DOI 10.31891/2307-5732-2025-347-63
УДК 519.7

ПЕТРУШКО ІРИНА
ДВНЗ «Ужгородський національний університет»
https://orcid.org/0009-0008-2303-7427
e-mail: irina.petrushko@uzhnu.edu.ua
ПОЛІЩУК ВОЛОДИМИР
ДВНЗ «Ужгородський національний університет»
https://orcid.org/0000-0003-4586-1333
e-mail: volodymyr.polishchuk@uzhnu.edu.ua
МАТЕЙ АНДРІЙ
ДВНЗ «Ужгородський національний університет»
https://orcid.org/0009-0001-0280-1763
e-mail: andrej.matey@uzhnu.edu.ua

ПОСТКВАНТОВА КРИПТОГРАФІЯ: ВИКЛИКИ ТА ПЕРСПЕКТИВИ РОЗРОБКИ КВАНТОВО-СТІЙКИХ АЛГОРИТМІВ ДЛЯ ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ ІНФОРМАЦІЙНИХ СИСТЕМ

Розвиток квантових комп'ютерів є однією з найвизначніших технологічних подій сучасності, що відкриває нові горизонти в обчислювальних можливостях. Однак це також створює серйозні загрози для існуючих криптографічних алгоритмів, які є основою безпеки сучасних інформаційних систем. В роботі наведено результати досліджень постквантової криптографії та її ролі у забезпеченні інформаційної безпеки в умовах розвитку квантових комп'ютерів. Метою даної роботи є порівняння сучасних постквантових, тобто, квантово-стійких криптографічних алгоритмів, оцінка їх застосовності для різного класу задач, а також прогнозування шляхів розвитку криптографічних методів захисту інформації. Для досягнення поставленої мети застосовуються методи порівняльного аналізу та математичного моделювання, що дозволяють оцінити ефективність та безпеку алгоритмів у різних умовах. Результати дослідження показують, що постквантові алгоритми забезпечують надійний захист інформації в умовах потенційних квантових атак, зберігаючи при цьому високий рівень ефективності. У висновках підкреслюється необхідність адаптації існуючих криптографічних систем до нових вимог безпеки, зокрема через інтеграцію постквантових алгоритмів у хмарні сервіси та блокчейн-технології. Результати досліджень можуть бути використані для вдосконалення механізмів захисту даних в інформаційних системах та для розвитку нових стандартів криптографії в еру квантових обчислень.

Ключові слова: постквантова криптографія; квантово-стійкі алгоритми; криптографічна безпека; квантові атаки; інформаційні системи.

PETRUSHKO IRYNA,
POLISHCHUK VOLODYMYR,
MATEI ANDRIY
Uzhhorod National University

POST-QUANTUM CRYPTOGRAPHY: CHALLENGES AND PROSPECTS FOR DEVELOPING QUANTUM-STABLE ALGORITHMS TO ENSURING THE SECURITY OF INFORMATION SYSTEMS

The development of quantum computers is one of the most significant technological developments of our time, opening new horizons in computing capabilities. However, it also poses serious threats to existing cryptographic algorithms, which are the basis of the security of modern information systems. The paper presents the results of research on post-quantum cryptography and its role in ensuring information security in the context of the development of quantum computers. The purpose of this paper is to compare modern post-quantum, i.e., quantum-stable cryptographic algorithms, assess their applicability for different classes of tasks, and predict the development paths of cryptographic methods for information protection. To achieve this goal, methods of comparative analysis and mathematical modeling are used, which allow for assessing the effectiveness and security of algorithms in different conditions. The study results show that post-quantum algorithms provide reliable information protection in the context of potential quantum attacks while maintaining a high-efficiency level. The conclusions emphasize the need to adapt existing cryptographic systems to new security requirements, particularly through integrating post-quantum algorithms into cloud services and blockchain technologies. The research results can be used to improve data protection mechanisms in information systems and to develop new cryptographic standards in the era of quantum computing. Therefore, plans for future research are outlined, namely: the effectiveness of implementing post-quantum algorithms in various industries, including finance, medicine, and government, will be analyzed; methods for optimizing cryptographic systems will be developed to ensure a balance between security and performance; new mathematical approaches will be studied that can be used to create quantum-resistant algorithms.

Keywords: post-quantum cryptography; quantum-stable algorithms; cryptographic security; quantum attacks; information systems.

Постановка проблеми у загальному вигляді та її зв'язок із важливими науковими чи практичними завданнями

Розвиток квантових комп'ютерів є однією з найвизначніших технологічних подій сучасності, що відкриває нові горизонти в обчислювальних можливостях. Однак це також створює серйозні загрози для існуючих криптографічних алгоритмів, які є основою безпеки сучасних інформаційних систем. Традиційні алгоритми, такі як RSA, DSA, та алгоритми на основі дискретного логарифмування, базують свою стійкість на обчислювальній складності певних математичних задач. Наприклад, RSA спирається на труднощі розкладання великих цілих чисел на прості множники, що досі вважалося обчислювально нездійсненним у прийнятний час [1].

Проте з появою квантових алгоритмів, таких як алгоритм Шора, ефективне розкладання великих чисел стало потенційно можливим, що ставить під загрозу криптографічну стійкість цих систем. Аналогічно, алгоритм Гровера значно скорочує час пошуку в невпорядкованій базі даних, що може бути використано для злому криптографічних хеш-функцій (наприклад, MD5, SHA-1, SHA-2, SHA-3) [2]. Наприклад, хеш-функція SHA-256, яка забезпечує криптографічну стійкість у традиційних системах, може бути скомпрометована потужним квантовим комп'ютером за допомогою алгоритму Гровера всього за 2^128 операцій.

Крім того, алгоритми на основі дискретного логарифмування, такі як Ель-Гамаль, які використовуються для електронного підпису та шифрування даних, також піддаються атакам із використанням модифікованих версій алгоритму Шора [3,4]. Це створює нагальну потребу у переосмисленні підходів до захисту інформації, оскільки ключові технології цифрової безпеки можуть втратити свою ефективність з розвитком квантових обчислень.

Для проактивного реагування на ці виклики постає новий напрям у криптографії – постквантова криптографія. Вона спрямована на розробку алгоритмів, стійких до атак як із використанням традиційних, так і квантових комп'ютерів. Постквантові алгоритми ґрунтуються на математичних задачах, які залишаються складними навіть для квантових обчислень, таких як теорія решіток, кодування, ізогенії еліптичних кривих тощо.

З огляду на швидкість розвитку квантових технологій і їхній потенціал у сфері безпеки, дослідження постквантових алгоритмів є не лише актуальним, а й критично важливим для забезпечення безпеки інформаційних систем у майбутньому.

Аналіз досліджень та публікацій

Постачальники хмарних сервісів, такі як AWS та Google Cloud, уже активно інтегрують постквантові криптографічні алгоритми у свої системи для захисту даних від загроз, з використанням квантових комп'ютерів. Зокрема, Google Cloud зосереджується на впровадженні алгоритмів, затверджених Національним інститутом стандартів і технологій (NIST). Наприклад, Google використовує постквантові алгоритми для захисту своїх сервісів, таких як Chrome та Android. Зараз ведеться адаптація таких алгоритмів, як Kyber, для своїх хмарних рішень, зокрема у протоколах Transport Layer Security (TLS) [3, 4]. Здійснено теоретико-множинний аналіз сучасних досліджень перспективи розвитку постквантових алгоритмів та встановлено параметри та оптимальність їх застосування. Результати наведені у Таблиці 1.

Таблиця 1

Оптимальність застосування та перспективи розвитку постквантових алгоритмів

Алгоритм	Математична основа базового алгоритму	Розмір відкритого/закритого ключа, Кб	Швидкість генерації пари ключів, мс	Швидкість зашифровування/ розшифровування, мс	Оптимальність застосування	Перспективи розвитку
Kyber (lattice-based)	Варіація задачі Learning with Errors (LWE): «кільцевих решіток», зокрема, схем з підписами та шифруванням на основі операцій з поліномами над кільцями. [6]	~0,8/0,05	~10	~2 /2	IoT, Blockchain, Cloud	Перспективи для широкого використання в блокчейні та IoT [5,6]
NTRU (lattice-based)	Операції з поліномами в кільцях, де шифрування і підписання базуються на важких для розв'язування задачах, таких як проблема пошуку коротких векторів в решітках. [7]	~1-2 /1	~50	~5 /10	Cloud, IoT, Edge computing	Підходить для мобільних і IoT пристроїв, має перспективи для хмарних технологій
FrodoKEM (lattice-based)	Псевдовипадкових матриць для симуляції «зашумлених» лінійних рівнянь алгоритму Learning with Errors (LWE) [8]	~1.5 /1	~30	~5 /10	Cloud, Blockchain, IoT	Тестується для великомасштабних застосувань

Продовження таблиці 1

SABER (lattice-based)	Задача Learning With Rounding (LWR), яка є варіантом класичної Learning With Errors (LWE), але з модифікацією, де "шум" (помилка) додається через округлення замість явного додавання випадкових помилок. Простий та ефективний [9].	~1-2/1	~60	~10 /12	IoT, Blockchain, Cloud	Потенціал для масштабованих застосувань в Edge computing
NTS-KEM (lattice-based)	Інформаційним декодуванням з помилками" (ISD) [10]	~1/1	~40	~8 /12	Blockchain, IoT, Cloud	Обіцяє хороші результати в забезпеченні безпеки в IoT
Post-Quantum RSA (hash-based)	Мерклівські дерева, де значення хешів побудовані від листових вузлів до кореневого хешу, який виступає в ролі підпису [11]	~2/1.5	~100	~15/ 20	Блокчейн, Digital signatures	Перспективи для інтеграції в системи аутентифікації
XMSS (hash-based)	Мерклівські дерева, де кожен лист дерева є результатом хешування. Кожен підпис є одноразовим, причому кожен підпис використовував новий підписний ключ [12]	~2-3/2	~250	~10 / 20	Digital signatures, IoT	Підходить для підвищення безпеки в підписах, перспективи для баз даних
SIKE (isogeny-based)	Властивість ізогенійних графів, утворених супер сингулярними еліптичними кривими, які обрані на скінченних полях, що є складною задачею навіть для квантових комп'ютерів [13]	~0.300-0.400/0.2	~80	~7 / 10	Blockchain, Cloud, Databases	Розвиток для високої безпеки в блокчейні та цифрових підписах

В даній таблиці приведено основні кількісні показники для восьми найсучасніших постквантових криптографічних механізмів, а також можливості їх застосування в IoT (інтернет речей) , базах даних, блокчейн-технологіях, хмарних і туманних обчисленнях.

Формулювання цілей статті

Метою роботи є: порівняння сучасних постквантових, тобто, квантово-стійких криптографічних алгоритмів, оцінка їх застосовності для різного класу задач, а також прогнозування шляхів розвитку криптографічних методів захисту інформації.

У зв’язку із вище наведеним можна сформулювати такі наукові питання дослідження:

1. Які основні загрози існуючим криптографічним алгоритмам становлять квантові комп'ютери, і як постквантові алгоритми можуть забезпечити безпеку даних?

Які перспективи розвитку постквантових криптографічних механізмів, зокрема на основі решіток, ізогеній та кодів, для забезпечення стійкості до квантових атак?

Виклад основного матеріалу

Представимо формальну постановку задачі розробки квантово-стійких алгоритмів для забезпечення безпеки інформаційних систем. Нехай дано систему криптографічних алгоритмів $A=\{A_1, A_2, \ldots, A_n\}$, де кожен A_i є стандартним криптографічним алгоритмом (наприклад, RSA, AES, SHA), що забезпечує захист інформації. Нехай також $K=\{K_1, K_2, \ldots, K_n\}$ – множина ключів, що використовуються цими алгоритмами, де K_i – це ключ, необхідний для роботи алгоритму A_i. Перш за все відбувається оцінка ймовірності успішного злому традиційних криптографічних алгоритмів за допомогою квантових алгоритмів, наприклад таких як алгоритми Шора та Гровера: $Q(A_i, K_i)$=Pr(успішний злому A_i за допомогою квантового алгоритму). Після цього, потрібно здійснити створення алгоритмів на основі математичних задач, стійких до квантових атак:

1. Решітки. Задача найкоротшого вектора (SVP) або задача найкоротшого вектора з обмеженнями (GapSVP). Формалізація для найкоротшого вектора:

$$\text{SVP: } |v|,\ v \in \Lambda \tag{1}$$

де Λ – решітка, v – вектор, для якого мінімізується його норма $|v|$.

2. Ізогенії. Використання ізогеній між еліптичними кривими. Задача полягає в побудові криптографічних систем, які використовують ізогенії:

$$I=\{\varphi: E_1 \rightarrow E_2\}, \tag{2}$$

де E_1 і E_2 – еліптичні криві, а φ – ізогенія між ними.

3. Кодові алгоритми. Використання кодування, зокрема Гоппа кодів (McEliece). Задача полягає у створенні алгоритмів, стійких до квантових атак за допомогою кодів:

$$C=\{C_1, C_2, \ldots, C_n\}\ . \tag{3}$$

Де C_i – код для шифрування та підпису.

Задача полягає оптимізувати алгоритм з точки зору безпеки та ефективності при великих обсягах даних.

Далі відбувається інтеграція квантово-стійких алгоритмів в існуючі криптографічні системи. Для цього необхідно розробити методи, що забезпечують збереження сумісності з класичними системами. Формулювання задачі інтеграції:

$$H(A_c, A_q)=\{\text{Алгоритм класичної криптографії}\}+\{\text{Алгоритм квантово-стійкої криптографії}\}, \tag{4}$$

де A_c – класичний криптографічний алгоритм, A_q – постквантовий алгоритм. Завдання полягає в розробці гібридних схем, які забезпечують стійкість до квантових атак і при цьому не вимагають кардинальних змін у системах.

Після цього, потрібно здійснити оптимізацію ефективності квантово-стійких алгоритмів. Задача полягає в мінімізації витрат на обчислення та зберігання для нових квантово-стійких алгоритмів, зокрема для алгоритмів на основі решіток та ізогеній.

Таким чином, основна задача полягає в розробці квантово-стійких криптографічних алгоритмів, здатних забезпечити високий рівень безпеки інформаційних систем у квантовій епосі, оптимізуючи їх ефективність і забезпечуючи сумісність з існуючими системами.

Далі, розглядаються найбільш ефективні сучасні квантово-стійкі алгоритми, які є фіналістами сертифікації і тестування NIST (Національним інститутом стандартів і технологій) з метою їх впровадження в наявні криптографічні системи.

Алгоритми на основі решіток (lattice based) це клас криптографічних алгоритмів, що базуються на математичних задачах теорії решіток [5,6], таких як проблема найкоротшого вектора (SVP) або проблема найкоротшого вектора з обмеженнями (GapSVP). Решітка визначається як дискретна множина точок у багатовимірному просторі, які формуються лінійними комбінаціями базисних векторів із цілими коефіцієнтами. Іншими словами як множина всіх лінійних комбінацій базисних векторів з цілими коефіцієнтами.

Базове математичне визначення решітки:

$$\Lambda=\{\Sigma z_i b_i : z_i \in Z\}, \tag{5}$$

Де: Λ – решітка; $b_1, b_2, \ldots, b_m$ – базисні вектори решітки; m – кількість базисних векторів; $z_i \in Z$ – цілі коефіцієнти.

Розвиток постквантових криптографічних механізмів триває, і хоча багато алгоритмів вже потрапили на етап NIST сертифікації, є кілька нових перспективних підходів, які ще не отримали широкого визнання. Розглянемо кілька таких напрямів для розуміння перспектив розвитку квантово-стійкої криптографії.

1)Алгоритми на основі ізогеній (Isogeny-Based Cryptography)

Ізогенії — це математичні функції між еліптичними кривими, які використовуються для створення нових криптографічних механізмів. Наприклад, SIKE (Supersingular Isogeny Key Encapsulation) вже навіть проходить NIST сертифікацію і продовжує розвиватися. Даний алгоритм має потенціал стати основою для більш безпечних систем, оскільки характеризується малим розміром ключів та високою ефективність навіть при великих обсягах оброблюваної інформації, а також має високі обчислювальні витрати.

2) Алгоритми на основі квантових мереж та квантового розподілу ключів (Quantum Network-Based Cryptography, Quantum Key Distribution)

базуються на інтеграції криптографії з квантовими мережами. Хоча ця технологія вже розвивається в лабораторіях, її реальне застосування вимагає значних інвестицій у інфраструктуру та нові апаратні засоби.

3) Механізми на основі кодування та парних кодів (Code-Based and Pairing-Based Cryptography), зокрема Гоппа (Goppa) кодах, є цікавими через свою стійкість до квантових атак. Наприклад, McEliece — один із найстаріших кодових механізмів, який продовжує вдосконалюватися для постквантового середовища. Інші варіанти, як Niederreiter або Fujisaki-Okamoto, обіцяють високу безпеку при достатньо великих ключах.

4) Гібридні підходи (Hybrid Cryptography) поєднують класичні і постквантові алгоритми, можуть бути використані для забезпечення стійкості до квантових атак при збереженні сумісності з існуючими

системами (наприклад, SHA-256). Зазначимо наявність складності інтеграції, а також необхідність подвійного управління ключами при використанні даних підходів.

5) Алгоритми на основі матриць (Matrix-Based Cryptography).

6) Фізична криптографія на основі топології (Topology-Based Cryptography) використовує топологічні структури (наприклад категорії або гомологічні простори) для створення нових квантово-стійких криптографічних систем. Зазначимо, що це новий і недостатньо вивчений напрямок

Ці нові підходи можуть стати основою для майбутнього розвитку постквантових криптографічних механізмів, але потребують подальших досліджень і оптимізації перед широким впровадженням.

Таким чином, під час проведеного дослідження було отримано відповіді на поставлені наукові питання.

Що стосується першого питання, стосовно загроз квантових комп'ютерів для існуючих криптографічних алгоритмів, можемо відмітити наступне. Квантові комп'ютери становлять значну загрозу для традиційних криптографічних алгоритмів, таких як RSA, які базуються на складності факторизації великих чисел, і хеш-функцій, таких як SHA, стійкість яких залежить від складності пошуку передумови хешу. Квантовий алгоритм Шора здатний ефективно розкладати числа на прості, а алгоритм Гровера може значно прискорити процес пошуку у невпорядкованих базах даних, що робить ці криптографічні методи вразливими до атак.

Постквантова криптографія пропонує рішення у вигляді алгоритмів, стійких до квантових атак. Сучасні постквантові алгоритми, такі як ті, що засновані на решітках, ізогеніях та кодах, використовують математичні проблеми, які квантові комп'ютери не можуть вирішити за розумний час. Алгоритми, засновані на решітках, зокрема, заважають вирішенню проблеми найкоротшого вектора, що забезпечує криптографічну стійкість. Крім того, ізогенії, як показує приклад SIKE, мають потенціал для забезпечення безпеки з малим розміром ключів і високою ефективністю навіть при великих обсягах даних. Так, технології оцінки втоми інтегруються в систему Інтернет речей (IoT) для моніторингу психо-фізіологічного стану диспетчерів [16] в поєднанні з постквантовою криптографією може бути використано для підсилення безпеки даних, що передаються між різними сенсорами, пристроями та централізованими системами, гарантуючи захист від квантових атак.

Що стосується другого питання, то перспективи розвитку постквантових криптографічних механізмів мають значний потенціал, оскільки квантові комп'ютери все більше наближаються до здатності зламувати існуючі криптографічні алгоритми. Алгоритми на основі решіток, такі як криптографічні схеми, що використовують проблеми найкоротшого вектора, продовжують удосконалюватися і мають високий рівень стійкості до квантових атак. Зокрема, алгоритми, засновані на решітках, здатні забезпечити не тільки безпеку даних, але й ефективність роботи при великих розмірах ключів.

Ізогенії, зокрема алгоритм SIKE, вже проходять етапи сертифікації в рамках NIST, що свідчить про їх потенціал у створенні безпечних квантово-стійких криптографічних систем. Ізогенії можуть запропонувати малі розміри ключів, що робить їх привабливими для використання в середовищах з обмеженими ресурсами.

Кодова криптографія, зокрема механізм McEliece, є ще одним перспективним напрямком, оскільки вона продовжує вдосконалюватися для постквантового середовища, забезпечуючи високу стійкість навіть при великих ключах. Інші варіанти, як Niederreiter або Fujisaki-Okamoto, обіцяють подальше підвищення безпеки.

Однак, для широкого впровадження цих технологій, потрібно буде вирішити кілька питань, зокрема щодо обчислювальних витрат і оптимізації систем для реальних умов використання, а також інвестувати в розробку нових апаратних і програмних засобів для підтримки таких алгоритмів. Підсумовуючи зазначимо необхідність творчих підходів при підготовці фахівців, готових свідомо використовувати наявні квантовоо-стійкі алгоритми, атакож працювати над розробкою нових алгоритмів для проактивного захисту інформаційно-комунікаційних систем [17].

Висновки з даного дослідження
і перспективи подальших розвідок у даному напрямі

Під час дослідження вперше проаналізовано сучасні постквантові криптографічні алгоритми, які здатні забезпечити стійкість до атак як із використанням класичних, так і квантових комп'ютерів. Отримані результати дозволяють зробити висновок, що кожен із запропонованих підходів має свої переваги та обмеження, і їхній вибір залежить від конкретних умов застосування.

Прогнозування розвитку криптографічних методів захисту інформації вказує на необхідність подальших досліджень для оптимізації існуючих рішень та інтеграції їх у наявні інформаційні системи. Зокрема, перспективним є проактивне впровадження алгоритмів із високою обчислювальною ефективністю, такими як алгоритми на основі решіток та ізогеній, а також розробка нових гібридних підходів, що поєднують класичні та постквантові технології. Тому окреслені плани на майбутні дослідження, а саме: буде проаналізовано ефективності впровадження постквантових алгоритмів у різних галузях, зокрема фінансовій, медичній та державній; буде розроблено методи оптимізації криптографічних систем для забезпечення балансу між безпекою та продуктивністю; буде здійснено

дослідження нових математичних підходів, які можуть бути використані для створення квантово-стійких алгоритмів. Важливим, також, є необхідність осучаснення навчальних планів ВНЗ, які готують фахівців з кібербезпеки для їх подальшої успішної роботи у умовах квантової епохи.

Таким чином, постквантова криптографія є ключовим напрямком забезпечення безпеки інформаційних систем у майбутньому, а її розвиток вимагає комплексного підходу, що включає фундаментальні дослідження, практичну реалізацію та інтеграцію з існуючими технологіями.

Література

1. Pilatte, S. (2024). Unconditional correctness of recent quantum algorithms for factoring and computing discrete logarithms. *Cryptology ePrint Archive*, (629). Retrieved from https://eprint.iacr.org/2024/629
2. Preston, R. (2022). Applying Grover's algorithm to hash functions: A software perspective. *IEEE Transactions on Quantum Engineering, 3*. https://doi.org/10.1109/TQE.2022.3233526
3. Proos, J., & Zalka, C. (2003). Shor's discrete logarithm quantum algorithm for elliptic curves. *Quantum Information and Computation, 3*(4), 317–344. https://doi.org/10.26421/QIC3.4-3
4. Новиков, Д., & Полторак, В. (2023). Технології постквантової криптографії. *Адаптивні системи автоматичного управління, 1*(42), 171–183. https://asac.kpi.ua/article/view/279169/273748
5. Wang, T., Zhang, C., Zhang, X., Gu, D., & Cao, P. (2024). Optimized hardware-software co-design for Kyber and Dilithium on RISC-V SoC FPGA. *IACR Transactions on Cryptographic Hardware and Embedded Systems, 2024*(3), 99–135. https://doi.org/10.46586/tches.v2024.i3.99-135
6. Wang, X., Xu, G., & Yu, Y. (2023). Lattice-based cryptography: A survey. *Chinese Annals of Mathematics B, 44*(6), 945–960. https://doi.org/10.1007/s11401-023-00313-2
7. Nisha, F., Lenin, J., Saravanan, S. K., Rohit, V. R., Selvam, P. D., & Rajmohan, M. (2024). Lattice-based cryptography and NTRU: Quantum-resistant encryption algorithms. *2024 International Conference on Emerging Systems and Intelligent Computing (ESIC), 509–514*. https://doi.org/10.1109/ESIC56704.2024.10481608
8. Howe, J., Oder, T., Krausz, M., & Güneysu, T. (2018). Standard lattice-based key encapsulation on embedded devices. *IACR Transactions on Cryptographic Hardware and Embedded Systems, 2018*(3), 372–393. https://doi.org/10.13154/tches.v2018.i3.372-393
9. Karmakar, A., Fan, X., Wang, Y., & Verbauwhede, I. (2021). Efficient implementations of lattice-based cryptographic primitives for post-quantum security. *ACM Transactions on Privacy and Security, 24*(4), 1–35. https://doi.org/10.1145/3508625
10. Richter, M., Bertram, M., Seidensticker, J., & Tschache, A. (2022). A mathematical perspective on post-quantum cryptography. *Mathematics, 10*(2579). https://doi.org/10.3390/math10152579
11. Buchmann, J., Dahmen, E., & Hülsing, A. (2011). XMSS - A practical forward secure signature scheme based on minimal security assumptions. In *Post-Quantum Cryptography. PQCrypto 2011, Lecture Notes in Computer Science* (Vol. 7071, pp. 117–129). Springer, Berlin, Heidelberg. https://doi.org/10.1007/978-3-642-25405-5_8
12. Ahmed, M., Saleh, R., & Liu, H. (2023). An overview of hash-based signatures. *International Journal of Information Security, 19*(2), 72–95. https://doi.org/10.1007/s10207-023-06600-w
13. Wu, B., Tian, J., Hu, X., & Wang, Z. (2020). A novel modular multiplier for isogeny-based post-quantum cryptography. *IEEE Computer Society Annual Symposium on VLSI (ISVLSI), 334–339*. https://doi.org/10.1109/ISVLSI49217.2020.00068
14. Astrizi, T. L., & Custódio, R. (2024). Seamless transition to post-quantum TLS 1.3: A hybrid approach using identity-based encryption. *Sensors, 24*(24), 7300. https://doi.org/10.3390/s24227300
15. Kwon, H.-Y., Bajuna, I., & Lee, M.-K. (2024). Compact hybrid signature for secure transition to post-quantum era. *IEEE Access, 12*, 39417–39429. https://doi.org/10.1109/ACCESS.2024.3374645
16. Polishchuk, V., Kelemen, M., Petrushko, I., Povkhanych, V., Matei, A., & Fedelesh, Y. (2024). Preliminary research of information technology for assessing the level of fatigue of air traffic controllers. *Acta Avionica, 26*(1), 5–11. https://doi.org/10.35116/aa.2024.0001
17. Petrushko, I., & Polishchuk, V. (2024). Cybersecurity teaching in higher education: Perspectives. *XIII International Scientific and Practical Conference, International Scientific Unity*, 91–95. https://doi.org/10.20998/2522-9052.2024.1.01

References

1. Pilatte, S. (2024). Unconditional correctness of recent quantum algorithms for factoring and computing discrete logarithms. Cryptology ePrint Archive, (629). Retrieved from https://eprint.iacr.org/2024/629
2. Preston, R. (2022). Applying Grover's algorithm to hash functions: A software perspective. IEEE Transactions on Quantum Engineering, 3. https://doi.org/10.1109/TQE.2022.3233526
3. Proos, J., & Zalka, C. (2003). Shor's discrete logarithm quantum algorithm for elliptic curves. Quantum Information and Computation, 3(4), 317–344. https://doi.org/10.26421/QIC3.4-3
4. Novykov, D., & Poltorak, V. (2023). Tekhnolohii postkvantovoi kryptohrafii. Adaptyvni systemy avtomatychnoho upravlinnia, 1(42), 171–183. https://asac.kpi.ua/article/view/279169/273748

5. Wang, T., Zhang, C., Zhang, X., Gu, D., & Cao, P. (2024). Optimized hardware-software co-design for Kyber and Dilithium on RISC-V SoC FPGA. IACR Transactions on Cryptographic Hardware and Embedded Systems, 2024(3), 99–135. https://doi.org/10.46586/tches.v2024.i3.99-135

6. Wang, X., Xu, G., & Yu, Y. (2023). Lattice-based cryptography: A survey. Chinese Annals of Mathematics B, 44(6), 945–960. https://doi.org/10.1007/s11401-023-00313-2

7. Nisha, F., Lenin, J., Saravanan, S. K., Rohit, V. R., Selvam, P. D., & Rajmohan, M. (2024). Lattice-based cryptography and NTRU: Quantum-resistant encryption algorithms. 2024 International Conference on Emerging Systems and Intelligent Computing (ESIC), 509–514. https://doi.org/10.1109/ESIC56704.2024.10481608

8. Howe, J., Oder, T., Krausz, M., & Güneysu, T. (2018). Standard lattice-based key encapsulation on embedded devices. IACR Transactions on Cryptographic Hardware and Embedded Systems, 2018(3), 372–393. https://doi.org/10.13154/tches.v2018.i3.372-393

9. Karmakar, A., Fan, X., Wang, Y., & Verbauwhede, I. (2021). Efficient implementations of lattice-based cryptographic primitives for post-quantum security. ACM Transactions on Privacy and Security, 24(4), 1–35. https://doi.org/10.1145/3508625

10. Richter, M., Bertram, M., Seidensticker, J., & Tschache, A. (2022). A mathematical perspective on post-quantum cryptography. Mathematics, 10(2579). https://doi.org/10.3390/math10152579

11. Buchmann, J., Dahmen, E., & Hülsing, A. (2011). XMSS - A practical forward secure signature scheme based on minimal security assumptions. In Post-Quantum Cryptography. PQCrypto 2011, Lecture Notes in Computer Science (Vol. 7071, pp. 117–129). Springer, Berlin, Heidelberg. https://doi.org/10.1007/978-3-642-25405-5_8

12. Ahmed, M., Saleh, R., & Liu, H. (2023). An overview of hash-based signatures. International Journal of Information Security, 19(2), 72–95. https://doi.org/10.1007/s10207-023-06600-w

13. Wu, B., Tian, J., Hu, X., & Wang, Z. (2020). A novel modular multiplier for isogeny-based post-quantum cryptography. IEEE Computer Society Annual Symposium on VLSI (ISVLSI), 334–339. https://doi.org/10.1109/ISVLSI49217.2020.00068

14. Astrizi, T. L., & Custódio, R. (2024). Seamless transition to post-quantum TLS 1.3: A hybrid approach using identity-based encryption. Sensors, 24(24), 7300. https://doi.org/10.3390/s24227300

15. Kwon, H.-Y., Bajuna, I., & Lee, M.-K. (2024). Compact hybrid signature for secure transition to post-quantum era. IEEE Access, 12, 39417–39429. https://doi.org/10.1109/ACCESS.2024.3374645

16. Polishchuk, V., Kelemen, M., Petrushko, I., Povkhanych, V., Matei, A., & Fedelesh, Y. (2024). Preliminary research of information technology for assessing the level of fatigue of air traffic controllers. Acta Avionica, 26(1), 5–11. https://doi.org/10.35116/aa.2024.0001

17. Petrushko, I., & Polishchuk, V. (2024). Cybersecurity teaching in higher education: Perspectives. XIII International Scientific and Practical Conference, International Scientific Unity, 91–95. https://doi.org/10.20998/2522-9052.2024.1.01