу цивільні та військові комунікації, системи контролю за критичною інфраструктурою, а також порушить протоколи безпеки для більшості фінансових операцій в Інтернеті. Таким чином, квантовий комп’ютер достатньої потужності та надійності зможе зламати існуючі стандарти криптографічних перетворень, таких як наприклад стандарти асиметричної криптографії з відкритим ключем [2, 6, 10].

Фізичні реалізації квантових комп’ютерів мають переваги та недоліки в розрізі порівняння за наступними факторами:

– масштабованість - здатність створювати і керувати все більшими квантовими пристроями з більшою кількістю кубітів, використовуючи фізичні та інженерні ресурси;

– простота реалізації та сумісність з різними обчислювальними моделями;

– типовий час декогерентності - період, протягом якого характеристики квантової системи залишаються стабільними і можуть використовуватися для квантових властивостей, зокрема для квантових суперпозицій;

– швидкість і точність застосування вентилів.

Варто зауважити, що наразі існують проблеми з обґрунтованим вибором фізичної реалізації квантових комп’ютерів. Перспективні фізичні реалізації можуть бути класифіковані наступним чином [6, 16, 23]:

– Квантова оптика - інформація зберігається і захищається в станах квантів світла за допомогою поляризації або певної кількості фотонів, що може бути реалізовано на чіпі з інтегрованою оптикою.

– Надпровідні системи - інформація зберігається та обробляється в електричних ланцюгах, які використовують властивості надпровідних матеріалів.

– Топологічні системи - інформація зберігається і захищається за допомогою топологічних властивостей, нечутливих до локальних змін.

– Іонні пастки - інформація зберігається і маніпулюється властивостями іонів, обмежених електромагнітними полями.

– Квантові спінові системи - інформація зберігається та маніпулюється квантовим спіном, що може бути реалізовано в кремнієвих мікрочіпах або алмазах з азотно-заміщеними вакансіями (точковими дефектами).

– Гази холодних атомів - нейтральні атоми охолоджуються до близьких до абсолютного нуля температур, нейтральні атоми (на відміну від іонів) не відштовхуються один від одного і можуть бути використані при утворенні регулярних масивів за допомогою лазерних променів.

Наразі створення квантових комп'ютерів та їх можливості у вирішенні задач криптоаналізу оцінюються наступним чином [29-33]:

– IBM розробили 127-кубітний процесор Eagle, 433-кубітний процесор Osprey та 1121-кубітний процесор Condor. Це відповідає дорожній карті IBM щодо квантових технологій.

– IBM створили нову інтегровану квантову обчислювальну систему IBM Quantum System Two на базі покращених чіпів. Вона є основою для масштабованих квантових обчислень та функціонує в лабораторії в Йорктаун-Хайтс, Нью-Йорк. Вона становить 22 фути завширшки, 12 футів заввишки, і складається з трьох процесорів IBM Quantum Heron (133-кубітний). За заявами IBM вона поєднує кріогенну інфраструктуру з контрольною електронікою третього покоління та класичними серверами.

– Компанія D-Wave, що своїми псевдо-квантовими (гібридними) комп'ютерами з великою загальною кількістю кубітів (понад 2000 та понад 5000 кубітів), планує представити машину з понад 7000 кубітів.

Хоча ці дані заслуговують довіри, фактичний стан розробки та застосування потужних квантових комп'ютерів залишається закритим. Зрозуміло, що створення квантових комп'ютерів потребує значних інвестицій і випереджає розробку математичних, логічних та програмних основ.

Ще одним моментом, що потребує уваги є те, що потрібні нові підходи до підготовки спеціалістів з числа математиків, фізиків, алгоритмістів та програмістів тощо. Це необхідно через те, що для розробки криптографічно стійких постквантових стандартів необхідні нові математичні методи, зокрема такі, що базуються на:

– використанні математичних решіток та кодів;
– математиці ізогеніїв еліптичних кривих;
– криптографічних перетвореннях в квадратичних полях;
– та ін.

До основних задач криптоаналізу, що можуть бути вирішені за допомогою квантового комп'ютера, можна віднести такі [6, 7]:

– квантовий алгоритм факторизації Шора;
– квантовий алгоритм Гровера пошуку елемента в несортованій базі;
– квантовий алгоритм Шора для розв'язку дискретного логарифму в скінченному полі;
– квантовий алгоритм розв'язку дискретного логарифму в групі точок ЕК Шора тощо.

Разом з класичною криптографією, що базується на математичних методах та алгоритмах, активно розвивається квантова. Квантові комп'ютери відкривають нові можливості для людства, але водночас роблять існуючі методи захисту інформації неефективними. Тому, хоч квантові комп'ютери ще перебувають на етапі виходу з лабораторій, необхідність у квантово-стійкій криптографії вже існує.

Безпека та захищеність сучасних інформаційних систем та технологій базується на стійкості криптографічних перетворень, які використовуються в КЗІ. Ця стійкість обумовлена складністю розв'язання певних математичних задач, таких як факторизація великих чисел або розв'язання дискретного логарифму, які мають субекспоненційну або експоненційну складність на сучасних (класичних) комп'ютерах. Однак, за допомогою квантових

алгоритмів, таких як Шора та Гровера, деякі математичні задачі можна вирішувати з поліноміальною складністю.

Так, наприклад, квантовий алгоритм факторизації Шора добре показує на недостатню захищеність існуючої криптографії від квантового криптоаналізу. Цей квантовий алгоритм був запропонований для вирішення задачі факторизації модуля криптоперетворення в кільці, наприклад, RSA криптоперетворення. Вирішення вказаної задачі зводиться до факторизації модуля перетворення N, а класичні алгоритми факторизації мають або експоненційну, або суб'експоненційну складність. При цьому вважається, що найкращим за критерієм мінімуму складності факторизації є алгоритм загального решета числового поля та при деяких обмеженнях його модифікації – спеціальні решета числового поля. У той же час алгоритм Шора, що орієнтований на квантовий комп'ютер, має поліноміальну складність. При його застосуванні факторизацію можна здійснити зі складністю

$$O(n^3) \tag{1.1}$$

та з використанням $O(n)$ кубітів.

Порівняльний аналіз складності факторизації для класичного та квантового алгоритмів наведено у табл. 1.1 [6].

Таблиця 1.1.

Порівняння класичного та квантового алгоритмів факторизації (RSA)

Розмір модуля N, бітів	Кількість необхідних кубітів $2n$	Складність квантового алгоритму $4n^3$	Складність класичного алгоритму
512	1024	$0.54 \cdot 10^9$	$1.6 \cdot 10^{19}$
3072	6144	$12 \cdot 10^{10}$	$5 \cdot 10^{41}$
15360	30720	$1.5 \cdot 10^{13}$	$9.2 \cdot 10^{80}$

Аналіз даних табл. 1.1 показує, що для зламу RSA криптосистеми з розміром модуля у 15360 бітів (а це розмір відкритого ключа сертифікату США), необхідно лише $1.5 \cdot 10^{13}$ операцій на квантовому комп'ютері, тоді як з

використання існуючих класичних обчислювальних систем потрібно виконати порядку 1080 операцій.

Таким чином, якщо з’явиться квантовий комп’ютер з відповідними характеристиками та параметрами, RSA система буде зламана за поліноміальний час. Таким чином, добре видно, що існуючі криптографічні стандарти не є захищеними від квантового криптоаналізу на міжнародному рівні.

У випадку появи квантового комп’ютера, здатного запускати алгоритми Шора для криптоаналізу або Гровера для пошуку в неупорядкованій базі даних, виникнуть серйозні загрози для криптографічної стійкості як асиметричних, так і деяких симетричних криптоперетворень. Важливими для цього є не лише факт створення такого комп’ютера, але й його технічні характеристики, або ж іншими словами: чи є він КЗКК.

У квантовому комп’ютері ключ шифрування передається за допомогою фотонів – елементарних часток світла, завдяки реалізації квантового протоколу розподілу ключів. Будь-яка спроба перехопити дані третьою стороною вплине на стан фотона, роблячи ключ недійсним. Фотони можна передавати через спеціальні оптоволоконні лінії, на кінцях яких встановлені спеціальні шифрувальні пристрої. При цьому, значним недоліком квантової криптографії є високі витрати на інфраструктуру.

Квантово-стійка криптографія, так само як і класична, базується на розв’язанні математичних задач. Проте нові алгоритми шифрування повинні відрізнятися, щоб бути такими, які не могли б розв’язати за допустимий час ані класичні, ані квантові комп’ютери.

1.2. Аналіз вимог до методів, алгоритмів та засобів електронних підписів у постквантовий період

На початку 2016 року NSA та NIST ініціювали роботи щодо організації конкурсу на новій стандарті квантово-захищених криптографічних алгоритмів [10]. NIST наразі завершили 3 раунди конкурсу, розробили орієнтовні стандарти, розпочали четвертий раунд конкурсу та додатковий конкурс зі стандартизації додаткових квантовостійких електронних підписів.

До кандидатів сформульовані мінімальні вимоги:

- відкритість алгоритму для криптографічної спільноти та аналізу;
- реалізація у широкому діапазоні платформ;
- забезпечення як мінімум однієї з функцій: цифровий підпис, шифрування або обмін ключами;
- наявність теоретичних та емпіричних доказів щодо забезпечення вимог безпеки (стійкості).

Більш конкретні вимоги формулюються у трьох напрямках: це вимоги з безпеки (вимоги до стійкості до криптографічного аналізу), техніко-економічні вимоги (обчислювальні витрати та витрати на пам’ять), технічні характеристики реалізації алгоритмів.

Вимоги до стійкості. Мінімальною вимогою до стійкості кандидатів є еквівалент стійкості у 128 біт.

Вимоги до стійкості мають бути сформульовані у відповідностей до таких моделей загроз:

- для шифрування – в умовах моделі IND-CCA2 (Indistinguishability under Adaptive Chosen Ciphertext Attack) - стійкість до адаптивної атаки на основі обраного шифр тексту [2];
- для цифрового підпису - в умовах моделі EUF-CMA (existentially unforgeable under adaptive chosen message attacks), тобто забезпечення захисту від екзіцтенціональній підробці в умовах адптивного вибору повідомлення. [15];

- для протоколу обміну ключів - в умовах моделі безпеки Canetti-Krawczyk (СК-безпека) [34].

Алгоритмі мають продемонструвати стійкість до найкращих відомих атак, до атак, що можуть бути реалізовані за допомогою квантових обчислень, до атак на множинні ключі, до атак, що допускають паралельні обчислення, а також до атак на основі обраних шифртекстів з встановленим обмеженням на кількість запросив на обрання шифр текстів. Стійкість має буди теоретично доведена, а також надані кількісні та якісні результати попереднього крипто аналізу.

Техніко-економічні вимоги. Техніко-економічні вимоги стають все більш важливими, тому що вони безпосередньо впливають на швидкість впровадження нових стандартів. Конкретні пар матери вимог ще не визначені, але визначено два основних критерію порівняння кандидатів – це обчислювальна ефективність та ефективність використання ресурсів (пам’яті) Обчислювальна ефективність має порівнюватися для апаратної та програмної реалізації за показниками:

- швидкість генерації ключів;
- швидкість за шифрування/розшифрування;
- швидкість накладення/перевірки підпису;
- швидкість обміну ключами.

Стосовно ефективності використання ресурсів визначають показники:

- довжина ключів та потужність множини ключів для конкретного рівня безпеки:
- розмір шифртексту та підпису.

Техніко-експлуатаційні вимоги. В якості техніко-експлуатаційних вимог висуваються вимоги легкості в реалізації, легкість використання та простота.

Легкість реалізації має бути забезпечена:

- настроюваністю параметрів алгоритму;

- можливість реалізації на широкому колі платформ (богатоплатформеність) та в широкому діапазоні прикладних додатків;
- можливістю паралелізуємої реалізації;
- стійкість до фізичних атак типу side-channel.

Легкість у використанні передбачає можливість вбудовування у більшість прикладних протоколів таких як TLS або IKE, тощо та стік остю до неправильного застосування.

Вимоги ETSI до квантово-стійких алгоритмів. На початку 2016 року ЕС також розпочав приймати рішення стосовно підготовки до переходу до квантово-захищених алгоритмів. У складі ETSI була сформована робоча група з розробки стандартів квантово-захищених алгоритмів. На першому етапі цією групою був проаналізований сучасній стан безпеки існуючих алгоритмів. На основі аналізу, робоча група сформувала рекомендації щодо параметрів криптографічних алгоритмів, які можуть використовуватися у приватній сфері, а частково і в державному секторі. У таблиці 1.2 знаходяться рекомендації ETSI щодо квантово-захищених алгоритмів [35].

Таблиця 1.2.

Рекомендації ETSI щодо квантово-захищених алгоритмів

Сфера	Рекомендації
Symmetric encryption	AES – 256, Salsa20 – 256, Serpent – 256
Symmetric authentication	GCM 96 bit none, 128 bit authenticator. Poly 1305
Public-key encryption	McEliece with binary Goppa code n=6990; k=5413; t=119 errors Quasi-cycle MDPC code N=2^16+6; k=2^15+3; d=274; t=264. NTRU
Public-key signature	XMSS, SPHINCS-256, HFEv

Окремо були проведені оцінки вже існуючих конкретних схем шифрування та цифрового підпису.

Впровадження квантово-стійких криптографічних алгоритмів в Україні.

В Україні в останні роки активно проводилися роботи щодо розробки національних криптографічних стандартів. Ця робота спиралася на великий досвід фахівців у гармонізації міжнародних криптографічних стандартів. За оцінками фахівців, вони можуть розглядадатися як квантово-захищені та можуть бути використані у пост квантовий період.

Аналіз показує, що в Україні є розуміння існування загроз стандартизованим існуючим асиметричним криптоперетворенням типу ЕП. Так, нині розроблено та прийнято національний стандарт «Алгоритми асиметричного шифрування та інкапсуляції ключів» [16], що побудований на основі застосування алгебраїчних решіток. Особливістю цього стандарту (ДСТУ 8961:2019) [16] є суттєве підвищення криптографічної стійкості асиметричного шифрування та інкапсуляції ключів у перехідний та постквантовий період, На відміну від пропозицій та можливостей, що затверджені та прийняті NIST 8309 [12], є можливість використовувати його з рівнями безпеки 384 та 512 бітів. Найвищий рівень безпеки проектів Crystals–Dilithium, Falcon та Rainbow 256 бітів проти класичного та 128 бітів квантового криптоаналізу. В той же час наші дослідження показали, що з урахування можливостей щодо забезпечення безпеки з використанням уже прийнятих в Україні симетричних криптоперетворень ДСТУ 7564:2014 [36], ДСТУ 7624:2014 [37] та ДСТУ 8845:2019 [27], національні стандарти ЕП повинні забезпечити в перспективі до 512 біт класичної та 256 біт квантової безпеки.

Необхідно відмітити, що в процесі формування вимог до ЕП, NIST у рамках конкурсу був зацікавлений тільки в наборах загальносистемних параметрів до 256 біт класичної безпеки включно. Проте, на національному рівні, на перспективу доцільним було визнано використання в Dilithium, 384 і 512 біт безпеки проти класичного криптоаналізу та 192 і 256 біт безпеки проти

квантового криптоаналізу. Але, як показали дослідження, як з точки зору теорії, так і практики, генерація загальносистемних параметрів для використання 256, 384 і 512 біт безпеки проти класичного криптоаналізу та 128, 192 і 256 біт безпеки проти квантового криптоаналізу, в фіналісті Crystals-Dilithium не реалізовано[38, 39].

Під час прийняття рішення стосовно фіналістів на прийняття стандарту ЕП у 3-му раунді кращими та отримали рекомендації визначені проекти ЕП Crystals-Dilithium та Falcon. У нинішньому представленні та оцінці NIST ці проекти на основі структурованої решітки представляються найбільш перспективними та універсальними алгоритмами для ЕП, асиметричного шифрування (АСШ) та протоколу інкапсуляції ключів (ПІК) [2, 3, 10-13].

1.3. Стан розробки квантовостійких електронних підписів на міжнародному та національному рівнях

1.3.1. Роботи зі стандартизації на міжнародному рівні.

За результатами проведення трьох раундів конкурсу NIST PQC було обрано для стандартизації чотири кандидати: механізм інкапсуляції ключа CRYSTALS-Kyber та електронні підписи CRYSTALS-Dilithium, Falcon і SPHINCS+. Крім того, визначено кандидатів для четвертого раунду: механізми інкапсуляції ключів BIKE, Classic McEliece, HQC і SIKE (який розробники визнали ненадійним) [13, 14].

Під час третього раунду було отримано деякі криптоаналітичні результати, які мали значний вплив на вибір NIST. Так, наприклад алгоритм Rainbow також зазнав значних атак під час третього раунду [2, 13]. Перша атака на початку третього раунду спричинила втрату наборами параметрів від 20 до 55 біт безпеки в моделі RAM, причому набори параметрів з вищим рівнем безпеки втрачали більше бітів безпеки. За цим послідувала більш серйозна атака наприкінці третього раунду, що призвела до відновлення особистого ключа для параметрів категорії безпеки 1 трохи більше, ніж за два дні обчислень на одному

ноутбуці. Через брак впевненості в безпеці NIST не вибрав Rainbow для стандартизації. Решту обраних кандидатів KEM було вирішено (BIKE, Classic McEliece, HQC, SIKE) продовжувати оцінювати у четвертому раунді.

У [2] NIST вказав на намір вибрати щонайменше одного з Dilithium та Falcon, оскільки обидва базуються на структурованих решітках і можуть використовуватися в більшості додатків. Зрештою, NIST вирішив вибрати обидві схеми для стандартизації. Ситуація з генерацією ключа та підпису для Falcon потребує більшої кількості ресурсів (гейтів та RAM), ніж для Dilithium, що може зробити Falcon непридатним для впровадження на обмежених пристроях, особливо у випадках, коли вимагається захист від атак бічними каналами. Крім того, NIST визнає, що простіша конструкція ключа та генерації підписів Dilithium допоможе забезпечити безпечні реалізації. З цих причин NIST вибрав Dilithium як основний алгоритм підпису, який він рекомендує для загального використання, і надасть пріоритет його стандартизації.

NIST розуміє, що деякі додатки не працюватимуть так, як вони були розроблені, якщо підпис та дані, що підписуються, не будуть вписуватися в один пакет даних. Для цих додатків складність реалізації генерації підпису Falcon може не викликати занепокоєння, але труднощі з модифікацією додатків для роботи з більшим розміром підпису Dilithium можуть створити бар'єр для переходу до постквантових схем підпису. З цієї причини NIST вирішив також стандартизувати Falcon. Враховуючи загальну кращу продуктивність Falcon, коли генерацію підписів не потрібно виконувати на обмежених пристроях, багато додатків можуть вважати за краще використовувати Falcon ніж Dilithium, навіть у випадках, коли розмір підпису Dilithium не буде перешкодою для реалізації.

Для того, щоб не покладатися повністю на безпеку решіток, NIST також стандартизує SPHINCS+. Безпека алгоритму підпису SPHINCS+ добре зрозуміла, хоча він набагато більший та повільніший, ніж алгоритми підпису на решітках. NIST визнає, що SPHINCS+ може не підходити для багатьох додатків,

враховуючи його профіль продуктивності. NIST зробив вибір вибрати SPHINCS+ зараз, замість того, щоб включити його в четвертий раунд.

Підводячи підсумок, NIST обрав чотири алгоритми з третього раунду для стандартизації та чотири алгоритми для просування до четвертого раунду для подальшої оцінки та вивчення. Див. таблиці 1.3 та 1.4 [2] для списку цих алгоритмів.

Таблиця 1.3.

Алгоритми до стандартизації

Шифрування на відкритому ключі/KEM	**Цифрові підписи**
CRYSTALS–KYBER	CRYSTALS-Dilithium
	Falcon
	SPHINCS+

Таблиця 1.4.

Кандидати, що переходять до четвертого раунду

Шифрування на відкритому ключі/KEM	**Цифрові підписи**
BIKE	
Classic McEliece	
HQC	
SIKE	

Через специфіку обраних алгоритмів NIST потребував додаткових кандидатів серед електронних підписів загального призначення, які не базуються на використанні решіток. У зв'язку з цим було розпочато процес стандартизації додаткових електронних підписів для квантово-стійкої криптографії. На першому етапі цього процесу було подано різні види підписів [3, 4]: засновані на кодах, ізогеніях, мультиваріативні, симетричні, MPC-in-the-head та ЕП, котрі NIST визначили як "інші" .

Конкурс NIST PQC спрямований на обрання кандидатів криптопримітивів для стандартизації як пост-квантових (квантово-стійких). З часом криптографічна спільнота вирішила замінити термін «пост-квантовий» на більш точний «квантово-стійкий» [23].

1.3.2. Роботи зі стандартизації на національному рівні.

Роботи щодо квантовостійких криптографічних стандартів в Україні було розпочато в той же час, як і на міжнародному рівні.

В процесі досліджень в Україні для кількісної оцінки безпеки можливих асиметричних алгоритмів запропоновано три можливі визначення безпеки – два для АСШ та ПІК і одне для ЕП. Також в Україні для класифікації обчислювальної складності атак, які порушують визначену безпеку використано сім категорій (рівнів) безпеки, але реалізовано відповідно 5, 6 та 7 рівні [40]. Це було зроблено з причини недостатності міжнародних вимог до стійкості до квантових атак та з урахуванням необхідної сумісності з міжнародними стандартами АСШ, ПІК та ЕП, які створені для 1–5 рівнів безпеки. Для 5–7 рівнів безпеки вимагається та повинно бути забезпечено відповідно 2^{256}, 2^{384} та 2^{512} біт безпеки від класичного криптоаналізу (з використанням класичного комп'ютерів, класичної математики та класичних алгоритмів), а для квантового комп'ютерів відповідно 2^{256}, 2^{384} та 2^{512} біт безпеки [39, 41]. Також необхідно було врахувати інші бажані властивості безпеки, такі як пряма безпечність, стійкість до атак бічними каналами та стійкість до багатоключових атак, а також стійкість до АСШ, ПІК та ЕП правильного використання.

В Україні експертами було визначено, що постквантові алгоритми ЕП повинні забезпечувати екзистенційну непідроблюваність ЕП стосовно атаки на основі адаптивно вибраного повідомлення (EUF-CMA безпека).

Особливості застосування криптографічних стандартів на національному рівні для забезпечення квантової стійкості наведено в Таблиці 1.5.

Таблиця 1.5.

Особливості застосування криптографічних стандартів на національному рівні для забезпечення квантової стійкості

Стандарт	**Рівні безпеки**
ДСТУ 7624:2014 (Калина)	5-7 рівні безпеки, розмір блоку і ключа (256-512 біт, 10 режимів роботи)
ДСТУ 7564:2014 (Купина)	5-7 рівні безпеки, довжиною геш від 8 до 512, крок 8 біт.
ДСТУ 8845-2019 (Струмок)	5-7 рівні безпеки, ключ 256-512 біт, IP швидкодія=$18*10^9$ біт
ДСТУ 8961-2019 (Скеля)	5-7 рівні безпеки, постквант. АСШ/ПІК, аматематичні решітки. V=4.10^6
ДСТУ 9212-2023 (Вершина) – постквант.	5-7 рівні безпеки, математичні решітки з відхиленнями. Стадія прийняття. (Dilithium).
Проєкт ЕП ДСТУ (Сокіл) – постквант.	5-7 рівні безпеки, маткматичні решітки з відхиленнями.Стадія обговорення(Falcon)

1.4. Постановка задач щодо методичних основ аналізу, оцінки та порівняння асиметричних квантовостійких криптоперетворень електронного підпису та протоколів інкапсуляції ключів

З метою формулювання методичних основ аналізу, оцінки та порівняння асиметричних квантовостійких криптоперетворень електронного підпису та протоколів інкапсуляції ключів необхідно виконати наступні задачі:

– Провести аналіз, оцінку та порівняння існуючих та кандидатів на песпективні квантовостійкі національні та міжнародні електронні підписи по безумовним критеріям (безпеці) (порівняння Falcon Соколом та «Вершина») для чого:

- Обгрунтувати моделі порушника, загроз та безпеки
- обгрунтувати множини безумовних критеріїв (критеріїв безпеки)
- обгрунтувати множини умовних критеріїв
- обгрунтувати множини прагматичних критеріїв
- обгрунтувати науково-методичні основи розробки, оцінки та порівняння існуючих та перспективних квантовостійких електронних підписів по безумовним, умовним та прагматичним критеріям

– Реалізувати результати розробки в якості інструментарію для практичної оцінки та порівняння проєктів та стандартизованих міжнародних та національних квантовостійких електронних підписів

– Провести аналіз, оцінку та порівняння існуючих та кандидатів на песпективні квантовостійкі національні та міжнародні електронні підписи

– Провести аналіз, оцінку та порівняння методів ЕП на основі математики Crystals-DELITHIUM (обґрунтувати основи та провести дослідження по методичним основам щодо методів

прийнятих на національному рівні на предмет забезпечення сформульованих вимог)

– Провести аналіз, оцінку та порівняння методів ЕП на основі математики Falcon (обґрунтувати основи та провести дослідження по методичним основам щодо методів прийнятих на національному рівні на предмет забезпечення сформульованих вимог)

– Розглянути специфіку критеріїв. Розробити практичну реалізацію результатів досліджень, програмну реалізацію, прийняти участь в розробці національного стандарту.

– Застосувати методику оцінки та порівняння та отримати практичні (експериментальні) результати.

1.5. Висновки до розділу 1

1. Проведений аналіз показав, що наразі спостерігається стійкий прогрес у створенні квантових комп'ютерів. Практично завершується створення математичних основ та програмного забезпечення для криптоаналітично значущих квантових комп’ютерів. Розробляються квантові комп'ютери, що призначаються для криптоаналізу існуючих стандартизованих криптосистем з відкритим ключем – електронних підписів, асиметричних шифрів та криптографічних протоколів різного призначення.

2. Показано, що на сьогоднішній день з боку технологічно розвинених держав запущено процеси підготовки до настання перехідного та квантового періодів. Яскравим прикладом дій, спрямованих на зниження ризиків та переведення потенційно вразливих комп’ютерних систем на квантово-стійку криптографію є запровадження з боку NIST США конкурсу на стандартизацію квантово-стійкої криптології та конкурсу на стандартизацію додаткових електронних підписів.

3. Обґрунтовано, що важливою задачею для забезпечення захищеності потенційно вразливих комп’ютерних систем є оцінка та порівняння існуючих та перспективних криптоперетворень. Показано, що актуальними з боку кватової стійкості є математичні апарати Crystals-Delithium та Falcon, котрі стали фіналістами та кандидатами на стандартизацію на міжнародному рівні.

4. Роботи щодо квантовостійких криптографічних стандартів в Україні було розпочато в той же час, як і на міжнародному рівні. В процесі досліджень в Україні для кількісної оцінки безпеки можливих асиметричних алгоритмів запропоновано три можливі визначення безпеки – два для АСШ та ПІК і одне для ЕП. Також в Україні для класифікації обчислювальної складності атак КВК, які порушують визначену безпеку використано сім категорій (рівнів) безпеки, але реалізовано відповідно 5, 6 та 7 рівні. Це було зроблено з причини недостатності міжнародних вимог до стійкості до квантових атак та з урахуванням необхідної сумісності з міжнародними стандартами АСШ, ПІК та ЕП, які створені для 1–5 рівнів безпеки.

5. Розкрито стан розробки криптоаналітично значущого квантового комп’ютера, постквантових електронних підписів на міжнародному та національному рівнях. Показаний приклад оцінки та порівняння кандидатів на стандартизацію в якості квантово-стійких електронних підписів за безумовними критеріями.

РОЗДІЛ 2. МОДЕЛЬ БЕЗПЕКИ ТА КРИТЕРІЇ ОЦІНКИ І ПОРІВНЯННЯ ПЕРСПЕКТИВНИХ ПОСТКВАНТОВИХ ЕЛЕКТРОННИХ ПІДПИСІВ

2.1. Особливості застосування електронних підписів на практиці

Електронний підпис призначений для виконання цілої низки задач та є частиною практичних систем, технологій і протоколів, таких як (Рис. 2.1):

1. Інфраструктура відкритих ключів (далі – ІВК, також PKI, Public Key Infrastructure)
   - SSL/TLS;
   - DNSSEC (Domain Name System Security Extensions);
   - Електронна пошта (S/MIME);
5. Підпис коду (Code Signing);
6. SIM-карти;
7. IPSec (Internet Protocol Security);
8. Електронні паспорти (e-Passports);
9. Підписання PDF;
10. Технології Blockchain;
11. Віртуальні приватні мережі (VPN).

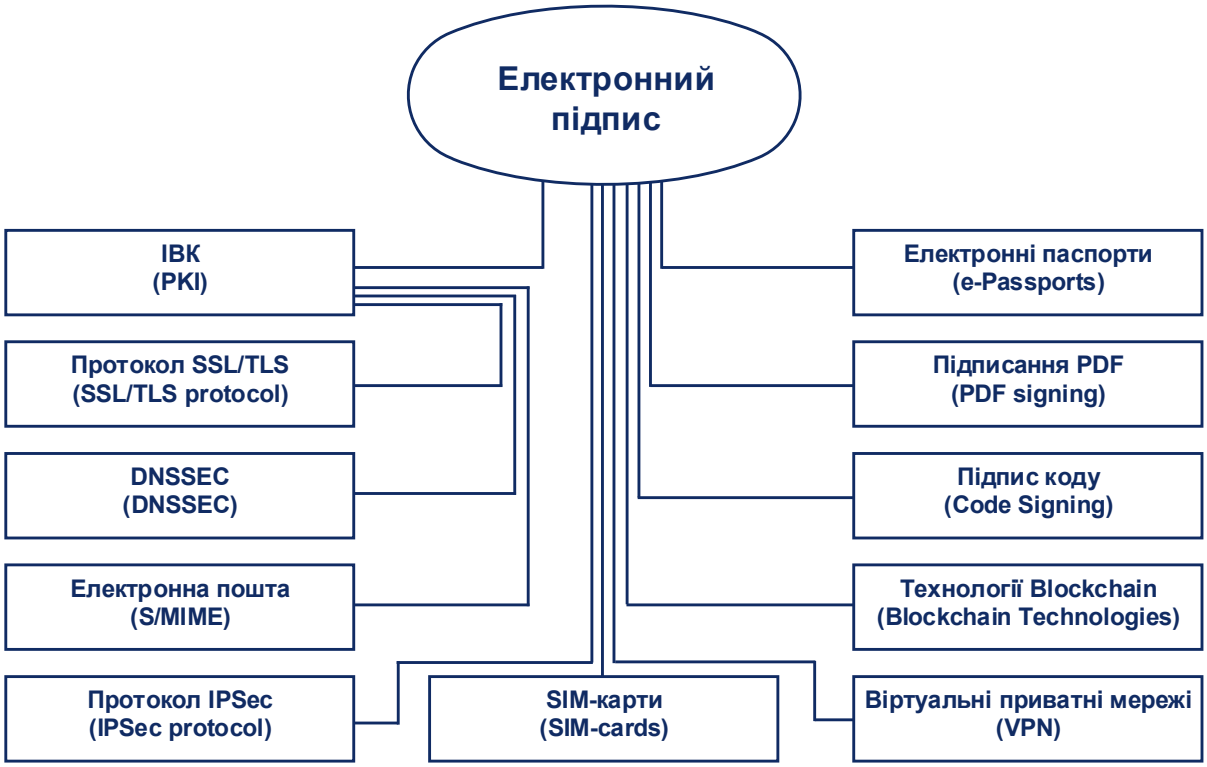

Рис. 2.1. Практичні застосування електронних підписів

Кожен з наведених практичних застосувань електронних підписів окремо висуває конкретні, відмінні від інших, вимоги. Тому варто розглянути їх детальніше.

Інфраструктура відкритих ключів (вона ж ІВК або PKI) являє собою комплекс методів та засобів для забезпечення експлуатації криптосистем з відкритими ключами. ІВК призначена для поєднання асиметричних алгоритмів шифрування, електронних цифрових сертифікатів та центрів сертифікації в єдину структуру. Окрім створення цифрових сертифікатів, ІВК також забезпечує зберігання ключів і сертифікатів, їх резервування та відновлення, взаємну сертифікацію, ведення списківф відкликаних сертифікатів (СВС).

ІВК зазвичай складається з центрів сертифікації, центрів реєстрації, репозиторіїв та архівів сертифікатів. Серед користувачів ІВК виділяють держателів та користувачів сертифікатів.

Приклади підходів до реалізації ІВК:

– PKIX, ІВК на сертифікатах X.509;
– DNS (DNSSEC), захищена система доменних імен;

– система захищеної електронної пошти (OpenPGP або S/MIME);

– автентифікація користувачів застосунків (за допомогою смарт-карток або за допомогою SSL/TLS);

– протоколи захищеного зв’язку початкового завантаження (IKE (Internet key exchange) та SSL/TLS);

– SET, система захищених електронних транзакцій.

Детальнішого розгляду заслуговують такі застосування ІВК: SSL/TLS, DNSSEC, захищена електронна пошта S/MIME.

SSL/TLS призначено для надання можливості безпечної передачі даних через інформаційно-комунікаційні мережі та він використовує для цього асиметричне шифрування і сертифікати X.509.

SSL/TLS складається із трьох основних фаз [42]:

– діалогу між сторонами для вибіру алгоритму шифрування для використання;

– обміну ключами або автентифікація за сертифікатами;

– передачі зашифрованих за допомогою симетричних алгоритмів шифрування даних.

Для створення та обміну таємним ключем для шифрування даних, відбувається процедура рукостискання. Під час цієї процедури відбувається: погодження версії протоколу, обрання криптографічних алгоритмів, автентифікація із використанням сертифікатів та використання асиметричних алгоритмів для створення таємного ключа.

В SSL/TLS можуть використовуватися такі алгоритми [42]:

– RSA, Diffie-Hellman, DSA – для здійснення обміну ключами та для перевірки їхньої справжності (комбіновано);

– RC2, RC4, IDEA, DES, Triple DES або AES – для симетричного шифрування;

– MD5 або SHA – в якості геш-функцій.

Також алгоритми можуть відрізнятися і доповнюватись в різних версіях протоколу.

DNSSEC є розширенням DNS, що додає здійснення автентифікації та забезпечення цілісності записів DNS завдяки використанню електронних підписів. У зв'язку з особливостями роботи DNS, DNSSEC спрямовано на аутентифікацію даних або інформації про їх відсутність та на цілісність.

Для забезпечення валідації даних DNS-відповідей, що передаються через DNSSEC, використовують ланцюжок довіри (сертифікатів) з початком в кореневій зоні DNS [43]. Це забезпечує захист користувачів DNS від атак, що використовують підробку DNS даних (таких як DNS poisoning).

Підписанню підлягають відповіді на запити DNS (DNS lookup). Завдяки цьому дані всередині відповіді не можуть бути змінені без секретного ключа шифрування, котрий знаходиться на DNS-сервері.

S/MIME є стандартом шифрування та підписання електронної пошти з використанням криптографії з відкритим ключем, що має підтримку та використовується в більшості сучасних поштових програм.

Особливостями використання S/MIME для електронної пошти є те, що для коректного використання повинні бути враховані наступні умови [44]:

– як відправник так і одержувач повинні узгодити застосування додатків електронної пошти з підтримкою S/MIME;
– захист повідомлень повинен бути наявним як на шляху від відправника до одержувача, так і у відповідних середовищах відправника і одержувача для комплексності підходу до забезпечення безпеки;
– несумісність S/MIME із вебпоштою через наявність загрози конфіденційності та цілісності повідомлень з боку провайдера сервісу вебпошти.

Також важливим практичним застосуванням електронних підписів є набір мережних протоколів IPsec (Internet Protocol Security), що призначено для

захисту мережних комунікацій за допомогою автентифікації та шифрування кожного IP-пакету.

IPsec працює на мережевому рівні за моделлю OSI та придатний для використання в захисті будь-яких протоколів на базі TCP та UDP. Цей набір протоколів спрямований на забезпечення цілісності та конфіденційності даних.

IPsec функціонує на використанні безпечних зв'язків (вони ж Security Association або ж SA), котрі зберігаються в базі даних безпечних зв'язків (Security Associations Database або ж SADB), та кожен з яких має ідентифікатор, що складається з [45]:

– індексу параметра безпеки (SPI);
– IP-адреси призначення;
– ідентифікатора протоколу безпеки (ESP або AH).

SADB в свою чергу містить наступні дані:

– алгоритм аутентифікації за AH;
– секретний ключ для аутентифікації за AH;
– алгоритм шифрування за ESP;
– секретний ключ шифрування за ESP;
– параметр використання аутентифікації за ESP;
– параметри обміну ключами;
– обмеження щодо маршрутизації;
– політика фільтрації IP.

В IPSec можуть використовуватись наступні алгоритми [45]:

– HMAC-SHA1/SHA2 – для забезпечення цілісності та справжності;
– TripleDES-CBC, AES-CBC та AES-CTR – для забезпечення конфіденційності;
– AES-GCM та ChaCha20-Poly1305 – для забезпечення конфіденційності та автентифікації (в комбінації);
– Diffie-Hellman та ECDH – для обміну ключовими даними;
– RSA, ECDSA, PSK, EdDSA – для автентифікації.

Також важливим практичним застосуванням електронних підписів є застосування їх для автентифікації абонентів у мережах GSM/UMTS/LTE. Це реалізується завдяки використання SIM-карти для генерації підпису на основі закритого ключа з карти та випадкового числа з базової станції. Автентифікація користувача в мережі здійснюється шляхом перевірки сформованого таким чином підпису. Для даного застосування важливу роль відіграє розмір підпису.

Ще одним важливим практичним застосуванням електронних підписів є застосування їх для захисту від підробки електронних паспортів, захист цілісності PDF-документів та підпис коду програмного забезпечення для підтвердження його цілісності та автентичності.

Електронні паспорти вирізняються тим, що містять чіп із підписаними електронним підписом даними про особу. Підпис здійснюється відповідними державними органами. За необхідності здійснення перевірки автентичності даних відбувається зчитування підпису та його перевірка. Велика увага приділяється цілісності та незаперечності.

Підписання PDF-документа здійснюється додаванням до документа цифрового підпису, котрий можна перевірити за допомогою сертифіката (часто X.509). Завдяки цьому забезпечується цілісність та незаперечність документа.

Аналогічним чином при підписанні коду відбувається процедура накладання цифрового підпису на бінарні файли або інсталяційні пакети програмного забезпечення. При встановленні підписаного програмного забезпечення, з боку операційної системи відбувається перевірка підпису для підтвердження відсутності модифікацій та надходження програмного забезпечення з перевіреного джерела.

Окремим прикладом практичного застосування електронних підписів є технології Blockchain, де автентичність транзакцій забезпечується накладанням електронного підпису.

Кожна транзакція у блокчейні підписується секретним ключем власника, в той час як інші вузли перевіряють підпис перед додаванням транзакції до

блоку. Основним є забезпечення цілісності даних блоку та запобігання внесенню несанкціонованих змін.

Також невід'ємним є застосування електронних підписів для автентифікації пристроїв і користувачів при підключенні до віртуальних приватних мереж (також відомих як VPN). VPN надають можливість об'єднувати віддалені мережі в одну віртуальну захищену мережу за допомогою створення шифрованих VPN-тунелів (закритих каналів обміну даними) між двома вузлами. Таким чином користувачі однієї мережі можуть бути учасниками віддаленої мережі та користуватись її сервісами.

Для отримання доступу до мережі за допомогою VPN-тунеля, віддалений користувач підключається до сервера доступу та проходить ідентифікацію, автентифікацію та авторизацію.

За умовами середовища розгортання VPN поділяються на захищені та довірчі [6, 7]. Найпоширенішим варіантом є захищені. Вони використовуються, коли виникає потреба в прокладанні захищеної підмережі через ненадійну мережу (як, наприклад, Інтернет). Довірчі ж використовуються у випадках, коли середовище передачі даних вважається надійним (захищеним). В таких випадках забезпечення мережевої безпеки покладається на інші засоби та заходи. Важливим аспектом такого застосування електронних підписів є швидкодія виконання процедур накладання та перевірки підпису.

Також слід зауважити, що в ході конкурсу на квантово-стійкий стандарт NIST PQC з боку NIST також враховувались можливі практичні застосування квантово-стійких алгоритмів. Так, для оцінки безпеки враховувалося, що стандарти відкритого ключа від NIST використовуються зокрема в TLS, SSH, IKE, IPsec, DNSSEC, для формування сертифікатів (в ІВК), для підписання коду та в безпечних завантажувачах (bootloaders). В розрахунок бралось те, що нові стандарти повинні зайняти всі ніші застосування попередніх і забезпечувати квантову стійкість для них[2].

2.2. Аналіз особливостей моделей порушника та загроз щодо безпеки постквантових електронних підписів

Модель порушника та її побудова є важливою через те, що надає можливість для розробки компетентного комплексу заходів захисту в інформаційно-комунікаційній системі криптографічного захисту інформації, особливо при застосуванні механізмів АСШ та ЕП. Модель порушника є актуальною при побудові систем, що повинні бути стійкими до криптоаналізу в тому числі і в перехідний і в постквантовий період.

2.2.1. Модель порушника

Згідно з [7, 46] модель порушника розробляється для того, щоб отримати відповіді на такі запитання щодо порушника за умови, що він може застосовувати класичний та квантовий криптоаналіз:

1) від кого необхідно захистити інформацію?
2) що становить мету порушника?
3) яким рівнем знань володіє порушник?
4) який рівень повноважень має потенційний порушник в рамках системи?
5) які методи, системи та засоби може використовувати порушник?

Як вказано в [46], модель порушника становить опис можливих дій порушника, що зазвичай формується в результаті аналізу типу зловмисника, його повноважень, теоретичних та практичних можливостей та рівня його знань.

Якщо класифікувати порушників за рівнями можливостей, що вони можуть отримати за рахунок використання штатних засобів інформаційно-комунікаційної системи, то можна виділити чотири ієрархічних рівні. Через ієрархічну побудову такої класифікації, припускається що кожен наступний (вищий) рівень включає можливість використання можливостей попереднього

рівня. Таким чином, найвищий (четвертий) рівень включає в себе максимальні можливості всіх осіб, в тому числі персоналу, що виконує проектування, обслуговування, ремонт компонентів ІКС та підключення до ІКС (включення до складу ІКС) додаткових засобів, здатних на обробку інформації та криптоаналіз.

Загальним призначенням наведеної класифікації порушників є застосування як частини процесу оцінки ризиків, виявлення вразливостей ІКС та оцінки ефективності заходів захисту та для забезпечення криптографічної стійкості до криптоаналізу (в тому числі квантового).

При побудові моделі порушника усі користувачі поділяються на категорії та серед них виділяються найбільш критичні. Згодом такі користувачі приймаються в моделі порушника в якості внутрішніх порушників. Після визначення внутрішніх порушників проходить процес визначення зовнішніх порушників.

Всі порушники класифікуються за різними показниками з метою утворення моделі порушника. В якості прикладів видів класифікацій можна навести [7, 46]: за метою здійснення порушення; за рівнем знань про алгоритм; за методами і способами, що можуть бути застосованими тощо.

В моделях порушника зловмисник (порушник) може використовувати різні методи та засоби для отримання доступу до конфіденційної інформації або інформації з обмеженим доступом. При цьому він може як використовувати певні засоби для отримання інформації, так і діяти без них. Методи, котрі застосовує порушник можуть сильно варіюватись та виходити за рамки дозволених, за умови якщо дозволеним є отримання інформації, що не передбачає порушення прав власності.

Виходячи з вищевказаного для електронних підписів, орієнтованих на стійкість до класичного та квантового криптоаналізу можна прийняти наступну модель порушника [46, 47]:

1) порушник четвертого рівня, що здатний на здійснення квантових атак щодо ІКС КЗІ, має доступ до КЗКК на будь-яку кількість часу та з необмеженою потужністю та має все необхідне математичне та програмне забезпечення, та на додаток до цього може отримати доступ до криптографічно захищених повідомлень;

2) група хакерів укомплектована на високому рівні чи атаки з боку великих професійних груп, що мають обмежені можливості порушника 4 рівня та можуть використовувати класичні кластери високої потужності та має все необхідне математичне та програмне забезпечення, та на додаток до цього може отримати доступ до криптографічно захищених повідомлень, і здійснюють класичні атаки;

3) порушник, що може не мати жодних знань про систему та алгоритми, що в ній використовуються та алгоритми АСШ та ЕП взагалі, але разом з цим порушник цілком може знати частину даних або може мати змогу перехоплювати частину захищеної інформації, або може бути інсайдером;

4) порушник, що може не мати жодних повноважень в ІКС щодо АСШ та ЕП. Але, за умови того, що порушник є інсайдером, або людиною, що змогла отримати адміністративний доступ, то він може мати змогу змінювати процеси в системі і переналаштовувати її за своїми потребами, хоча при цьому він може і не мати повного доступу до функціоналу та елементів системи.

Найгіршим випадком для системи є порушник, що є криптоаналітиком 4-го рівня (найвищого), має знання про метод перспективного АСШ, ПІК та ЕП, його криптографічні властивості та механізми безпеки методу, за виключенням особистого ключа.

Найкращим випадком для системи є порушник, який не знає нічого про систему, метод, системні параметри та ключі.

Найактуальнішими для оцінки та порівняння квантовостійких асиметричних ЕП є порушники 2-х найвищих рівнів (3-го та 4-го).

2.2.2. Модель загроз

Разом з моделлю порушника для розробки компетентного комплексу заходів захисту в інформаційно-комунікаційній системі криптографічного захисту інформації, а особливо при застосуванні механізмів АСШ та ЕП, розробляється також модель загроз.

Процес розробки моделі загроз може мати різний вигляд, але одним з найпоширеніших варіантів є вибір загроз із вже існуючих криптографічних концепцій або стандартів. Одним з яскравих прикладів є директиви Німеччини «IT-Grundschutz-Compendium» [48] (далі - криптографічна Концепція).

Так, для електронних підписів, орієнтованих на стійкість до класичного та квантового криптоаналізу, за допомогою криптографічної Концепції [48] можна виділити такі загрози та вразливості, що мають підвищену загрозу:

- атака "Людина посередині";
- атака Clickjacking;
- викрадення даних за допомогою мобільних носіїв інформації;
- викрадення пристроїв, носіїв чутливої інформації та документів;
- витік каналами побічних електромагнітних випромінювань і наведень;
- відмова від дій;
- відмова криптомодулю;
- відсутнє або недостатнє оповіщення при виникненні інцидентів безпеки;
- відсутність дозволів для обробки персональних даних;
- відсутність прозорості для особи, що зацікавлена та уповноважена контролювати захист даних;
- відсутня або неповна документація;
- втрата цілісності інформації, яка повинна бути захищена;
- застаріння криптографічних методів;

- зловживання повноваженнями, зловживання правами адміністратора, зловживання правами користувачів;
- компрометація криптографічних ключів;
- крадіжка чутливих даних;
- не виявлені інциденти інформаційної безпеки;
- невірне тлумачення події інформаційної безпеки;
- недооцінення актуальності виправлень і змін;
- неналежне зберігання носіїв інформації в разі виникнення надзвичайної ситуації;
- необережне знищення обладнання або даних;
- неправильне використання криптомодулів;
- несанкціоноване використання криптомодулів;
- несанкціоноване використання прав;
- нестійкі криптографічні алгоритми;
- неякісна або відсутня автентифікація;
- підробні сертифікати;
- порушення законів або правил;
- проблеми при автоматизації поширення виправлень і змін;
- розголошення чутливої інформації;
- систематичний перебір паролів, троянський кінь;
- уразливості або помилки ПЗ, шкідливе програмне забезпечення.

Серед них можуть бути використані порушниками 3-го та 4-го рівнів, а отже є особливо актуальними, наступні загрози [47]:

- атака "Людина посередині";
- атака Clickjacking;

итік каналами побічних електромагнітних випромінювань і наведень;

- застаріння криптографічних методів;
- компрометація криптографічних ключів;
- нестійкі криптографічні алгоритми;

- підробні сертифікати;
- систематичний перебір паролів, троянський кінь;
- уразливості або помилки ПЗ, шкідливе програмне забезпечення.

2.3. Модель безпеки щодо постквантових електронних підписів

Комплексна модель безпеки складається з моделі порушника, моделі загроз та моделі безпеки асиметричних криптоперетворень для постквантового періоду, яка враховує тип асиметричного криптографічного примітиву та їх застосування в ІКС. Модель безпеки визначає формальні умови безпеки, в той час як достатні умови визначаються рівнями безпеки.

Для стандартів ЕП орієнтованих на квантову стійкість прийнято використовувати модель екзистенційної (існуючої) непідроблюваності ЕП при атаках, що базуються на адаптивно вибраних повідомленнях. Передбачається, що при виконанні атаки криптоаналітик отримує доступ до оракула, що за результатами реалізації спроб криптоаналізу чи навіть безпосередньо успішного криптоаналізу, надає у відповідь на запит дані щодо результату проведення атаки, і також безпосередньо щодо запиту до функції ЕП. Передбачається, що оракул повинен створити дійсний ЕП для повідомлення, котре до цього ще не було підписане оракулом. Така властивість позначається як EUF-CMA [15] (Existential Unforgeability under Chosen Message Attack) – Екзистенційна непідроблюваність при атаці на основі адаптивно вибраних повідомлень.

Для цієї моделі використовується два загальних формальних визначення забезпечення безпеки з боку схеми ЕП щодо екзистенційної непідроблюваності ЕП. Обидва визначення базуються на "грі" (експерименті), що здійснюється між зловмисником та законним користувачем.

Більшу вагу в плані безпеки ЕП має безпека від SUF-CMA [2] (Strong Existential Unforgeability under Chosen Message Attack) – Сильна екзистенційна непідроблюваність при атаці на основі адаптивно вибраних повідомлень.

Головною відмінністю моделі SUF-CMA є те, що вона гарантує, що атакуючий не зможе підібрати ЕП.

2.4. Опис безумовних критеріїв

Безумовні критерії оцінки та порівняння АСШ, ПІК та ЕП обрані згідно до висунутих з боку NIST [2, 3, 15] вимог до часткових безумовних критеріїв асиметричних криптоперетворень типу АСШ, ПІК та ЕП, досягнутих результати при практичному розв'язанні задач криптоаналізу, в тому числі на основі реалізації алгоритмів квантового криптоаналізу, а саме [5]:

– W_1 – Надійність, простота та прозорість математичної бази (математичних перетворень), що застосовуються при реалізації постквантових криптоперетворень АСШ, ПІК та ЕП;

– W_2 – Практична захищеність криптоперетворень типу АСШ та ПІК при реалізації алгоритму «семантично безпечного шифрування» від відомих атак з використанням квантового комп'ютера та доступу криптоаналітика до 2^{64} обраних шифртекстів, але для моделі безпеки IND-CCA2;

– W_3 – Практична захищеність криптоперетворення типу ЕП від відомих атак з використанням квантового комп'ютера та доступу криптоаналітика до 2^{64} обраних повідомлень, для моделі безпеки EUF-CMA;

– W_4 – Обґрунтованість реальної стійкості криптоперетворень АСШ, ПІК та ЕП від усіх відомих та потенційно можливих криптоаналітичних атак постквантового періоду на основі використання загальних параметрів та ключів з необхідними розмірами та властивостями (ключі 128 біт квантової безпеки та 256 біт і більше класичної стійкості (безпеки)), включаючи статистичну безпеку;

– W_5 – Теоретична захищеність криптоперетворень типу АСШ, ПІК та ЕП в постквантовий період проти існуючих силових, аналітичних та спеціальних атак для діючих моделей загроз (мінімум для моделі EUF-CMA для ЕП та IND-CCA2 для АСШ);

– W_6 – Можливість заміни існуючих стандартизованих криптопримітивів на постквантові та застосування в діючих криптосистемах та протоколах в певних умовах та обмеженнях;

– W_7 – Обчислювальна ефективність – складність прямого $I_{пр.}$ та зворотного $I_{зв.}$ криптоперетворень АСШ, ПІК та ЕП, а також генерування асиметричних пар ключів $I_{кл.}$ не вище за поліноміальну складність, забезпечення необхідних значень складності (швидкодії) $I_{пр.}$, $I_{зв.}$ та $I_{кл.}$ при практичному застосуванні в додатках з апаратно-програмною та програмною реалізацією;

– W_8 – Виконання обмежень на мінімальну та максимальну довжини особистих та відкритих ключів, розміри та збитковість шифртексту та ЕП, відсутність слабких особистих ключів для моделей безпеки постквантового періоду EUF-CMA для ЕП та IND-CCA2 для АСШ;

– W_9 – Обґрунтованість реальної стійкості криптоперетворень АСШ, ПІК та ЕП від усіх відомих та потенційно можливих криптоаналітичних атак постквантового періоду на основі використання загальних параметрів та ключів з необхідними розмірами та властивостями (довжини ключів 256/128, 384/192 та 512/256 біт відповідно класичної стійкості та квантової безпеки (стійкості));

– W_{10} – Забезпечення захисту від атак на основі сторонніх каналів (наприклад, витоку технічними каналами) та на основі помилок.

У ході проведення досліджень перелік безумовних критеріїв можна, за необхідності, розширити, як от наприклад [5]:

1) Надійність, простота та прозорість математичної бази криптоперетворень типу АСШ, ПІК та ЕП. Це означає практичну відсутність з боку порушника можливості здійснювати атаки певних типів, як от «універсальне розкриття» за рахунок недосконалості математичного апарату відносно схеми ЕП. Також це означає відсутність слабкостей, які можуть бути зумовлені специфічними властивостями загальних параметрів і ключів. В якості критерію оцінки надійності математичної бази може бути те, що складність атаки типу «універсальне розкриття» $I_{ур}$ матиме експоненційний характер, а в

якості критерію ненадійності – те, що така атака матиме суб'експоненційну або поліноміальну складність.

2) Практична захищеність криптоперетворень під час реалізації алгоритму «семантично безпечного шифрування» від таких відомих класичних та постквантових атак, які стосуються криптоперетворень АСШ та ПІК, та пов'язані з доступом порушника до 2^{64} обраних шифртекстів, але це актуально за умови використання моделі безпеки IND-CCA2.

3) Реальна захищеність АСШ, ПІК та ЕП від усіх відомих та потенційних криптоаналітичних атак постквантового періоду. В даному випадку захищеність - це факт того, що всі відомі атаки, що відносяться до типу «повне розкриття» матимуть експоненційну складність I_{ec}, а в якості критерію незахищеності виступатиме суб'експоненційне значення I_{ce} і нижча складність атаки, що відноситься до типу «повне розкриття».

4) Теоретична захищеність криптоперетворень, що перевіряються, в постквантовий період проти всіх існуючих силових, аналітичних та спеціальних атак, що є актуальними для діючих моделей загроз (як мінімум, розглядаються модель EUF-CMA для ЕП та IND-CCA2 для АСШ та ПІК) та складність яких є меншою за складність атаки, що відноситься до типу «повне розкриття».

5) Можливість заміни сучасних стандартизованих криптопримітивів на перспективні кватовостійкі з метою застосування в діючих криптосистемах та протоколах за дотримання певних умов та обмежень.

6) Статистична безпечність криптоперетворення, що перевіряється. Це означає статистичну незалежність результату криптоперетворення від вхідного блоку, котрий проходить процес зашифрування (підпису), та використовуваного особистого ключа.

7) Відсутність слабких особистих ключів криптоперетворення, що перевіряється, які призводять до зниження складності криптоаналітичних атак, що відносяться до типу «повне розкриття» та «універсальне розкриття», у порівнянні зі складністю атаки «повне розкриття» для інших собистих ключів.

8) Обчислювальна ефективність, що означає, що складність прямого $I_{пр}$ та зворотного $I_{зв}$ криптоперетворень, що перевіряються, є не вищою за поліноміальний характер, а також забезпечуються необхідні значення складності (швидкодії) $I_{пр}$, $I_{зв}$ та $I_{кл}$ під час практичного застосування у додатках з апаратно-програмною та програмною реалізацією.

9) Виконання обмежень на мінімальну та максимальну довжини особистих та відкритих ключів, розміри та збитковість шифротексту та ЕП, відсутність слабких особистих ключів для таких моделей безпеки як EUF-CMA для ЕП та IND-CCA2 для АСШ та ПІК.

10) Забезпечення захисту від атак, що базуються на сторонніх каналах (наприклад, вимірювання складності криптоперетворення, вимірювання потужності, небхідної для криптоперетворення, витоку технічними каналами тощо).

11) Забезпечення захисту від атак на основі помилок (наприклад, внесення помилок в процеси криптоперетворень, ключів тощо).

Перелік інших безумовних критеріїв, що можуть бути використані для дослідження для оцінки АСШ, ПІК та ЕП, включає наступні [5, 22]:

1) $I_{ст.}$ – рівень криптографічної стійкості з використанням безумовних критеріїв;

2) $l_{в.к.}$ – можливі довжини відкритого ключа криптопримітиву;

3) $l_{о.к.}$ – можливі довжини особистого (секретного) ключа криптопримітиву;

4) $l_{рез.}$ – довжина результату криптографічного перетворення (так звана збитковість);

5) $T_{пр.}$ – складність (швидкість) прямого криптоперетворення;

6) $T_{зв.}$ – складність (швидкість) зворотного криптоперетворення;

7) $T_{ген.зп.}$ – складність (швидкість) процесу генерування загальних параметрів для обраного режиму роботи криптоперетворення (це залежить від довжин загальних параметрів та довжин ключів);

8) $T_{ген.кл.}$ – складність (швидкість) генерації ключа (ключової пари) в залежності від обраного режиму роботи тощо.

Якщо врахувати наведені вище часткові безумовні критерії та

$$W_1, W_2, W_3, W_4, W_5, W_6, W_7, W_8, W_9, W_{10}, \quad (2.1)$$

що наведені та формулі (2.1), то функцію відповідності криптоперетворення вимогам можна записати у вигляді наступного інтегрального безумовного критерію:

$$f() = (W_1 \wedge W_2 \wedge W_3 \wedge W_4 \wedge W_5 \wedge W_6 \wedge WW_7 \wedge W_8 \wedge W_9 \wedge W_{10}) \in (1,0), \quad (2.2)$$

де символ «∧» позначає кон'юнкцію булевих змінних.

Таким чином, можна отримати, що якість квантовостійкого криптоперетворення АСШ, ПІК та ЕП цілком може бути оцінена за допомогою застосування безумовного інтегрального критерію, що є функцією відповідності у вигляді наступного інтегрального безумовного критерію

$$f_{фв}=1, \quad (2.3)$$

якщо криптоперетворення, що перевіряється, відповідає висунутим вимогам та наступного

$$f_{фв}=0, \quad (2.4)$$

якщо криптоперетворення, що перевіряється, не відповідає висунутим вимогам.

2.5. Опис умовних критеріїв

За Методикою якісну й кількісну оцінку та порівняння криптоперетворень типу АСШ, ПІК та ЕП варто проводити із застосуванням часткових умовних та узагальненого умовного критерію. Перелік та позначення часткових умовних критеріїв, що можуть бути застосовані для оцінки криптоперетворень типу АСШ, ПІК та ЕП, та вимоги до яких висунуті з боку NIST США та ETSI ЄС, виглядає наступним чином [5]:

– К1 – Додаткові властивості безпеки: «perfect forward secrecy» (удосконалена пряма безпека); стійкість до атак сторонніми каналами; стійкість до мультиключових атак; стійкість до відмов.

– K2 – Вимоги до безпеки (стійкості): 1) 128 біт класичної безпеки / 64 біт квантової безпеки (запас стійкості AES-128); 2) 128 біт класичної безпеки / 80 біт квантової безпеки (запас стійкості SHA-256/SHA3-256); 3) 192 біт класичної безпеки / 96 біт квантової безпеки (запас стійкості AES-192); 4) 192 біт класичної безпеки / 128 біт квантової безпеки (запас стійкості SHA-384/SHA3-384); 5) 256 біт класичної безпеки /128 біт квантової безпеки (запас стійкості SHA2-512, SHA3-512).

– K3 – Додаткові вимоги до стійкості: 1) 512 біт класичної безпеки / 256 біт квантової безпеки (запас стійкості SHA-512/SHA3-512, ДСТУ 7564:2014 – 512 біт); 2) 512 біт класичної безпеки /від 128 до 256 біт квантової безпеки (запас стійкості ДСТУ 7624:2014 (Калина – 512)); 3) 512 біт класичної безпеки / 256 біт квантової безпеки (запас стійкості ДСТУ 7624:2014 (Калина – 512)).

– K4 – Помилки шифрування. Низький відсоток помилок шифрування ПІК та ЕП.

– K5 – Можливість багаторазового АСШ, ПІК та ЕП.

– K6 – Гнучкість: 1) додаткові можливості схеми (оптимізація, неявний обмін ключами тощо); 2) кросплатформеність; 3) можливість розпаралелювання.

– K7 – Перевірка на коректність. Перевірка правильності опорних та оптимізованих реалізацій.

– K8 – Перевірка на ефективність: Обчислення часу, що необхідний для генерації ключа, зашифрування, розшифрування, підпису, перевірки підпису, або встановлення ключів (тестування проводиться на оптимізованих версіях).

– K9 – Умови випробувань: Основні платформи: NIST PQC Reference Platform; Intel x64; Windows або Linux, компілятор GCC. Проведення додаткових тестувань інших умов (8-бітових процесорів, цифрових сигнальних процесорів, виділених CMOS, тощо).

– K10 – Можливість і умови вільного поширення постквантових криптоперетворень АСШ, ПІК та ЕП.

– К11 – Рівень довіри до постквантових криптоперетворень АСШ, ПІК та ЕП на різних рівнях застосування.

– К12 – Перспективність та виправданість застосування постквантових криптоперетворень АСШ, ПІК та ЕП.

Так як вони є основними складовими узагальненого критерію переваги, то варто використовувати часткові умовні критерії саме згідно цього переліку. Цей перелік не є вичерпним і часткові критерії не є обов'язковими, тому вони можуть бути змінені, замінені, розширений їх перелік чи взагалі, якщо того вимагають моделі загроз тощо, відкинуті.

Варто зауважити, що інтегральний умовний критерій, за своєю суттю, представляє усереднене певним чином значення і базується на методах експертних оцінок. Рішення про відповідність умовним критеріям приймається за результатами проведеного експертною комісією аналізу, згідно висунутих вимог до асиметричного криптографічного перетворення.

Основним методом обчислення значення інтегрального умовного критерію є поєднання часткових умовних критеріїв в умовний інтегральний критерій. В якості основних методів згортання часткових умовних критеріїв можуть бути використані метод аналізу ієрархій на основі попарних порівнянь або метод визначення вагових коефіцієнтів.

2.6. Опис прагматичних критеріїв

Третім етапом комплексної методики є методика оцінювання за прагматичними критеріями та результати дослідження перспективних стандартизованих криптоперетворень. Сутність комплексної методики загалом та конкретно її третього етапу (прагматичні критерії) можна виразити наступним чином.

Згідно комплексної методики, перші два етапи використовують безумовні та умовні критерії. Таким чином, на першому етапі проводиться оцінювання та перевірка криптопримітивів на предмет відповідності системі часткових

безумовних критеріїв та обчислюється безумовний інтегральний критерій. На другому етапі проводиться оцінювання з використанням часткових умовних критеріїв і обчислюється інтегральний умовний критерій.

Третій етап залежить від вимог, що висуваються до криптопримітивів, та за необхідності проводиться оцінювання та порівняння альтернативних примітивів за техніко-економічними та техніко-експлуатаційними критеріями. В якості основних прагматичних критеріїв варто використовувати такі характеристики, як довжини особистих та відкритих ключів, довжини електронних підписів та довжини блоків, складність генерування (обчислення) ключів та параметрів тощо. Третій етап є важливим через те, що на ньому здійснюється перевірка відповідності часткових безумовних та умовних критеріїв тим вимогам, котрі висуваються щодо них відповідними нормативними документами.

Порядок процесу оцінювання та порівняння криптопримітивів має наступний вигляд [5]:

1. Аналізу та порівнянню підлягають тільки такі криптоперетворення, які успішно пройшли тестування згідно вимог 3-го етапу.

2. Подальший аналіз проводиться з використанням умовних часткових та інтегрального умовного критеріїв щодо усіх криптопримітивів, що пройшли відбір згідно безумовних критеріїв.

3. Визначається перелік прагматичних критеріїв щодо кожного класу проектів криптоперетворень.

4. На основі експериментальних та теоретичних оцінок, визначаються основні показники щодо техніко-економічних та техніко-експлуатаційних характеристик, такі як:

1) $I_{ст.}$ – рівень криптографічної стійкості;

2) $l_{в.к.}$ – довжина відкритого ключа;

3) $l_{о.к.}$ – довжина особистого ключа;

4) $l_{рез.}$ – довжина АСШ, ПІК (ЕП);

5) $T_{пр.}$ – складність (швидкість) обчислення;

6) $T_{зв.}$ – складність (швидкість) перевірки;

7) $T_{ген.зп.}$ – складність (швидкість) генерування загальних параметрів;

8) $T_{ген.кл.}$ – складність (швидкість) генерування ключа (ключової пари) з урахуванням особливостей.

5. На основі експериментальних та теоретичних оцінок, визначаються залежності необхідних показників у відповідності до їх техніко-економічних та техніко-експлуатаційних характеристик, але з урахуванням криптографічної стійкості.

6. Після аналізу значень показників, їх залежностей та значень умовних та безумовних критеріїв, що були отримані на попередніх етапах, приймаються рішення про переваги певних кандидатів та розробляються рекомендації щодо прийняття в якості стандартів тих чи інших кандидатів.

7. Визначаються такі залежності як:

– довжини відкритого ключа від довжини особистого (закритого) ключа у залежності від математичного методу асиметричної пари ключа;

– складності генерування відкритого ключа від складності генерування особистого ключа у залежності від математичного методу, який застосовується при побудові асиметричної пари ключа;

– складності генерування загальних параметрів від математичного методу, який застосовується;

– довжини ЕП від математичного методу, який застосовується;

– збитковості від математичного методу, який застосовується.

Застосування прагматичної методики стає необхідним у випадках, коли є потреба у забезпеченні виконання вимог ТЗ та ТТЗ щодо розмірів ключів та параметрів та інших параметрів та критеріїв.

2.7. Особливості процесу оцінки та порівняння

Для порівняння з вимогами та критеріями, що існують на міжнародному рівні варто поглянути на приклади критеріїв та вимог згідно NIST.IR 8413 та IT Grundschutz Compendium.

Критерії та вимоги у відповідності до NIST.IR 8413 [2]:

1. Відповідність моделі безпеки: так, наприклад для АСШ, ПІК – IND-CPA та IND-CCA2; а для ЕП – EUF-CMA.

2. Відповідність наборів параметрів категоріям безпеки: наприклад 1, 2, 3 та 5.

3. Гнучкість, простота та адаптація криптоперетворення, що позначає відсутність факторів, які могли б перешкодити адаптації.

4. Стійкість до атак бічними каналами.

5. Патентна незалежність.

6. Залежність показників криптоперетворення від використовуваного процесора.

7. Розміри параметрів та основних перетворень досліджуваного криптоперетворення.

Критерії та вимоги у відповідності до IT Grundschutz Compendium [48]:

1. Забезпечення реалізації захисту від несанкціонованого доступу до ІТ-систем під час застосування обраного криптографічного алгоритму.

2. Забезпечення реалізації захисту від вразливостей програмного забезпечення або помилок під час застосування обраного криптографічного алгоритму.

3. Забезпечення запобігання неправильного використання дозволу (авторизації) під час застосування обраного криптографічного алгоритму.

4. Забезпечення запобігання заперечення (відмови) дій під час застосування обраного криптографічного алгоритму.

5. Забезпечення реалізації захисту від застосування зловмисного програмного забезпечення під час застосування обраного криптографічного алгоритму.

6. Забезпечення запобігання відмови в обслуговуванні під час застосування обраного криптографічного алгоритму.

7. Забезпечення запобігання втрати цілісності конфіденційної інформації під час застосування обраного криптографічного алгоритму.

8. Забезпечення реалізації визначеної криптографічної концепції під час застосування обраного криптографічного алгоритму.

9. Забезпечення захисту даних під час застосування обраного криптографічного алгоритму.

10. Забезпечення використання хмари (за необхідності) під час застосування обраного криптографічного алгоритму.

11. Забезпечення реалізації механізму виявлення подій, релевантних для безпеки, під час застосування обраного криптографічного алгоритму.

Загальний вигляд процесу оцінювання та порівняння криптопримітивів згідно Методики за всіма видами критеріїв (безумовні, умовні, прагматичні) наведено у вигляді блок-схеми, що демонструє послідовність дій, на Рисунку 2.2.

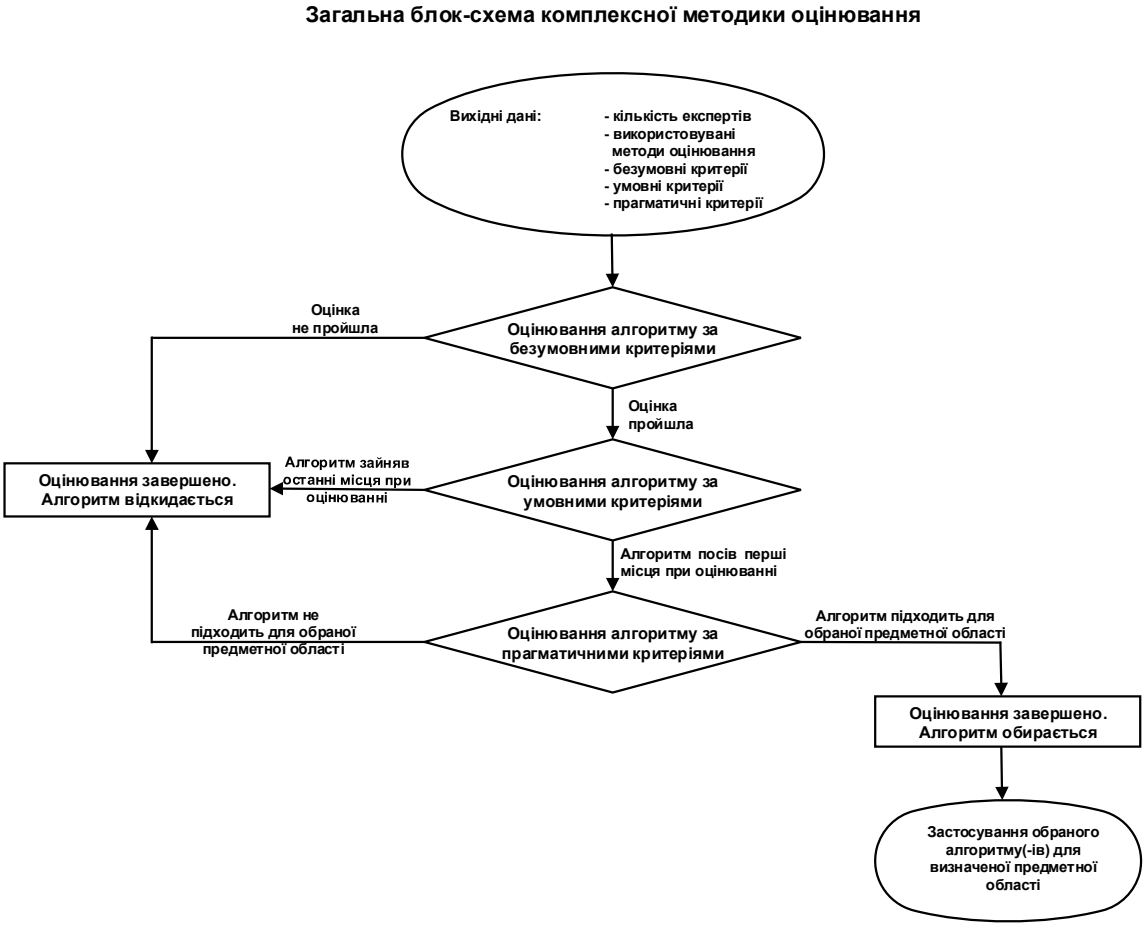

Рис. 2.2. Загальний вигляд процесу оцінювання та порівняння криптопримітивів згідно Методики

2.8. Висновки до розділу 2

1. У другому розділі розглянуто та сформульовано перелік основних варіантів застосування ЕП, котрі впливають на конкретизовані вимоги до безпеки та інших параметрів ЕП. До нього входять: Інфраструктура відкритих ключів (SSL/TLS; DNSSEC; S/MIME), Підпис коду, SIM-карти, IPSec, Електронні паспорти, Підписання PDF, Blockchain, VPN.

2. Показано, що моделі порушника, загроз і безпеки, орієнтовані на асиметричні крптографічні перетворення, що в тому числі є кандидатами на стандартизацію в якості квантовостійких стандартів, мають загальну основу з іншими моделями порушника, загроз і безпеки. Також показано, що у моделі порушника, згідно із суттєво посиленими вимогами, повинен забезпечуватися

захист від класичних та квантових атак від порушника 3-го та 4-го рівнів, для яких майже не існує обмежень щодо матеріально-технічного та фінансового забезпечення.

3. Безумовні критерії оцінки та порівняння АСШ, ПІК та ЕП обираються згідно до безпекових вимог (вимог до стійкості), досягнутих завдяки результатам практичного розв’язання задач криптоаналізу, в тому числі на основі реалізації алгоритмів квантового криптоаналізу. Оцінювання за безумовними критеріями складається із оцінки за частковими безумовними критеріями та подавльшою їх кон’юнкцією для отримання інтегрального безумовного критерію.

4. Умовні критерії оцінки та порівняння АСШ, ПІК та ЕП є основними складовими узагальненого критерію переваги. Аналогічно до безумовних критеріїв, часткові умовні критерії призначені для поєднання з метою отримання інтегрального умовного критерію. Варто зауважити, що інтегральний умовний критерій, за своєю суттю, представляє усереднене певним чином значення і базується на методах експертних оцінок (метод аналізу ієрархій на основі попарних порівнянь або метод визначення вагових коефіцієнтів). Рішення про відповідність умовним критеріям приймається за результатами проведеного експертною комісією аналізу, згідно висунутих вимог до асиметричного криптографічного перетворення.

5. Прагматичні критерії залежать від вимог, що висуваються до криптопримітивів, та за необхідності проводиться оцінювання та порівняння альтернативних примітивів за техніко-економічними та техніко-експлуатаційними критеріями. В якості основних прагматичних критеріїв варто використовувати такі характеристики, як довжини особистих та відкритих ключів, довжини електронних підписів та довжини блоків, складність генерування (обчислення) ключів та параметрів тощо.

6. Сформовано переліки безумовних, умовних та прагматичних критеріїв.

РОЗДІЛ 3. НАУКОВО-МЕТОДИЧНІ ОСНОВИ РОЗРОБКИ, ОЦІНКИ ТА ПОРІВНЯННЯ ІСНУЮЧИХ ТА ПЕРСПЕКТИВНИХ КВАНТОВОСТІЙКИХ ЕЛЕКТРОННИХ ПІДПИСІВ ЗА БЕЗУМОВНИМИ, УМОВНИМИ ТА ПРАГМАТИЧНИМИ КРИТЕРІЯМИ

3.1. Обгрунтування, опис, призначення та застосування комплексної методики оцінки, аналізу та порівняння

3.1.1. Обгрунтування поняття комплексної методики оцінки та порівняння

З метою практичної оцінки та порівняння застосовують різноманітні методики послуг (продуктів тощо). Використання методик дозволяє ідентичним чином контролювати за затвердженим порядком практичну якість надання послуг, товарів або виконання різноманітних умов. Для криптографічних систем особливо важливим є забезпечення надання наступних послуг: конфіденційність, цілісність, доступність, неспростовність, захищеність від несанкціонованого доступу, неспростовність, криптоживучість тощо.

З урахування перехідного та постквантового періодів при прийнятті стандартів криптографічних перетворень (в тому числі ЕП) важливим є питання розробки та застосування відповідним чином комплексної методики оцінки та порівняння криптографічної стійкості нових та існуючих перспективних, доказовостійких криптографічних алгоритмів і протоколів, зокрема для перехідного та постквантового періодів.

Для формулювання та коректного використання методики було досліджено визначення, вимоги та сутності існуючих методик. Також було розглянуто їх придатність до використання в контексті криптології. Так, зокрема було розглянуто наступні визначення поняття методики [49]:

1. Методика – фіксована сукупність прийомів практичної діяльності, яка призводить до заздалегідь визначеного результату. У науковому пізнанні

методика грає важливу роль в емпіричному дослідженні (спостереженні і експерименті). На відміну від методу, у завдання методики не входить теоретичне обґрунтування отриманого результату, вона концентрується на технічну сторону експерименту і на регламентації дій дослідника.

Наведені вище визначення було обрано з урахуванням специфіки криптології (криптографії та криптоаналізу), в якості вихідних. Вони будуть використані з метою обґрунтування вимог та умов застосування.

Під час розроблення методики необхідно передбачати:

- попереднє цілеспрямоване спостереження за об’єктом або явищем, що вивчається, з метою визначення вихідних даних (гіпотез, обрання змінних факторів);
- створення умов, у яких можливе експериментування (добір об’єктів для експериментальної дії, усунення впливу випадкових факторів);
- визначення області інтересу для змінних факторів та меж вимірювання;
- можливість систематичного спостереження за розвитком явища і точного опису фактів;
- проведення систематичної реєстрації замірів і оцінок фактів різними засобами і способами;
- створення складних ситуацій з метою підтвердження або спростування раніше отриманих даних;
- перехід від емпіричного вивчення з логічним узагальненням до аналізу та теоретичного оброблення отриманих фактичних даних.

Після вибору методики, необхідно підтвердити можливість її практичного застосування та, за необхідності, усунути невідповідності наявним умовам її використання. За неможливості усунення невідповідностей, в силу специфічних особливостей середи застосування варто відмовитись від обраної методики на користь більш підходящої.

Важливо виділити у наведених визначеннях методики сутності, наведені далі.

У визначенні вказується, що [49]:

- це фіксована сукупність прийомів практичної діяльності;
- вона призводить до заздалегідь визначеного результату;
- грає важливу роль в емпіричному дослідженні (спостереженні і експерименті);
- на відміну від методу в завдання методики не входить теоретичне обґрунтування отриманого результату;
- вона концентрується на технічну сторону експерименту і на регламентації дій дослідника.

Виходячи із сутностей визначень та проблемних питань криптології [2, 6-8, 10-12, 24-26], стає можливим визначити наступні вимоги до методики аналізу криптографічної стійкості та властивостей існуючих та перспективних (постквантових) криптографічних алгоритмів і протоколів, у тому числі у перехідний та постквантовий періоди:

- методика повинна бути фіксованою сукупністю прийомів практичної діяльності щодо аналізу криптографічної стійкості та властивостей існуючих та перспективних (постквантових) АСШ, ПІК та ЕП, у тому числі у перехідний та постквантовий періоди;
- методика повинна призводити до заздалегідь визначеного результату оцінки криптографічної стійкості та аналізу і порівняння властивостей існуючих та перспективних (постквантових) АСШ, ПІК та ЕП, у тому числі у перехідний та постквантовий періоди;
- методика повинна ґрунтуватись на спостереженні і експерименті, що направлені на оцінку криптографічної стійкості та аналізу і порівняння існуючих та перспективних (постквантових) АСШ, ПІК та ЕП;
- методика повинна концентруватись на алгоритмічній та технічній стороні експерименту і на регламентації дій дослідника при його проведенні;
- повинні визначатись вихідні дані щодо криптографічної стійкості та властивостей існуючих та перспективних (постквантових) АСШ, ПІК та ЕП;

- потрібно здійснити попередні дослідження та розробки щодо моделей порушника та моделей загроз, які можуть бути застосовані в процесі зламу асиметричних криптоперетворень існуючих та перспективних (постквантових) АСШ, ПІК та ЕП;

- повинне бути цілеспрямоване спостереження та збір необхідних даних щодо асиметричних криптоперетворень існуючих та перспективних (постквантових) АСШ, ПІК та ЕП (математичні основи побудування, розміри загальних параметрів та ключів, середовище застосування, критичність інформації та ресурсів, що захищаються, математичні основи та системи класичного та квантового криптоаналізу, їх можливості, прогнозування розвитку криптології та уточнення даних тощо);

- створення умов, у яких можливе експериментальне дослідження та випробовування методики, наявність програмних моделей як криптопримітивів, так і засобів криптоаналізу та аналізу властивостей існуючих та перспективних (постквантових) АСШ, ПІК та ЕП;

- визначення та врахування в експериментах можливих значень довжин параметрів та ключів існуючих та перспективних (постквантових) АСШ, ПІК та ЕП, а також математичних, алгоритмічних та програмних особливостей, включаючи комп’ютерну алгебру в галузі криптології тощо;

- можливості систематичного відслідковування та використання в методиці змінних параметрів та змінного середовища, а також врахування в максимально можливій мірі розвитку асиметричної криптології існуючих та перспективних (постквантових) АСШ, ПІК та ЕП;

- систематичний аналіз стійкості асиметричних криптографічних алгоритмів та безпечності криптографічних протоколів існуючих та перспективних (постквантових) АСШ, ПІК та ЕП з використанням відомих та потенційних криптоаналітичних атак;

- можливість реалізації в методиці існуючих та потенційних моделей порушника та моделей загроз, моделювання та створення критичних ситуацій з

метою підтвердження або спростування раніше отриманих даних з використанням інших методик;

- можливість переходу від емпіричного вивчення з логічним узагальненням стійкості та властивостей асиметричних криптографічних алгоритмів та безпечності криптографічних протоколів існуючих та перспективних (постквантових) АСШ, ПІК та ЕП, до аналізу та теоретичного оброблення отриманих фактичних даних.

Таким чином, в подальшому під комплексною методикою аналізу криптографічної стійкості існуючих та перспективних (постквантових) криптографічних перетворень (в тому числі ЕП), у перехідний та постквантовий періоди, будемо розуміти фіксовану сукупність прийомів практичної діяльності щодо аналізу криптографічної стійкості та властивостей існуючих та перспективних (постквантових) криптографічних перетворень, у перехідний та постквантовий періоди, що відповідає наведеним вище вимогам.

3.1.2. Обгрунтування, призначення та застосування комплексної методики оцінки, аналізу та порівняння

Для оцінки, аналізу і порівняння криптографічної стійкості та властивостей існуючих та перспективних (тих, що претендують на звання квантово-стійких) АСШ, ПІК та ЕП може бути застосована комплексна методика оцінки, аналізу та порівняння криптографічної стійкості та властивостей. Вона може бути застосована у явному вигляді при дослідженнях, оцінці та порівнянні існуючих, нині стандартизованих та альтернативних криптопримітивів типу АСШ, ПІК та ЕП, та перспективних криптопримітивів АСШ, ПІК та ЕП, що призначені для стандартизації в якості квантово-стійких.

Комплексна методика безпосередньо призначена для використання при оцінці, аналізі та порівнянні криптографічної стійкості та властивостей існуючих та постквантових криптографічних перетворень. Також ця методика може бути у явному вигляді застосована при дослідженнях, оцінці та порівнянні

існуючих стандартизованих та альтернативних криптографічних примітивів типу АСШ, ПІК та ЕП, включаючи перспективні криптографічні примітиви цих типів.

Комплексна методика аналізу існуючих та постквантових криптографічних перетворень є комплексною та визначає три наступні методики [5]:

- методику оцінки та порівняння криптографічної стійкості існуючих та постквантових криптографічних перетворень на основі використання безумовних критеріїв стійкості;

- методику оцінки та порівняння існуючих та постквантових криптографічних перетворень на основі використання умовних критеріїв;

- методику оцінки та порівняння властивостей існуючих та постквантових криптографічних перетворень на основі прагматичних критеріїв.

Ці методики можуть застосовуватись незалежно одна від одної, але основним застосуванням є їх застосування у вказаній послідовності – спочатку з використанням на основі безумовних критеріїв, потім на основі умовних критеріїв та при необхідності на основі прагматичних критеріїв.

Методика може бути застосована при:

- обґрунтуванні та розробленні порядку застосування методик оцінки та порівняльного аналізу асиметричних існуючих та перспективних, в тому числі стандартизованих, криптографічних примітивів АСШ, ПІК та ЕП;

- обґрунтуванні та вибору критеріїв та показників оцінки криптографічної стійкості та інших властивостей, в тому числі стандартизованих криптопримітивів типу АСШ, ПІК та ЕП;

- оцінці, аналізі та порівнянні асиметричних існуючих та перспективних постквантових, в тому числі стандартизованих, криптографічних примітивів АСШ, ПІК та ЕП на основі застосування безумовних критеріїв;

- оцінці, аналізі та порівнянні асиметричних існуючих та перспективних, в тому числі стандартизованих, криптопримітивів АСШ, ПІК та ЕП на основі застосування умовних критеріїв;

- оцінці, аналізі та порівнянні асиметричних існуючих та перспективних, в тому числі стандартизованих, криптопримітивів АСШ, ПІК та ЕП на основі застосування прагматичних критеріїв;

- обґрунтуванні та виборі основних методів експертного оцінювання криптографічної стійкості та інших властивостей існуючих та постквантових, в тому числі стандартизованих, криптопримітивів типу АСШ, ПІК та ЕП;

- реалізації методу ієрархій на основі попарних порівнянь та врахуванні особливостей його застосування для оцінки та порівняння властивостей існуючих та постквантових криптографічних примітивів АСШ, ПІК та ЕП;

- обґрунтуванні та виборі для оцінки та порівняльного аналізу існуючих та перспективних криптопримітивів АСШ, ПІК та ЕП в тому числі стандартизованих, методу вагових коефіцієнтів;

- розробці рекомендації щодо оцінки та порівняння альтернативних криптопримітивів типу АСШ, ПІК та ЕП за прагматичними техніко-економічними та техніко-експлуатаційними критеріями.

Методики оцінювання та порівняльного аналізу криптопримітивів базуються на використанні системи безумовних та умовних часткових та інтегральних критеріїв, прагматичних критеріїв, а також показників, які дозволяють оцінити ступінь виконання висунутих до криптоперетворення вимог. Основним завданням таких методик є формалізація процесів прийняття рішень відносно виконання висунутих до них вимог, врахування переваг та недоліків криптопримітивів, що є кандидатами на постквантовий стандарт, зменшення впливу суб’єктивних факторів на прийняття рішень, в тому числі несанкціонованого впливу сторонніх організацій тощо. Наприклад, такі методики можуть бути застосованими щодо оцінки та порівняння алгоритмів АСШ, ПІК та ЕП, в тому числі тих, що є кандидатами на постквантовий стандарт.

На формальному рівні такі методики оцінки та порівняння криптографічних перетворень можуть бути узагальненими (базовими, комплексними). Але, оскільки до названих криптопримітивів висуваються різні

вимоги, то для кожного із примітивів вони можуть доповнятись чи спрощуватись та відображати весь спектр висунутих вимог. Також такі методики можуть забезпечити прозорість прийняття рішень, незалежність експертів, та допомогти обґрунтувати прийняття відповідних рішень та довіру до них. В подальшому під методикою буде розумітись фіксована сукупність прийомів практичної діяльності щодо аналізу криптографічної стійкості та властивостей нових, доказовостійких криптоалгоритмів і протоколів, у тому числі у перехідний та постквантовий періоди, що відповідає наведеним вище вимогам та призводить до заздалегідь визначеного результату.

Наведені методики оцінювання та порівняльного аналізу криптопримітивів грунтуються на застосуванні системи безумовних критеріїв, умовних критеріїв, прагматичних критеріїв відповідно, а також виведених показників, які дають змогу оцінити виконання висунутих до криптоперетворень вимог.

Методики сформовано таким чином, що основним їх завданням є формалізація процесів прийняття рішень щодо виконання криптопримітивами, що є кандидатами на квантовостійкий стандарт, висунутих до них вимог, врахування їх переваг та недоліків, зі зменшенням впливу на прийняття рішень різних суб’єктивних факторів, в тому числі несанкціонованого впливу третіх сторін тощо. Так, наприклад, такі методики можуть бути застосованими для оцінки та порівняння алгоритмів АСШ, ПІК та ЕП, що є потенційними кандидатами на квантовостійкий міжнародний або національний стандарт.

Методики оцінки та порівняння цілком можуть бути узагальненими. Але, оскільки до квантовостійких криптопримітивів висуваються різні вимоги, то для кожного із примітивів вони можуть доповнятись або спрощуватись в залежності від потреб та відображати весь спектр висунутих вимог або тільки релевантні для конкретного порівняння. Також цілком можливим є забезпечення прозорості прийняття рішень, незалежності експертів, та більш зрозуміле та загальноприйнятне обґрунтування прийнятого на базі використання таких методик рішень.

3.2. Обґрунтування та вибір критеріїв та показників оцінки та порівняння

Як вже було зазначено, методики базуються на використанні критеріїв. Критерії є ознаками, на основі яких здійснюється оцінка, визначення чи класифікація чого-небудь, мірилом оцінки [50].

Порівняння криптопримітивів є можливим з використанням трьох сукупностей критеріїв: безумовних, умовних та прагматичних. Це дозволяє зробити оцінку та порівняння криптопримітивів, що є кандидатами на постквантові стандарти у 3 етапи оцінки за частковими та інтегральними критеріями. Також важливим є врахування чи використання експертних оцінок.

На першому етапі спочатку перевіряється відповідність криптопримітиву системі часткових безумовних критеріїв, а потім для кожного криптопримітиву на основі часткових обчислюється безумовний інтегральний критерій.

На другому етапі отримуються відповідні оцінки з використанням спочатку системи часткових умовних критеріїв, а потім на їх основі обчислюється інтегральний умовний критерій.

На третьому етапі отримуються відповідні оцінки з використанням системи прагматичних критеріїв.

У цілому, такий підхід дозволяє відкинути криптоперетворення, що не відповідають безумовним вимогам, тобто вимогам, які повинні бути виконані безумовно. Причому інтегральний безумовний критерій дозволяє прийняти рішення відносно кожного із криптопримітивів. У нашому випадку це різні криптопримітиви ЕП.

Застосування часткових умовних критеріїв, а потім на їх основі інтегрального умовного критерію, дозволяють оцінити якість криптопримітиву у широкому змісті, як якість у середньому, а потім і порівняти криптопримітиви, що є кандидатами на постквантовий алгоритм.

Третій етап передбачає отримання відповідних оцінок з використанням системи прагматичних критеріїв.

До безумовних критеріїв відносяться ті критерії, виконання яких для криптопримітиву є обов'язковим, тобто безумовним [5]. При чому, для асиметричних криптоперетворень типу АСШ, ПІК та ЕП можна вибрати однакову систему безумовних критеріїв. Але це не виключає можливостей врахування особливостей вимог та відповідно вибору при аналізі та оцінці криптопримітивів додаткових часткових безумовних критеріїв.

Аналіз вимог, що висунуті NIST [2, 3, 15] до часткових безумовних критеріїв асиметричних криптоперетворень типу АСШ, ПІК та ЕП та певних національних нормативно-правових документів [24-26], а також досягнуті результати при практичному розв'язанні задач криптоаналізу, в тому числі на основі реалізації алгоритмів квантового криптоаналізу, дозволяють вибрати сукупність безумовних критеріїв оцінки АСШ, ПІК та ЕП.

Розглянемо систему часткових безумовних критеріїв, орієнтуючись на вимоги NIST та певні національні нормативно-правові документи.

До безумовних критеріїв оцінки ПІК можна відносити:

1. Практично реалізований рівень моделі безпеки IK-CPA/CCA2.
2. Криптостійкість (складність криптоаналізу) щодо криптоперетворення ЕП – $W_{ЕП}$, що застосовуються в протоколі ПІК.
3. Криптостійкість (складність криптоаналізу) щодо криптоперетворення інкапсуляції – $W_{ПІК}$, та АСШ – $W_{АСШ}$, що застосовуються в протоколі інкапсуляції та асиметричного шифрування.
4. Криптоживучість ключів щодо криптоперетворення АСШ – $G_{АСШ}$ та АСШ – $W_{АСШ}$ (ЕП – $G_{ЕП}$), що застосовуються в протоколі ПІК (ЕП).
5. Криптоживучість ключів, що застосовуються в протоколі ПІК – $G_{ПІК}$.
6. Захищеність криптопротоколу від раніше переданих повідомлень – $W_{рпп}$.
7. Неспростовності криптоперетворень АСШ – $N_{АСШ}$, що встановлені

для криптографічного захисту.

8. Неспростовності криптоперетворень ЕП – $N_{ЕП}$, що встановлені для криптографічного захисту.

9. Новизну ключів АСШ (ЕП) – $W_{кл.}$, що застосовуються в протоколі інкапсуляції ПІК та для АСШ (в кращому випадку використання ключів сеансу).

10. Характеристику степеню нерозрізнюваності для ключів АСШ, ПІК та ЕП.

3.3. Опис комплексної методики оцінки та порівняння

3.3.1. Загальний зміст та опис комплексної методики

Основним вмістом методики досліджень криптопримітивів є сукупність наведених нижче елементів.

Основним призначенням методики є її використання для оцінювання будь-яких криптографічних примітивів. Для кожного окремого випадку оцінювання необхідно лише обирати відповідні часткові критерії та показники. Сама методика є універсальною.

Методика може бути застосована для оцінювання будь-яких систем у будь-якій предметній області, у тому числі для оцінювання криптографічних систем (криптопримітивів). Перевагою методики є універсальність математичного апарату, що використовується. Для кожного окремого випадку, потрібно змінювати лише необхідні критерії/показники оцінки, а сама послідовність дій залишається однаковою.

Необхідними вихідними даними, у першу чергу, є визначені часткові безумовні та умовні критерії і показники. Крім того, вихідними даними методики є значення коефіцієнтів для часткових критеріїв/показників, що представлені у вигляді вектор-строки та значення коефіцієнтів для кожного криптографічного примітиву, що представлені у вигляді вектор-строки. Вихідні

дані отримуються наступним чином: значення коефіцієнтів як для часткових критеріїв/показників, так і для кожного криптографічного примітиву знаходяться за відповідними математичними виразами для визначення коефіцієнтів, що наведені у відповідних методах оцінювання, на основі оцінок (балів), що виставляють експерти.

При виборі експертів, які будуть проводити оцінювання, необхідно враховувати їх рівень компетентності у визначеній предметній області та ступінь довіри до них.

На основі отриманих від експертів даних, виконується спочатку математична обробка згідно з правилами, описаними у кожному методі оцінювання, а потім на основі отриманих результатів математичної обробки виконується програмне моделювання.

У якості математичного забезпечення, у розробленій методиці використовуються:

- функції булевої алгебри (функція відповідності криптоперетворення);
- метод аналізу ієрархій, метод попарних порівнянь, метод визначення вагових коефіцієнтів;
- математичні методи визначення інтегрального умовного критерію (метод аналізу ієрархій на основі попарних порівнянь та метод визначення вагових коефіцієнтів).

Основними діями щодо оцінювання криптопримітивів, у відповідності до даної методики, є наступні:

1) Визначаються часткові умовні та безумовні критерії і показники.

2) Обираються експерти, згідно їх рівня компетенції у визначеній предметній області.

3) Проводиться оцінка обраних криптопримітивів за частковими безумовними критеріями.

4) На основі безумовного інтегрального критерію (за допомогою функції відповідності криптоперетворення) приймається рішення, на основі оцінки, яку отримано (позитивну чи негативну), про те, чи буде проводитись подальше

порівняння та оцінювання на основі часткових умовних критеріїв та інтегрального умовного критерію.

Для криптопримітивів, що отримали позитивну оцінку за інтегральним безумовним критерієм, подальше порівняння та оцінювання можна зробити на основі умовних критеріїв та інтегрального умовного критерію.

5) Дослідження криптографічних примітивів за сукупністю умовних критеріїв. Проводиться оцінювання на основі часткових та інтегрального умовного критерію. В якості методів оцінювання на основі умовних критеріїв, використовуються метод аналізу ієрархій на основі попарних порівнянь та методи визначення вагових коефіцієнтів.

6) Отримання кінцевих результатів. Для отримання кінцевого результату за даними методами (для кожного методу окремо), необхідно перемножити вектор пріоритетів 1 рівня і матрицю набутих значень 1 рівня, і впорядкувати отримані чисельні значення від найбільшого до найменшого. На основі розміщення значень коефіцієнтів для визначених криптопримітивів від найбільшого до найменшого, робиться висновок про те, який з криптопримітивів є найкращим (перше місце), а який – гіршим (останнє місце).

Отримуються та наводяться результати за обраними методами оцінювання. Після отримання усіх результатів за усіма методами оцінки, будується графік на основі результатів оцінювання криптографічних примітивів за різними методами оцінки.

3.3.2. Результати використання методики та практичні рекомендації

Після проведення оцінювання за даною методикою, необхідно навести висновки та рекомендації згідно результатів оцінювання у наступному вигляді.

1) За результатами порівняльного аналізу стандартизованих криптопримітивів максимальне значення умовного інтегрального критерію досягається для криптопримітиву (криптопримітивів) *XXX* (вказати за якими саме методами оцінки, чи за усіма методами).

2) Такий результат обумовлений насамперед тим, що...

3) За результатами порівняльного аналізу стандартизованих криптопримітивів мінімальне значення умовного інтегрального критерію досягається для криптопримітиву (криптопримітивів) *XXX* (вказати за якими саме методами оцінки, чи за усіма методами).

4) Такий результат обумовлений насамперед тим, що...

5) Числовий розкид значень вагових коефіцієнтів для одного криптопримітиву є значним/незначним/майже незначним (якщо за якимось методом оцінки отримуються результати, що достатньо відрізняються від інших – зазначити цей факт і пояснити, чим саме обумовлено такий результат).

6) На рис. *X* графічно зображено результати оцінювання визначених криптопримітивів за різними методами оцінювання (наводиться графік на основі результатів оцінювання криптографічних примітивів за різними методами оцінювання).

7) Для отримання більш точних результатів оцінювання, а також для точного співпадіння розташування визначених криптопримітивів за усіма методами оцінки, необхідно виконати процедуру оцінювання декілька разів та ретельно підійти до вибору експертів, що будуть проводити оцінювання (вказати у випадку, якщо отримані результати недостатньо вдовольняють).

На рис 3.1 зображено загальну блок-схему комплексної методики оцінювання. На рис. 3.2 наведено блок-схему процесу оцінювання за комплексною методикою оцінювання.

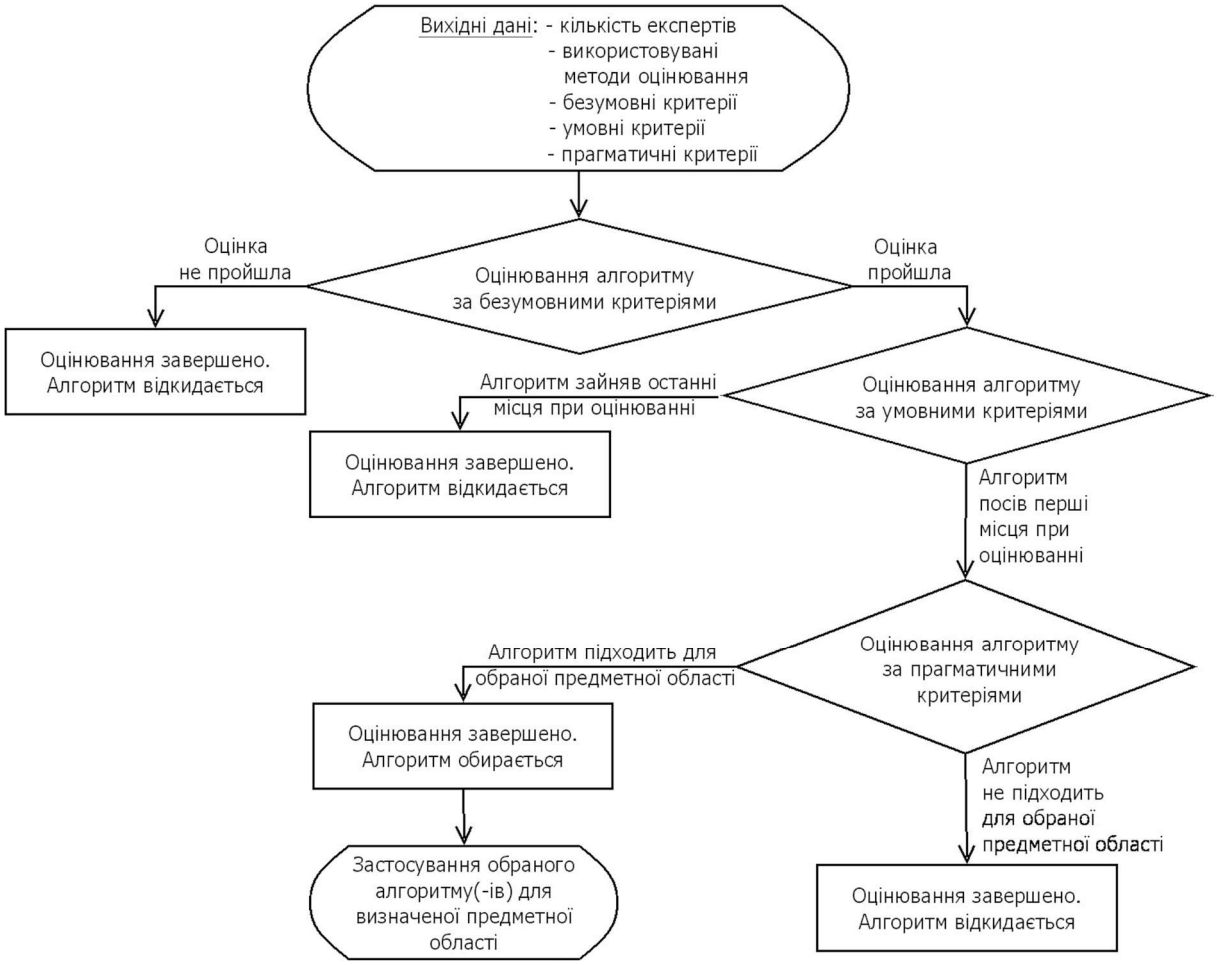

Рис. 3.1. Загальна блок-схема комплексної методики оцінювання

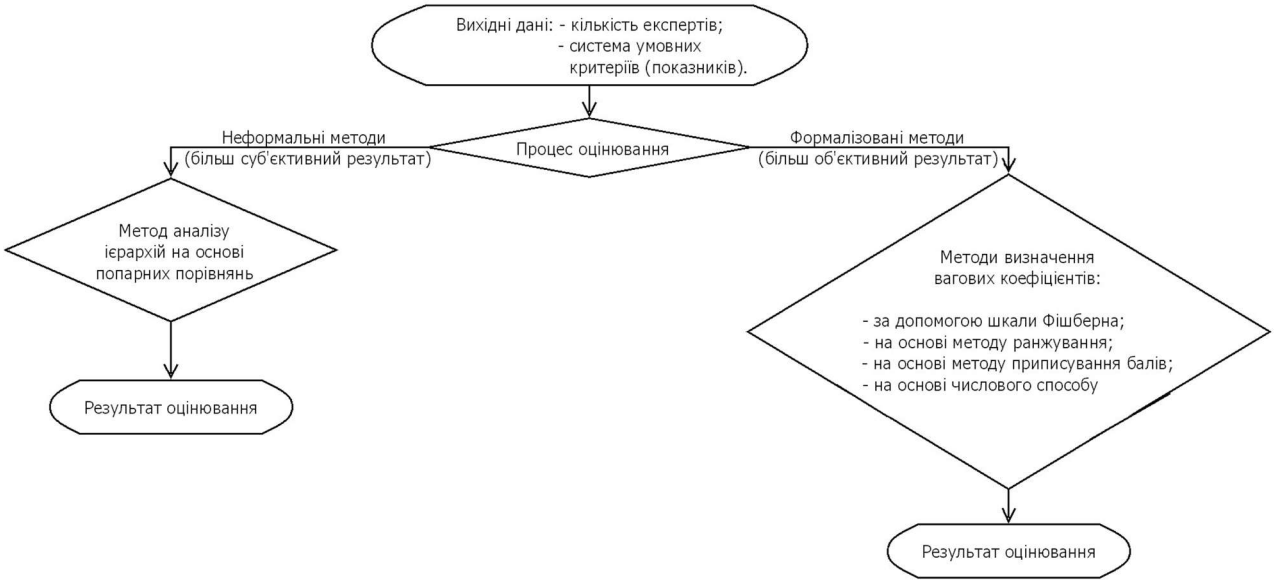

Рис. 3.2. Блок-схема процесу оцінювання за комплексною методикою оцінювання

3.4. Обґрунтування особливостей застосування методів експертних оцінок

Застосування методу експертних оцінок у загальному випадку пов’язується з виконанням процедур вибору експертів, підбору експертів та встановлення ступеня узгодженості думок експертів.

Експертні оцінки можуть розглядатись і як метод пошуку і як результат застосування методу, котрий отримано за рахунок використання персональної думки експерта або групи експертів. Разом з тим, експертні оцінки є комплексом логічних та математичних процедур, що направлені на отримання інформації з боку спеціалістів, та її подальший аналіз та узагальнення для підготовки та прийняття раціональних рішень (Рис. 3.3) [51].

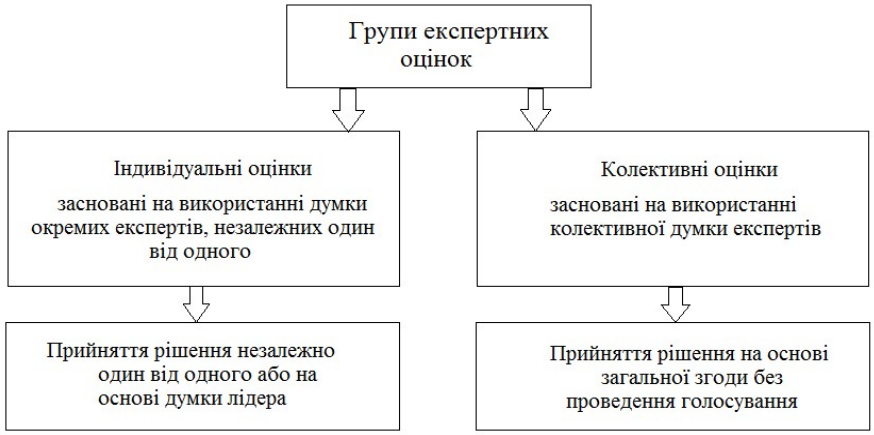

Рис. 3.3. Схема аналізу груп експертних оцінок

Методи експертних оцінок призначено для використання думки спеціаліста або колективу спеціалістів, отриманих за рахунок їх знань і практичного професійного досвіду, як основи для прийняття рішення, прогнозу чи висновку. Експертні методи оцінки застосовують в ситуаціях, коли вибір, обґрунтування і оцінка рішень не можуть бути виконані на основі точних розрахунків [51].

Нині популярними є методи експертних оцінок, що отримуються таким чином:

– на основі індивідуальних думок експертів;

– на основі колективної роботи групи експертів;

– на основі індивідуальних та колективних думок експертів.

Статистична обробка результатів експертних оцінок подібна статистичній обробці результатів вимірювань. На достовірність експертизи істотно впливають такі чинники, як чисельний склад експертної групи, рівень компетентності експертів, склад питань, пропонованих експертам, і т.д. [51].

Індивідуальні експертні оцінки також носять на собі печатку випадковості: настрій, самопочуття, обстановка, а також знання і досвід експерта.

Загально прийнято виконувати експертне оцінювання у наступні етапи:

1) постановка мети;

2) вибір форми та визначення бюджету дослідження;

3) підготовка інформації, анкет, відповідально за процедуру;

4) вибір релевантних експертів;

5) проведення експертизи;

6) проведення аналізу отриманих результатів;

7) підготовка звіту з фінальними результатами.

Такий підхід має успіх і поширення через те, що спільна думка має більшу точність, ніж окрема індивідуальна думка кожного з експертів. Даний метод дуже поширений у сферах, де необхідне отримання кількісних оцінок якісних характеристик та вивчення властивостей.

Різновидом самооцінювання є диференційний метод, у якому, як правило, оцінка дається за двома групами критеріїв, що характеризують знайомство експерта з об’єктами експертизи та за критеріями, а також знайомство експерта з основними джерелами інформації в даній області.

Можливо визначення рівня компетентності експерта і при взаємному оцінюванні. У простішому випадку кожний експерт з даної групи експертів вказує список спеціалістів, яких він вважає компетентними в даній області. Коефіцієнт компетентності експерта визначається як відношення числа списків,

в яких є даний експерт, до загального числа списків. Цей метод дозволяє отримати збільшені оцінки експертів.

Інший підхід виходить з того, що компетентність експерта треба оцінювати по тому, наскільки узгоджені його оцінки з оцінками більшості.

Достовірність оцінок групи експертів залежить від рівня знань окремих експертів і кількості експертів в групі.

У разі участі в опитуванні декількох експертів розбіжності в їхніх оцінках неминучі, однак величина цієї розбіжності має важливе значення. Групова оцінка може вважатися достатньо надійною тільки за умови гарної узгодженості відповідей окремих фахівців.

Для аналізу розкиду і узгодженості оцінок можуть застосовуватись статистичні характеристики – міри розкиду або статистична варіація [51].

3.5. Обгрунтування вдосконалення точності комплексної методики оцінки та порівняльного аналізу

Для покращення якості порівняння є доцільним враховувати особливості застосування порівнюваних алгоритмів після проведення оцінки. З цією метою розроблено вдосконалення етапу порівняння за прагматичними критеріями:

– Обирається набір варіантів застосування алгоритмів асиметричних криптоперетворень з урахуванням як національного так і міжнародного досвіду,

– Проводиться оцінювання важливості критеріїв, за якими відбувається порівняння криптоперетворень

– Проводиться корекція фінальної оцінки кожного алгоритму з виокремленям оцінок для всіх обраних варіантів застосування.

На Рисунку 3.4 наведено узагальнену структуру вдосконаленого застосування етапу оцінки та порівняння за прагматичними критеріями Методики з врахуванням особливостей різних варіантів застосування.

Рис. 3.4. Узагальнена структура вдосконаленого порівняння

3.6. Висновки до розділу 3

1. У даному розділі було обгрунтовано як поняття методики так і загальний вигляд комплексної методики оцінки та порівняння існуючих та перспективних (тих, що претендують на звання квантово-стійких) АСШ, ПІК та ЕП.

2. У даному розділі визначено, що під комплексною методикою аналізу криптографічної стійкості існуючих та перспективних (постквантових) криптографічних перетворень (в тому числі ЕП), у перехідний та постквантовий періоди, розуміється фіксована сукупність прийомів практичної діяльності щодо аналізу криптографічної стійкості та властивостей існуючих та перспективних (постквантових) криптографічних перетворень, у перехідний та постквантовий періоди.

3. У даному розділі обґрунтовано, що для коректного та універсального порівняння криптографічної стійкості та властивостей існуючих та перспективних (тих, що претендують на звання квантово-стійких) АСШ, ПІК та ЕП комплексна методика оцінки та порівняння має проходити у три етапи:

– використання безумовних критеріїв;

– використання умовних критеріїв;

– використання прагматичних критеріїв.

4. У процесі застосування комплексної методики в частині оцінки та порівняння за безумовними критеріями основними діями щодо оцінювання криптопримітивів, у відповідності до комплексної методики, є наступні:

– Визначаються часткові умовні та безумовні критерії і показники.

– Обираються експерти, згідно їх рівня компетенції у визначеній предметній області.

– Проводиться оцінка обраних криптопримітивів за частковими безумовними критеріями.

– На основі безумовного інтегрального критерію (за допомогою функції відповідності криптоперетворення) приймається рішення, на основі оцінки, яку отримано (позитивну чи негативну), про те, чи буде проводитись подальше порівняння та оцінювання на основі часткових умовних критеріїв та інтегрального умовного критерію.

5. У третьому розділі показано, що невід’ємною частиною комплексної методики є застосування методів експертних оцінок. Також обгрунтовано особливості застосування методів експертних оцінок.

6. У даному розділі було обґрунтувано та описано вибір критеріїв та показників оцінки та порівняння, зокрема часткових безумовних критеріїв оцінки та порівняння існуючих та персективних криптографічних перетворень. Зокрема цей вибір грунтується на врахуванні безпекових вимог (вимог до стійкості), досягнутих завдяки результатам практичного розв’язання задач

криптоаналізу, в тому числі на основі реалізації алгоритмів квантового криптоаналізу.

7. У даному розділі вдосконалено комплексну методику оцінки та порівняльного аналізу в частині оцінки та порівняння за прагматичними критеріями, що призодить до збільшення точності та відповідності отриманого результату вихідним вимогам.

РОЗДІЛ 4. АНАЛІЗ, ОЦІНКА ТА ПОРІВНЯННЯ ІСНУЮЧИХ ТА КАНДИДАТІВ НА ПЕРСПЕКТИВНІ КВАНТОВОСТІЙКІ НАЦІОНАЛЬНІ ТА МІЖНАРОДНІ ЕЛЕКТРОННІ ПІДПИСИ ЗА БЕЗУМОВНИМИ КРИТЕРІЯМИ

4.1. Аналіз кандидатів додаткового конкурсу на квантово-стійкий електронний підпис

В результаті проведення трьох раундів NIST PQC було обрано для стандартизації 4 кандидати (механізм інкапсуляції ключа CRYSTALS-Kyber та електронні підписи (ЕП) CRYSTALS-Dilithium, Falcon та SPHINCS+) та визначено кандидатів для проведення четвертого раунду (механізми інкапсуляції ключів BIKE, Classic McEliece, HQC та SIKE (котрий розробники визнали ненадійним)) [13, 14].

Через специфіку обраних алгоритмів NIST потребував додаткових кандидатів з числа ЕП загального призначення, котрі не були б засновані на використанні решіток. Через це було розпочато процес стандартизації додаткових ЕП для квантовостійкої криптографії. Серед поданих на розгляд до першого раунду цього процесу стандартизації можна виділити наступні види підписів [3,4]: підписи засновані на кодах, підписи на ізогеніях, мультиваріативні підписи, симетричні підписи, MPC-in-the-head та підписи визначені NIST як "інші".

Метою роботи є аналіз та порівняння кандидатів на квантовостійкий ЕП, що грунтуються на нових та перспективних квантовостійких проблемах, стійких до класичних та квантових атак та атак бічними каналами.

Конкурс NIST PQC було спрямовано на обрання пост-квантових кандидатів криптопримітивів для стандартизації. З часом, під час розгляду та відкритого коментування проектів стандартів, криптографічною спільнотою було прийнято замінити термін «пост-квантовий» на більш точний «квантовостійкий» [23]. Саме тому в цій роботі буде використовуватись саме термін «квантовостійкий».

В межах роботи розглядаються кандидати на квантовостійкий ЕП, що були представлені на процес стандартизації додаткових ЕП від NIST.

Особливий інтерес для порівняння представляють підписи котрі не були віднесені до жодної з груп та були об'єднані під назвою "інші підписи". Серед них наявні наступні варіанти ЕП [4]: ALTEQ, eMLE-Sig 2.0, KAZ-SIGN, Xifrat1-Sign.I, Preon.

В даній роботі розглянуто лише схеми ЕП ALTEQ, eMLE-Sig 2.0, KAZ-SIGN, Xifrat1-Sign.I.

Розглянемо схему ЕП **ALTEQ.**

Схема ЕП ALTEQ грунтується на складності проблеми рівності альтернованих трилінійних форм (ATFE), котра використовує групову дію загальної лінійної групи над скінченним полем.

Загальна структура ALTEQ полягає в наступному.

Спочатку за прикладом Голдеріх-Мікалі-Вігдерсон (GMW) розроблено протокол з нульовим розголошенням, що опирається на складність ATFE. Далі застосовується перетворення Фіат-Шаміра (FS) для усунення взаємодії від протоколу нульового розголошення, що приводить до схеми ЕП.

Протокол складається з двох частин [52]. Спочатку йде застосування протоколу GMW до рівності альтернованих трилінійних форм для отримання протоколу ідентифікації (або Сігма протоколу). Далі йде застосування перетворення Фіат-Шаміра до протоколу ідентифікації.

Базова структура GMW-FS. GMW-FS приймає групову дію і надає схему ЕП.

Групова дія, що лежить в основі ATFE [52]. Нехай G - скінченна група, S - скінченна множина, а $\alpha : G \times S \to S$ - групова дія. Припускається що елементи цих групи та множини ефективно представлені в алгоритмах, α може бути ефективно обчислено та елементи з G та S можуть бути ефективно відібрано випадковим чином.

Схема ALTEQ отримується шляхом інстанціювання групової дії $\alpha : G \times S \to S$ наступним чином.

Параметри для групової дії ATFE.

1. *n:* розмірність векторного простору.

2. *q:* порядок кінечного поля.

Визначення групової дії ATFE.

1. Група G є GL(n,q), загальна лінійна група над скінченним полем порядку q.

2. Набір S є набором альтернуючих трилінійних форм

ATF(n,q):=$\{\phi: \mathbb{F}_q^n \times \mathbb{F}_q^n \times \mathbb{F}_q^n \to \mathbb{F}_q\}$, де ϕ є трилінійним (лінійним в кожному аргументі) та альтернуючим (ϕ прирівнюється до 0 коли два аргументи ідентичні).

3. Дія α визначається наступним чином. Для $A \in$GL(n,q) та $\phi \in$ATF(n,q), $\phi \circ A$ становить альтернуючу трилінійну форму визначену $(\phi \circ A)(u,\upsilon,w) = \phi\left(A^t(u), A^t(\upsilon), A^t(w)\right)$.

Нотація. Для $n \in \mathbb{N}$, $[n] := \{1,2,...,n\}$. Нотація $\leftarrow_R$ позначає рівномірну випадкову вибірку; наприклад $g \leftarrow_R G$ позначає що g є рівномірною випадковою виборкою з G.

Параметри для базової структури GMW-FS.

1. $C = 2^c$: Число наборів елементів в якості відкритого ключа та число груп елементів в якості секретного ключа.

2. r: Число раундів схеми.

Генерація ключів.

1. $s_1 \leftarrow_R S$.

2. $g_1 := Id$, елемент ідентичності в групі G.

3. $g_2,...,g_C \leftarrow_R G$.

4. Для $i = 2,...,C, s_i := \alpha(g_i, s_1)$.

5. Відкритий ключ $(s_1,...,s_C) \in S^C$.

6. Секретний ключ $(g_1,...,g_C) \in G^C$.

Алгоритм генерації ключів ЕП ALTEQ [53] наведено на Рис. 4.1.

Input: The variable number $n \in \mathbb{N}$, a prime power q, the alternating trilinear form number $C+1$.
Output: Public key: $C+1$ alternating trilinear forms $\phi_i \in \mathrm{ATF}(n,q)$ such that $\phi_i \cong \phi_j$ for any $i,j \in \{0,\ldots,C\}$.
Private key: C matrices $A_0,\ldots,A_{C-1}$, such that $\phi_i \circ A_i = \phi_C$.

1 Randomly sample an alternating trilinear form $\phi_C : \mathbb{F}_q^n \times \mathbb{F}_q^n \times \mathbb{F}_q^n \to \mathbb{F}_q$.
2 Randomly sample C invertible matrices, $A_0,\ldots,A_{C-1} \in \mathrm{GL}(n,q)$.
3 For every $i \in \{0,\ldots,C-1\}$, $\phi_i \leftarrow \phi_C \circ A_i$.
4 For every $i \in \{0,\ldots,C-1\}$, $A_i \leftarrow A_i^{-1}$.
5 **return** *Public key:* $\phi_0,\phi_1,\phi_2,\ldots,\phi_C$. *Private Key:* $A_0,\ldots,A_{C-1}$.

Рис. 4.1. Алгоритм генерації ключів ЕП ALTEQ

Підпис. Нехай M - підписуване повідомлення. Нехай $H:\{0,1\}^* \to \{0,1\}^l$ - геш-функція, де $l = r \cdot c$.

1. *Для* $i \in [r]$, $h_i \leftarrow_R G$. *Нехай* $t_i := \alpha(h_i, s_1)$.
2. *Нехай* $L := H(M \mid t_1 \mid \ldots \mid t_r) \in \{0,1\}^l$.

   L розділяється на r c-бітних рядків, наприклад $L = b_1 \mid \ldots \mid b_r$, *де* $b_i \in \{0,1\}^c$.
3. *Для* $i \in [r]$, *нехай* $f_i := h_i \cdot g_{b_i}^{-1}$.
4. *Підпис* $(b_1,\ldots,b_r,f_1,\ldots,f_r)$.

Варто зауважити, що $\alpha(f_i s_{b_i}) = \alpha(h_i \cdot g_{b_i}^{-1}, s_{b_i}) = \alpha(h_i, \alpha(g_{b_i}^{-1}, s_{b_i})) = \alpha(h_i, s_1) = t_i$.

Алгоритм генерації підпису ЕП ALTEQ [53] наведено на Рис. 4.2.

Input: The public key $\phi_0,\ldots,\phi_C \in \mathrm{ATF}(n,q)$. The private key $A_0,\ldots,A_{C-1} \in \mathrm{GL}(n,q)$. r, C, $\lambda \in \mathbb{N}$. Let $A_C = I$, the identity matrix. The message M. A hash function $H:\{0,1\}^* \to \{0,1\}^{2\lambda}$. An expander $\mathsf{Expand}:\{0,1\}^{2\lambda} \to \{a_i\}_{i\in\{0,\ldots,r-1\}}$, where $a_i \in \{0,\ldots,C\}$.
Output: The signature S on M.

for $i \in \{0,\ldots,r-1\}$ **do**
  Randomly sample $B_i \in \mathrm{GL}(n,q)$.
  $\psi_i \leftarrow \phi_C \circ B_i$.
end
Compute $\mathsf{cha} = H(M|\psi_0|\ldots|\psi_{r-1}) \in \{0,1\}^{2\lambda}$.
$(b_0,\ldots,b_{r-1}) \leftarrow \mathsf{Expand}(\mathsf{cha})$
for $i \in \{0,\ldots,r-1\}$ **do**
  $D_i \leftarrow A_{b_i} B_i$; // Note that $\phi_{b_i} \circ D_i = \psi_i$.
end
return $S = (\mathsf{cha}, D_0,\ldots,D_{r-1})$.

Рис. 4.2. Алгоритм генерації підпису ЕП ALTEQ

Перевірка. Перевірювач отримує повідомлення M та підпис $(b_1,...,b_r,f_1,...,f_r)$

.

1. *Для* $i \in [r]$, *нехай* $t'_i := \alpha\left(f_i, s_{b_i}\right)$.
2. *Нехай* $L' := H\left(M \mid t'_1 \mid ... \mid t'_r\right)$.
3. *Прийняти якщо* L' *ідентично* $L = b_1 \mid ... \mid b_r$. *В іншому випадку відхилити.*

Алгоритм перевірки підпису ЕП ALTEQ [53] наведено на Рис. 4.3.

Input: The public key $\phi_0, \ldots, \phi_C \in \mathrm{ATF}(n,q)$. The signature $S = (\mathsf{cha}, D_0, \ldots, D_{r-1})$, $b_i \in \{0, \ldots, C\}$, $D_i \in \mathrm{GL}(n,q)$. The message M. A hash function $H : \{0,1\}^* \to \{0,1\}^{2\lambda}$. An expander $\mathsf{Expand} : \{0,1\}^{2\lambda} \to \{a_i\}_{i \in \{0,\ldots,r-1\}}$, where $a_i \in \{0, \ldots, C\}$.
Output: "Yes" if S is a valid signature for M. "No" otherwise.

for $i \in \{0, \ldots, r-1\}$ **do**
  Compute $\psi'_i = \phi_{b_i} \circ D_i$.
end
Compute $\mathsf{cha}' = H(M|\psi'_0| \ldots |\psi'_{r-1}) \in \{0,1\}^{2\lambda}$.
$(b'_0, \ldots, b'_{r-1}) \leftarrow \mathsf{Expand}(\mathsf{cha}')$
if *for every* $i \in \{0, \ldots, r-1\}$, $b_i = b'_i$ **then**
  return *Yes*
else
  return *No*

Рис. 4.3. Алгоритм перевірки підпису ЕП ALTEQ

Реалізація схеми ALTEQ включає декілька заходів для підвищення продуктивності системи.

У схемі впроваджено незбалансовані виклики. В протоколі ідентифікації GMW кількість викликів встановлюється на певне значення, так що відповідь складає випадкову матрицю, що розгортається з короткого seed, котрий призначений для передачі (таким чином досягається скорочення підпису). З іншого боку впровадження такого seed призводить до збільшення кількості раундів, а отже і збільшення часу підпису та перевірки.

Заявлено два варіанти підпису: Balanced з малим відкритим ключем та звичайним підписом та ShortSig з коротким підписом (розмір відкритого ключа значно більший).

Запропоновано набори параметрів для категорій безепеки NIST I та III, а також виділено орієнтовний набір параметрів для категорії безпеки NIST V. Загальносистемні параметри для схеми наведено в таблиці 4.1 [52].

Таблиця 4.1.

Загальносистемні параметри для схеми ЕП ALTEQ (біт)

Категорія безпеки NIST	Режим	Параметри (n, q, r, K, C)	Секретний ключ	Відкритий ключ	Підпис
I	Збалансований	$(13, 2^{32}-5, 84, 22, 7)$	128	64192	127168
	Короткий підпис	$(13, 2^{32}-5, 16, 14, 458)$	128	4191744	76224
III	Збалансований	$(20, 2^{32}-5, 201, 28, 7)$	192	255552	392000
	Короткий підпис	$(20, 2^{32}-5, 39, 20, 229)$	192	8354112	260032
V	Збалансований	$(25, 2^{32}-5, 119, 48, 8)$	256	589056	978688
	Короткий підпис	$(25, 2^{32}-5, 67, 25, 227)$	256	16707456	511264

В ході першого раунду конкурсу зі стандартизації додаткових схем ЕП було виявлено недоліки в схемі підпису ALTEQ, що призвело до розробки нової версії у відповідь на критику та наведені вектори та приклади атак.

Зокрема Маркку-Джухані О. Саарінен [54] було приведено приклад атаки на підробку підпису, що основується на зниженні складності підробки за умови, що частини підпису "seed_i" та "D_i" встановлено нулями, при тому що підпис складається з трьох частин cha, seed_i, D_i. Сама атака складається зі знаходження підходящого результуючого значення функції expandChallenge() в зменшеному просторі.

В результаті розробниками було додано перевірку зворотності матриць в процесі перевірки підпису та покращено швидкодію на ~2x для процедури перевірки для збалансованого варіанту та ~4x для варіанту з коротким підписом, що в поєднанні з незначним прискоренням процедури підпису та процедури генерації ключів в частини наборів параметрів не призвело до загального зниження швидкодії через додавання перевірки зворотності матриць.

Далі розглянемо **eMLE-Sig 2.0.**

eMLE-Sig 2.0 є схемою ЕП, що грунтується на новій, оптимізованій для практичного застосування, версії проблеми eMLE (англ. Embedded Multilayer Equations) та базується на алгебраїчних решітках. Заявлено покращення безпеки та ефективності нової eMLE у порівнянні зі звичайною. Особливу увагу автори звернули на атаку редукції решіток запропоновану Пенні Лоренц, котру було застосовано до попередньої версії схеми eMLE.

Сутність проблеми eMLE полягає в наступному [55]: Нехай d позначає кількість шарів в eMLE, а p - перелік з d цілих чисел, що виступають в якості модулів для кожного шару. Таким чином для нижнього шару модулем виступає $p[0]$, для верхнього $p[d-1]$. Всі числа в p - взаємно прості, а $p[i] < p[j]$ для $0 \le i < j < d$. Нехай n - ціле число, що визначає вимірність векторів.

Приклад нового запропонованого eMLE з трьома шарами (тобто $d = 3$), де відкритими є лише $h \in \mathbb{Z}^n_{p[2]}$ та $g_l \in \mathbb{Z}^n_{p[l]} \left(l \in \{0,1,2\} \right)$

$$h = g_2 \otimes x + h_1 \bmod p[2]$$
$$h_1 = \left(g_1 \otimes x + h_0 \bmod p[1] \right) + k_1 * p[1]$$
$$h_0 = \left(g_0 \otimes x \bmod p[0] \right) + k_0 * p[0]$$

Тут оператор $\otimes$ позначає результат згортки двох векторів.

Нотація [55, 56]:

- n: вимірність за замовчуванням для всіх векторів;
- d: кількість шарів в eMLE (в поданні на конкурс зафіксовано як 3);
- p: перелік з d цілих взаємно простих чисел, з $p[l]$ в якості модуля для шару l при $0 \le l \le d-1$;
- G: перелік з d векторів, з $G[l]$ використовується для побудування значення шару l;
- $x\_\max$: ціле число, що вказує на максимальні абсолютні значення елементів секретного вектору x;
- $c\_\max$: ціле число, що обмежує елементи у змагальному векторі, що використовується у підписанні та верифікації алгоритмів;

– vc: перелік, що складається з чотирьох цілих чисел, що використовується для перевірки розмірів значень при перевірці підпису;

– $\mathcal{H}$: геш-функція, накшталт SHA3-256.

Алгоритм генерації ключів ЕП eMLE-Sig 2.0 [56] наведено на Рис. 4.4.

input : $n, d, x\_max, c\_max, \mathbf{p}, \mathbf{G}$
output: $\mathbf{x}_1, \mathbf{x}_2, \mathbf{F}_1, \mathbf{F}_2, \mathbf{h}_1, \mathbf{h}_2, pkh$

while `true` **do**
  $\mathbf{x}_1 \leftarrow [-x\_max, x\_max]^n$
  $\mathbf{x}_2 \leftarrow [-x\_max, x\_max]^n$
  $sumX = \Sigma_{i=0}^{n-1}(\mathbf{x}_1[i] + \mathbf{x}_2[i]))$
  if $|sumX| < \frac{n}{2}$ **then**
    break
  end
end
while `true` **do**
  $\mathbf{h}_1, \mathbf{F}_1, sumR_1 = \texttt{eMLE}(n, d, c\_max, \mathbf{p}, \mathbf{G}, \mathbf{x}_1, \mathbf{G}[1], 0)$
  $\mathbf{h}_2, \mathbf{F}_2, sumR_2 = \texttt{eMLE}(n, d, c\_max, \mathbf{p}, \mathbf{G}, \mathbf{x}_2, \mathbf{G}[1], 0)$
  if $|sumR_1 + sumR_2| < n * n$ **then**
    break
  end
end
$pkh = \mathcal{H}(\mathbf{h}_1, \mathbf{h}_2)$
return $\mathbf{x}_1, \mathbf{x}_2, \mathbf{F}_1, \mathbf{F}_2, \mathbf{h}_1, \mathbf{h}_2, pkh$

Рис. 4.4. Алгоритм генерації ключів ЕП eMLE-Sig 2.0

Алгоритм генерації підпису ЕП eMLE-Sig 2.0 [56] наведено на Рис. 4.5.

input : $n, d, x\_max, c\_max, \mathbf{p}, \mathbf{G}, \mathbf{vc}, \mathbf{x}_1, \mathbf{x}_2, \mathbf{F}_1, \mathbf{F}_2, pkh, m, mlen$
output: $\mathbf{u}, \mathbf{s}$

Let $sumXn$ be the sum of negative integers in $\mathbf{x}_1$ and $\mathbf{x}_2$
Let $sumXp$ be the sum of positive integers in $\mathbf{x}_1$ and $\mathbf{x}_2$
$\mathbf{c}'_1, \mathbf{c}'_2 = \texttt{hashVec}(n, c\_max, m, mlen, \texttt{null}, pkh)$
while `true` **do**
  if $sumXp > |sumXn|$ **then**
    $y\_min \leftarrow [\lfloor \frac{|sumXn| * c\_max}{10} \rfloor, \lfloor \frac{|sumXn| * c\_max}{8} \rfloor]$
    $y\_gap \leftarrow [\lfloor \frac{sumXp * c\_max}{7} \rfloor, \lfloor \frac{sumXp * c\_max}{5} \rfloor]$
  else
    $y\_min \leftarrow [\lfloor \frac{|sumXn| * c\_max}{7} \rfloor, \lfloor \frac{|sumXn| * c\_max}{5} \rfloor]$
    $y\_gap \leftarrow [\lfloor \frac{sumXp * c\_max}{10} \rfloor, \lfloor \frac{sumXp * c\_max}{8} \rfloor]$
  end
  $\mathbf{y} \leftarrow [y\_min, \lfloor \frac{n * x\_max * c\_max}{2} \rfloor - y\_gap]^n$
  $\mathbf{u}, \mathbf{F}, \_ = \texttt{eMLE}(n, d, c\_max, \mathbf{p}, \mathbf{G}, \mathbf{y}, \mathbf{c}'_1 + \mathbf{c}'_2, 1)$
  $\mathbf{c}_1, \mathbf{c}_2 = \texttt{hashVec}(n, c\_max, m, mlen, \mathbf{u}, pkh)$
  $\mathbf{s} = \mathbf{x}_1 \otimes \mathbf{c}_1 + \mathbf{x}_2 \otimes \mathbf{c}_2 + \mathbf{y}$
  $v = \texttt{check}(n, d, x\_max, c\_max, \mathbf{p}, \mathbf{G}, \mathbf{vc}, \mathbf{F}_1, \mathbf{F}_2, \mathbf{F}, \mathbf{s}, \mathbf{c}_1, \mathbf{c}_2, \mathbf{c}'_1 + \mathbf{c}'_2)$
  if $v =$ `true` **then**
    break
  end
end
return $\mathbf{s}, \mathbf{u}$

Рис. 4.5. Алгоритм генерації підпису ЕП eMLE-Sig 2.0

Алгоритм перевірки підпису ЕП eMLE-Sig 2.0 [56] наведено на Рис. 4.6.

input : $n, d, x\_max, c\_max, \mathbf{p}, \mathbf{G}, \mathbf{vc}, \mathbf{h}_1, \mathbf{h}_2, \mathbf{s}, \mathbf{u}, m, mlen$
output: `true` or `false`

$pkh = \mathcal{H}(\mathbf{h}_1, \mathbf{h}_2)$
$\mathbf{c}'_1, \mathbf{c}'_2 = \texttt{hashVec}(n, c\_max, m, mlen, \texttt{null}, pkh)$
$\mathbf{c}_1, \mathbf{c}_2 = \texttt{hashVec}(n, c\_max, m, mlen, \mathbf{u}, pkh)$
$v = \texttt{checkS}(n, d, x\_max, c\_max, \mathbf{vc}, \mathbf{s})$
$\mathbf{t} = \mathbf{h}_1 \otimes \mathbf{c}_1 + \mathbf{h}_2 \otimes \mathbf{c}_2 + \mathbf{u} \bmod \mathbf{p}[d-1]$
for $l = d-1$ **to** 0 **do**
  if $l = 0$ **then**
    $\mathbf{g} = \mathbf{G}[1] \otimes (\mathbf{c}_1 + \mathbf{c}_2) \bmod \mathbf{p}[0]$
    $\mathbf{k} = \frac{\mathbf{t} - (\mathbf{G}[0] \otimes (\mathbf{s} + \mathbf{g} + \mathbf{c}'_1 + \mathbf{c}'_2) \bmod \mathbf{p}[0])}{\mathbf{p}[0]}$
    $a = \lfloor \frac{\sum_{i=0}^{n-1} \mathbf{k}[i]}{n} \rfloor$
    $\mathbf{k} = \mathbf{k} - \mathbf{1} * a$
    $v = v$ and $(\sum_{i=0}^{n-1} (\mathbf{k}[i] * \mathbf{k}[i]) \geq \mathbf{vc}[2])$ and $(\sum_{i=0}^{n-1} (\mathbf{k}[i] * \mathbf{k}[i]) \leq \mathbf{vc}[3])$
    $\mathbf{t} = \mathbf{t} - \mathbf{G}[l] \otimes (\mathbf{s} + \mathbf{g} + \mathbf{c}'_1 + \mathbf{c}'_2) \bmod \mathbf{p}[l]$
  else
    $\mathbf{t} = \mathbf{t} - \mathbf{G}[l] \otimes \mathbf{s} \bmod \mathbf{p}[l]$
  end
end
$v = v$ and $(\mathbf{t} = 0)$
return v

Рис. 4.6. Алгоритм перевірки підпису ЕП eMLE-Sig 2.0

Авторами заявлено, що ця версія eMLE у порівнянні зі старою версією має підвищені безпеку та ефективність за рахунок таких факторів [55]:

- Рандомізація внутрішніх шарів h_1 та h_0 за рахунок рандомізованих шумів k_1 та k_0. За рахунок використання в них більших рандомізованих цілих чисел очікуваний вектор рішень збільшується у просторі розв'язку.
- Використання згортки векторів в кожному шарі дозволяє збільшити розмірність векторів (збільшити n) без збільшення розмірів підпису.
- Секретний вектор x може бути зконфігурований таким чином, щоб в ньому були менші значення для зменшення розмірів підпису та підвищення стійкості.

Запропоновано набори загальносистемних параметрів для відповідних категорій безпеки NIST наведені в Таблиці 4.2 [56].

Таблиця 4.2.

Загальносистемні параметри для схеми ЕП eMLE-Sig 2.0 (біт)

Категорія безпеки NIST	n	d	x_max $/c\_max$	vc	p	G	Секретний ключ	Відкритий ключ	Підпис
I	64	3	4	vc64	[5,557, 67108864]	GG64	6400	3328	2240
III	96	3	4	vc96	[5,823, 268435456]	GG96	9600	5376	3648
V	128	3	4	vc128	[5,1097, 1073741824]	GG128	12800	7680	5120

В ході першого раунду конкурсу зі стандартизації додаткових схем ЕП було виявлено недоліки в схемі підпису eMLE-Sig 2.0, що призвело до доробки схеми підпису у відповідь на критику та наведені вектори та приклади атак. Незважаючи на це, було наведено приклади успішних атак на актуальну версію

підпису та визнано схему недостатньо захищеною від витоку секретного ключа в підписах. Тібоучі запропонував атаку на основі цього, а Лоренц реалізував програмне забезпечення для здійснення атаки [57].

Розглянемо ЕП **KAZ-SIGN**.

Kriptografi Atasi Zarah Digital Signature (KAZ-SIGN) грунтується на математичній проблемі 2-DLP (з англ. проблема дискретного логарифму другого порядку), котра ще потребує більш детального криптоаналізу для визначення потенційної стійкості як до класичного так і квантового криптоаналізу [58, 59]. Ідея полягає в складності відтворення DLP (проблеми дискретного логарифму) з відомого параметру для отримання секретного параметру. KAZ-SIGN спрямований на отримання квантової стійкості з короткими ключами та підписами та високою швидкістю виконання за умови використання простої математики для отримання потенційного кандидата для легкого переходу сучасного програмного та апаратного забезпечення.

Сутність проблеми 2-DLP можна пояснити наступним чином [58]: Нехай N - складене число, g - випадкове просте число з $\mathbb{Z}_N$ порядку G_g, де $G_g \approx N^\delta$ щонайбільше для $\delta \in (0,1)$ та $\delta \to 0$. Потрібно обрати випадкове просте число $Q \in \mathbb{Z}_{\phi(N)}$ порядку G_Q, де $G_Q \approx \phi(N)^\varepsilon$ для $\varepsilon \to 1$. Тобто, обрати Q великого порядку з $\mathbb{Z}_{\phi(N)}$. Таке Q має власний натуральний порядок із $\mathbb{Z}_{\phi(G_g)}$. Цей порядок буде позначено як G_{Qg}. Відношення може бути відображено як $Q^{G_{Qg}} \equiv 1 \left(\mathrm{mod}\, G_g\right)$ та $\phi(N) \equiv 0 \left(\mathrm{mod}\, G_g\right)$.

Після цього обирається випадкове ціле число $x \in \mathbb{Z}_{\phi(G_g)}$, де $x \approx \phi\left(G_g\right)$. З рівняння $g^{Q^x \left(\mathrm{mod}\, \phi(N)\right)} \equiv A \left(\mathrm{mod}\, N\right)$ проблему дискретного логарифму (DLP) вирішено за поліноміальний час на класичному комп'ютері та отримано значення X при відсутності еквівалентності $Q^x \equiv X \left(\mathrm{mod}\, \phi(N)\right)$ та при виконанні $g^X \equiv A \left(\mathrm{mod}\, N\right)$.

2-DLP полягає в тому, що при заданих значеннях (A, g, N, Q), потрібно визначити $x \in \phi(G_g)$ при $x \approx \phi(G_g)$ такому, що виконується $g^{Q^x (\mathrm{mod}\, \phi(N))} \equiv A (\mathrm{mod}\, N)$.

Алгоритм генерації ключів ЕП KAZ-SIGN [59] наведено на Рис. 4.7.

Input: System parameters $(g, n, n_{\phi(G_g)}, N, \phi(N), \phi(\phi(N)), R, G_g)$
Output: Public verification key, V, and private signing key, α

1: Choose random $\alpha \in (2^{n_{\phi(G_g)}-2}, 2^{n_{\phi(G_g)}-1})$.
2: Compute verification key, $V \equiv g^{R^\alpha \pmod{\phi(N)}} \pmod{N}$.
3: Compute the discrete logarithm $v = \mathrm{DLog}_g(V \pmod{N})$.
4: Compute $z_1 = v - R^\alpha \pmod{\phi(N)}$.
5: **if** $z_1 \equiv 0 \pmod{\phi(N)}$ **then**
6: repeat steps 1 till 4.
7: **else** continue step 9
8: **end if**
9: Compute the discrete logarithm $z_2 = \mathrm{DLog}_R(v \pmod{\phi(N)})$.
10: **if** z_2 has a solution **then**
11: repeat steps 1 till 9.
12: **else** continue step 14
13: **end if**
14: Output public verification key V and private signing key α.

Рис. 4.7. Алгоритм генерації ключів ЕП KAZ-SIGN

Алгоритм генерації підпису ЕП KAZ-SIGN [59] наведено на Рис. 4.8.

Input: System parameters $(g, n, n_{\phi(G_g)}, N, \phi(N), \phi(\phi(N)), R, G_g)$, private signing key, α, and message to be signed, $m \in \mathbb{Z}_N$
Output: Signatures, (S_1, S_2), salt, σ.

1: Generate a random salt, $\sigma \in \{0,1\}^{32}$ corresponding to message, m.
2: Compute the hash value of the message, $h = H(m \| \sigma)$.
3: Choose random ephemeral prime $r \in (2^{n_{\phi(G_g)}-2}, 2^{n_{\phi(G_g)}-1})$.
4: Compute $S_0 \equiv g^{R^r \pmod{\phi(N)}} \pmod{N}$.
5: Compute the discrete logarithm $S_1 = \mathrm{DLog}_g(S_0 \pmod{N})$.
6: Compute $z_3 = S_1 - R^r \equiv 0 \pmod{\phi(N)}$.
7: **if** $z_3 = S_1 - R^r \equiv 0 \pmod{\phi(N)}$ **then**
8: Repeat steps 3 till 6.
9: **else** Continue step 11
10: **end if**
11: Compute the discrete logarithm $z_4 = \mathrm{DLog}_R(S_1 \pmod{\phi(N)})$.
12: **if** z_4 has a solution **then**
13: Repeat steps 3 till 11.
14: **else** Continue step 16
15: **end if**
16: Compute $S_2 \equiv (\alpha + h) r^{-1} \pmod{\phi(\phi(N))}$.
17: Compute the discrete logarithm $v = \mathrm{DLog}_g(V \pmod{N})$.
18: Compute the discrete logarithm $S_{2f} = \mathrm{DLog}_{S_1}(vR^h \pmod{\phi(N)})$.
19: **if** $S_2 \equiv S_{2f} \pmod{\phi(\phi(N))}$ **then**
20: Repeat steps 3 till 18
21: **else** Continue step 23.
22: **end if**
23: Compute $\alpha_F = \mathrm{DLog}_R(v \pmod{G_g})$.
24: Compute $W_0 \equiv (\alpha_F + h) S_2^{-1} \pmod{\phi(\phi(N))}$.
25: **if** W_0 does not exist **then**
26: Repeat steps 1 till 24.
27: **else** Continue 29.
28: **end if**
29: Compute $w_1 \equiv g^{S_1} \pmod{N}$.
30: Compute $w_2 \equiv g^{R^{W_0} \pmod{\phi(N)}} \pmod{N}$.
31: **if** $w_1 = w_2$ **then**
32: Repeat steps 1 till 30.
33: **else** Continue 35.
34: **end if**
35: Output signature (S_1, S_2), salt, σ and destroy r.

Рис. 4.8. Алгоритм генерації підпису ЕП KAZ-SIGN

Кроки 17, 18, 19 та 20 процедури підписання утворюють процедуру виявлення підробки ЕП KAZ-SIGN type-1.

Кроки 23, 24, 25, 26, 27, 28, 29, 30, 31 та 32 становлять процедуру виявлення придатності параметрів KAZ-SIGN.

Алгоритм перевірки підпису ЕП KAZ-SIGN [59] наведено на Рис. 4.9.

Input: System parameters $(g, n, n_{\phi(G_g)}, N, \phi(N), \phi(\phi(N)), R, G_g)$, public verification key, V, message, m, signatures, (S_1, S_2) and salt corresponding to M, σ.
Output: Accept or reject

1: Compute the hash value of the message and its corresponding salt, σ to be verified, $h = H(m\|\sigma)$.
2: Compute the discrete logarithm $v = \mathrm{DLog}_g(V \pmod N)$.
3: Compute the discrete logarithm $S_{2f} = \mathrm{DLog}_{S_1}(vR^h \pmod{\phi(N)})$.
4: **if** $S_2 \equiv S_{2f} \pmod{\phi(\phi(N))}$ **then**
5: reject signature $\perp$
6: **else** continue step 9
7: **end if**
8: Compute $\alpha_F = \mathrm{DLog}_R(v \pmod{G_g})$.
9: Compute $W_0 \equiv (\alpha_F + h)S_2^{-1} \pmod{\phi(\phi(N))}$.
10: Compute $w_1 \equiv g^{S_1} \pmod N$.
11: Compute $w_2 \equiv g^{R^{W_0 \pmod{\phi(N)}}} \pmod N$.
12: **if** $w_1 = w_2$ **then**
13: reject signature $\perp$
14: **else** continue step 16
15: **end if**
16: Compute $y_1 \equiv g^{S_1^{S_2 \pmod{\phi(N)}}} \pmod N$.
17: Compute $y_2 \equiv v^{R^{h \pmod{\phi(N)}}} \pmod N$.
18: **if** $y_1 = y_2$ **then**
19: accept signature
20: **else** reject signature $\perp$
21: **end if**

Рис. 4.9. Алгоритм перевірки підпису ЕП KAZ-SIGN

Кроки 2, 3, 4 та 5 в процедурі перевірки утворюють процедуру виявлення підробки ЕП KAZ-SIGN type-1.

Кроки 8, 9, 10, 11, 12 та 13 утворюють процедуру виявлення підробки ЕП KAZ-SIGN type-2.

Складність вирішення 2-DLP може бути описана наступним чином [59]: Нехай $n_{\phi(G_g)} = \ell\left(\phi\left(G_g\right)\right)$. Складність отримання x становить $O\left(2^{n_{\phi(G_g)}}\right)$. За умови застосування алгоритму Гровера на квантовому комп'ютері, складність отримання x становить $O\left(2^{\frac{n_{\phi(G_g)}}{2}}\right)$. Іншими словами, так як $\phi\left(G_g\right) \approx G_g \approx N^{\delta}$,

складність отримання x становить $O\left(N^{\delta}\right)$. За умови застосування алгоритму Гровера на квантовому комп'ютері, складність отримання x становить $O\left(N^{\frac{\delta}{2}}\right)$.

Запропоновані авторами набори загальносистемних параметрів для відповідних категорій безпеки NIST [58] наведені в Таблиці 4.3.

Таблиця 4.3.

Загальносистемні параметри для схеми ЕП KAZ-SIGN (біт)

Категорія безпеки NIST	Число простих множників в P, j	Рівень безпеки, k	Довжина параметра N	Розмір ключа, (V, N)	Розмір підпису (S_1, S_2)	Розмір ключа ЕК
I	68	128	458	916	590	256
III	100	192	738	1476	930	384
V	125	256	970	1940	1220	521

В ході першого раунду конкурсу зі стандартизації додаткових схем ЕП було виявлено недоліки в схемі підпису KAZ-SIGN, що призвело до розробки чотирьох оновлень схеми підпису у відповідь на критику та наведені вектори та приклади атак (зокрема Бернштейном [60]). Незважаючи на це, було наведено приклади успішних атак з підробки підпису на актуальну версію підпису. Атака створює підпис для будь-якого бажаного повідомлення з будь-яким відкритим ключем і перевіряє, чи підпис проходить перевірку за допомогою еталонної реалізації. Стверджується, що атака працює для всіх 100 KAT у каталогах kaz1509, kaz2321 і kaz3241.

Xifrat1-Sign.I є схемою ЕП, що входить до сімейства криптоалгоритмів що грунтуються на використанні випадково згенерованих абелевих квазігруп з 16 елементів та передбачає створення трьох шарів абелевих квазігруп зі зростаючим розміром. В рамках Xifrat1-Sign.I передбачається використання геш-функції з безпекою 256 біт та виводом 768 біт, дві половини якого оброблюються Dup-функцією.

Також автори заявляють про подвоєння безпеки проти атак "грубої сили" проти Dup-функції з 192 біт до 384 біт.

Авторами Xifrat1-Sign.I передбачається лише категорія безпеки NIST III [61].

У схемі підпису використовується геш-функція, створена на основі XOF SHAKE-256. Її початкові вихідні дані у розмірі 768 біт інтерпретуються як 12 64-бітних непідписаних цілих чисел малого порядку. Ця геш-функція позначається як $Hx_{768}(m)$.

Алгоритм генерації ключів ЕП Xifrat1-Sign.I [62] зводиться до наступного:

1. Рівномірно випадково згенерувати 3 криптограми: c, k та q.
2. Обчислити $p_1 = D(c,k)$, $p_2 = D(k,q)$,
3. Повернути відкритий ключ $pk = (c, p_1, p_2)$ та секретний ключ $sk = (c,k,q)$.

Алгоритм генерації підпису ЕП Xifrat1-Sign.I [62] зводиться до наступного:

1. Вхідні дані: m – повідомлення
2. Обчислити $h = Hx_{768}(m)$,
3. Обчислити $s = D(h,q)$,
4. Повернути s.

Алгоритм перевірки підпису ЕП Xifrat1-Sign.I [62] зводиться до наступного:

1. Вхідні дані: m – повідомлення, S – підпис
2. Обчислити $h = Hx_{768}(m)$,
3. Обчислити $t_1 = D(p_1, s)$,
4. Обчислити $t_2 = D(D(c,h), p_2)$,
5. Якщо $t_1 = t_2$ повернути [VALID]; у іншому випадку повернути [INVALID].

Доказом коректності схеми полягає в наступному:

$t_1 = D(p_1, s) = D(D(c,k), D(h,q))$

$t_2 = D\left(D(c,h), p_2\right) = D\left(D(c,h), D(k,q)\right)$

За обмеженою комутативністю $t_1 = t_2$.

Запропоновані набори загальносистемних параметрів для категорії безпеки NIST III [61] наведені в Таблиці 4.4.

Таблиця 4.4.

Загальносистемні параметри для схеми ЕП Xifrat1-Sign.I (біт)

Параметри	Особистий ключ	Відкритий ключ	Підпис
Xifrat1-Sign.1	3840	2304	768
Варіант з обмеженою безпекою	2560	1536	512

В ході першого раунду конкурсу зі стандартизації додаткових схем ЕП було виявлено недоліки в схемі підпису Xifrat1-Sign.I. Пенні Лоренц в офіційних коментарях [63] наведено приклад атаки, котра розраховує секретний ключ з відкритого. Заявлено, що виконання атаки займає 4 хвилини на комп'ютері з 24 ядрами. Атака заснована на тому, що множення квазігруп x*y переписується як C + Ax + By, де + позначає абелеву групу, а A та B є комутативними автоморфізмами. У зв'язку з тим, що всі використані функції змішування є афінно-лінійними картами щодо +, система, що пов'язує секретний та відкритий ключі є лінійною і може бути зведена до лінійної алгебри. Через це використана група є ізоморфною до $\mathbb{F}_2^4$, що полегшує реалізацію атаки, котра також є актуальною і для загального випадку.

На жаль, жодного рішення для цієї атаки з боку розробників не було надано.

4.2. Порівняння кандидатів додаткового конкурсу на квантово-стійкий електронний підпис

Порівняння підписів можливе за певними параметрами або критеріями. В даному випадку будемо використовувати деякі із безумовних критеріїв.

До безумовних критеріїв [5] відносяться ті критерії, виконання яких для криптопримітиву є обов'язковим, тобто безумовним. Для асиметричних криптоперетворень типу АСШ, ПІК та ЕП цілком можна вибрати однакову систему безумовних критеріїв.

Як вже було наведено в Розділі 3, до переліку безумовних критеріїв можна віднести наступні:

1) $I_{ст.}$ – рівень криптографічної стійкості з використанням безумовних критеріїв;

2) $l_{в.к.}$ – можливі довжини відкритого ключа;

3) $l_{о.к.}$ – можливі довжини особистого (секретного) ключа;

4) $l_{рез.}$ – довжина результату криптоперетворення (збитковість);

5) $T_{пр.}$ – складність (швидкість) прямого криптоперетворення;

6) $T_{зв.}$ – складність (швидкість) зворотного криптоперетворення;

7) $T_{ген.зп.}$ – складність (швидкість) генерування загальних параметрів для відповідного режиму роботи криптоперетворення (у залежності від довжин загальних параметрів та ключів);

8) $T_{ген.кл.}$ – складність (швидкість) генерування ключа (ключової пари) у залежності від режиму роботи тощо.

В даному контексті із наведеного переліку розглядаються наступні безумовні критерії:

- можливі довжини відкритого ключа;
- можливі довжини особистого (секретного) ключа;
- довжина результату криптоперетворення (збитковість);

Порівняння цих параметрів для наведених схем ЕП наведено у Таблиці 4.5 та на Рисунку 4.10 [5].

Таблиця 4.5.

Розміри підпису та ключів (біт)

	ALTEQ (збалансований)			eMLE-Sig 2.0			KAZ-SIGN			Xifrat 1-Sign.1
	I	III	V	I	III	V	I	III	V	III
Особистий ключ	128	192	256	6400	9600	12800	256	384	521	3840
Відкритий ключ	64192	255552	589056	3328	5376	7680	916	1476	1940	2304
Підпис	127168	392000	978688	2240	3648	5120	590	930	1220	768

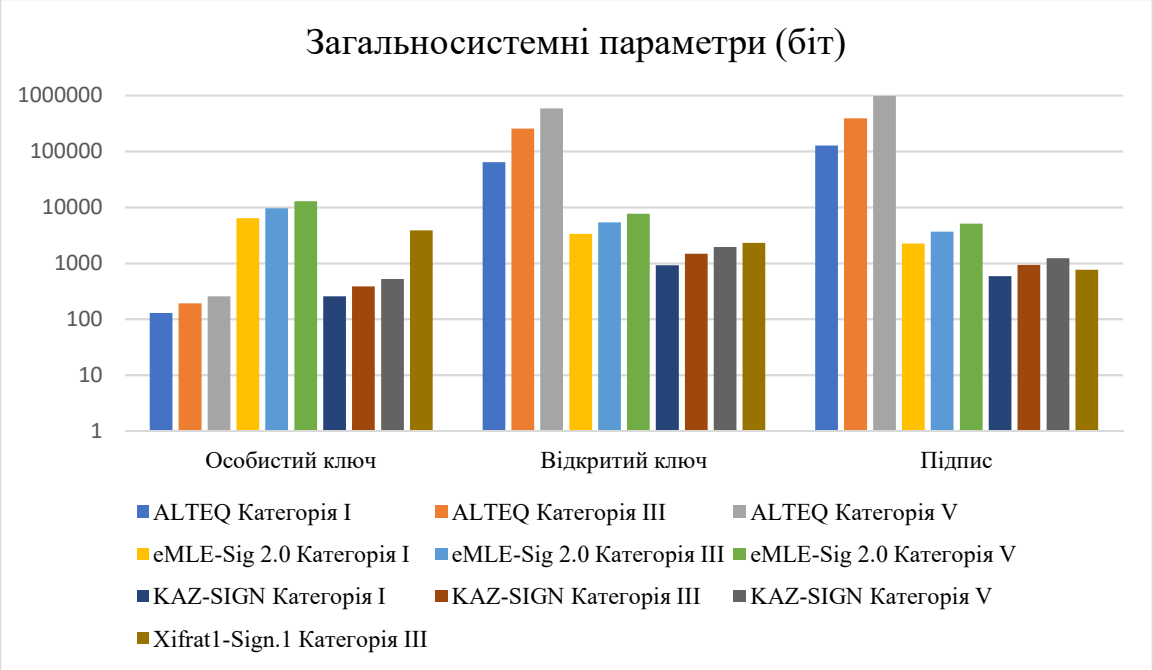

Рис. 4.10. Розміри загальносистемних параметрів наведених алгоритмів ЕП

З Таблиці 4.5 та Рисунку 4.10 видно, на що робився більший наголос при розробці схем ЕП. Так, наприклад ALTEQ явно зосереджено на зведенні до мінімуму розміру особистого ключа, хоча це і призвело до неймовірного збільшення розмірів відкритого ключа та підпису. eMLE-Sig 2.0 та Xifrat1-Sign.1 зводять до мінімуму розмір підпису. KAZ-SIGN має розміри особистого

ключа близькі до розмірів особистого ключа ALTEQ, але розміри відкритого ключа та підписа найменші з усіх порівнюваних.

Таким чином можна побачити, що наведені схеми можуть використовуватись в різних ситуаціях. Так, наприклад, якщо дуже важливий розмір особистого ключа, але взагалі не важливі розміри відкритого ключа та підпису – цілком доцільним є використання ALTEQ. Якщо, навпаки, неважливий розмір особистого ключа, але важливі інші параметри – краще обрати іншу схему. Якщо дуже важливо звести всі розміри до мінімуму – кращим з наведених варіантів буде KAZ-SIGN.

Важливо зазначити, що таке порівняння за частиною критеріїв не є повним та не враховує затрат швидкодії та захищеність схем ЕП від конкретних атак.

Якщо розширити фокус, то можна побачити, що до кожної з наведених схем підпису було знайдено вектори атак. Додатково вартим уваги є те, що атаки бічними каналами на схеми підпису зазвичай обходять увагою, а навіть якщо на них звертають увагу, то здебільшого в контексті того, що схема підпису або цілком від них незахищена, або захищена тільки від окремих векторів атак бічними каналами, в той час як захищеність від решти навіть не розглядалась.

Також було виявлено зосередженість різних схем ЕП на зменшенні розміру різних параметрів, що призводить до переваг для різних застосувань цих схем. Таким чином виконується одна із основних задач додаткового раунду відбору, а саме урізноманітнення набору ЕП для стандартизації.

Окрім підписів, що можуть бути віднесені до категорій: підписи засновані на кодах, підписи на ізогеніях, мультиваріативні підписи, симетричні підписи, MPC-in-the-head; кандидати що визначені NIST як "інші" представляють можливі підходи до квантовостійкої стійкості за рахунок використання нових, покращених та перспективних підходів та надають набори параметрів, що задовольняють вимоги NIST за різними категоріями безпеки NIST за умови використання криптографічно адекватних системних параметрів.

4.3. Порівняння перспективних механізмів ЕП

За безумовними критеріями було проведено порівняння, в котрому відбувалось порівняння алгоритмів таких проектів стандартів як «Вершина», «Сокіл» та алгоритм Dilithium, котрий мав одні з кращих результатів за попередніми дослідженнями серед квантовостійких алгоритмів ЕП, зокрема серед тих, що засновані на перетвореннях на алгебраїчних решітках.

Також варто пояснити параметр рівня стійкості в табл 4.6 [5]. У зв'язку з тим, що стійкість алгоритму «Вершини» 128 біт відповідає 3-му рівню стійкості NIST, а стійкість алгоритму «Вершини» 256 – 5-му рівню стійкості NIST, то завдяки пропорційному проеціюванню для виконання порівняння алгоритму «Вершини» 384 був наданий 7-й рівень стійкості NIST, а алгоритму «Вершини» 512 – 9-й рівень стійкості NIST.

Результати досліджень та порівнянь, такі як відносна перевага алгоритмів ЕП, що отримана за допомогою методу попарних порівнянь за кожною з характеристик наведено у табл. 4.7 Також загальна відносна перевага алгоритмів наведена на Рис. 4.11. Слід зауважити, що на Рис.4.11 враховано вагові коефіцієнти критеріїв.

Таблиця 4.6.

Характеристики алгоритмів ЕП, що засновані на перетвореннях на алгебраїчних решітках

Алгоритми	$I_{ст.}$	$l_{в.к.}$	$l_{о.к.}$	$l_{рез.}$	$T_{пр.}$	$T_{зв.}$	$T_{гк.}$
Dilithium_round3_sec2	2	1 312	3 504	2 420	259 172	118 412	124 031
Dilithium_round3_sec3	3	1 952	3 856	3 293	428 587	179 424	256 403
Dilithium_round3_sec5	5	2 592	5 792	4595	538 986	279 936	298 050
Вершина_128	3	1 472	3 488	2 693	133 340	109 818	90 328
Вершина_256	5	2 624	5 792	5 345	259 103	233 712	229 669
Вершина_384	7	4 528	9 088	6762	411 040	398 029	317 324
Вершина_512	9	5 824	11 008	10708	643 744	620 989	485 471

Продовження Таблиці 4.6.

Алгоритми	$I_{ст.}$	$l_{в.к.}$	$l_{о.к.}$	$l_{рез.}$	$T_{пр.}$	$T_{зв.}$	$T_{гк.}$
Сокіл_128	3	897	4097	666	655 672	139 620	33 696 000
Сокіл_256	5	1 793	8193	1 280	1 338 825	285 714	107 055 000
Сокіл_512	9	3 585	5121	2 515	2 600 053	265 416	28 493 603 229

Таблиця 4.7.

Відносна перевага алгоритмів ЕП за кожною з характеристик

Алгоритми	$I_{ст.}$	$l_{в.к.}$	$l_{о.к.}$	$l_{рез.}$	$T_{пр.}$	$T_{зв.}$	$T_{гк.}$
Dilithium_round3_sec2	0,0198	0,1770	0,1816	0,1131	0,1583	0,1857	0,2090
Dilithium_round3_sec3	0,0299	0,0965	0,1475	0,0606	0,0849	0,0984	0,1082
Dilithium_round3_sec5	0,0697	0,0655	0,0768	0,0507	0,0666	0,0506	0,0915
Вершина_128	0,0299	0,1395	0,1816	0,0800	0,3006	0,2195	0,2696
Вершина_256	0,0697	0,0655	0,0768	0,0339	0,1583	0,0716	0,1388
Вершина_384	0,1453	0,0327	0,0407	0,0261	0,0975	0,0348	0,0797
Вершина_512	0,2681	0,0233	0,0296	0,0173	0,0479	0,0218	0,0608
Сокіл_128	0,0299	0,2487	0,1212	0,3211	0,0479	0,1466	0,0192
Сокіл _256	0,0697	0,1108	0,0467	0,1989	0,0238	0,1130	0,0146
Сокіл _512	0,2681	0,0406	0,0973	0,0984	0,0143	0,0581	0,0086

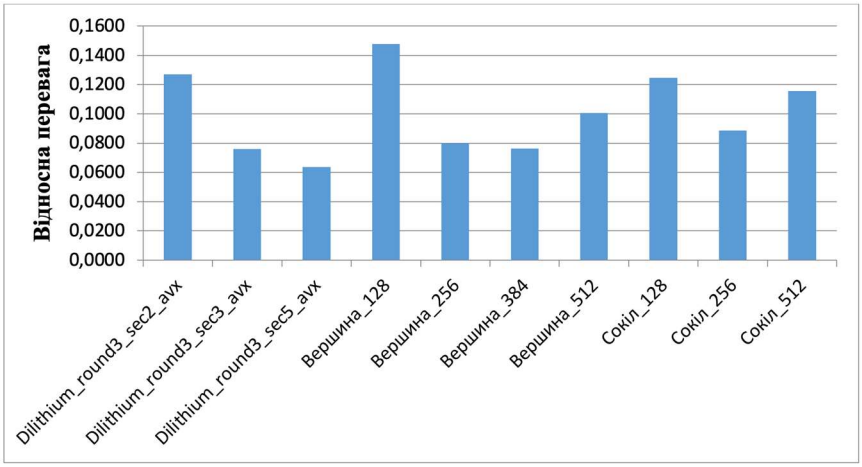

Рис. 4.11. Переваги алгоритмів ЕП

Як видно з наведених результатів, найбільшу перевагу серед алгоритмів отримує алгоритм «Вершина» з параметрами стійкості 128 біт.

Далі до кінцевого порівняння було залучено алгоритми, котрі змогли продемонструвати одні з кращих результатів на попередньому етапі – SPHINCS+_s, «Вершина» та «Сокіл» (завдяки тому, що на різних рівнях стійкості перевагу отримували різні алгоритми), а також Rainbow (для порівняння була обрана оптимізована реалізація з використанням стандартних параметрів з метою отримання якомога кращої конкурентності [18]).

Результати досліджень, що були отримані за допомогою використання методу попарних порівнянь за кожною з виділених характеристик, наведені у вигляді відносної переваги алгоритмів ЕП у табл. 4.8 [5].

На Рис. 4.12 та 4.13 відображено гістограми, що зображують загальну відносну перевагу алгоритмів ЕП, в значеннях яких вже було враховано вагові коефіцієнти характеристик.

Таблиця 4.8.

Відносна перевага алгоритмів ЕП за кожною з характеристик

Алгоритми	$I_{ст.}$	$l_{в.к.}$	$l_{о.к.}$	$l_{рез.}$	$T_{пр.}$	$T_{зв.}$	$T_{гк.}$
SPHINCS+_128s	0,0155	0,2658	0,2675	0,0189	0,0090	0,0117	0,0164
SPHINCS+_192s	0,0331	0,2289	0,2304	0,0107	0,0090	0,0102	0,0139
SPHINCS+_256s	0,0794	0,1953	0,1984	0,0082	0,0090	0,0079	0,0101
Вершина_128	0,0331	0,0599	0,0664	0,0385	0,2036	0,1525	0,2908
Вершина_256	0,0794	0,0416	0,0433	0,0240	0,1340	0,0713	0,2232
Вершина_512	0,2596	0,0279	0,0274	0,0142	0,0619	0,0305	0,1712
RAINBOW_I_round3_avx	0,0155	0,0117	0,0120	0,2924	0,2864	0,2913	0,0960
RAINBOW_III_round3_avx	0,0331	0,0082	0,0082	0,2043	0,1148	0,1229	0,0500
RAINBOW_VI_round3_avx	0,0794	0,0064	0,0064	0,1746	0,0494	0,0438	0,0263
Сокіл_128	0,0331	0,0770	0,0578	0,1007	0,0619	0,1095	0,0622
Сокіл_256	0,0794	0,0495	0,0337	0,0683	0,0363	0,0898	0,0341
Сокіл_512	0,2596	0,0279	0,0486	0,0451	0,0247	0,0586	0,0057

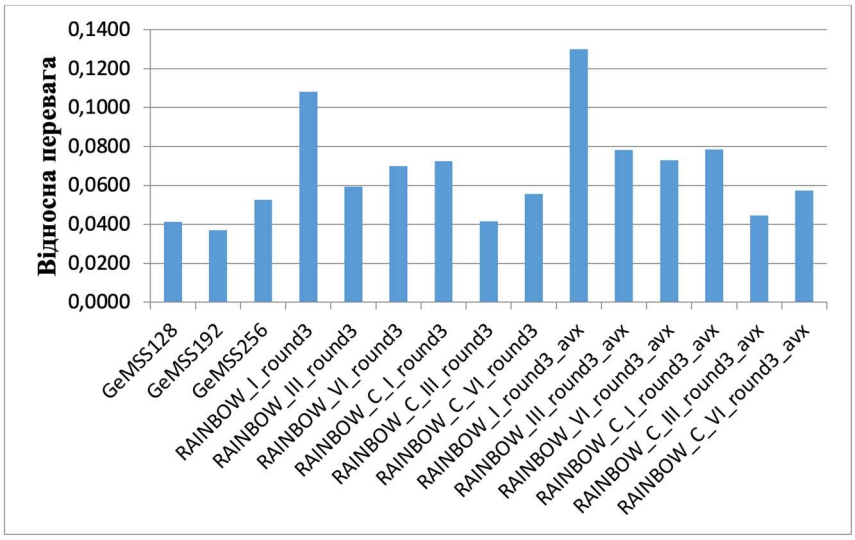

Рис. 4.12. Переваги алгоритмів ЕП

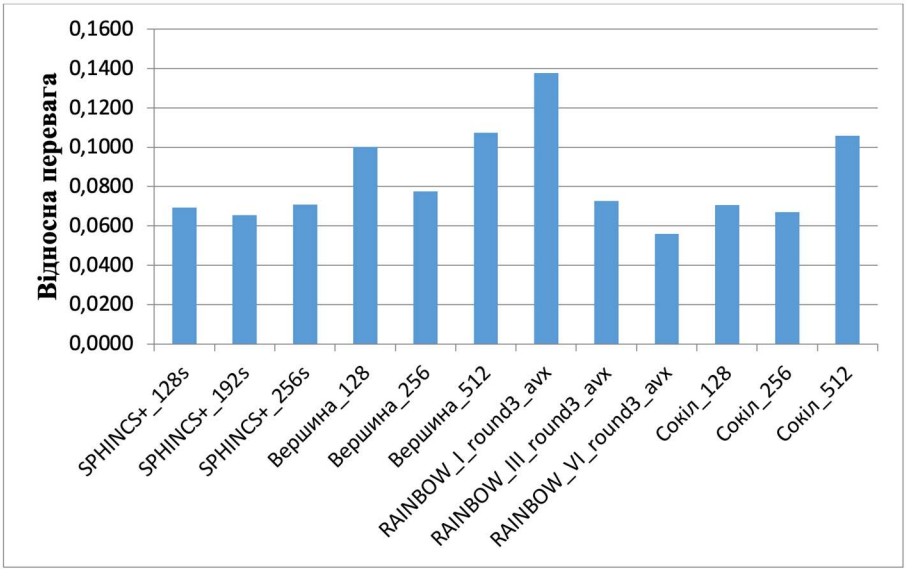

Рис. 4.13. Переваги алгоритмів ЕП

Серед усіх наведених в цьому порівнянні алгоритмів найкращий результат отримано RAINBOW_I_round3_avx. Так відбулось через те, що він має невелику довжину підпису та значну швидкодію. Проте також слід зауважити, що за умови використання параметрів, котрі гарантують підвищену стійкість, цей алгоритм втрачає позиції та опиняється на останньому місці.

За умови використання всіх можливих параметрів у порівнянні алгоритмів на перше місце виходить «Вершина» (що при порівнянні з іншими

алгоритмами, котрі базуються на використанні інших математичних апаратів за загальною сукупністю оцінок обходить «Сокіл»).

Таким чином можна зробити висновки щодо того, що за умови що потрібен лише мінімальний рівень захисту із порівнюваних, то найкращі результати отримує Rainbow. За умови ж, коли потрібен більш універсальний алгоритм, кращим варіантом буде «Вершина», для котрого не було представлено параметрів на рівні безпеки NIST 1 та 2, наявність котрих могла б змінити результат.

Також було проведено додаткове порівняння за методом ранжування, при якому варіанти реалізації порівнюваних алгоритмів було розбито за параметрами на 2 групи рівнів захисту: група параметрів середнього (3-4 рівні) та високого.

На Рис. 4.14 відображено гістограму загальної відносної переваги алгоритмів ЕП (з параметрами високого рівня захисту) з урахуванням вагових коефіцієнтів характеристик з використанням методу ранжування.

За результатами порівняння методом ранжування кращі оцінки отримали алгоритми, котрі базуються на перетвореннях в решеті числового поля.

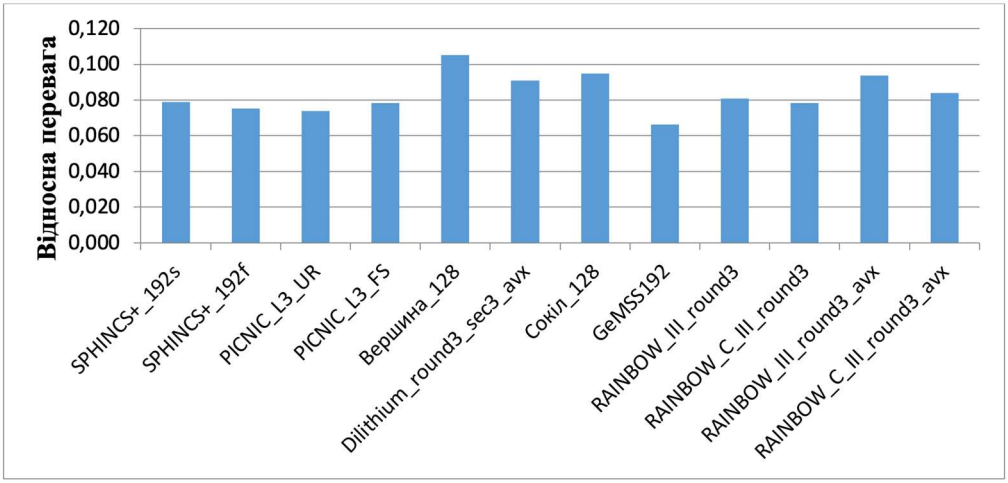

Рис. 4.14. Переваги алгоритмів ЕП середнього рівня захисту коефіцієнтів характеристик з використанням методу ранжування

4.4. Порівняння отриманих результатів з міжнародними оцінками перспективних механізмів ЕП

Як вже було вказано, міжнародна спільнота також зацікавлена в отриманні оцінок та порівнянні асиметричних криптографічних перетворень і саме для цього з боку NIST було розпочато конкурс NIST PQC. У звіті про стан третього раунду NIST PQC [2] було наведено результати порівнянь обраних в якості фіналістів на другому раунді схем підпису загального призначення Dilithium і Falcon. Третій фіналіст, Rainbow, не зважаючи на привабливий профіль продуктивності для додатків, що вимагають малих підписів або швидкої перевірки, зазнав втрат безпеки, через що у звіті з третього раунду показники ефективності Rainbow не розглядались. На Рисунку 4.15 навелено показники обчислювальної продуктивності з [64] для процесора x86-64 з розширеннями AVX2 для Dilithium і Falcon, що були розглянуті у звіті NIST. На Рисунку 4.16 показано «загальні витрати» для Dilithium і Falcon з доданою вартістю передачі відкритого ключа та підпису (використовується оціночна вартість 2000 циклів/байт). При використанні процесора x86-64 генерація підпису Dilithium відбувається трохи швидше, ніж Falcon. Однак загальна вартість Falcon нижча через його менший відкритий ключ і розмір підпису. За висновками NIST, для більшості програм, які використовують процесор x86-64 або подібний, показники продуктивності для Dilithium або Falcon мають бути прийнятними. Однак, на відміну від Falcon, підписи Dilithium не можуть поміститися в один інтернет-пакет, тому це може ускладнити адаптацію деяких програм для використання Dilithium, ніж їх адаптацію для використання Falcon.

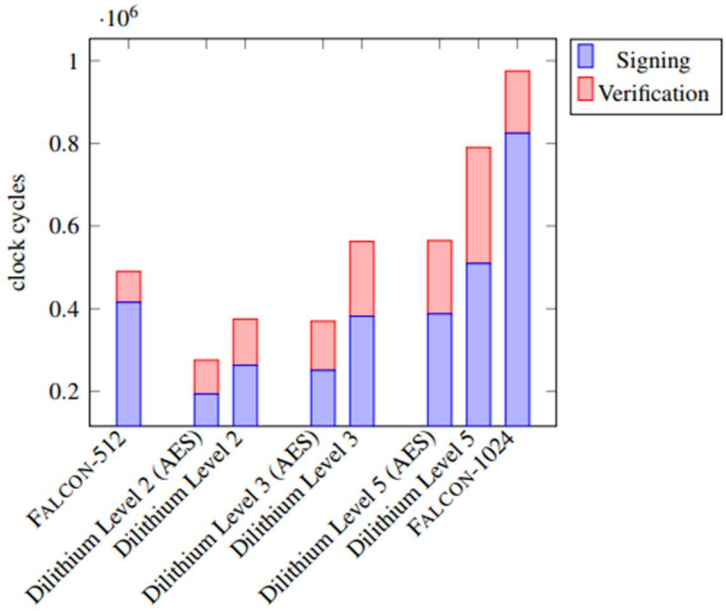

Рис. 4.15. Сигнатурні тести на процесорі x86-64 із розширеннями AVX2

На малюнку 4.17 показано показники обчислювальної продуктивності з [65] для процесора ARM CortexM4 наборів параметрів Dilithium і Falcon для категорій безпеки 1, 2 і 3. На рисунку 4.18 показані «загальні витрати» з додаванням приблизної вартості передачі 2000 циклів/байт. Як продемонстровано у звіті [2], через те, що ARM Cortex-M4 не підтримує операції з плаваючою точкою, генерація підпису за допомогою Falcon набагато повільніша, ніж генерація підпису за допомогою Dilithium, і різниця настільки велика, що загальна вартість використання Dilithium нижча, навіть якщо взяти до уваги вищі витрати Dilithium на передачу даних.

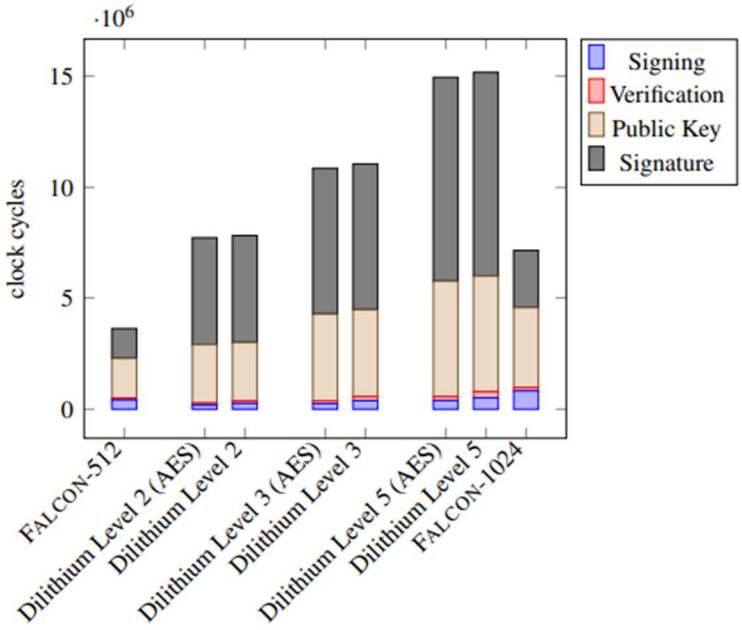

Рис. 4.16. Сигнатурні тести на процесорі x86-64 із розширеннями AVX2 із витратами на передачу 2000 циклів/байт

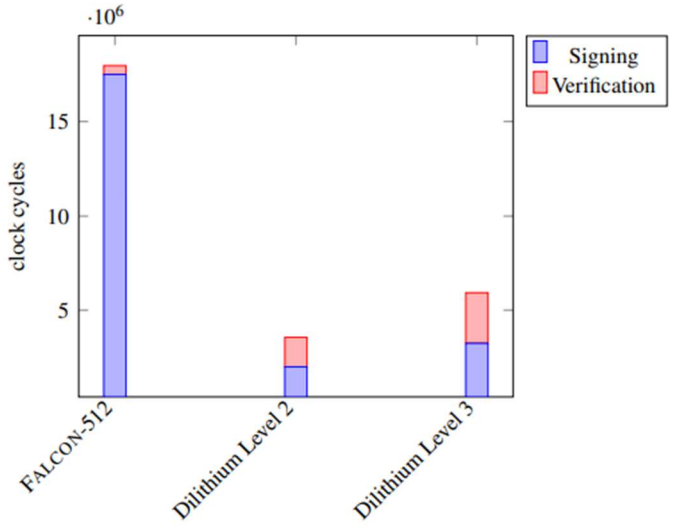

Рис. 4.17. Сигнатурні тести на процесорі ARM Cortex-M4

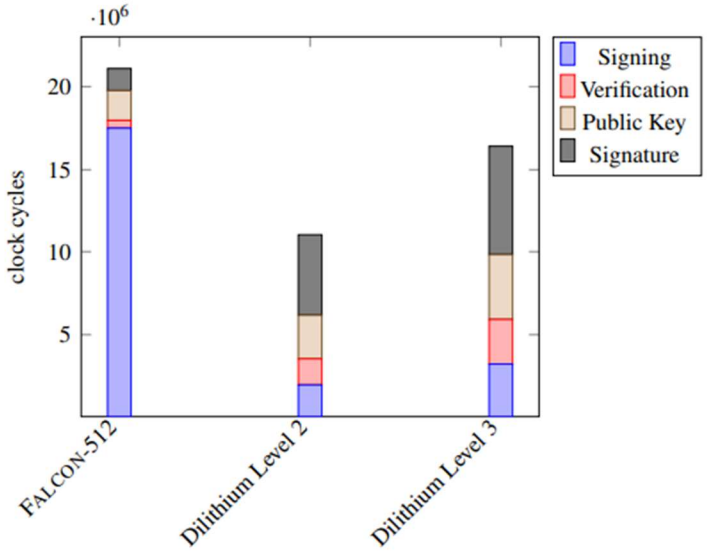

Рис. 4.18. Сигнатурні тести на процесорі ARM Cortex-M4 із витратами на передачу 2000 циклів/байт

Для схем цифрового підпису, [66] продемонстрував, що перевірку підпису для кожного з фіналістів можна реалізувати, використовуючи менше 8 КіБ оперативної пам’яті та менше 8 КіБ пам’яті для коду, і [67] представив реалізацію перевірки підпису FPGA як для Dilithium, так і для Falcon.

Таким чином, при порівнянні з міжнародними результатами можна зробити висновок про відповідність отриманих результатів результатам міжнародних досліджень, хоч і з деякими розбіжностями, зумовленими особливостями проведення порівняння. Також слід зазначити, що частина порівнюваних алгоритмів не була задіяна в процесі порівняння на міжнародному рівні, зокрема Вершина та Сокіл (хоча присутні алгоритми на основі тієї ж самої математики, що використовують ці алгоритми).

4.5. Висновки до розділу 4

1. У даному розділі було наведено приклад використання удосконаленої методики оцінки та порівняння криптографічних перетворень, що претендують на квантовостійкий стандарт. Разом із тим, що методика чудово відпрацювала на цільових об’єктах порівняння, було показано, що вона здатна на достатню гнучкість для того, щоб виходити за рамки цільових об’єктів оцінки та порівняння і навіть поєднувати цільові об’єкти порівняння із нецільовими придатними для її застосування об’єктами порівняння.

2. Проведено аналіз та порівняння кандидатів додаткового конкурсу на квантово-стійкий електронний підпис: ALTEQ (збалансований), eMLE-Sig 2.0 KAZ-SIGN, Xifrat1-Sign.1. З аналізу та порівняння можна зробити висновки, що при розробці схем ЕП робився наголос на різні аспекти, що впливає на безпеку алгоритмів. Так, ALTEQ зосереджено на зведенні до мінімуму розміру особистого ключа, хоча це і призвело до неймовірного збільшення розмірів відкритого ключа та підпису. eMLE-Sig 2.0 та Xifrat1-Sign.1 зводять до мінімуму розмір підпису. KAZ-SIGN має розміри особистого ключа близькі до розмірів особистого ключа ALTEQ, але розміри відкритого ключа та підписа найменші з усіх порівнюваних.

3. Проведено порівняння інших перспективних механізмів ЕП, таких як Dilithium, Вершина, Сокіл. За результатами досліджень, найбільшу перевагу серед алгоритмів отримує алгоритм «Вершина» з параметрами стійкості 128 біт. До кінцевого порівняння було залучено алгоритми, котрі змогли продемонструвати одні з кращих результатів на попередньому етапі – SPHINCS+_s, «Вершина» та «Сокіл» (завдяки тому, що на різних рівнях стійкості перевагу отримували різні алгоритми), а також Rainbow. За умови використання всіх можливих параметрів у порівнянні алгоритмів на перше місце виходить «Вершина».

4. Було проведено порівняння отриманих результатів з міжнародними оцінками перспективних механізмів ЕП. Так, у звіті про стан третього раунду

NIST PQC було наведено результати порівнянь обраних в якості фіналістів на другому раунді схем підпису загального призначення Dilithium і Falcon. Третій фіналіст, Rainbow, зазнав втрат безпеки, через що його було усунуто із розгляду. При порівнянні отриманих результатів порівняння виявлено відмінності, проте здебільшого отримані під час дослідженння результати корелюють з міжнародними.

РОЗДІЛ 5. МОДЕЛЮВАННЯ ТА ЕКСПЕРИМЕНТАЛЬНІ ДОСЛІДЖЕННЯ ПРОЦЕСІВ ПОРІВНЯННЯ ТА ЇХ МОДИФІКАЦІЇ

5.1. Постановка задач експериментальних досліджень з порівняння існуючих та перспективних електронних підписів

Як було зазначено вище (в Розділі 1), з метою проведення аналізу, оцінки та порівняння асиметричних квантовостійких криптоперетворень електронного підпису та протоколів інкапсуляції ключів необхідно виконати наступні задачі експериментальних досліджень:

- Реалізувати результати розробки в якості інструментарію для практичної оцінки та порівняння проєктів та стандартизованих міжнародних та національних квантовостійких електронних підписів;
- Провести аналіз, оцінку та порівняння існуючих та кандидатів на песпективні квантовостійкі національні та міжнародні електронні підписи;
- Розробити практичну реалізацію результатів досліджень, програмну реалізацію, прийняти участь в розробці національного стандарту;
- Застосувати методику оцінки та порівняння та отримати практичні (експериментальні) результати.

Виходячи з цього, сформовано наступні задачі щодо моделювання та експериментальних досліджень процесів оцінки та порівняння існуючих та перспективних квантовостійких криптоперетворень електронного підпису:

1) Відібрати варіанти застосування алгоритмів електронних підписів, актуальні для мети оцінки та порівняння;

2) Відібрати актуальні алгоритми електронних підписів;

3) Провести оцінку алгоритмів електронного підпису в кожному варіанті застосування (із застосуванням методу експертних оцінок);

4) Обрати найкращий підпис для застосування в кожному варіанті;

5) Виявити недоліки в безпеці алгоритмів електронних підписів та запропонувати можливі варіанти усунення цих недоліків.

5.2. Логіка побудови модифікованої моделі для проведення порівняння

Для покращення якості порівняння є доцільним враховувати особливості застосування порівнюваних алгоритмів після проведення оцінки. З цією метою було розроблено покращення етапу порівняння за прагматичними критеріями: було обрано набір варіантів застосування алгоритмів асиметричних криптоперетворень з урахуванням як національного так і міжнародного досвіду, проведено оцінювання важливості критеріїв, за якими відбувається порівняння криптоперетворень та проведена корекція фінальної оцінки кожного алгоритму з виокремленям оцінок для всіх обраних варіантів застосування.

На Рисунку 5.1 наведено узагальнену структуру моделі модифікації порівняння за Методикою з врахуванням особливостей різних варіантів застосування.

Рис. 5.1. Узагальнена структура моделі модифікації порівняння за Методикою з врахуванням особливостей застосування

Детальний розгляд логічної структури моделі модифікації наведено далі.

1) Першим кроком є формулювання набору варіантів застосування порівнюваних криптоперетворень.

Стандарти відкритого ключа NIST наразі використовуються в широкому спектрі програм, включаючи протоколи Інтернету, такі як TLS, SSH, IKE, IPsec і DNSSEC, а також для сертифікатів, підпису програмного коду та безпечних завантажувачів. Нові стандарти відкритого ключа NIST повинні забезпечувати постквантову безпеку для кожного із цих застосувань. З метою кількісної оцінки безпеки потенційних алгоритмів NIST надав три можливі визначення безпеки — два для шифрування та одне для підписів. NIST також призначив п'ять категорій безпеки для класифікації обчислювальної складності атак, які порушують визначення безпеки (див. [68]).

Враховуючи позицію міжнародної та національної спільноти та з метою охоплення важливих аспектів застосування електронних підписів та різноманітність вимог, доцільним признано розглянути такі застосування електронного підпису:

- PKI (Public Key Infrastructure)
- Протокол SSL/TLS
- SIM-карти
- IPSec (Internet Protocol Security)
- DNSSEC (Domain Name System Security Extensions)
- Віртуальні приватні мережі (VPN)

2) Другим кроком є обрання порівнюваних криптоперетворень, що здатні на вирішення задач із переліку варіантів застосування, сформульованого на пгпередньому кроці.

З точки зору релевантності та необхідності проведення порівняння було обрано наступні криптоперетворення: на основі математики Falcon (Falcon та Сокіл), на основі математики Delithium (Delithium та Вершина), кандидати з додаткового конкурсу на квантовостійкий стандарт електронного підпису (ALTEQ, eMLE-Sig 2.0, KAZ-SIGN, Xifrat1-Sign.I).

3) Третім кроком є формулювання переліку критеріїв для оцінки та порівняння.

Оцінки обраних криптографічних перетворень проведено за такими критеріями:

- Додаткові властивості безпеки;
- Вимоги до стійкості;
- Помилки шифрування;
- Можливість багаторазового застосування;
- Гнучкість і простота;
- Коректність та оптимізація;

- Ефективність та час проведення перетворень;
- Тестування неосновних умов використання;
- Можливість і умови вільного поширення;
- Рівень довіри на різних рівнях застосування;
- Перспективність та виправданість застосування;
- Легкість у використанні та інтеграції.

4) Четвертим кроком є отримання оцінок обраних криптоперетворень для кожного критерію із переліку, сформульованого на третьому кроці.

Оцінки за критеріями для обраних алгоритмів наведено в Таблиці 5.1.

Таблиця 5.1.

Оцінки алгоритмів за прагматичними критеріями

	Додаткові властивості безпеки	Вимоги до стійкості	Помилки шифрування	Можливість багаторазового застосування	Гнучкість і простота	Коректність та оптимізація	Ефективність та час проведення	Тестування неосновних умов	Можливість і умови вільного поширення	Рівень довіри на різних рівнях	Перспективність та виправданість	Легкість у використанні та інтеграції
Falcon	8	7	9	7	8	8	8	7	7	7	8	8
Сокіл	9	8	9	7	9	9	8	8	8	7	9	8
Delithium	9	8	9	7	9	8	8	9	7	8	8	7
Вершина	9	9	9	7	9	9	8	9	8	8	9	8

Продовження Таблиці 5.1.

ALTEQ	5	6	7	4	5	6	5	5	5	5	7	6
eMLE-Sig 2.0	6	5	7	5	9	6	6	5	5	5	7	6
KAZ-SIGN	5	5	7	5	9	6	7	6	5	5	7	6
Xifrat1-Sign.I	5	4	7	5	9	6	6	6	5	5	7	6

5) П’ятим кроком є оцінка значущість параметрів для обраних на першому кроці варіантів застосування та утворення таким чином коефіцієнтів значущості для параметрів в умовах кожного із варіантів застосування. Отримані оцінки наведено в Таблиці 5.2.

Таблиця 5.2.

Оцінки коефіцієнтів важливості прагматичних критеріїв для різних варіантів використання

	SSL/TLS	SIM-карти	IPSec	DNSSEC	VPN	Підписання PDF
Додаткові властивості безпеки	9	6	9	8	7	7
Вимоги до стійкості	8	7	9	9	9	7
Помилки шифрування	9	7	9	9	8	8
Можливість багаторазового застосування	7	5	5	7	5	9
Гнучкість і простота	7	9	5	7	6	9
Коректність та оптимізація	8	9	7	8	7	5

Продовження Таблиці 5.2.

Ефективність та час проведення перетворень	8	9	8	7	7	5
Тестування неосновних умов використання	8	5	7	5	7	5
Можливість і умови вільного поширення	7	9	8	9	5	9
Рівень довіри на різних рівнях застосування	7	5	9	9	9	7
Перспективність та виправданість застосування	7	7	9	7	9	5
Легкість у використанні та інтеграції	8	9	7	9	5	9

6) Шостим кроком є застосування коефіцієнтів значущості до оцінок порівнюваних криптоперетворень. Отримані на попередньому кроці коефіцієнти значущості використовуються для корекції оцінки криптографічного перетворення у відповідності до застосування, для використання в якому проводиться оцінка. Застосування коєфіцієнтів значущості виглядає наступним чином: оцінки криптографічного перетворення для кожного критерію, отримані за допомогою експертної оцінки премножаються із коефіцієнтами значущості відповідного критерію для окремого застосування криптографічного перетворення та отримане значення ділиться на базис системи оцінки, котрий в даному випадку приймає значення 10. Тобто, це приймає наступний вигляд для одного криптографічного перетворення та одного застосування:

$$a[i] = (signatures\_values[i]*use\_cases\_values[i])/10, \quad (5.1)$$

де a – фінальна оцінка за одним критерієм, signatures_values – набір значень оцінок криптографічного перетворення за всіма обраними критеріями, use_cases_values – набір значень коефіцієнтів значущості для застосування для всіх обраних критеріїв, і – індекс критерію для якого проводиться оцінка.

7) Після застосування коефіцієнтів значущості до оцінок криптоперетворення длякритерію порівняння із врахуванням варіанту застосування, отримані зважені значення оцінок одного критерію порівняння додаються до інших зважених оцінок цього ж криптоперетворення для цього ж варіанту застосування і діляться на сумарну кількість зважених оцінок. Таким чином отримується інтегральна оцінка конкретного криптоперетворення для конкретного варіанту застосування.

Лістінг розробленого коду в частині, спрямованій на проведення оцінювання із врахуванням особливостей впливу варіантів застосування криптоперетворень наведено в Додатку В.

5.3. Результати експериментальних досліджень оцінки та порівняння методів електронного підпису

Результати експериментального проходження шостого та сьомого етапів (зважені значення оцінок за обраними критеріями та інтегральні оцінки за варіантами застосування) із застосуванням програмного забезпечення для алгоритму Falcon для всіх обраних варіантів застосування наведено в Таблиці 5.3.

Таблиця 5.3.

Оцінки Falcon за прагматичними критеріями для різних варіантів використання

Falcon	SSL/TLS	SIM-карти	IPSec	DNSSEC	VPN	Підписання PDF
Додаткові властивості безпеки	7,2	4,8	8,2	6,4	5,6	5,6
Вимоги до стійкості	5,6	4,9	7,3	6,3	6,3	4,9
Помилки шифрування	8,1	4,3	8,1	8,1	7,2	7,2
Можливість багаторазового застосування	4,9	3,5	5,5	4,9	3,5	6,3
Гнучкість і простота	5,6	6,2	5	5,6	4,8	7,2
Коректність та оптимізація	6,4	5,2	6,6	6,4	5,6	4
Ефективність та час проведення перетворень	6,4	5,2	7,4	5,6	5,6	4
Тестування неосновних умов використання	5,6	3,5	5,9	3,5	4,9	3,5
Можливість і умови вільного поширення	4,9	4,3	6,6	6,3	3,5	6,3
Рівень довіри на різних рівнях застосування	4,9	3,5	7,3	6,3	6,3	4,9
Перспективність та виправданість застосування	5,6	4,6	8,2	5,6	7,2	4
Легкість у використанні та інтеграції	6,4	5,2	6,6	7,2	4	7,2
Інтегральна оцінка	5,96	4,6	6,89	6,01	6,25	5,42

Результати експериментального проходження шостого та сьомого етапів (зважені значення оцінок за обраними критеріями та інтегральні оцінки за варіантами застосування) із застосуванням програмного забезпечення для алгоритму Сокіл для всіх обраних варіантів застосування наведено в Таблиці 5.4.

Таблиця 5.4.

Оцінки Сокіл за прагматичними критеріями для різних варіантів використання

Сокіл	SSL/TLS	SIM-карти	IPSec	DNSSEC	VPN	Підписання PDF
Додаткові властивості безпеки	8,1	5,4	8,1	7,2	6,3	6,3
Вимоги до стійкості	6,4	5,6	8,2	7,2	7,3	5,6
Помилки шифрування	8,1	5,3	8,1	8,1	7,2	7,2
Можливість багаторазового застосування	4,9	3,5	5,5	4,9	3,5	6,3
Гнучкість і простота	6,3	6,1	6,5	6,3	5,4	8,1
Коректність та оптимізація	7,2	6,1	7,3	7,2	6,3	4,5
Ефективність та час проведення перетворень	6,4	5,2	7,4	5,6	5,6	4
Тестування неосновних умов використання	6,4	4	7,6	4	5,6	4
Можливість і умови вільного поширення	5,6	6,2	7,4	7,2	4	7,2
Рівень довіри на різних рівнях застосування	4,9	3,5	7,3	6,3	6,3	4,9

Продовження Таблиці 5.4.

Перспективність та виправданість застосування	6,3	4,3	8,1	6,3	8,1	4,5
Легкість у використанні та інтеграції	6,4	5,2	6,6	7,2	4	7,2
Інтегральна оцінка	6,41	5,03	7,34	6,45	5,8	5,81

Результати експериментального проходження шостого та сьомого етапів (зважені значення оцінок за обраними критеріями та інтегральні оцінки за варіантами застосування) із застосуванням програмного забезпечення для алгоритму Delithium для всіх обраних варіантів застосування наведено в Таблиці 5.5.

Таблиця 5.5.

Оцінки Delithium за прагматичними критеріями для різних варіантів використання

Delithium	SSL/TLS	SIM-карти	IPSec	DNSSEC	VPN	Підписання PDF
Додаткові властивості безпеки	8,1	5,4	8,1	7,2	6,3	6,3
Вимоги до стійкості	6,4	5,6	7,2	7,2	7,2	5,6
Помилки шифрування	8,1	6,3	8,1	8,1	7,2	7,2
Можливість багаторазового застосування	4,9	3,5	5,5	4,9	3,5	6,3
Гнучкість і простота	6,3	8,1	6,5	6,3	5,4	8,1
Коректність та оптимізація	6,4	7,2	5,6	6,4	5,6	4

Продовження Таблиці 5.5.

Ефективність та час проведення перетворень	6,4	7,2	6,4	5,6	5,6	4
Тестування неосновних умов використання	7,2	4,5	6,3	4,5	6,3	4,5
Можливість і умови вільного поширення	4,9	6,3	6,6	6,3	3,5	6,3
Рівень довіри на різних рівнях застосування	5,6	4	7,2	7,2	7,2	5,6
Перспективність та виправданість застосування	5,6	5,6	7,2	5,6	7,2	4
Легкість у використанні та інтеграції	5,6	6,3	5,9	6,3	3,5	6,3
Інтегральна оцінка	6,29	5,83	6,71	6,3	5,7	5,68

Результати експериментального проходження шостого та сьомого етапів (зважені значення оцінок за обраними критеріями та інтегральні оцінки за варіантами застосування) із застосуванням програмного забезпечення для алгоритму Вершина для всіх обраних варіантів застосування наведено в Таблиці 5.6.

Таблиця 5.6.

Оцінки Вершина за прагматичними критеріями для різних варіантів використання

Вершина	SSL/TLS	SIM-карти	IPSec	DNSSEC	VPN	Підписання PDF
Додаткові властивості безпеки	8,1	5,4	8,1	7,2	6,3	6,3
Вимоги до стійкості	7,2	6,3	8,1	8,1	8,1	6,3
Помилки шифрування	8,1	6,3	8,1	8,1	7,2	7,2
Можливість багаторазового застосування	4,9	3,5	4,5	4,9	3,5	6,3
Гнучкість і простота	6,3	8,1	5,5	6,3	5,4	8,1
Коректність та оптимізація	7,2	8,1	6,3	7,2	6,3	4,5
Ефективність та час проведення перетворень	6,4	7,2	6,4	5,6	5,6	4
Тестування неосновних умов використання	7,2	4,5	6,3	4,5	6,3	4,5
Можливість і умови вільного поширення	5,6	7,2	6,8	7,2	4	7,2
Рівень довіри на різних рівнях застосування	5,6	4	7,2	7,2	7,2	5,6
Перспективність та виправданість застосування	6,3	6,3	8,1	6,3	8,1	4,5
Легкість у використанні та інтеграції	6,4	7,2	5,6	7,2	4	7,2
Інтегральна оцінка	6,6	6,17	6,75	6,65	6	5,97

Результати експериментального проходження шостого та сьомого етапів (зважені значення оцінок за обраними критеріями та інтегральні оцінки за варіантами застосування) із застосуванням програмного забезпечення для алгоритму ALTEQ для всіх обраних варіантів застосування наведено в Таблиці 5.7.

Таблиця 5.7.

Оцінки ALTEQ за прагматичними критеріями для різних варіантів використання

ALTEQ	SSL/TLS	SIM-карти	IPSec	DNSSEC	VPN	Підписання PDF
Додаткові властивості безпеки	4,5	3	4,5	4	3,5	3,5
Вимоги до стійкості	4,8	4,2	5,4	5,4	5,4	4,2
Помилки шифрування	6,3	4,9	6,3	6,3	5,6	5,6
Можливість багаторазового застосування	2,4	2	2	2,4	2	3,6
Гнучкість і простота	3,5	4,5	2,5	3,5	3	4,5
Коректність та оптимізація	4,8	5,4	4,2	4,8	4,2	3
Ефективність та час проведення перетворень	4	4,5	4	3,5	3,5	2,5
Тестування неосновних умов використання	4	2,5	3,5	2,5	3,5	2,5
Можливість і умови вільного поширення	3,5	4,5	4	4,5	2,5	4,5
Рівень довіри на різних рівнях застосування	3,5	2,5	4,5	4,5	4,5	3,5

Продовження Таблиці 5.7.

Перспективність та виправданість застосування	4,9	4,9	6,3	6,3	6,3	3,5
Легкість у використанні та інтеграції	4,8	5,4	4,2	5,4	3	5,4
Інтегральна оцінка	4,25	4,02	4,28	4,42	3,91	3,85

Результати експериментального проходження шостого та сьомого етапів (зважені значення оцінок за обраними критеріями та інтегральні оцінки за варіантами застосування) із застосуванням програмного забезпечення для алгоритму eMLE-Sig 2.0 для всіх обраних варіантів застосування наведено в Таблиці 5.8.

Таблиця 5.8.

Оцінки eMLE-Sig 2.0 за прагматичними критеріями для різних варіантів використання

eMLE-Sig 2.0	SSL/TLS	SIM-карти	IPSec	DNSSEC	VPN	Підписання PDF
Додаткові властивості безпеки	5,4	3,6	5,4	4,8	4,2	4,2
Вимоги до стійкості	4	3,5	4,5	4,5	4,5	3,5
Помилки шифрування	6,3	4,9	6,3	6,3	5,6	5,6
Можливість багаторазового застосування	3,5	2,5	2,5	3,5	2,5	4,5
Гнучкість і простота	6,3	8,1	4,5	6,3	5,4	8,1
Коректність та оптимізація	4,8	5,4	4,2	4,8	4,2	3

Продовження Таблиці 5.8.

Ефективність та час проведення перетворень	4,8	5,4	4,8	4,2	4,2	3
Тестування неосновних умов використання	4	2,5	3,5	2,5	3,5	2,5
Можливість і умови вільного поширення	3,5	4,5	4	4,5	2,5	4,5
Рівень довіри на різних рівнях застосування	3,5	2,5	4,5	4,5	4,5	3,5
Перспективність та виправданість застосування	4,9	4,9	6,3	4,9	6,3	3,5
Легкість у використанні та інтеграції	4,8	5,4	4,2	5,4	3	5,4
Інтегральна оцінка	4,65	4,43	4,55	4,68	4,2	4,27

Результати експериментального проходження шостого та сьомого етапів (зважені значення оцінок за обраними критеріями та інтегральні оцінки за варіантами застосування) із застосуванням програмного забезпечення для алгоритму KAZ-SIGN для всіх обраних варіантів застосування наведено в Таблиці 5.9.

Таблиця 5.9.

Оцінки KAZ-SIGN за прагматичними критеріями для різних варівантів використання

KAZ-SIGN	SSL/TLS	SIM-карти	IPSec	DNSSEC	VPN	Підписання PDF
Додаткові властивості безпеки	4,5	3	4,5	4	3,5	3,5
Вимоги до стійкості	4	3,5	4,5	4,5	4,5	3,5
Помилки шифрування	6,3	4,9	6,3	6,3	5,6	5,6
Можливість багаторазового застосування	3,5	2,5	2,5	3,5	2,5	4,5
Гнучкість і простота	6,3	8,1	4,5	6,3	5,4	8,1
Коректність та оптимізація	4,8	5,4	4,2	4,8	4,2	3
Ефективність та час проведення перетворень	5,6	6,3	5,6	4,9	4,9	3,5
Тестування неосновних умов використання	4,8	3	4,2	3	4,2	3
Можливість і умови вільного поширення	3,5	4,5	4	4,5	2,5	4,5
Рівень довіри на різних рівнях застосування	3,5	2,5	4,5	4,5	4,5	3,5
Перспективність та виправданість застосування	4,9	4,9	6,3	4,9	6,3	3,5
Легкість у використанні та інтеграції	4,8	5,4	4,2	5,4	3	5,4
Інтегральна оцінка	4,7	4,5	4,6	4,71	4,25	4,3

Результати експериментального проходження шостого та сьомого етапів (зважені значення оцінок за обраними критеріями та інтегральні оцінки за варіантами застосування) із застосуванням програмного забезпечення для алгоритму Xifrat1-Sign.I для всіх обраних варіантів застосування наведено в Таблиці 5.10.

Таблиця 5.10.

Оцінки Xifrat1-Sign.I за прагматичними критеріями для різних варівантів використання

Xifrat1-Sign.I	SSL/TLS	SIM-карти	IPSec	DNSSEC	VPN	Підписання PDF
Додаткові властивості безпеки	4,5	3	4,5	4	3,5	3,5
Вимоги до стійкості	3,2	2,8	3,6	3,6	3,6	2,8
Помилки шифрування	6,3	4,9	6,3	6,3	5,6	5,6
Можливість багаторазового застосування	3,5	2,5	2,5	3,5	2,5	4,5
Гнучкість і простота	6,3	8,1	4,5	6,3	5,4	8,1
Коректність та оптимізація	4,8	5,4	4,2	4,8	4,2	3
Ефективність та час проведення перетворень	4,8	5,4	4,8	4,2	4,2	3
Тестування неосновних умов використання	4,8	3	4,2	3	4,2	3
Можливість і умови вільного поширення	3,5	4,5	4	4,5	2,5	4,5
Рівень довіри на різних рівнях застосування	3,5	2,5	4,5	4,5	4,5	3,5

Продовження Таблиці 5.10.

Перспективність та виправданість застосування	4,9	4,9	6,3	4,9	6,3	3,5
Легкість у використанні та інтеграції	4,8	5,4	4,2	5,4	3	5,4
Інтегральна оцінка	4,57	4,36	4,46	4,58	4,12	4,2

В Таблиці 5.11 наведено результуючі інтегральні оцінки відібраних алгоритмів, за якими можна обрати найкращий варіант для використання в кожному з обраних варіантів застосування електронного підпису.

Таблиця 5.11.

Інтегральні оцінки алгоритмів за прагматичними критеріями для різних варіантів використання

	SSL/TLS	SIM-карти	IPSec	DNSSEC	VPN	Підписання PDF	Інтегральна оцінка без варіантів застосування
Falcon	5,96	4,6	6,89	6,01	6,25	5,42	7,6
Сокіл	6,41	5,03	7,34	6,45	5,8	5,81	8,25
Delithium	6,29	5,83	6,71	6,3	5,7	5,68	8,08
Вершина	6,6	6,17	6,75	6,65	6	5,97	8,5
ALTEQ	4,25	4,02	4,28	4,42	3,91	3,85	5,5
eMLE-Sig 2.0	4,65	4,43	4,55	4,68	4,2	4,27	6
KAZ-SIGN	4,7	4,5	4,6	4,71	4,25	4,3	6,08
Xifrat1-Sign.I	4,57	4,36	4,46	4,58	4,12	4,2	5,92

Рисунок 5.2 демонструє вплив варіанту застосування на результуючі інтегральні оцінки відібраних алгоритмів, а отже і на найкращий варіант при порівнянні для використання в різноманітних варіантах застосування електронного підпису.

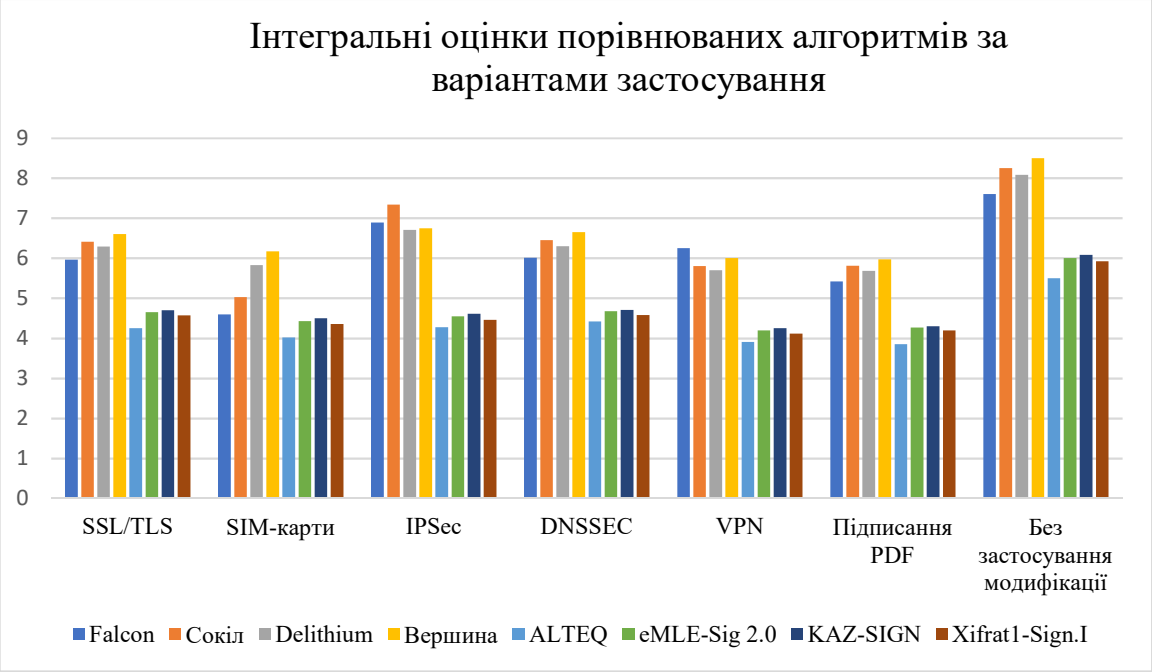

Рис. 5.2. Результати оцінювання за варіантами застосування

З наведеного в Таблиці 5.11 та на Рисунку 5.2 результату чітко видно, що застосування модифікації до процесу оцінювання за умовними критеріями з метою врахування впливу особливостей застосування електронних підписів призводить до загального зниження оцінок через те, що проводиться застосування коефіцієнтів значущості до результатів оцінювання. В ході дослідження помічено загальне зниження оцінок приблизно на 10-20%, що призводить до загального зниження максимального значення можливої оцінки. До виняткових випадків належать наступні: - коли оцінюваний алгоритм має максимальну оцінку за наведеним критерієм та цей критерій має максимальну важливість для потрібного варіанту застосування; - коли алгоритм має дуже низьку оцінку та відповідний критерій має мінімальну оцінку для потрібного

варіанту застосування. Підтвердженням цьому на Рисунку 5.2 є відмінність в значеннях між стандартизованими алгоритмами, що довели свої властивості, та перспективними кандидатами, котрі потребують доопрацювання для підтвердження та стандартизації.

Також важливим результатом цього дослідження є підтвердження теоретичного припущення про те, що врахування впливу особливостей застосування електронних підписів може призводити до цілковитої зміни пріоритетного для обрання кандидата. Так, наприклад, можна помітити, що для застосування в SIM-картах оцінки підписів на базі математики Falcon значно впали через складнощі реалізації таких алгоритмів в умовах обмежених ресурсів, що було також відзначено в [2]. У варіантах застосування для IPSec та у VPN, можна помітити, що оцінки алгоритмів на основі математики Falcon піднімаються і змінюють пріоритетного кандидата. Те, що для кожного з цих варіантів пріоритетний кандидат відрізняється пов’язано з важливістю критеріїв, котрі відрізняються між Falcon та Сокіл, як от «Можливість і умови вільного поширення» та ін. Інші ж варіанти застосування приводять до отримання результатів порівняння близьких до тих, які можна отримати без застосування модифікації, що підтверджує загальну правильність методики оцінювання навіть без врахування особливостей застосування для 3 із 6 досліджених варіантів застосування електронних підписів.

5.4. Виявлені в ході дослідження недоліки в безпеці методів електронного підпису

Під час проведеного дослідження з оцінки та порівняння існуючих та перспективних електронних підписів на предмет відповідності їх вимогам для визнання квантово-стійкими було виявлено недоліки в безпеці алгоритмів електронних підписів на основі математики Falcon. Так зокрема в [19, 20] було запропоновано атаку на алгоритм електронного підпису Falcon.

Слід одразу зауважити, що алгоритм електронного підпису Falcon є одним з фіналістів конкурсу NIST PQC з квантово-стійкої (постквантової) криптографії.

Однією з головних особливостей схеми ЕП Falcon є використання обчислень з плаваючою точкою. Для обчислень з плаваючою точкою зазвичай характерним є шум у молодших бітах, який визначається порядком обчислень [69]. Це є причиною виникнення додаткових ризиків і створює необхідність більш детального вивчення впливу цього явища на безпеку схем ЕП.

Схема ЕП Falcon використовує перетворення у полі $\mathbb{Z}$q[X]/(xn+1), де q=12289 та n – степінь двійки (512 або 1024). Таємним ключем є поліноми f,g,F,G$\in\mathbb{Z}$q[X]/(xn+1), коефіцієнти яких є малими і виконується NTRU-рівняння:

$$fG - gF = q \bmod x^n + 1. \tag{5.2}$$

Відкритим ключем є поліном $h \in \mathbb{Z}_q[X]/(x^n+1)$, для якого виконується рівняння:

$$h = g \cdot f^{-1} \bmod x^n + 1 \bmod q. \tag{5.3}$$

Поліноми f, g, F, G утворюють базис NTRU-решітки:

$$B = \begin{pmatrix} g & -f \\ G & -F \end{pmatrix}. \tag{5.4}$$

При обчисленнях у ЕП Falcon для оптимізації використовується швидке перетворення Фур'є. Фур'є-образ довільного полінома b позначено як $\hat{b}$. Відповідно, Фур'є-образ базису B визначено наступним чином:

$$\hat{B} = \begin{pmatrix} \hat{g} & -\hat{f} \\ \hat{G} & -\hat{F} \end{pmatrix}. \tag{5.5}$$

Специфікація ЕП Falcon передбачає використання властивостей поля $\mathbb{Z}_q[X]/(\mathrm{x}^n+1)$. Зокрема, використовуються наступні ізоморфізми:

$$\mathbb{Z}^n \cong (\mathbb{Z}[X]/(x^2+1))^{n/2} \cong \ldots \cong (\mathbb{Z}[X]/(x^{n/2}+1))^2 \cong \mathbb{Z}[X]/(x^n+1). \tag{5.6}$$

Формула (5.6) означає, що будь-який поліном у $\mathbb{Z}_q[X]/(\mathrm{x}^n+1)$ має ізоморфне представлення у вигляді вектора з двох поліномів у $\mathbb{Z}_q[X]/(\mathrm{x}^{n/2}+1)$, вектора з чотирьох поліномів у $\mathbb{Z}_q[X]/(\mathrm{x}^{n/4}+1)$ і т. д.

Зокрема, ця властивість була використана авторами ЕП Falcon для побудови алгоритма вибірки. У загальному випадку алгоритм вибірки *Sampler* приймає на вхід деякий базис решітки A, цільовий вектор c та повертає достатньо малий вектор s, для якого виконується:

$$sA = c \bmod q. \tag{5.7}$$

В ЕП Falcon алгоритм вибірки ffSampling рекурсивно проводить процедуру вибірки. Обчислення починаються у $\mathbb{Z}$n і рекурсивно підіймаються у поле $\mathbb{Z}$q[X]/(xn+1). Для цього ffSampling використовує так звану структуру даних «Falcon Tree», що зберігає інформацію про базис (5.5) у зручній для обчислень формі. Деталі реалізації можливо знайти в специфікації [70]. Єдиний суттєвий фактор для цієї атаки – ffSampling працює з Фур'є образами і повертає Фур'є образ полінома s. Згідно до специфікації структура «Falcon Tree» [70] для базису (5.5) має позначення $T = T(\hat{B})$.

Процедуру підпису ЕП Falcon, можливо узагальнити як:

Алгоритм Sign

Вхідні дані: повідомлення m представлене у форматі бітового рядка, базис NTRU-решітки $\hat{B}$.

Вихідні дані: підпис (s1,nonce), за умови, що s1 – поліноми у $\mathbb{Z}$ q[X]/(xn+1), nonce – випадковий бітовий рядок, що призначено для рандомізації повідомлення.

1. Отримання nonce із рівномірного розподілу

2. Обчислення випадкового поліному c у представленні геш-значення від m||nonce

3. Обчислення $\hat{t} = (\hat{c}, \hat{0}) \cdot \hat{B}^{-1}$

4. Обчислення вектора $\hat{z}=(\hat{z}_0,\hat{z}_1)$ за допомогою використання алгоритму вибірки ffSampling (і $T=T(\hat{B})$) для цільової точки $\hat{t}$.

5. Обчислення $\hat{s}=(\hat{s}_0,\hat{s}_1)=(\hat{t}-\hat{z})\hat{B}$ у базисі Фур'є та відповідного вектора s=(s0,s1) за допомогою використання зворотного перетворення Фур'є.

6. За умови, якщо норма вектора s є достатньо малою, то повернути підпис (s1,nonce), у іншому випадку – повернутися до кроку 4.

Перевірка підпису, згідно до специфікації ЕП Falcon, відбувається з використанням рівняння:

$$s_0 + s_1 h = c. \tag{5.8}$$

Рівняння (5.8) встановлює зв'язок між підписом, повідомленням та публічним ключем. Поліном s0 з підпису (s1,nonce) можливо відновити як s0=c–s1h. Якщо поліном відновлюється правильно, то підпис вважається дійсним.

Шум округлення зазвичай виникає у молодших бітах змінних, проте має властивість зростати з кількістю обчислень, тому має сенс очікувати найбільшої різниці в змінних, для обчислення яких використовуються найбільш складні перетворення. Обчислення, яке вимагає найбільшої кількості операцій, є результатом роботи алгоритму ffSampling, який активно використовує перетворення Фур'є і є найскладнішою з алгоритмічної точки зору частиною ЕП Falcon.

Для подальшого необхідно, як описано в [42, 44] припустити, що існує дві реалізації ЕП Falcon, які з однакових значеннях seed та nonce для однакових ключів утворюють різні підписи за рахунок шуму під час обчислень. Надалі верхніми індексами буде позначено відповідні змінні. Таким чином, (s_0^0,s_1^0) – вектор s у першому підписі та (s_0^1,s_1^1) – вектор s у другому підписі.

Після цього потрібно ввести позначення $\delta_0=z_0^1-z_0^0$ та $\delta_1=z_1^1-z_1^0$.

Твердження 1. Для заданих δ_0,δ_1 зв'язок між публічним ключем *h* та таємним ключем f,g,F,G, описується відношенням:

$$h = \frac{g\delta_0 + G\delta_1}{f\delta_0 + F\delta_1}. \tag{5.9}$$

Якщо розглянути обчислення підпису s=(s0,s1) на ключі f,g,F,G, тоді відповідно до визначення алгоритму підпису, можна отримати:

$$\hat{s} = (\hat{t} - \hat{z})\hat{B} = \hat{t}\hat{B} - \hat{z}\hat{B} = (\hat{c}, \hat{0})\hat{B}^{-1}\hat{B} - \hat{z}\hat{B} = \begin{pmatrix} \hat{c} \\ \hat{0} \end{pmatrix} - \begin{pmatrix} \hat{z}_0\hat{g} + \hat{z}_1\hat{G} \\ -\hat{z}_0\hat{f} - \hat{z}_1\hat{F} \end{pmatrix} = \begin{pmatrix} \hat{c} - \hat{z}_0\hat{g} - \hat{z}_1\hat{G} \\ \hat{z}_0\hat{f} + \hat{z}_1\hat{F} \end{pmatrix}. \tag{5.10}$$

Тож, має місце рівність:

$$\begin{aligned} s_0 &= c - z_0 g - z_1 G, \\ s_1 &= z_0 f + z_1 F. \end{aligned} \tag{5.11}$$

Враховуючи зв'язок між підписом, повідомленням та публічним ключем, що описується рівністю (5.8), можна отримати, що *h* можливо виразити через (s_0^0, s_1^0) та (s_0^1, s_1^1).

Якщо підставити (5.11) у вираз для *h*, то можна отримати:

$$h = \frac{c - z_0^0 g - z_1^0 G - c + z_0^1 g + z_1^1 G}{z_0^1 f + z_1^1 F - z_0^0 f - z_1^0 F} = \frac{g(z_0^1 - z_0^0) + G(z_1^1 - z_1^0)}{f(z_0^1 - z_0^0) + F(z_1^1 - z_1^0)}. \tag{5.12}$$

Оскільки $\delta_0 = z_0^1 - z_0^0$ та $\delta_1 = z_1^1 - z_1^0$, то з виразу (5.12) випливає вираз (5.9), що і треба було довести.

Якщо підібрати повідомлення *m* таким чином, щоб δ1=0, а δ0 було деяким достатньо малим для того, що можливо було використати алгоритм для пошуку найбільшого спільного дільника поліномом, то можливо буде легко відновити таємний ключ. Слід також зауважити, що ситуація, коли δ0=0, а δ1≠0 є не можливою через структуру алгоритму вибірки ffSampling.

Якщо δ1≠0, то, за визначенням, значення z_1^1, z_1^0 будуть відрізнятися. Тоді на 10 кроці алгоритму ffSampling будуть відрізнятися значення $t_0^{'}$, що у свою чергу призведе до змін у обчисленні z_0^1, z_0^0 на кроках 10-13.

З формули (5.9) та визначених умов значного впливу шуму округлення на безпеку випливає, що стає можливим обчислити таємний ключ $\widetilde{f},\widetilde{g}$ у наступному вигляді:

$$\begin{aligned}\widetilde{f} &= (s_1^1 - s_1^0) / \gcd(s_1^1 - s_1^0, s_0^0 - s_0^1),\\ \widetilde{g} &= (s_0^0 - s_0^1) / \gcd(s_1^1 - s_1^0, s_0^0 - s_0^1).\end{aligned} \tag{5.13}$$

Де gcd – найбільший спільний дільник поліномів.

Еталонна реалізація ЕП Falcon [46] особлива тим, що надає два інтерфейси для користувачів. Перший інтерфейс використовується для обчислення $T = T(\hat{B})$ у процедурі вироблення підпису. Другий же інтерфейс в свою чергу передбачає передачу $T = T(\hat{B})$ у якості аргумента. В реалізаціях це призводить до того, що порядок обчислень змінюється і виникають умови проведення атаки. Перший інтерфейс реалізований функцією sign_dyn, другий інтерфейс функцією sign_tree. Обидва інтерфейси замість повідомлення приймають вже поліном *c*.

Відповідно до [19, 20] ймовірність того, що $(\delta_0, \delta_1) \neq (0,0)$ складає близько 0,00003. Таким чином виходить, що в середньому атака працює у 76 % випадків для Flacon512 та у 70 % випадків для Falcon1024.

Після проведення аналіз конкретних випадків реалізації було визначено, що всі випадки, коли виконується (δ0,δ1)≠(0,0), є можливим розділити на чотири класи випадків, три з котрих є варіаціями одного [19, 20].

Випадок I. δ1≠0. У зв'язку із структурою алгоритму вибірки можна отримати δ0≠0, тож формула (5.13) не буде давати коректний результат. Таких випадків близько 24 % для Falcon512 і близько 29 % для Falcon1024.

Випадку δ1=0 є тим випадком, котрий має три варіанти в залежності від значення δ0.

Випадок II-а. За умови, що δ1=0 і δ0=*a*, *a*∈ℤ. У цьому випадку формула (5.13) дає коректний результат. У такому випадку, значення *a* становить менше

10. Таких випадків для Falcon512 складає близько 29 % від загальної кількості і близько 26 % для Falcon1024.

Випадок II-b. За умови, що $\delta 1=0$ і $\delta 0=a\cdot xn/2$, $a\in\mathbb{Z}$. У цьому випадку формула (5.13) дає коректний результат. У такому випадку, значення a становить менше 10. Таких випадків для Falcon512 складає близько 38 % від загальної кількості і близько 35 % для Falcon1024.

Випадок II-c. За умови, що $\delta 1=0$ і $\delta 0=a+b\cdot xn/2$, де $a,b\in\mathbb{Z}$. Цей випадок являє собою комбінацію попередніх випадків і формула (5.13) також буде давати коректний результат, але на відміну від інших випадків $\delta 0$.є поліномом. Така ситуація трапляється близько у 7 % випадків для Falcon512 та у 9 % випадків для Falcon1024.

Аналіз конкретних випадків показав, що різниця виникає в алгоритмі ffSampling. Атака на відновлення таємних ключів з використанням формули (5.13) є можливою, оскільки еталонна реалізація електронного підпису Falcon має два інтерфейси, що використовують різний порядок обчислень.

Важливою ця атака є з тієї точки зору, що вона була виявлена після того, як схему ЕП Falcon було визнано фіналістом конкурсу, а отже процес відбору є неідеальним та може покращуватись. Особливо варто звернути увагу на розширення спектру векторів атак та покращення моделі загроз для кандидатів на квантовостійкий стандарт.

5.5. Пропозиції з усунення виявлених недоліків в безпеці методів електроннного підпису

Також було проведено дослідження з метою отримання методів запобігання отримання різних підписів, а отже і захисту від наведеної атаки. Оскільки атака ґрунтується на використанні шуму обчислень з плаваючою точкою, то одним з шляхів захисту є використання операцій з фіксованою

точкою замість плаваючої точки. Ідея методу полягає в тому, що замість звичайної плаваючої точки задається масштабоване число.

Відправною точкою для досліджень використання фіксованої точки слугує робота [71]. У роботі [71] було запропоновано використовувати в якості масштабу значення 2^{32}. Будемо позначати цей масштаб кількістю бітів для цілої частини SCALE = 32. Для переходу до масштабованого числа воно множиться на масштаб 2^{SCALE}. У цій же роботі був запропонований набір функцій для найпростіших операцій над реальними та комплексними даними для таких чисел [71].

Таким чином, для завдання нецілої частини в числі відводиться 32 біта, що і визначає точність завдання числа. Для завдання цілої частини відводиться 31 біт, один біт відводиться для знаку числа. Для успішного застосування такого задання необхідною умовою є застосування числових значень, які за модулем не перевищують 2^{31}, в тому числі усі проміжні результати повинні задовольняти цій умові. Для генерації ЕП необхідно обчислити LDL дерево [70,72]. На жаль, при обчисленні LDL дерева проміжні результати при роботі з комплексними даними перевищують допустимі значення, тому застосування цього методу завдання для обчислення (генерації) ЕП не можливо, треба збільшувати довжину цілої частини числа, що можливо за рахунок:

- зменшення точності числа;
- збільшення загальної довжини числа.

Збільшення загальної довжини числа (більше 64 бітів) не розглядалося, так як це привело б до значного зменшення продуктивності, далі розглянуто рішення проблеми за рахунок зменшення довжини нецілої частини числа.

Проведено експеримент, в якому для ключів, генерованих еталонною реалізацією, постійними значеннями seed2 та nonce підбиралися повідомлення для підпису, яке має довжину 33 байти і містить значення 0, 1, 2, … до тих пір, поки не отримували різні пари значень компонентів ЕП. Для кожної пари значень виконувалася перевірка підпису.

Таблиця 5.12.

Статистична перевірка гіпотези про експоненціальний розподіл номерів повідомлень для рівня значущості $\alpha = 0.01$.

Тест	Статистика	P-значення	Результат
Хі-Квадрат	10.694	0.2972	Гіпотеза приймається
Колмогорова-Смірнова	0.0728	0.6358	Гіпотеза приймається

Додатково було побудувано Q-Q графік [73]. Q-Q Графік (квантиль-квантиль графік) є методом візуального порівняння емпіричного розподілу даних з теоретичним розподілом. Він показує наскільки гарно данні підпорядковуються даному розподілу. Квантилі емпіричного та теоретичного розподілу мають формувати пряму лінію. Відхили на графіку слугують індикатором систематичних відмінностей в розподілі. На рисунку 3 наведено Q-Q графік для отриманого емпіричного розподілу ймовірностей.

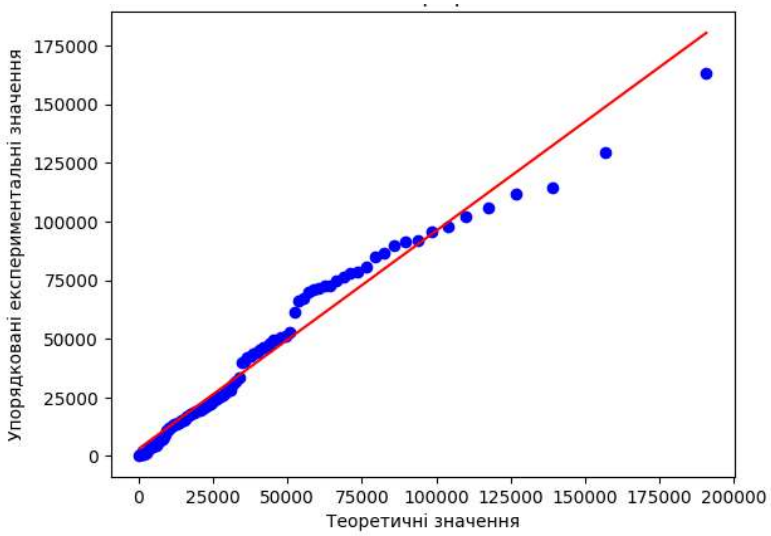

Рис. 5.3. Q-Q графік для отриманого емпіричного розподілу ймовірностей

З таблиці 5.12 та рисунка 5.3 можливо зробити висновок, що розподіл повідомлень дійсно підпорядковується експоненціальному розподілу.

Тож, фактор масштабу 2^{32} не впливає на ймовірність отримання різних підписів.

Ми експериментально визначили максимальне значення за модулем для усіх обчислень з плаваючою точкою при с обчисленні ЕП, сформованих за

допомогою еталонної реалізації. Максимальні значення виникають при множенні та діленні комплексних чисел. Для перших 1000 ключів еталонної реалізації максимальне значення менше ніж 2^{36}, тобто значення SCALE = 37, довжина дрібної частини дорівнює 64 – 37 = 27 бітів.

Спроба застосування операцій з фіксованою точкою для масштабу 2^{32} не була успішною, оскільки під цілу частину чисел було виділено занадто мало біт. Експериментально знайдено масштаб 2^{37}, який дозволяє застосовувати фіксовану точку для формування ЕП і захиститися від атаки відновлення ключів [21].

5.6. Рекомендації із застосування комплексної методики оцінки та порівняння постквантових електронних підписів

Комплексна методика оцінки та порівняльного аналізу криптографічних перетворень, стійких до класичного та квантового криптоаналізу спрямована на зручне і точне оцінювання і порівняння алгоритмів квантовостійких криптографічних перетворень з метою вибору найкращого з них для використання та стандартизації у перехідний та постквантовий періоди.

Таким чином, основним застосуванням для неї є обрання найкращих асиметричних квантовостійких криптоперетворень електронного підпису та протоколів інкапсуляції ключів для прийняття в якості стандарта.

Комплексна методика також може бути використана з метою оцінки та порівняльного аналізу інших криптографічних перетворень з мінімальними модифікаціями за умови наявності вимог до них, аналогічних тим, які покладено в основу сформованих безумовних, умовних та прагматичних критеріїв, та даних щодо можливих практичних застосувань порівнюваних криптографічних перетворень.

Додаткові допрацювання, пов’язані із підвищенням точності оцінок порівнюваних криптографічних перетворень шляхом врахування практичних застосувань, для яких проводиться оцінка, надають інструменти для більш

точного підлаштування комплексної методики до впровадження результатів застосування методики на практиці.

Спектр можливих галузей для впровадження результатів використання комплексної методики та самої методики включає в себе:

- стандартизацію асиметричних криптографічних перетворень на різних рівнях;
- обрання для застосування асиметричних криптографічних перетворень в різноманітних інформаційних, комунікаційних та інформаційно-комунікаційних системах та їх складових;
- обрання асиметричних криптографічних перетворень та вимог до них при створенні та впровадженні КСЗІ, СУІБ або інших систем програмних та апаратних рішень, спрямованих на забезпечення безпеки інформації.

При впровадженні комплексної методики оцінки та порівняльного аналізу асиметричних криптографічних перетворень слід враховувати актуальні тенденції в сфері криптології та кібербезпеки та використовувати для оцінки лише актуальні вимоги до безпеки (зокрема це стосується безумовних критеріїв) та актуальні вимоги до безпеки в практичних застосуваннях порівнюваних криптографічних перетворень.

У зв’язку з тим, що практичні використання криптографічних перетворень та вимоги до їх безпеки можуть підлягати значним змінам з часом та розвитком технологій та програмних і апаратних ресурсів доступних порушникам, повинні виконуватись наступні дії для актуалізації методології:

- оцінки, що отримуються методом експертної оцінки, повинні бути отримані від кваліфікованих у сфері кібербезпеки та конкретних її відгалудженнях спеціалістів;
- критерії та варіанти застосування електронних підписів повинні оновлюватись у відповідності до найбільш актуальних вимог у сфері кібербезпеки на час здійснення оцінки та порівняння;

- обрання для застосування асиметричних криптографічних перетворень в різноманітних інформаційних, комунікаційних та інформаційно-комунікаційних системах та їх складових має здійснюватись як складова частина системного впровадження та підтримки безпеки інформації (наприклад, КСЗІ або СУІБ) та бути частиною політики безпеки установи чи підприємства.

5.7. Висновки до розділу 5

1. Вирішено задачі щодо програмного моделювання та експериментальних досліджень процесів оцінки та порівняння існуючих та перспективних квантовостійких криптоперетворень електронного підпису. Для покращення якості порівняння розроблено вдосконалення етапу порівняння за прагматичними критеріями: було обрано набір варіантів застосування алгоритмів асиметричних криптоперетворень з урахуванням як національного так і міжнародного досвіду, проведено оцінювання важливості критеріїв, за якими відбувається порівняння криптоперетворень та проведена корекція фінальної оцінки кожного алгоритму з виокремленям оцінок для всіх обраних варіантів застосування.

2. Враховуючи позицію міжнародної та національної спільноти та з метою охоплення важливих аспектів застосування електронних підписів та різноманітність вимог, було виконанно порівняння наступних криптоперетворень: на основі математики Falcon (Falcon та Сокіл), на основі математики Delithium (Delithium та Вершина), кандидати з додаткового конкурсу на квантовостійкий стандарт електронного підпису (ALTEQ, eMLE-Sig 2.0, KAZ-SIGN, Xifrat1-Sign.I) за такими застосуваннями електронного підпису: PKI, SSL/TLS, SIM-карти, IPSec, DNSSEC, VPN.

3. Було виявлено і підтверджено вплив варіанту застосування на результуючі інтегральні оцінки відібраних алгоритмів, а отже і на найкращий

варіант при порівнянні для використання в різноманітних варіантах застосування електронного підпису. Особливо чітко це видно на прикладі застосування для VPN, де Falcon обходить інші алгоритми. Також за результатами добре видно перевагу вже стандартизованих алгоритмів над кандидатами.

4. В ході дослідження безпеки алгоритмів ЕП було виявлено атаку на на алгоритм ЕП Falcon [19, 21]. Середня ймовірність того, що атака працює становить 76 % випадків для Falcon512 та 70 % випадків для Falcon1024 [19, 21]. Аналіз конкретних випадків показав, що атака на відновлення таємних ключів є можливою, через те, що еталонна реалізація електронного підпису Falcon має два інтерфейси, які використовують різний порядок обчислень.

5. Також було проведено дослідження з метою отримання методів запобігання отримання різних підписів, а отже і захисту від наведеної атаки [21]. Оскільки атака ґрунтується на використанні шуму обчислень з плаваючою точкою, то одним з шляхів захисту є використання операцій з фіксованою точкою замість плаваючої точки. Проте спроба застосування операцій з фіксованою точкою для масштабу 2^{32} не була успішною. Експериментально знайдено масштаб 2^{37}, який дозволяє застосовувати фіксовану точку для формування ЕП і захиститися від атаки відновлення ключів [21].

6. Було сформульовано рекомендації щодо застосування комплексної методики оцінки та порівняння. Так, особливої уваги заслуговує те, що при впровадженні комплексної методики оцінки та порівняльного аналізу асиметричних криптографічних перетворень слід враховувати актуальні тенденції в сфері криптології та кібербезпеки та використовувати для оцінки лише актуальні вимоги до безпеки та актуальні вимоги до безпеки в практичних застосуваннях порівнюваних криптографічних перетворень.

ВИСНОВКИ

В дисертаційній роботі розв’язана актуальна задача аналізу, розробки та покращення методів оцінки та порівняльного аналізу асиметричних електронних підписів та обгрунтування на їх основі національних стандартів асиметричних криптоперетворень електронного підпису.

Для вирішення поставленої наукової задачі використано методи системного аналізу та прийняття рішень, методи прикладної криптології, методи класичного та квантового криптоаналізу, методи оцінки та порівяння асиметричних електронних підписів, що відповідають сучасним вимогам до національних та міжнародних стандартів, методи математичного моделювання, методи захищеності від квантового криптоаналізу на основі масштабування. Чисельні розрахунки на обчислюваній системі виконувалися з використанням середовища розробки Visual Studio Code з процесором 1.6 GHz Intel Core i5 та обсягом оперативної пам’яті 16 ГБ на базі Windows 10. Для здійснення програмного моделювання оцінки безпеки використовувалася мова програмування Python.

Основні наукові та практичні результати, отримані в дисертації.

1. Вперше отримано оцінки порівняльного аналізу вже стандартизованих та кандидатів на стандартизацію квантовостійких ЕП із математичною адаптацією вимог, викликаних особливостями різних варіантів застосування. Попередні дослідження фокусувалися на безпекових вимогах, котрі входять до першого та частково другого етапів комплексної методики оцінки та порівняльного аналізу квантовостійких та перспективних асиметричних криптоперетворень. Отримані оцінки дозволяють більш точно оцінити придатність до використання оцінюваних криптоперетворень в перехідний та пост-квантовий періоди.

2. Удосконалено комплексну методику оцінки та порівняльного аналізу асиметричних ЕП, стійких до класичного та квантового криптоаналізу,

що відрізняється від існуючих тим, що враховує спрямованість та мету здійснення оцінки та порівняльного аналізу та вводить коефіцієнти значущості, котрі збільшують точність визначення найбільш відповідного переможця.

3. Вперше отримано оцінку ймовірності реалізації атаки та впливу виявлених недоліків методу та потенційних векторів атак на захищеність Falcon із врахуванням релевантних моделей безпеки.

4. Обгрунтовано особливостей заміни плаваючої точки на фіксовану точку з метою усунення загрози атаки на відновлення ключів на алгоритм з переліку порівнюваних.

Достовірність результатів дисертаційної роботи забезпечується адекватністю припущень, які лежать в основі проведених наукових досліджень, а також коректним застосуванням відомих математичних методів та методів експертної оцінки. Результати проведених чисельних розрахунків та експерементальних досліджень узгоджуються з отриманими теоретичними висновками.

Значення наукових результатів дисертації для теорії полягає в тому, що отримані результати мають універсальний характер, що дозволяє використовувати їх в подальшому при дослідженні безпеки широкого класу криптографічних перетворень.

Практичне значення роботи. Результати дисертаційних досліджень впровадженні у Приватному акціонерному товаристві «Інститут інформаційних технологій», м. Харків (акт від 06.12.2023 р.) та були використані при розробці стандартів ДСТУ 8961:2019, ДСТУ 9212:2023.

Розроблено програмну реалізацію, яка дозволяє здійснювати частину процесів оцінки та порівняння з комплексної методики в значно розширених масштабах та з більшою точністю оцінки для конкретної мети проведення оцінки. Особливістю розробленої програмної реалізації є її адаптивність. Вона дозволяє використовувати комплексну методику не тільки для порівняння асиметричних ЕП та швидко розширювати кодову базу для інших напрямків.

Розроблені програмні засоби можуть бути корисними як при оцінці безпеки криптографічних перетворень з метою стандартизації, так і при проведенні оцінки та порівняльного аналізу з метою інтеграції їх в інші системи, оскільки кодова база розроблялася з врахуванням можливості подальшого удосконалення та доповнення алгоритмів, варіантів застосувань і критеріїв.

Математичні моделі та аналітичні співвідношення знайшли практичне застосування в ХНУ імені В. Н. Каразіна на кафедрі БІСТ в дисциплінах першого рівня вищої освіти “Прикладна криптологія”, другого рівня освіти “Криптографічні методи в кібербезпеці” та третього рівня освіти «Математичні методи в кібербезпеці» при проведенні лабораторних робіт.

Висновки та рекомендації по науковому та практичному використанню наукових результатів.

1. Отримані експериментальні оцінки вказують на значну перевагу вже стандартизованих ЕП у порівнянні з кандидатами додаткового конкурсу, що дозволяє стверджувати про ефективність порівняння за безумовними критеріями, а отже оцінка за безумовними критеріфми є невід'ємною частиною комплексної методики оцінки та порівняльного аналізу асиметричних ЕП, стійких до класичного та квантового криптоаналізу.

2. Отримані експериментальні оцінки криптографічних перетворень дозволяють стверджувати, що врахування варіанту застосування криптографічного перетворення при проведенні оцінювання, призводить до відмінностей в отримуваних оцінках та загального зниження значень отримуваних оцінок (порядку 1-2 балів, що становить приблизно до 10-20%), що призводить до зміни пріоритетного кандидата в 3 із 6 досліджених варіантів застосування ЕП.

3. Врахування варіантів застосування ЕП дає збільшення точності визначення найкращого алгоритму в більшості ситуацій та може призводити до значних змін в пріоритеті використання. Для застосування в SIM-картах оцінки підписів на базі математики Falcon значно впали через складнощі реалізації таких алгоритмів в умовах обмежених ресурсів. У варіантах застосування для

IPSec та у VPN, оцінки алгоритмів на основі математики Falcon піднімаються і змінюють пріоритетного кандидата в залежності від критеріїв таких як «Можливість і умови вільного поширення» та ін.

4. Запропонована атака відновлення ключів на Falcon та пропозиції з її усунення вказують на необхідність в розробці більш точних та конкретизованих методів оцінки та порівняння криптографічних перетворень для більш швидкого виявлення та усунення недоліків безпеки.

5. Розроблена програмна реалізація підвищувати точність оцінки та порівняння з використанням комплексної методики і буде корисною навіть при оцінці та порівнянні інших криптографічних перетворень та при оцінці та порівнянні з метою інтеграції порівнюваних криптоперетворень в інші системи з незначними допрацюваннями, оскільки вона є адаптивною.

6. Основні наукові та практичні результати дисертаційної роботи реалізовані при розробці стандартів ДСТУ 8961:2019 та ДСТУ 9212:2023, що виконувалася в ПАТ «Інститут Інформаційних Технологій». Отримані результати можуть використовуватися при проведенні експертних досліджень для отримання науково обґрунтованих висновків про можливість застосування в Україні перспективних квантово-стійних алгоритмів асиметричних електронних підписів.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Neal Koblitz, Alfred J. Menezes. A Riddle Wrapped in an Enigma. Cryptology ePrint Archive. URL: https://eprint.iacr.org/2015/1018.pdf .

2. NIST IR 8413. Status Report on the Third Round of the NIST Post-Quantum Cryptography Standardization Process. July 2022 (Updated 9/26/2022). DOI: 10.6028/NIST.IR.8413-upd1.

3. Call for Additional Digital Signature Schemes for the Post-Quantum Cryptography Standardization Process. URL: https://csrc.nist.gov/csrc/media/Projects/pqc-dig-sig/documents/call-for-proposals-dig-sig-sept-2022.pdf

4. Post-Quantum Cryptography: Digital Signature Schemes. Round 1 Additional Signatures. URL: https://csrc.nist.gov/projects/pqc-dig-sig/round-1-additional-signatures

5. Yu.I. Gorbenko, M.V. Yesina, V.A. Ponomar, I.D. Gorbenko, E.Yu. Kapt'ol Scientific and methodological bases of analysis, evaluation and results of comparison of existing and promising (post-quantum) asymmetric cryptographic primitives of electronic signature, protocols of asymmetric encryption and key encapsulation protocols // Ю.І. Горбенко, М.В. Єсіна, В.А. Пономар, І.Д. Горбенко, Є.Ю. Каптьол. Науково-методичні основи аналізу, оцінки та результати порівняння існуючих та перспективних (постквантових) асиметричних криптографічних примітивів електронного підпису, протоколів асиметричного шифрування та протоколів інкапсуляції ключів. Radiotekhnika, 212, 42-66. DOI: https://doi.org/10.30837/rt.2023.1.212.05

6. Горбенко І. Д., Горбенко Ю. І. Прикладна криптологія: Підручник / І. Д. Горбенко, Ю. І. Горбенко. 2-ге видання. Х. : Форт, 2013. – 878 с.

7. Горбенко Ю.І. Методи побудування та аналізу криптографічних систем: монографія. / Ю. І. Горбенко. Х. : Форт, 2015. – 959 с.

8. Gorbenko I.D. Methods of building general parameters and keys for NTRU Prime Ukraine of 5th–7th levels of stability. Product form / I.D. Gorbenko, O.G. Kachko, Yu.I. Gorbenko, I.V. Stelnik, S.O. Kandyi, M.V. Yesina // Telecommunications and Radio Engineering, 2019. – Volume 78, Issue 7 – P. 579-594. DOI: 10.1615/TelecomRadEng.v78.i7.30.

9. Gorbenko I. D. Calculation of general parameters for NTRU Prime Ukraine of 6-7 levels of stability / I. D. Gorbenko, A. N. Alekseychuk, O. G. Kachko, M. V. Yesina, I. V. Stelnik, S. O. Kandy, V. A. Bobukh, V. A. Ponomar // Telecommunications and Radio Engineering, 2019. – Volume 78, Issue 4 – P. 327-340. DOI: 10.1615/TelecomRadEng.v78.i4.40.

10. NIST IR 8105. Report on Post-Quantum Cryptography. April 2016. DOI: 10.6028/NIST.IR.8105.

11. NIST IR 8240. Status Report on the First Round of the NIST Post-Quantum Cryptography Standardization Process. January 2019. DOI: 10.6028/NIST.IR.8240.

12. NIST IR 8309. Status Report on the Second Round of the NIST Post-Quantum Cryptography Standardization Process. July 2020. DOI: 10.6028/NIST.IR.8309.

13. Post-Quantum Cryptography PQC. Selected Algorithms 2022 : web-site. URL: https://csrc.nist.gov/Projects/post-quantum-cryptography/selected-algorithms-2022

14. Post-Quantum Cryptography PQC. Round 4 Submissions. URL: https://csrc.nist.gov/Projects/post-quantum-cryptography/round-4-submissions

15. NIST Special Publication 800-208 Recommendation for Stateful Hash-Based Signature Schemes. / David A. Cooper, Daniel C. Apon, Quynh H. Dang, Michael S. Davidson, Morris J. Dworkin, Carl A. Miller //. – URL: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-208.pdf.

16. ДСТУ 8961:2019 Інформаційні технології. Криптографічний захист інформації. Алгоритми асиметричного шифрування та інкапсуляції

ключів. – URL: http://online.budstandart.com/ua/catalog/doc-page.html?id_doc=88056 .

17. ДСТУ 9212:2023 Інформаційні технології. Криптографічний захист інформації. Алгоритм електронного підпису на алгебраїчних решітках із відхилами. – URL: https://online.budstandart.com/ua/catalog/doc-page.html?id_doc=102150.

18. Kaptiol, Y. Y. (2022). Analysis of the RAINBOW post-quantum electronic signature algorithm state and attacks on it for the period of the NIST PQC third round completion. // Каптьол, Є. Ю. Аналіз стану постквантового алгоритму електронного підпису RAINBOW та атак на нього на період завершення третього раунду NIST PQC. Radiotekhnika, 2(209), 87–92. DOI: https://doi.org/10.30837/rt.2022.2.209.09.

19. Potii, O., Kachko, O., Kandii, S., & Kaptol, Y. (2024). Determining the effect of a floating point on the Falcon digital signature algorithm security. Eastern-European Journal of Enterprise Technologies, 1(9 (127), 52–59. DOI: https://doi.org/10.15587/1729-4061.2024.295160

20. Потій О. В., Качко О. Г., Кандій С. О., Каптьол Є. Ю. Дослідження впливу плаваючої точки на безпеку алгоритму електронного підпису Falcon // Кіберборотьба: розвідка, захист та протидія: тези доповідей II Міжнародної науково-практичної конференції. - Київ: Військовий інститут телекомунікацій та інформатизації імені Героїв Крут, 2024. - 57 с.

21. Kachko O.G., Gorbenko Y.I., Kandii S.O., Kaptol Y.Y. Improving protection of falcon electronic signature software implementations against attacks based on Floating Point Noise // Eastern-European Journal of Enterprise Technologies. 2024. Vol. 4, Is. 9, P. 6–17. DOI:10.15587/1729-4061.2024.310521

22. Gorbenko, I., & Kaptol, Y. (2023). Analysis and comparison of the security of electronic signatures based on new quantum-resistant problems. Radiotekhnika, 4(215), 31–45. https://doi.org/10.30837/rt.2023.4.215.04 .

23. Public Comments on draft FIPS 203. Comment period: August 24, 2023 – November 22, 2023. URL: https://csrc.nist.gov/files/pubs/fips/203/ipd/docs/fips-203-initial-public-comments-2023.pdf

24. Закон України «Про захист інформації в інформаційно-комунікаційних системах». Верховна Рада України. Закон від 05.07.1994 № 80/94-ВР (Із змінами від 28.06.2024). URL: https://zakon.rada.gov.ua/laws/show/80/94-%D0%B2%D1%80#Text .

25. Закон України «Про електронну ідентифікацію та електронні довірчі послуги». Верховна Рада України. Закон від 05.10.2017 № 2155-VIII (Із змінами від 18.12.2024). URL: https://zakon.rada.gov.ua/laws/show/2155-19#Text .

26. Закон України «Про основні засади забезпечення кібербезпеки України». Верховна Рада України. Закон від 05.10.2017 № 2163-VIII (Із змінами від 28.06.2024). URL: https://zakon.rada.gov.ua/laws/show/2163-19#Text .

27. ДСТУ 8845:2019 Інформаційні технології. Криптографічний захист інформації. Алгоритм симетричного потокового перетворення. – URL: http://online.budstandart.com/ua/catalog/doc-page.html?id_doc=82494 .

28. ДСТУ ISO/IEC 14888-3:2014 Інформаційні технології – Методи захисту – Цифрові підписи з доповненням – Частина 3. Механізми, що ґрунтуються на дискретному логарифмі (ISO/IEC 14888-3:2008, IDT). – 113 с.

29. IBM Unveils Breakthrough 127-Qubit Quantum Processor. Hugh Collins, Hugh Collins. Nov 16, 2021. IBM Newsroom. URL: https://newsroom.ibm.com/2021-11-16-IBM-Unveils-Breakthrough-127-Qubit-Quantum-Processor

30. IBM Unveils 400 Qubit-Plus Quantum Processor and Next-Generation IBM Quantum System Two. Hugh Collins, Chris Nay. Nov 9, 2022. IBM Newsroom. URL: https://newsroom.ibm.com/2022-11-09-IBM-Unveils-400-

Qubit-Plus-Quantum-Processor-and-Next-Generation-IBM-Quantum-System-Two

31. The hardware and software for the era of quantum utility is here. Jay Gambetta. Dec 4, 2023. IBM Quantum Research Blog. URL: https://www.ibm.com/quantum/blog/quantum-roadmap-2033

32. IBM Debuts Next-Generation Quantum Processor & IBM Quantum System Two, Extends Roadmap to Advance Era of Quantum Utility. Erin Angelini, Hugh Collins, Dec 4, 2023. IBM Newsroom. URL: https://newsroom.ibm.com/2023-12-04-IBM-Debuts-Next-Generation-Quantum-Processor-IBM-Quantum-System-Two,-Extends-Roadmap-to-Advance-Era-of-Quantum-Utility

33. D-Wave. [Електронний ресурс]. – URL: https://www.dwavesys.com/solutions-and-products/systems/

34. Єсіна М. В. Модель безпеки постквантових протоколів інкапсуляції ключів / М. В. Єсіна // Прикладная радиоэлектроника. - 2018. - Т. 17, № 3-4. - С. 160-167. - URL: http://nbuv.gov.ua/UJRN/Prre_2018_17_3-4_13.

35. ETSI TR 103 619 CYBER; Migration strategies and recommendations to Quantum Safe schemes. July 2020. URL: https://www.etsi.org/deliver/etsi_tr/103600_103699/103619/01.01.01_60/tr_103619v010101p.pdf.

36. ДСТУ 7564:2014 Інформаційні технології. Криптографічний захист інформації. Функція гешування. – URL: http://online.budstandart.com/ua/catalog/doc-page.html?id_doc.66229.

37. ДСТУ 7624:2014 Інформаційні технології. Криптографічний захист інформації. Алгоритм симетричного блокового перетворення. – URL: https://www.twirpx.com/file/2878521/.

38. Горбенко І. Д. Основні положення та результати порівняння властивостей електронних підписів постквантового періоду на алгебраїчних решітках / І. Д. Горбенко, О. Г. Качко, О. В. Потій, А. М.

Олексійчук, Ю. І. Горбенко, М. В. Єсіна, І. В. Стельник, В. А. Пономар // Радіотехніка. – Х. : Харківський національний університет радіоелектроніки, 2021. – Випуск 205. – С. 5-21.

39. Горбенко І. Д. Методи обчислення системних параметрів для електронного підпису «Crystals-Dilithium» 128, 256, 384 та 512 біт рівнів безпеки / І. Д. Горбенко, А. М. Олексійчук, О. Г. Качко, Ю. І. Горбенко, М. В. Єсіна, С. О. Кандій // Радіотехніка. – Х. : Харківський національний університет радіоелектроніки, 2020. – Випуск 202. – С. 5-27.

40. Gorbenko I. D. Algorithms of asymmetric encryption and encapsulation of keys of post-quantum period of 5-7 levels of stability and their application / I. D. Gorbenko, O. G. Kachko, O. M. Aleksiychuk, O. O. Kuznetsov, Yu. I. Gorbenko, V. V. Onoprienko, M. V. Yesina, S. O. Kandy // Радіотехніка. – Х. : Харківський національний університет радіоелектроніки, 2019. – Випуск 198.– С. 5-18.

41. Gorbenko I. D. Generation of general system parameters for Falcon cryptosystem for 256, 384, and 512 security bits / I. D. Gorbenko, S. O. Kandy, M. V. Yesina, Ye. V. Ostryanska // Telecommunications and Radio Engineering, 2022. – Volume 81, Issue 2. – P. 49-59.

42. RFC 5246. The Transport Layer Security (TLS) Protocol Version 1.2. URL: https://datatracker.ietf.org/doc/html/rfc5246

43. RFC 2535. Domain Name System Security Extensions. URL: https://datatracker.ietf.org/doc/html/rfc2535

44. RFC 8551. Secure/Multipurpose Internet Mail Extensions (S/MIME) Version 4.0 Message Specification. URL: https://datatracker.ietf.org/doc/html/rfc8551

45. RFC 8221. Cryptographic Algorithm Implementation Requirements and Usage Guidance for Encapsulating Security Payload (ESP) and Authentication Header (AH). URL: https://datatracker.ietf.org/doc/html/rfc5406

46. Горбенко Ю. І. Модель порушника систем електронних цифрових підписів в умовах квантового криптоаналізу / Ю. І. Горбенко, О. В. Шевцов, Т. Ю. Кузнецова // Радіотехніка. – 2016. – Вып. 186. – С. 53-63.

47. Горбенко Ю. І. Моделі загроз щодо асиметричних криптоперетворень перспективного електронного підпису / Ю. І. Горбенко, М. В. Єсіна, В. В. Онопрієнко, Г. А. Малєєва // Радіотехніка : Всеукр. міжвід. наук.-техн. зб. 2020. Вип. 202. – С. 72-78.

48. IT-Grundschutz-Compendium. Final Draft, 1 February 2022 // Federal Office for Information Security. Germany. – URL: https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Grundschutz/International/bsi_it_gs_comp_2022.pdf?__blob=publicationFile&v=2.

49. Каблак Н.І. «Методологія та методика наукових досліджень» - Методичні вказівки до курсу «Методологія та методи наукових досліджень», Ужгород.: УжНУ, 2019.

50. Порівняльний аналіз властивостей електронних підписів згідно з ДСТУ ISO/IEC 9796-3:2014 / М. В. Єсіна, Н. В. Ковальова, І. Д. Горбенко // Радиотехника. - 2016. - Вып. 186. - С. 160-171. - URL: http://nbuv.gov.ua/UJRN/rvmnts_2016_186_15

51. Горбенко І. Д. Методи, методика та результати порівняльного аналізу електронних підписів згідно ДСТУ ISO/IEC 14888-3:2014 / І. Д. Горбенко, М. В. Єсіна // Вісник Національного університету “Львівська політехніка”: серія “Автоматика, вимірювання та керування”. – Л. : Національний університет “Львівська політехніка”, 2016. – № 852. – С. 9–22.

52. The ALTEQ Signature Scheme: Algorithm Specifications and Supporting Documentation. ALTEQ Specification Document. URL: https://csrc.nist.gov/csrc/media/Projects/pqc-dig-sig/documents/round-1/spec-files/ALTEQ-Spec-web.pdf

53. Gang Tang, Dung Hoang Duong, Antoine Joux, Thomas Plantard, Youming Qiao, and Willy Susilo. Practical post-quantum signature schemes

from isomorphism problems of trilinear forms. In Orr Dunkelman and Stefan Dziembowski, editors, Advances in Cryptology - EUROCRYPT 2022 - 41st Annual International Conference on the Theory and Applications of Cryptographic Techniques, Trondheim, Norway, May 30 - June 3, 2022, Proceedings, Part III, volume 13277 of Lecture Notes in Computer Science, pages 582–612. Springer, 2022.

54. Official Comments (Round 1 Additional Signatures) – ALTEQ. URL: https://csrc.nist.gov/csrc/media/Projects/pqc-dig-sig/documents/round-1/official-comments/ALTEQ-round1-dig-sig-official-comment.pdf

55. eMLE-Sig 2.0: A Signature Scheme based on Embedded Multilayer Equations with Heavy Layer Randomization. eMLE-Sig 2.0 Specification Document. URL: https://csrc.nist.gov/csrc/media/Projects/pqc-dig-sig/documents/round-1/spec-files/eMLE-spec-web.pdf

56. Liu, D.: Embedded multilayer equations: a new hard problem for constructing post-quantum signatures smaller than RSA (without hardness assumption). IACR Cryptol. ePrint Arch. (2021). URL: https://eprint.iacr.org/2021/1338

57. Official Comments (Round 1 Additional Signatures) - eMLE-Sig 2.0. URL: https://csrc.nist.gov/csrc/media/Projects/pqc-dig-sig/documents/round-1/official-comments/emle-sig2.0-round1-dig-sig-official-comment.pdf

58. Kriptografi Atasi Zarah Digital Signature (KAZ-SIGN) Algorithm Specifications and Supporting Documentation. KAZ-SIGN Specification Document. URL: https://csrc.nist.gov/csrc/media/Projects/pqc-dig-sig/documents/round-1/spec-files/kaz-sign-spec-web.pdf

59. KAZ-SIGN PQC Digital Signature Scheme. KAZ-SIGN NIST submissions official site. URL: https://www.antrapol.com/KAZ-SIGN

60. Official Comments (Round 1 Additional Signatures) - KAZ-SIGN. URL: https://csrc.nist.gov/csrc/media/Projects/pqc-dig-sig/documents/round-1/official-comments/KAZ-SIGN-round1-dig-sig-official-comment.pdf

61. NIST Submission: Xifrat1-Sign.I DSS. Xifrat1-Sign.I DSS Specification Document. URL: https://csrc.nist.gov/csrc/media/Projects/pqc-dig-sig/documents/round-1/spec-files/xifrat1-sign-i-spec.pdf

62. Jianfang "Danny" Niu. Resurrecting Xifrat - Compact Cryptosystems 2ndAttempt. URL: https://ia.cr/2022/429

63. Official Comments (Round 1 Additional Signatures) - Xifrat1-Sign.I. URL: https://csrc.nist.gov/csrc/media/Projects/pqc-dig-sig/documents/round-1/official-comments/Xifrat1-Sign-I-round1-dig-sig-official-comment.pdf

64. Bernstein D, Lange T (eds.), eBACS: ECRYPT Benchmarking of Cryptographic Systems - SUPERCOP (2020). URL: https://bench.cr.yp.to/supercop.html.

65. pqm4: Post-quantum crypto library for the ARM Cortex-M4 (2020). URL: https://github.com/mupq/pqm4.

66. Gonzalez R, Hulsing ¨ A, Kannwischer MJ, Kramer ¨ J, Lange T, Stottinger ¨ M, Waitz E, Wiggers T, Yang BY (2021) Verifying post-quantum signatures in 8 kB of RAM. Post-Quantum Cryptography, eds Cheon JH, Tillich JP (Springer International Publishing, Cham), pp 215–233.

67. Beckwith L, Nguyen DT, Gaj K (2022) High-performance hardware implementation of lattice-based digital signatures, Cryptology ePrint Archive, Report 2022/217. URL: https://ia.cr/2022/217.

68. National Institute of Standards and Technology (2016) Submission requirements and evaluation criteria for the post-quantum cryptography standardization process. URL: https://csrc.nist.gov/CSRC/media/Projects/Post-QuantumCryptography/documents/call-for-proposals-final-dec-2016.pdf

69. Tran Thong and B. Liu. (1977). Accumulation of roundoff errors in floating point FFT. IEEE Transactions on Circuits and Systems, 24, 132–143. DOI: 10.1109/TCS.1977.1084316 . Available at: https://www.researchgate.net/publication/3184996_Accumulation_of_roundoff_errors_in_floating_point_FFT

70. Fouque, P., Hoffstein, J., Kirchner, P., Lyubashevsky, V., Pornin, T., Prest, T., Ricosset, T., Seiler, G., Whyte, W., & Zhang, Z. (2019). Falcon: Fast-Fourier Lattice-based Compact Signatures over NTRU. URL: https://www.semanticscholar.org/paper/Falcon%3A-Fast-Fourier-Lattice-based-Compact-over-Fouque-Hoffstein/423e31b1b96ffa0559078961963baeeb98f01e19

71. T. Pornin, "Improved Key Pair Generation for Falcon, BAT and Hawk," Cryptology ePrint Archive (eprint.iacr.org), 2023. Available at: https://eprint.iacr.org/2023/290.

72. Pornin, T., Prest, T. (2019). More Efficient Algorithms for the NTRU Key Generation Using the Field Norm. In: Lin, D., Sako, K. (eds) Public-Key Cryptography – PKC 2019. PKC 2019. Lecture Notes in Computer Science(), vol 11443. Springer, Cham. DOI: https://doi.org/10.1007/978-3-030-17259-6_17.

73. M. Wilk and R. Gnanadesikan, "Probability plotting methods for the analysis of data," Biometrika, vol. 55, no. 1, pp. 1–17, 1968, DOI: https://doi.org/10.1093/biomet/55.1.1.

Додаток А.

СПИСОК ПУБЛІКАЦІЙ ЗДОБУВАЧА ЗА ТЕМОЮ ДИСЕРТАЦІЇ

Наукові публікації у періодичних виданнях, включених до наукометричних баз Scopus

1. Potii, O., Kachko, Potii, O., Kachko, O., Kandii, S., & Kaptol, Y. (2024). Determining the effect of a floating point on the Falcon digital signature algorithm security. Eastern-European Journal of Enterprise Technologies, 1(9 (127), 52–59.
   Keywords: quantum-resistant transformations, lattice-based cryptography, attack on implementation, NIST PQC, NTRU
   DOI: 10.15587/1729-4061.2024.295160 **(Scopus)**
   URL: https://journals.uran.ua/eejet/article/view/295160/291714
2. Kachko O.G., Gorbenko Y.I., Kandii S.O., Kaptol Y.Y. Improving protection of falcon electronic signature software implementations against attacks based on Floating Point Noise // Eastern-European Journal of Enterprise Technologies. 2024. Vol. 4, Is. 9, P. 6–17.
   Keywords: quantum-resistant transformations, Falcon, floating point, NIST PQC, NTRU
   DOI:10.15587/1729-4061.2024.310521 **(Scopus)**
   URL: https://journals.uran.ua/eejet/article/view/310521/302039

Наукові публікації у фахових виданнях України

3. Kaptiol, Y. Y. (2022). Analysis of the RAINBOW post-quantum electronic signature algorithm state and attacks on it for the period of the NIST PQC third round completion. // Каптьол, Є. Ю. Аналіз стану постквантового алгоритму електронного підпису RAINBOW та атак на нього на період завершення третього раунду NIST PQC. Radiotekhnika, 2(209), 87–92.
   Keywords: electronic signature, cryptographic stability, cryptanalysis, quantum cryptanalysis
   DOI: 10.30837/rt.2022.2.209.09

URL: http://rt.nure.ua/article/view/262495/258911

4. Yu.I. Gorbenko, M.V. Yesina, V.A. Ponomar, I.D. Gorbenko, E.Yu. Kapt'ol Scientific and methodological bases of analysis, evaluation and results of comparison of existing and promising (post-quantum) asymmetric cryptographic primitives of electronic signature, protocols of asymmetric encryption and key encapsulation protocols // Ю.І. Горбенко, М.В. Єсіна, В.А. Пономар, І.Д. Горбенко, Є.Ю. Каптьол. Науково-методичні основи аналізу, оцінки та результати порівняння існуючих та перспективних (постквантових) асиметричних криптографічних примітивів електронного підпису, протоколів асиметричного шифрування та протоколів інкапсуляції ключів. Radiotekhnika, 212, 42-66.

   Keywords: post-quantum cryptography, quantum computer, electronic signature, asymmetric encryption protocol, key encapsulation protocol

   DOI: 10.30837/rt.2023.1.212.05

   URL: http://rt.nure.ua/article/view/286512/280398

   (Особистий внесок здобувача: Формування безумовних критеріїв оцінки та порівняння із врахуванням моделей порушника, загроз та безпеки, що базуються на міжнародних вимогах дотримання моделей EUF-CMA для ЕП та IND-CCA2 для АСШ. Аналіз та оцінка за критеріями безумовної стійкості, програмне моделювання процесів оцінки за безумовними критеріями. Особистий внесок Ю.І. Горбенко: Дослідження та вирішення питань впровадження методики оцінки та порівняння квантовостійких криптографічних перетворень за сукупностями безумовних, умовних та прагматичних критеріїв. Особистий внесок М.В. Єсіна: Пошук та формування сукупностей безумовних, умовних та прагматичних критеріїв для процесу оцінки та порівняння. Формування критеріїв вимог у відповідності до міжнародних та національних нормативних документів, таких як NIST.IR 8413 та IT Grundschutz Compedium. Особистий внесок В.А. Пономар: програмне моделювання процесів оцінки за сукупностями умовних та прагматичних критеріїв. Особистий внесок І.Д. Горбенко: постановка

проблеми дослідження, перевірка наукової достовірності отримуваних результатів, перевірка тексту роботи, вибір методів та проведення порівняння за методами експертних оцінок).

5. Є. Ю. Каптьол, І. Д. Горбенко. Аналіз можливостей та особливості програмування задач криптології на квантовому комп'ютері. Radiotekhnika, 202, 37-48.

   Keywords: quantum computer, quantum computer programming, Grover's method, Grover's algorithm, unsorted database search, practical search example, examples of search on a quantum computer

   DOI: 10.30837/rt.2020.3.202.03

   URL: http://rt.nure.ua/article/view/215822/215989

   (Особистий внесок здобувача: Дослідження стану побудови квантових комп'ютерів на предмет оцінки можливості створення криптоаналітично значущого квантового комп'ютера. Виділення математичних методів квантового криптоаналізу для оцінки властивостей існуючих квантових комп'ютерів. Реалізація масштабованого методу квантового криптоаналізу на квантовому комп'ютері. Порівняння теоретичних розрахунків застосування обраного методу з результатами практичного застосування. Особистий внесок І.Д. Горбенко: постановка проблеми дослідження, перевірка наукової достовірності отримуваних результатів, перевірка тексту роботи).

6. Gorbenko, I., & Kaptol, Y. (2023). Analysis and comparison of the security of electronic signatures based on new quantum-resistant problems. Radiotekhnika, 4(215), 31–45.

   Keywords: quantum-resistant cryptography, digital signature, ALTEQ, eMLE-Sig 2.0, KAZ-SIGN, Xifrat1-Sign.I, standardization, NIST

   DOI: 10.30837/rt.2023.4.215.04

   URL: http://rt.nure.ua/article/view/299724/292240

   (Особистий внесок здобувача: Дослідження кандидатів стандартизацію в якості квантовостійкого стандарту електронного підпису на конкурсі NIST

зі стандартизації додаткових електронних підписів. Виділення безумовних критеріїв для оцінки та порівняння кандидатів на стандартизацію, що базуються на нових квантовостійких проблемах. Оцінка та порівняння обраних кандидатів на стандартизацію за безумовними критеріями. Особистий внесок Gorbenko, I.: постановка проблеми дослідження, перевірка наукової достовірностіотримуваних результатів, перевірка тексту роботи).

Наукові праці, які засвідчують апробацію матеріалів дисертації

7. Євгеній Каптьол. Key encapsulation mechanisms security in the random oracle model / Безпека механізмів інкапсуляції ключів у моделі випадкового оракула // “Захист інформації і безпека інформаційних систем” збірник матеріалів IX Міжнародної науково-технічної конференції. Львів – 2023. pp. 67 – 68.
8. Каптьол Є.Ю. Аналіз квантових методів криптоаналізу постквантового електронного підпису Rainbow // “Системи і технології зв’язку, інформатизації та кібербезпеки: актуальні питання і тенденції розвитку” збірник матеріалів I Міжнародної науково-технічної конференції. Київ – 2021. pp. 146 – 147.
9. Yevhenii Kaptol. Analysis of quantum attacks against rainbow post-quantum electronic signature // Information protection and information systems security proceedings of VIIIth International Scientific and Technical Conference November 11–12, 2021. Lviv Polytechnic Publishing House 2021. pp. 77-78.
10. Каптьол. Є.Ю. Порівняння електронних підписів, що грунтуються на нових постквантових проблемах // Системи і технології зв’язку, інформатизації та кібербезпеки: актуальні питання і тенденції розвитку: збірник матеріалів III Міжнародної науково-технічної конференції. - Київ: Військовий інститут телекомунікацій та інформатизації імені Героїв Крут, 2023, pp. 166-167 DOI: https://doi.org/10.61929/viti.mntk.3.2023

11. Потій О. В., Качко О. Г., Кандій С. О., Каптьол Є. Ю. Дослідження впливу плаваючої точки на безпеку алгоритму електронного підпису Falcon // Кіберборотьба: розвідка, захист та протидія: тези доповідей II Міжнародної науково-практичної конференції. - Київ: Військовий інститут телекомунікацій та інформатизації імені Героїв Крут, 2024.-57с.

Додаток Б

АКТ ВПРОВАДЖЕННЯ РЕЗУЛЬТАТІВ ДИСЕРТАЦІЙНОЇ РОБОТИ у Приватному акціонерному товаристві «Інститут інформаційних технологій»

«ЗАТВЕРДЖУЮ»
Виконавчий директор
АТ «ІІТ»
_____ В.Д. Кравченко
«06» 12 2023 р.

АКТ

впровадження результатів дисертаційної роботи
на здобуття ступеня доктора філософії
Каптьола Євгенія Юрійовича
у Приватному акціонерному товаристві «Інститут інформаційних технологій»

Комісія у складі голови комісії, наукового співробітника АТ «ІІТ», кандидата технічних наук Єсіної Марини Віталіївни та членів комісії, інженера-конструктора АТ «ІІТ» Єлакова Сергія Геннадійовича та наукового співробітника АТ «ІІТ» Кандія Сергія Олеговича встановила, що у Приватному акціонерному товаристві «Інститут інформаційних технологій» впроваджені та використані наступні результи досліджень Каптьола Євгенія Юрійовича.

1. Результати використані та впроваджені в Науково-дослідних роботах «Скіл», «Імпульс» та «Стохід». в частині обгрунтування та розробки за його участі проектів стандартів «Скеля» та «Вершина», які наразі уже є затвердженими національними стандартами ДСТУ 8961:2019 «Інформаційні технології. Криптографічний захист інформації. Алгоритми асиметричного шифрування та інкапсуляції ключів»; ДСТУ 9212:2023 «Інформаційні технології. Криптографічний захист інформації. Алгоритм електронного підпису на алгебраїчних решітках із відхилами».

Голова комісії:
науковий співробітник АТ «ІІТ», к.т.н. _____ Марина ЄСІНА

Члени комісії:
інженер-конструктор АТ «ІІТ» _____ Сергій ЄЛАКОВ

науковий співробітник АТ «ІІТ» _____ Сергій КАНДІЙ

Додаток В

ЛІСТІНГ КОДУ ЧАСТИНИ МОДЕЛІ МОДИФІКАЦІЇ ПРОЦЕСУ ОЦІНКИ ТА ПОРІВНЯННЯ ЕЛЕКТРОННИХ ПІДПИСІВ

```
signatures_names = ["Falcon", "Сокіл", "Delithium", "Вершина", "ALTEQ", "eMLE-Sig
2.0", "KAZ-SIGN", "Xifrat1-Sign.I"]
falcon = [1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12]
sokil = [1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12]
delithium = [1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12]
vershina = [1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12]
alteq = [1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12]
emle = [1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12]
kaz = [1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12]
xifrat = [1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12]
signatures_values = [falcon, sokil, delithium, vershina, alteq, emle, kaz, xifrat]
criteria_names = ["Додаткові властивості безпеки", "Вимоги до стійкості", "Помилки
шифрування", "Можливість багаторазового застосування", "Гнучкість і простота",
                  "Коректність та оптимізація", "Ефективність та час проведення
перетворень", "Тестування неосновних умов використання", "Можливість і умови вільного
поширення",
                  "Рівень довіри на різних рівнях застосування", "Перспективність та
виправданість застосування", "Легкість у використанні та інтеграції"]
use_cases_names = ["SSL/TLS", "SIM-карти", "IPSec", "DNSSEC", "VPN", "Підписання
PDF"]
ssltls = [1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12]
sim = [1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12]
ipsec = [1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12]
dnssec = [1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12]
vpn = [1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12]
pdf = [1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12]
use_cases_expert_marks = [ssltls, sim, ipsec, dnssec, vpn, pdf]

integral_ssltls = [1, 1, 1, 1, 1, 1, 1, 1]
integral_sim = [1, 1, 1, 1, 1, 1, 1, 1]
integral_ipsec = [1, 1, 1, 1, 1, 1, 1, 1]
integral_dnssec = [1, 1, 1, 1, 1, 1, 1, 1]
integral_vpn = [1, 1, 1, 1, 1, 1, 1, 1]
integral_pdf = [1, 1, 1, 1, 1, 1, 1, 1]
integral_per_use_case = [integral_ssltls, integral_sim, integral_ipsec,
integral_dnssec, integral_vpn, integral_pdf]

a = 0


def compare_entities():
    n = int(input("Введіть кількість сутностей: "))
    m = int(input("Введіть кількість параметрів: "))

    entities = []
    for i in range(n):
        print(f"Введіть значення параметрів для сутності {i + 1}:")
        entity = [float(input(f"Параметр {j + 1}: ")) for j in range(m)]
        entities.append(entity)

    print("Введіть значення коефіцієнтів значущості для кожного параметра:")
    coefficients = [float(input(f"Коефіцієнт для параметра {i + 1}: ")) for i in
range(m)]

    weighted_entities = []
```

```
    for entity in entities:
        weighted_values = [param * coeff for param, coeff in zip(entity,
coefficients)]
        weighted_entities.append(weighted_values)

    sorted_entities = sorted(weighted_entities, key=lambda x: x[0], reverse=True)

    print("Список сутностей з отриманими значеннями:")
    for i, entity in enumerate(sorted_entities):
        print(f"Сутність {i + 1}: {entity}")

if __name__ == "__main__":
    print("Список алгоритмів:")
    print("1) Falcon")
    print("2) Сокіл")
    print("3) Delithium")
    print("4) Вершина")
    print("5) ALTEQ")
    print("6) eMLE-Sig 2.0")
    print("7) KAZ-SIGN")
    print("8) Xifrat1-Sign.I")
    print("")

    print("Список варіантів застосування:")
    print("1) SSL/TLS")
    print("2) SIM-карти")
    print("3) IPSec")
    print("4) DNSSEC")
    print("5) VPN")
    print("6) Підписання PDF")
    print("")

    print("Список критеріїв:")
    print("1) Додаткові властивості безпеки")
    print("2) Вимоги до стійкості")
    print("3) Помилки шифрування")
    print("4) Можливість багаторазового застосування")
    print("5) Гнучкість і простота")
    print("6) Коректність та оптимізація")
    print("7) Ефективність та час проведення перетворень")
    print("8) Тестування неосновних умов використання")
    print("9) Можливість і умови вільного поширення")
    print("10) Рівень довіри на різних рівнях застосування")
    print("11) Перспективність та виправданість застосування")
    print("12) Легкість у використанні та інтеграції")
    print("")


    for j in range(6):
        for k in range(8):
            for i in range(12):
                a = (signatures_values[k][i]*use_cases_expert_marks[j][i])/10


                print(f"{signatures_names[k]};      {use_cases_names[j]};
критерій {i+1}")
                print(f"{a}")
                print("")
                integral_per_use_case[j][k] += a
            print(f"{integral_per_use_case[j][k]/12}")
            print("")


    integral_per_use_case
    compare_entities()
```

Онлайн сервіс створення та перевірки кваліфікованого та удосконаленого електронного підпису

ПРОТОКОЛ
створення та перевірки кваліфікованого та удосконаленого електронного підпису

Дата та час: 10:02:42 18.03.2025

Назва файлу з підписом: Каптьол_дисертація_підписана.pdf
Розмір файлу з підписом: 3.7 МБ

Назва файлу без підпису: Каптьол_дисертація_підписана.verified.pdf
Розмір файлу без підпису: 3.7 МБ

Результат перевірки підпису: Підпис створено та перевірено успішно. Цілісність даних підтверджено

Підписувач: КАПТЬОЛ ЄВГЕНІЙ ЮРІЙОВИЧ
П.І.Б.: КАПТЬОЛ ЄВГЕНІЙ ЮРІЙОВИЧ
Країна: Україна
РНОКПП: 3558312978
Організація (установа): ФІЗИЧНА ОСОБА
Час підпису (підтверджено кваліфікованою позначкою часу для підпису від Надавача): 19:44:26 17.03.2025
Сертифікат виданий: КНЕДП АЦСК АТ КБ "ПРИВАТБАНК"
Серійний номер: 5E984D526F82F38F040000008E5EBD01DDCF1F06
Тип носія особистого ключа: ЗНКІ криптомодуль ІІТ Гряда-301
Серійний номер носія особистого ключа: 020
Алгоритм підпису: ДСТУ 4145
Тип підпису: Кваліфікований
Тип контейнера: Підпис та дані в одному файлі (CAdES enveloped)
Формат підпису: З позначкою часу від ЕП (CAdES-T)
Сертифікат: Кваліфікований

Версія від: 2025.01.15 13:00