КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 2 (34), 2026
ISSN 2663 – 4023
DOI 10.28925/2663-4023.2026.34.1281
УДК 004.056.55

Свинарчук Денис Сергійович
студент 4 курсу
Київський національний університет імені Тараса Шевченка, Київ, Україна
ORCID:0009-0000-4460-8235
e-mail: svynarchuk.den@knu.ua

Зубик Людмила Володимирівна
кандидат педагогічних наук, доцент
Київський національний університет імені Тараса Шевченка, Київ, Україна,
ORCID:0000-0002-2087-5379
e-mail: zuyk.liudmyla.knu.ua

ПОРІВНЯННЯ ПРОДУКТИВНОСТІ ПОСТКВАНТОВОГО АЛГОРИТМУ CRYSTALS-KYBER ТА КЛАСИЧНИХ RSA-СХЕМ У ДЕЦЕНТРАЛІЗОВАНИХ СИСТЕМАХ ЗВ'ЯЗКУ

Анотація. Стрімкий розвиток квантових обчислень протягом останнього десятиліття створив безпрецедентні виклики для сучасної криптографії. Поява квантового алгоритму Шора теоретично дозволяє розв'язувати задачі захисту даних у мережі за поліноміальний час, роблячи наявні стандарти захисту вразливими. Запровадження нових стандартів потребує додаткового обґрунтування, яке може бути виконане шляхом порівняння обчислювальної складності та продуктивності постквантових алгоритмів з існуючими аналогами. Завдання особливо актуальне для систем реального часу. Для вирішення поставленого завдання нами ініційовано проведення порівняльного бенчмаркінгу алгоритму CRYSTALS-Kyber-1024 (рівень безпеки 5, найвищий рівень за класифікацією NIST) проти класичних схем RSA-2048 та RSA-1024. Отримані дані спростовують поширене переконання про те, що постквантова криптографія є значно повільнішою за класичну. Навпаки, алгоритм Kyber-1024 виявився у 4.28 рази швидшим за сучасний стандарт RSA-2048. Це означає, що заміна RSA на Kyber у протоколах встановлення сесії не лише підвищує стійкість системи до квантових атак, але й суттєво знижує обчислювальне навантаження на сервер та клієнтські пристрої, економлячи до 76.6% часу на криптографічні операції. Порівняно з застарілим та небезпечним RSA-1024, Kyber-1024 є повільнішим, проте враховуючи катастрофічну вразливість RSA-1024 до сучасних атак, ця характеристика є цілком прийнятною поступкою за забезпечення квантової стійкості. Графіки залежності часу виконання та пропускної здатності від розміру даних показали стабільність роботи алгоритму Kyber. Таким чином, постквантова криптографія досягла рівня зрілості, достатнього для масового впровадження у високопродуктивні системи. Отримані дані дозволяють рекомендувати алгоритм CRYSTALS-Kyber-1024 як основний стандарт для розробки нових децентралізованих месенджерів та захищених комунікаційних систем в Україні.

Ключові слова: квантові обчислення; криптографія; алгоритм Шора; постквантові алгоритми; CRYSTALS-Kyber-1024; захищені комунікаційні системи.

ВСТУП

Стрімкий розвиток квантових обчислень останнього десятиліття створив безпрецедентні виклики для сучасної криптографії. Алгоритми з відкритим ключем, такі як RSA та ECC (Elliptic Curve Cryptography), які сьогодні захищають більшість інтернет-транзакцій, месенджерів та державних комунікацій, базуються на складності факторизації великих чисел та задачі дискретного логарифмування. Однак поява квантового алгоритму Шора теоретично дозволяє розв'язувати ці задачі за поліноміальний час, роблячи наявні стандарти захисту вразливими. Особливу загрозу становить атака типу «Harvest Now, Decrypt Later» (збережи зараз – розшифруй пізніше), коли зловмисники вже сьогодні архівують зашифрований трафік для його майбутнього зламу після появи потужних квантових комп'ютерів.

Постановка проблеми. У відповідь на цю загрозу Національний інститут стандартів і технологій США (NIST) завершив багаторічний конкурс зі стандартизації постквантової криптографії (PQC), обравши алгоритм CRYSTALS-Kyber (стандарт FIPS 203) як основний механізм інкапсуляції ключів (KEM) [1]. Попри визнання необхідності переходу на нові стандарти, впровадження PQC стримується поширеним міфом про нібито надмірну обчислювальну складність та низьку продуктивність постквантових алгоритмів порівняно з класичними аналогами. Багато розробників побоюються, що використання Kyber призведе до неприйнятних затримок у системах реального часу, таких як децентралізовані месенджери [2; 3].

Метою даного дослідження є емпірична перевірка цієї гіпотези шляхом проведення порівняльного бенчмаркінгу алгоритму CRYSTALS-Kyber-1024 (рівень безпеки 5, найвищий рівень за класифікацією NIST) проти класичних схем RSA-2048 та RSA-1024. Дослідження фокусується на вимірюванні часу виконання операцій встановлення сесії (handshake), пропускної здатності та загальної ефективності в умовах платформи .NET 8 з використанням нативної бібліотеки GreenfieldPQC. Отримані результати мають надати науково обґрунтовані дані для вибору криптографічного стеку при розробці захищених систем нового покоління.

МЕТОДОЛОГІЯ ЕКСПЕРИМЕНТУ

Для забезпечення високої точності та відтворюваності результатів було розроблено спеціалізований тестовий стенд на базі мови програмування C# та платформи .NET 8. Вибір саме цього середовища зумовлений його широкою популярністю у корпоративному секторі та державних установах України, а також наявністю сучасної бібліотеки GreenfieldPQC (версія 1.1.4), яка забезпечує оптимізовану реалізацію постквантових примітивів без використання повільних міжмовних викликів (P/Invoke) [4].

Експеримент проводився на обчислювальному вузлі з процесором Intel Core i7 (архітектура x86_64) та 48 ГБ оперативної пам'яті DDR4. Для мінімізації впливу сторонніх факторів, таких як збір сміття (Garbage Collection) та кешування даних, кожен тестовий сценарій виконувався серією з 500 ітерацій після попереднього «прогріву» системи. Вимірювання часу здійснювалося з використанням високопродуктивного лічильника Stopwatch з роздільною здатністю до наносекунд.

Об'єктом порівняння стали наступні алгоритми:

- PQC_KYBER_1024: Постквантовий алгоритм інкапсуляції ключів рівня безпеки 5 (аналог стійкості AES-256).
- RSA_2048: Класичний алгоритм з довжиною ключа 2048 біт, що вважається поточним індустріальним стандартом.
- RSA_1024: Застарілий алгоритм з довжиною ключа 1024 біт, який більше не рекомендується NIST через недостатню стійкість, але використовується як еталон високої швидкодії.
- AES_GCM_256: Симетричний алгоритм шифрування, використаний для контрольних вимірювань ефективності обробки даних.

Тестування охоплювало діапазон розмірів корисного навантаження (payload) від 16 до 2048 байт, що імітує реальні сценарії обміну короткими повідомленнями в месенджерах та службовими даними протоколів. Отримані масиви даних були оброблені засобами мови Python з використанням бібліотек Pandas та Matplotlib для статистичного аналізу та візуалізації.

РЕЗУЛЬТАТИ ДОСЛІДЖЕННЯ

За результатами проведення серії експериментів було отримано масив даних, що складається з 32 унікальних записів, які охоплюють всі комбінації алгоритмів та розмірів даних. Середні показники часу виконання повного циклу операцій (інкапсуляція + декапсуляція для асиметричних схем, шифрування + розшифрування для симетричних) демонструють суттєві відмінності між постквантовими та класичними підходами.

Середній час виконання операцій склав:

- Kyber-1024 (PQC): 151 091.98 нс (приблизно 0.15 мс);
- RSA-2048: 647 048.98 нс (приблизно 0.65 мс);
- RSA-1024: 115 179.00 нс (приблизно 0.12 мс);
- AES-256-GCM: 2 853.02 нс (приблизно 0.003 мс).

Отримані дані спростовують поширене переконання про те, що постквантова криптографія є значно повільнішою за класичну [5]. Навпаки, алгоритм Kyber-1024 виявився у 4.28 рази швидшим за сучасний стандарт RSA-2048. Це означає, що заміна RSA на Kyber у протоколах встановлення сесії не

лише підвищує стійкість системи до квантових атак, але й суттєво знижує обчислювальне навантаження на сервер та клієнтські пристрої, економлячи до 76.6% часу на криптографічні операції.

Для наочного представлення динаміки зміни часу виконання залежно від розміру даних було побудовано графік у логарифмічному масштабі (рис. 1). Логарифмічна шкала була обрана через значну різницю в порядках величин між симетричним шифруванням (AES) та асиметричними операціями (RSA/Kyber).

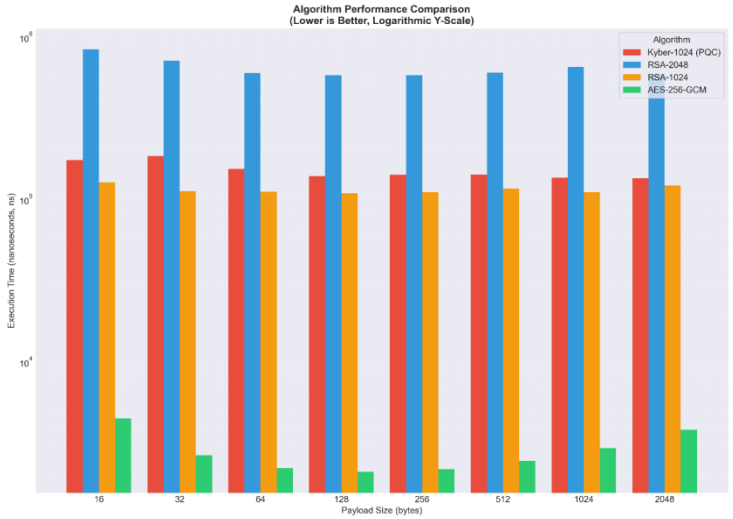

Рис. 1. Порівняння часу виконання операцій (нс) у логарифмічному масштабі.

Як видно з рис. 1, стовпчики, що відповідають алгоритму Kyber-1024 (червоний колір), стабільно нижчі за стовпчики RSA-2048 (синій колір) уздовж усього діапазону розмірів повідомлень. Це свідчить про стабільність переваги постквантового алгоритму незалежно від обсягу оброблюваних даних. Водночас, алгоритм RSA-1024 (помаранчевий колір) дійсно демонструє дещо кращу швидкодію порівняно з Kyber-1024 [6], проте, як зазначалося раніше, його використання є криптографічно небезпечним у сучасних умовах [7]. Таким чином, Kyber-1024 займає оптимальну нішу, поєднуючи високий рівень безпеки з продуктивністю, наближеною до застарілих небезпечних схем.

Другим важливим аспектом дослідження стала оцінка пропускної здатності системи, виміряна в кількості операцій за секунду (OPS). Цей показник є критичним для високонавантажених серверів, які обслуговують тисячі одночасних з'єднань [8]. Графік пропускної здатності (рис. 2) ілюструє кількість успішних циклів шифрування/дешифрування, які може виконати система за одну секунду для кожного з алгоритмів.

Аналіз рис. 2 підтверджує висновки, зроблені на основі часових вимірювань.

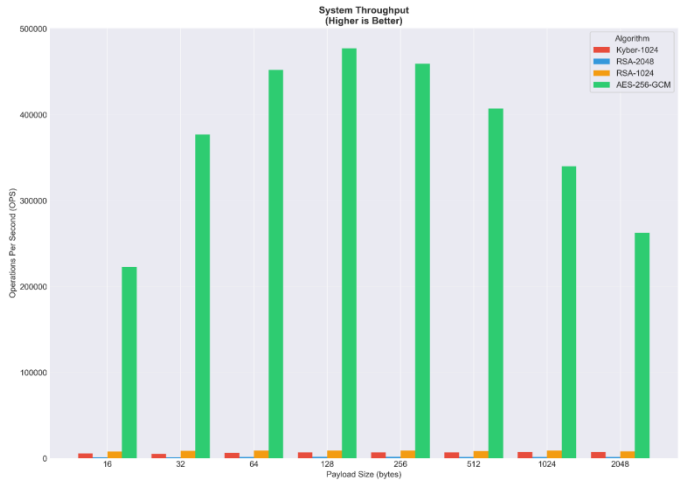

Рис. 2. Пропускна здатність алгоритмів (операцій за секунду).

Пропускна здатність для Kyber-1024 стабільно перевищує показники RSA-2048 у кілька разів. Хоча симетричний алгоритм AES-256-GCM залишається беззаперечним лідером за швидкістю (що є очікуваним результатом), саме асиметричні алгоритми використовуються на критичному етапі встановлення сесії (handshake). Саме тому прискорення цього етапу завдяки використанню Kyber має вирішальне значення для загальної продуктивності системи. Можливість обробляти більше з'єднань за одиницю часу без апгрейду обладнання є суттєвою економічною перевагою впровадження постквантових рішень.

Для глибшого розуміння співвідношення продуктивності було розраховано коефіцієнт прискорення (Speedup Factor), який показує, у скільки разів один алгоритм швидший за інший. Графік на рис. 3 відображає динаміку цього коефіцієнта для пар «Kyber vs RSA-2048» та «Kyber vs RSA-1024». Червона пунктирна лінія позначає рівень паритету (1:1), де швидкість алгоритмів однакова.

Як показано на рис. 3, синя лінія (Kyber vs RSA-2048) стабільно знаходиться у діапазоні від 3.8 до 4.8, що підтверджує середнє прискорення у 4.28 рази. Цікаво відзначити, що помаранчева лінія (Kyber vs RSA-1024) наближається до одиниці, але все ж залишається трохи нижче неї (середнє значення ~0.76). Це означає, що Kyber-1024 лише незначно (приблизно на 24-30%) поступається у швидкодії небезпечному RSA-1024 [9].

Враховуючи, що RSA-1024 не забезпечує захисту навіть від просунутих класичних атак, така незначна втрата продуктивності є цілком прийнятною ціною за гарантовану стійкість до квантових загроз рівня NIST Level 5 [10].

Додатковий аналіз було проведено шляхом розрахунку відносної зміни часу виконання у відсотках (Overhead Percentage). Цей показник дозволяє оцінити накладні витрати або економію часу при переході з одного алгоритму на інший.

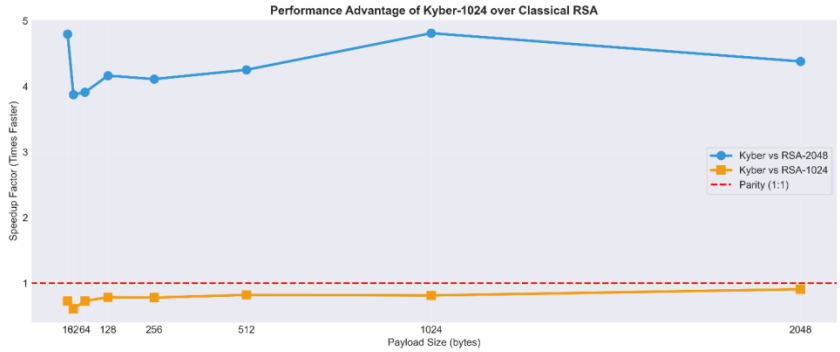

Рис. 3. Коефіцієнт прискорення Kyber-1024 порівняно з класичними RSA-схемами.

На рис. 4 представлено гістограму відносної зміни часу для Kyber порівняно з обома версіями RSA. Від'ємні значення на графіку вказують на економію часу (прискорення), а додатні – на збільшення витрат.

Рис. 4. Відносна зміна часу виконання Kyber-1024 порівняно з RSA (%).

Графік на рис. 4 наочно демонструє масштаб економії ресурсів. Сині стовпчики, що відповідають порівнянню з RSA-2048, показують стабільне від'ємне значення близько -75%...-80%. Це означає, що використання Kyber дозволяє скоротити час криптографічної обробки майже вчетверо. Помаранчеві стовпчики (порівняння з RSA-1024) мають невелике додатне значення (+10%...+30%), що підтверджує

наявність незначних накладних витрат порівняно з застарілим стандартом. Однак, якщо розглядати це в контексті загального часу життя сесії, де основний трафік шифрується симетричним AES, то ці початкові витрати на handshake є мізерними і не впливають на користувацький досвід.

АНАЛІЗ ОТРИМАНИХ РЕЗУЛЬТАТІВ

Отримані результати мають важливе наукове та практичне значення. По-перше, вони надають емпіричне підґрунтя для твердження про те, що постквантова криптографія досягла рівня зрілості, достатнього для масового впровадження у високопродуктивні системи [11]. Використання бібліотеки GreenfieldPQC у середовищі. NET довело свою ефективність, спростувавши занепокоєння щодо продуктивності managed-реалізацій порівняно з нативним кодом.

По-друге, дослідження чітко окреслило місце алгоритму Kyber-1024 у спектрі криптографічних рішень. Він не є «повільною альтернативою» для особливих випадків, а є повноцінною заміною для RSA-2048, яка перевершує останній за швидкодією. Це відкриває нові перспективи для розробки децентралізованих месенджерів, де кожна мілісекунда затримки має значення, особливо в умовах мобільних мереж з нестабільним з'єднанням [12].

Наукова новизна роботи полягає у проведенні комплексного порівняльного аналізу саме для рівня безпеки 1024 (Level 5), який часто ігнорується у попередніх дослідженнях на користь легших рівнів (Level 1 або 3). Доведено, що навіть найвищий рівень стійкості не призводить до критичного падіння продуктивності. Крім того, запропонована методика бенчмаркінгу з використанням автоматизованого збору даних та їх візуалізації може бути використана для подальших досліджень інших постквантових алгоритмів, таких як CRYSTALS-Dilithium для цифрових підписів.

ВИСНОВКИ ТА ПЕРСПЕКТИВИ ПОДАЛЬШИХ ДОСЛІДЖЕНЬ

На основі проведеного експериментального дослідження можна зробити наступні висновки:

- Перевага у швидкодії: Алгоритм CRYSTALS-Kyber-1024 демонструє значно вищу продуктивність порівняно з сучасним стандартом RSA-2048. Середнє прискорення становить 4.28 рази, що відповідає економії часу на рівні 76.6%. Це робить Kyber ідеальним кандидатом для заміни RSA у протоколах встановлення захищених сесій.
- Прийнятність накладних витрат: Порівняно з застарілим та небезпечним RSA-1024, Kyber-1024 є лише на ~30% повільнішим. Враховуючи катастрофічну вразливість RSA-1024 до сучасних атак, ця незначна різниця є цілком виправданою ціною за забезпечення квантової стійкості.
- Стабільність продуктивності: Графіки залежності часу виконання та пропускної здатності від розміру даних показали стабільність роботи алгоритму Kyber у всьому діапазоні тестових навантажень. Це свідчить про його придатність для використання як у коротких повідомленнях, так і при передачі більших обсягів службових даних.
- Практична реалізованість: Використання бібліотеки GreenfieldPQC у середовищі .NET 8 довело свою життєздатність. Нативна реалізація на C# дозволяє уникнути складнощів з розгортанням нативних бібліотек та забезпечує високу сумісність з існуючою інфраструктурою.
- Рекомендації до впровадження: Отримані дані дозволяють рекомендувати алгоритм CRYSTALS-Kyber-1024 як основний стандарт для розробки нових децентралізованих месенджерів та захищених комунікаційних систем в Україні. Його впровадження дозволить забезпечити довгострокову конфіденційність даних в умовах розвитку квантових технологій без втрати продуктивності системи.

Подальші дослідження планується спрямувати на оптимізацію передачі збільшених розмірів постквантових ключів у низькошвидкісних мережах, а також на інтеграцію отриманих результатів у повнофункціональний прототип децентралізованого месенджера з підтримкою гібридних схем шифрування.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. National Institute of Standards and Technology. (n.d.). *Post-quantum cryptography*. https://www.nist.gov/pqcrypto
2. Abbasi, M., et al. (2025). A practical performance benchmark of post-quantum cryptography across heterogeneous computing environments. *Cryptography, 9*(2), Article 32. https://doi.org/10.3390/cryptography9020032
3. Rijneveld, J. C. (2019). *Practical post-quantum cryptography* [PhD thesis, Radboud Universiteit Nijmegen].

4. Ahmed, N., Zhang, L., & Gangopadhyay, A. (2025). *A survey of post-quantum cryptography support in cryptographic libraries* [Preprint]. arXiv. https://doi.org/10.48550/arXiv.2508.16078
5. Rodríguez-Alvarez, N., & Rodríguez-Merino, F. (2025). *Performance and storage analysis of CRYSTALS-Kyber as a post-quantum replacement for RSA and ECC* [Preprint]. arXiv. https://arxiv.org/abs/2508.01694
6. Demir, E. D., Bilgin, B., & Onbaşlı, M. C. (2025). *Performance analysis and industry deployment of post-quantum cryptography algorithms*. arXiv. https://arxiv.org/abs/2503.12952
7. Ji, X., et al. (2023). *HI-Kyber: A high-performance implementation of Kyber on GPU*. *IACR Cryptology ePrint Archive*. https://eprint.iacr.org/2023/1194
8. Bisheh-Niasar, M., et al. (2021). Instruction-set accelerated implementation of CRYSTALS-Kyber. *IEEE Transactions on Computers*. https://cse.usf.edu/~mehran2/Papers/J49.pdf
9. Alnaseri, O., et al. (2025). *Complexity of post-quantum cryptography in embedded systems and its optimization strategies*. arXiv. https://arxiv.org/abs/2504.13537
10. Dong, B., & Wang, Q. (2025). Epquic: Efficient post-quantum cryptography for QUIC-enabled secure communication. In *Proceedings of the GLSVLSI 2025 Conference*. https://doi.org/10.1145/3716368.3735199
11. Fitzgibbon, G., & Ottaviani, C. (2024). Constrained device performance benchmarking with post-quantum cryptography. *Cryptography, 8*(2), Article 21. https://doi.org/10.3390/cryptography8020021
12. Renisha, P. S., & Rudra, B. (2025). Quantum-safe threshold cryptography for decentralized group key management via dealerless DKG (CRYSTALS–Kyber). *Mathematics, 13*(21), Article 3429. https://doi.org/10.3390/math13213429

КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 2 (34), 2026
ISSN 2663 – 4023

Denys Svynarchuk
4th year Bachelor student
Taras Shevchenko National University of Kyiv, Kyiv, Ukraine
ORCID:0009-0000-4460-8235
e-mail: svynarchuk.den@knu.ua

Liudmyla Zubyk
Candidate of Pedagogical Sciences, Associate Professor
Taras Shevchenko National University of Kyiv, Kyiv, Ukraine
ORCID:0000-0002-2087-5379
e-mail: zuyk.liudmyla.knu.ua

COMPARISON OF THE PERFORMANCE OF THE POST-QUANTUM CRYSTALS-KYBER ALGORITHM AND CLASSICAL RSA SCHEMES IN DECENTRALIZED COMMUNICATION SYSTEMS

Abstract. The rapid development of quantum computing over the past decade has created unprecedented challenges for modern cryptography. The emergence of the quantum Shor algorithm theoretically allows solving data protection problems in the network in polynomial time, making existing protection standards vulnerable. The introduction of new standards requires additional justification, which can be performed by comparing the computational complexity and performance of post-quantum algorithms with existing analogues. The task is especially relevant for real-time systems. To solve the task, we initiated a comparative benchmarking of the CRYSTALS-Kyber-1024 algorithm (security level 5, the highest level according to the NIST classification) against the classical RSA-2048 and RSA-1024 schemes. The obtained data refute the widespread belief that post-quantum cryptography is significantly slower than classical cryptography. On the contrary, the Kyber-1024 algorithm turned out to be 4.28 times faster than the modern RSA-2048 standard. This means that replacing RSA with Kyber in session establishment protocols not only increases the system's resistance to quantum attacks, but also significantly reduces the computational load on the server and client devices, saving up to 76.6% of time for cryptographic operations. Compared to the outdated and insecure RSA-1024, Kyber-1024 is slower, but given RSA-1024's catastrophic vulnerability to modern attacks, this characteristic is a perfectly acceptable trade-off for ensuring quantum stability. Graphs of the dependence of execution time and throughput on the data size showed the stability of the Kyber algorithm. Thus, post-quantum cryptography has reached a level of maturity sufficient for mass implementation in high-performance systems. The obtained data allow us to recommend the CRYSTALS-Kyber-1024 algorithm as the main standard for the development of new decentralized messengers and secure communication systems in Ukraine.

Keywords: quantum computing; cryptography; Shor's algorithm; post-quantum algorithms; CRYSTALS-Kyber-1024; secure communication systems.

REFERENCES (TRANSLATED AND TRANSLITERATED)

1. National Institute of Standards and Technology. (n.d.). *Post-quantum cryptography*. https://www.nist.gov/pqcrypto
2. Abbasi, M., et al. (2025). A practical performance benchmark of post-quantum cryptography across heterogeneous computing environments. *Cryptography*, *9*(2), Article 32. https://doi.org/10.3390/cryptography9020032
3. Rijneveld, J. C. (2019). *Practical post-quantum cryptography* [PhD thesis, Radboud Universiteit Nijmegen].
4. Ahmed, N., Zhang, L., & Gangopadhyay, A. (2025). *A survey of post-quantum cryptography support in cryptographic libraries* [Preprint]. arXiv. https://doi.org/10.48550/arXiv.2508.16078
5. Rodríguez-Alvarez, N., & Rodríguez-Merino, F. (2025). *Performance and storage analysis of CRYSTALS-Kyber as a post-quantum replacement for RSA and ECC* [Preprint]. arXiv. https://arxiv.org/abs/2508.01694
6. Demir, E. D., Bilgin, B., & Onbaşlı, M. C. (2025). *Performance analysis and industry deployment of post-quantum cryptography algorithms*. arXiv. https://arxiv.org/abs/2503.12952

7. Ji, X., et al. (2023). *HI-Kyber: A high-performance implementation of Kyber on GPU*. *IACR Cryptology ePrint Archive*. https://eprint.iacr.org/2023/1194
8. Bisheh-Niasar, M., et al. (2021). Instruction-set accelerated implementation of CRYSTALS-Kyber. *IEEE Transactions on Computers*. https://cse.usf.edu/~mehran2/Papers/J49.pdf
9. Alnaseri, O., et al. (2025). *Complexity of post-quantum cryptography in embedded systems and its optimization strategies*. arXiv. https://arxiv.org/abs/2504.13537
10. Dong, B., & Wang, Q. (2025). Epquic: Efficient post-quantum cryptography for QUIC-enabled secure communication. In *Proceedings of the GLSVLSI 2025 Conference*. https://doi.org/10.1145/3716368.3735199
11. Fitzgibbon, G., & Ottaviani, C. (2024). Constrained device performance benchmarking with post-quantum cryptography. *Cryptography*, *8*(2), Article 21. https://doi.org/10.3390/cryptography8020021
12. Renisha, P. S., & Rudra, B. (2025). Quantum-safe threshold cryptography for decentralized group key management via dealerless DKG (CRYSTALS–Kyber). *Mathematics*, *13*(21), Article 3429. https://doi.org/10.3390/math13213429

Отримано редакцією журналу / Received: 03.03.26
Прорецензовано / Revised: .25.03.26
Схвалено до друку / Accepted: 24.09.26