УДК 004.6

Аліна ДАВЛЕТОВА
Західноукраїнський національний університет

ДОСЛІДЖЕННЯ МЕТОДІВ ПОСТКВАНТОВОЇ КРИПТОГРАФІЇ

Вступ. Зростання обсягів даних та масштабів обміну інформацією через незахищені канали роблять питання захисту конфіденційності і цілісності інформації актуальним. Криптографічні методи є основою сучасних систем безпеки, забезпечуючи надійний захист інформації у широкому спектрі застосувань. Однак, із розвитком квантових обчислень традиційні криптографічні алгоритми, як-от RSA [1] або протокол Діффі-Хеллмана [2], які ґрунтуються на складності факторизації та дискретного логарифма, стають вразливими. Квантові комп'ютери можуть обробляти інформацію набагато швидше за класичні комп'ютери, і, використовуючи спеціалізовані алгоритми, наприклад алгоритм Шора, алгоритм Гровера [3], дозволять розв'язувати математичні задачі, на яких базуються сучасні криптографічні методи, що створює новий виклик для кібербезпеки.

Дослідження у сфері постквантової криптографії (PQC) [4] обумовлена необхідністю розробки нових алгоритмів, стійких до атак квантових комп'ютерів. Розробка постквантових методів криптографії є перспективним напрямом, спрямованим на забезпечення конфіденційності, доступності та цілісності даних в умовах, де традиційні алгоритми перестануть відповідати вимогам сучасних загроз.

Мета: дослідження та аналіз методів постквантової криптографії та визначення практичних можливостей їх впровадження та адаптації для забезпечення надійного захисту інформації в умовах загроз з боку квантових комп'ютерів.

1. Аналіз напрямів розвитку постквантової криптографії

PQC- це напрям криптографії, метою якого є розробка алгоритмів та протоколів захисту інформації, стійких до атак з використанням квантових комп'ютерів. Постквантові алгоритми можуть ґрунтуватися на математичних проблемах, які є складними для квантових комп'ютерів (рисунок 1).

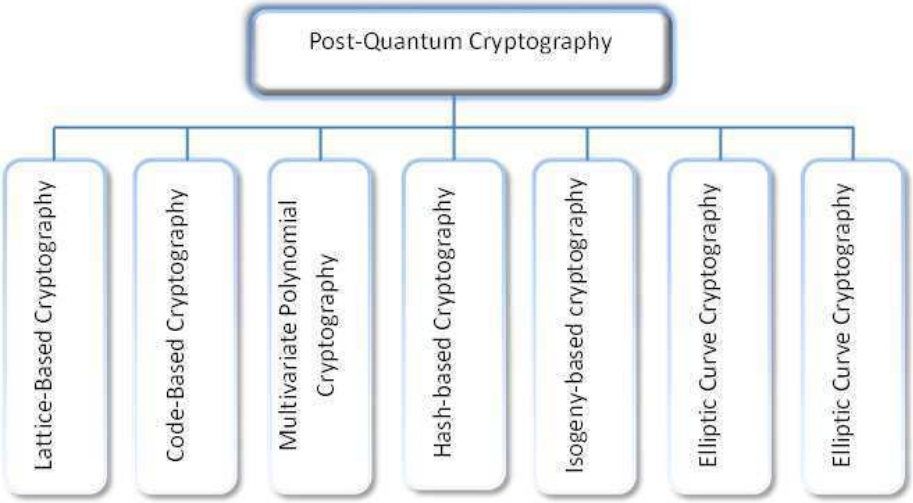

Рисунок 1 - Постквантова криптографія

Криптографія на основі решіток (Lattice-Based Cryptography, LBC) ґрунтується на складних задачах, пов'язаних з решітками - структурами, які можна уявити як множини точок у просторі. Одна з основних задач у цьому напрямку є пошук найкоротшого вектора в решітці (SVP), що є NP-повною задачею, або пошук найближчого вектора до заданого(CVP). Прикладом є LBC алгоритми: NTRU, Kyber, і FrodoKEM, Saber.

Криптографія на основі кодів (Code-Based Cryptography, CBC) використовує складність декодування випадкових лінійних кодів, що є NP-повною задачею. Це означає, що проблема декодування таких кодів є складною для класичних і квантових комп'ютерів. Алгоритми цього напрямку стійкі до атак квантових комп'ютерів, оскільки квантові алгоритми не дають значної переваги у вирішенні цієї задачі. Класичним прикладом CBC є криптосистема McEliece, що є стійкою до квантових атак і має перспективу для тривалого зберігання даних. Прикладом також є HQC, BIKE.

Багатовимірна поліноміальна криптографія (Multivariate Polynomial Cryptography, MPC) використовує багатовимірні (квадратичні) рівняння, визначені на кінцевому полі. Основною проблемою, на якій базується даний напрям, є розв'язання систем багатовимірних рівнянь, що також є NP-повними. Прикладом MPC є система HFE (Hidden Field Equations), Rainbow.

Криптографія на основі хешів (Hash-based Cryptography, HBC) базуються на безпеці хеш-функцій, які використовуються для перевірки цілісності даних або для створення цифрових підписів. Прикладом HBC є Lamport One-time Signature і більш сучасні схеми, зокрема XMSS (eXtended Merkle Signature Scheme), SPHINCS+, SIDH. Такі криптосистеми вважаються стійкими до квантових атак і вже використовуються у певних додатках.

Криптографія на основі ізогеній (Isogeny-Based Cryptography, ISC) базується на задачі пошуку ізогенії (відображення) між двома суперсингулярними еліптичними кривими. Це спеціальна задача, яка є складною для квантових комп'ютерів. Задача ізогенії вважається стійкою до атак квантових комп'ютерів і є перспективним напрямком постквантової криптографії. Прикладом систем ISC є SIKE SIDH.

Криптографія на основі еліптичних кривих (Elliptic Curve Cryptography, ECC) ґрунтується на складності обчислення ізогеній між суперсингулярними еліптичними кривими. Це порівняно новий напрямок у PQC, який має потенціал для використання в обміні ключами за рахунок їх компактних кормірів.

Метою постквантової криптографії є забезпечення довготривалого захисту даних в умовах розвитку квантових технологій.

2. Дослідження постквантових криптоалгоритмів

У контексті PQC, Національний інститут стандартів і технологій США (NIST) ініціював процес стандартизації криптографічних алгоритмів, які повинні бути стійкими до атак з використанням квантових комп'ютерів [5]. Одним із етапів цього процесу є тестування та вибір найбільш надійних алгоритмів для захисту даних у майбутньому, коли квантові комп'ютери стануть реальністю.

Для оцінки стійкості алгоритмів NIST визначено рівні безпеки з 1 по 5, які відповідають рівню безпеки AES128, SHA256, AES192, SHA384 та AES256 відповідно. У 2023 році завершено черговий етап відбору під час якого було розглянуто алгоритми наведені в таблиці 1.

Таблиця 1 - Алгоритми, що розглядалися на третьому етапі стандартизації NIST

Алгоритм шифрування та обміну ключами		**Алгоритм створення та перевірки цифрового підпису**	
Фіналісти	Альтернативні кандидати	Фіналісти	Альтернативні кандидати
CRYSTALS-Dilithium	GeMSS	Classic McEliece	BIKE
	Picnic	CRYSTALS-Kyber	HQC
Falcon	SPHINCS+	NTRU	FrodoKEM
Rainbow		Saber	NTRU Prime
			SIKE

Ці алгоритми є прикладами постквантових криптографічних схем, що базуються на різних математичних проблемах, таких як багатовимірні поліноміальні рівняння (Rainbow, GeMSS), ізогенії еліптичних кривих (SIKE), і хеш-функціях (Picnic).

В результаті криптоаналізу деякі з цих алгоритмів, зокрема Rainbow, GeMSS, Picnic та SIKE, були зламані або виявлені їх вразливості до квантових атак, що поставило під сумнів їх здатність забезпечувати безпеку в умовах квантових комп'ютерів. Через це вони не будуть розглядатися на наступному етапі відбору NIST.

Для розширення початкового набору алгоритмів PQC планується додати нові криптосистеми, які базуються на двох класах складних математичних задач, які, як вважається, є стійкими до квантових атак [6]. Алгоритми, що будуть розглядатися в наступному раунді є криптосистема Classic McEliece [7] на основі кодів, BIKE [8] (Bit-Flipping Key Encapsulation) - алгоритм обміну ключами, заснований на задачі, яка полягає у вирішенні декодування коду в бітових просторах та алгоритм HQC [9] (Hybrid Quasi-Cyclic), який використовує квізіциклічні коди для забезпечення безпеки.

У наступному раунді стандартізації NIST будуть активно розглядатися алгоритми, що базуються на решітках та кодах, оскільки вони вважаються більш стійкими до квантових атак, на відміну від раніше зламаних алгоритмів, що базуються на різних математичних проблемах, зокрема багатовимірні поліноміальні рівняння (Rainbow, GeMSS), ізогенії еліптичних кривих (SIKE), і геш-функціях (Picnic).

3. Перспективи розвитку криптографії на основі кодів у контексті постквантової криптографії

СВС є одним із перспективних напрямків постквантової криптографії. Це підтверджується включенням алгоритмів на основі теорії кодів, у процес стандартизації NIST для постквантових криптосистем. Такі алгоритми

використовують складні математичні, які на відміну від класичних криптографічних проблем, не піддаються ефективним квантовим алгоритмам, що робить їх стійкими до квантових. СВС має довгострокову стабільність у порівнянні з іншими методами, оскільки складність задачі декодування лінійних кодів, не змінюється із розвитком квантових обчислень. Криптосистеми на основі кодів забезпечують обчислювальну ефективність при збереженні високого рівня безпеки та дозволяють працювати з великими обсягами даних, що є важливим для застосувань у реальних системах безпеки.

На рисунках 2-4 наведено графіки, що відображають розмірів ключів та шифротексту алгоритмів СВС [10].

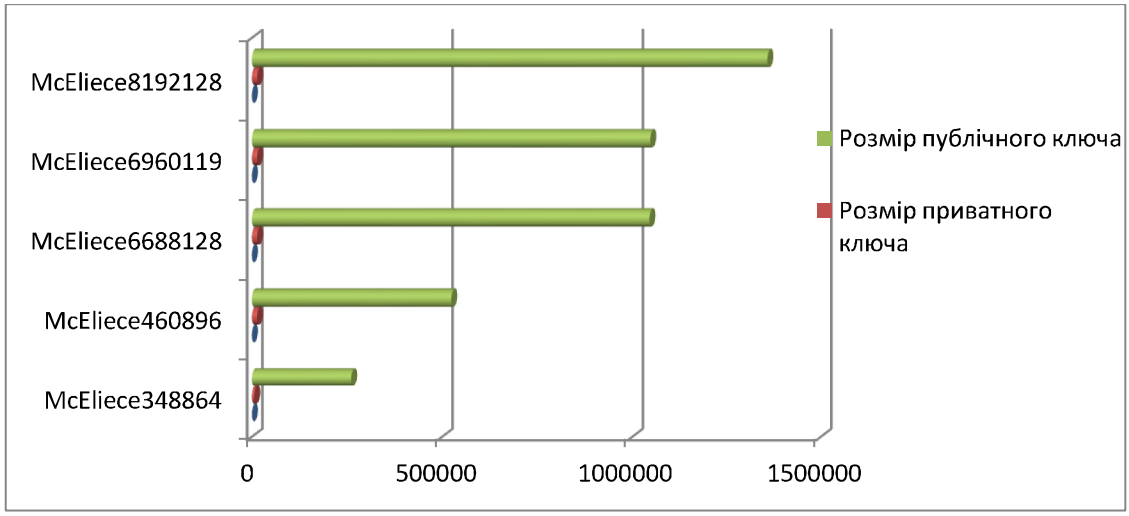

Рисунок 2 - Криптосистема McEliece

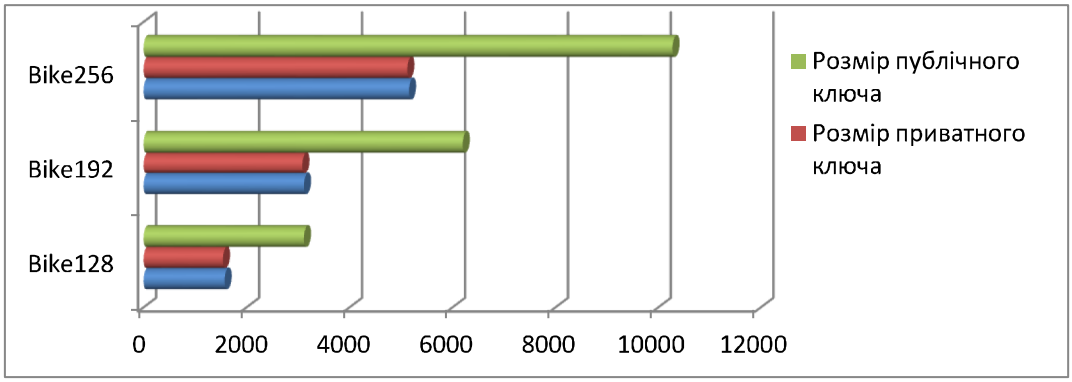

Рисунок 3 - Криптографічний алгоритм BIKE

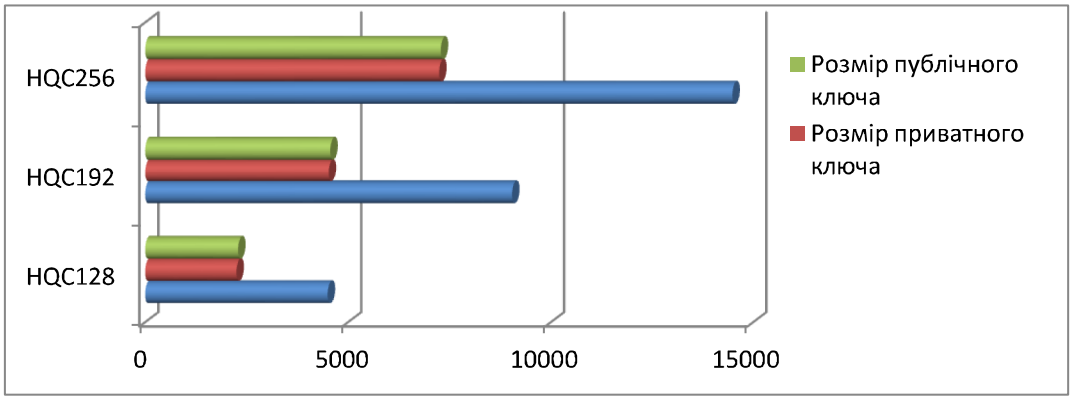

Рисунок 4 - Гібридна криптографічна система HQC

З наведених рисунків видно, що McEliece8192128 має найбільший розмір публічного 1357824 біт та приватного 14120 біт ключів серед розглянутих алгоритмів. Для алгоритмів Bike максимальні значення у Bike256, з публічним ключем 5122 біт та приватним 10276 біт. HQC256 розмір публічного ключа складає 7245 біт, приватного ключа 7285 біт та шифротексту 14485 біт.

З точки зору безпеки McEliece8192128 забезпечує найвищий рівень серед криптосистем McEliece, оскільки має найбільший розмір публічного ключа і шифротексту, що дозволяє досягти вищого рівня стійкості до атак, але вимагає більше ресурсів для зберігання та обробки. Параметри HQC256 та Bike256 також вказують на підвищену стійкість, хоча й вимагатимуть більше обчислювальних потужностей.

Висновок. Завдяки складності декодування випадкових лінійних кодів, CBC алгоритми є стійкими до квантових атак, що зумовлює їх актуальність в умовах, коли традиційні алгоритми більше не можуть забезпечувати належний рівень безпеки. Математична основа CBC добре вивчена, це забезпечує її надійність і передбачуваність, що є важливим для безпеки в PQS.

Незважаючи на великі розміри ключів і шифротексту McEliece8192128 та HQC256, пропонують високий рівень стійкості до квантових атак, що робить їх перспективними для застосування в постквантових криптографічних системах.

Перелік використаних джерел.

1. Rivest R.L., Shamir A., Adleman L. A Method for Obtaining Digital Signature and Public-Key Cryptosystems. Communications of the ACM., Vol. 21, No. 2. 1978. pp. 120-126.

2. Diffie W., Hellman M., New directions in cryptography. IEEE Transactions on Information Theory, vol. 22, no. 6, pp. 644-654, November 1976, doi: 10.1109/TIT.1976.1055638.

3. Shiu H.-J., Yang C.-T., Tsai Y.-R., Lin W.-C., Lai C.-M. Maintaining Secure Level on Symmetric Encryption under Quantum Attack. Applied Sciences. 2023. 13(11):6734. https://doi.org/10.3390/app13116734

4. Bagirovs E., Provodin G., Sipola T., Hautamaki J. Applications of Post-Quantum Cryptography. European Conference on Cyber Warfare and Security. 2024. 23. 49-57. 10.34190/eccws.23.1.2247.

5. Post-Quantum Cryptography. [Електронний ресурс].- Режим доступу: https://csrc.nist.gov/projects/post-quantum-cryptography

6. NIST. Post-Quantum Cryptography. Round 3 Submissions [Електронний ресурс].- Режим доступу: https://csrc.nist.gov/Projects/post-quantum-cryptography/post-quantum-cryptography-standardization/round-3-submissions

7. Classic McEliece [Електронний ресурс].- Режим доступу: https://classic.mceliece.org/

8. BIKE - Bit Flipping Key Encapsulation [Електронний ресурс].- Режим доступу: https://bikesuite.org/

9. HQC [Електронний ресурс].- Режим доступу: https://pqc-hqc.org/

10. PQC Key Encapsulation Mechanism (KEM) Speed Tests. [Електронний ресурс].- Режим доступу: https://asecuritysite.com/mceliece/pqc_kem