УДК 004.056.55

doi.org/10.15407/fmmit2023.37.052

Поточний стан стандартизації постквантової криптографії

Єлизавета Острянська[1], Юрій Горбенко[2]

[1] аналітик з систем захисту інформації, АТ «Інститут інформаційних технологій», вул. Коломенська, 15, 61166, Харків, e-mail: antelizza@gmail.com
[2] к. т. н., перший заступник головного конструктора АТ «Інститут інформаційних технологій», вул. Коломенська, 15, 61166, Харків, e-mail: uigorbenko@gmail.com

У роботі наведено огляд та аналіз поточного стану стандартизації постквантової криптографії. Розвиток квантових комп'ютерів загрожує безпеці криптографічних алгоритмів, які застосовуються сьогодні. Щоб протистояти цій загрозі, була започаткована область постквантової криптографії. Але розгортання нових криптографічних систем потребує багато часу та зусиль. Таким чином, політики та власники систем повинні підготуватися. Наразі органи стандартизації продовжують стандартизувати протоколи, створені з використанням доквантових систем, які не витримають квантових атак. До таких протоколів доцільно застосовувати концепції гібридних систем (подвійне шифрування, подвійний KEM, подвійні підписи тощо). Однак цього немає в поточному плані. Тому рекомендується враховувати постквантову інтеграцію при розробці нових стандартів або оновленні існуючих.

Ключові слова: постквантова криптографія; цифровий підпис; механізм встановлення ключа (KEM), квантовобезпечний

Вступ. Криптографія є вирішальним інструментом для безпеки сучасного цифрового суспільства і використовується практично всюди. Розвиток квантових комп'ютерів загрожує безпеці криптографічних алгоритмів, які застосовуються сьогодні. Щоб протистояти цій загрозі, була започаткована область постквантової криптографії. Постквантова криптографія – це область криптографії, в якій системи вивчаються за припущення безпеки, що криптоаналітик має квантовий комп'ютер, тоді як користувач має бути звичайним користувачем сучасних систем без квантових можливостей. На даний момент існуючі квантові комп'ютери недостатньо великі, щоб становити загрозу сучасній криптографії. Однак розгортання нових криптографічних систем забирає багато часу та зусиль, і тому важливо мати заміни ще до того, як з'являться великі потужні квантові комп'ютери. Але як показує практика, просто взяти і замінити існуючі стандарти та протоколи на постквантові не так легко і є багато складнощів: необхідно визначити нові моделі безпеки, розробити нові методи доказів, тощо.

1. Родини постквантових алгоритмів

Наразі у світі триває кілька великих конкурсних процесів задля знаходження ефективних постквантових алгоритмів шифрування та підписів, основним з яких

є конкурс NIST. З самого початку конкурсного процесу у 2017 році NIST виділив 5 основних проблем безпеки: на основі кодів, на основі ізогеній, на основі гешу, на основі багатоваріативних перетворень та на алгебраїчних решітках. В результаті трьох турів залишилися криптопримітиви лише з трьох класів вищеперерахованих проблем, які будуть розглянуті у наступних підрозділах.

1.1. На основі коду. Криптографія на основі кодів використовує теорію кодів, що виправляють помилки. Для деяких спеціально побудованих кодів можна виправити багато помилок, тоді як для випадкових лінійних кодів це складна проблема. Системи шифрування на основі коду сходять до пропозиції McEliece від 1978 року [1] і є одними з найбільш вивчених постквантових схем. Деякі системи підпису на основі коду були розроблені таким чином, щоб пропонувати короткі підписи за рахунок дуже великих розмірів ключів.

Складність проблем загального та синдромного декодування (і деяких їх варіантів) є складовою аргументу безпеки для трьох KEM на основі коду, які проходять до 4-го раунду конкурсу NIST: BIKE, Classic McEliece і HQC. Усі три схеми забезпечують IND-CPA безпеку PKE з доказами.

1.2. На основі багатоваріативних перетворень. Багатоваріативна криптографія належить до кінця вісімдесятих років і ґрунтується на складності пошуку рішення системи багатоваріативних квадратних рівнянь над кінцевими полями. Можна побудувати схеми підписів із систем рівнянь з рівномірно випадковими коефіцієнтами, і вони вважаються найбільш безпечними багатоваріантивними системами. Однак у більш ефективних схемах використовуються односторонні системи рівнянь з секретом. Їх часто називають схемами Oil-and-Vinegar. В даний час багатоваріативні схеми шифрування не дуже ефективні, часто з дуже великими відкритими ключами та довгим часом криптоаналізу.

1.3. На основі алгебраїчних решіток. На високому рівні описи решіток дуже схожі на описи кодів – елементи є векторами довжини n у деякому просторі і до них додаються помилкові вектори. Проблеми, що лежать в основі криптографічних конструкцій, полягають у тому, щоб знайти вихідний вектор з урахуванням помилкового. Решітки пропонують більше параметрів, ніж коди, що означає, що вони можуть запропонувати рішення, краще адаптовані до даної ситуації, але також з'являється більше поверхні для атаки.

Схеми на основі решіток, подані до NIST, переважно використовують наступні дві основні складні проблеми: Module-Learning-with-Errors (Module-LWE) та Module-Learning-with-Rounding (Module-LWR). У цих схемах вибирається поліноміальне кільце $R = \mathbb{Z}[X]/f$, де ступінь f дорівнює n, і розглядається за модулем q (що дає R_q). Крім того, існує ще один цілий параметр d, який називається ступенем модуля. Для Ring-LWE та Ring-LWR встановлюється $d = 1$, а для стандартних LWE та LWR $d = n = 1$.

1.4 Фіналісти 3-го раунду конкурсу NIST. У таблицях 1.1 та 1.2 наведено перелік фіналістів третього раунду NIST, тобто KEM та підписи, що були вибрані для стандартизації і альтернативних кандидатів, що рекомендовані для 4-

го раунду, відповідно, поділяючи їх на дві групи схеми шифрування та підпису, деталізуючи також складні проблеми, на яких вони ґрунтуються.

Таблиця 1

KEM та підписи вибрані для стандартизації

Схема	KEM/підпис	Родина	Складна проблема
Crystals-Kyber	Шифрування на відкритому ключі/KEM	На основі решітки	Кільцевий Module-LWE
Crystals-Dilithium	Підпис	На основі решітки	Кільцевий Module-LWE і Module-SIS
Falcon	Підпис	На основі решітки	Кільцевий SIS
SPHINCS+	Підпис	На основі гешу	Опір попереднього зображення геш-функції

Таблиця 2

Альтернативні кандидати третього раунду

Схема	KEM/підпис	Родина	Складна проблема
BIKE	KEM	На основі коду	Декодування квазі-циклічних кодів
Classic McEliece	KEM	На основі коду	Декодування випадкових бінарних кодів Гоппа
HQC	KEM	На основі коду	Варіант кодування Ring-LWE
SIKE	KEM	На основі ізогеній	Проблема ізогеній з додатковими точками

2. Інтеграція постквантових схем в існуючі протоколи

2.1. Постквантовий WireGuard. WireGuard [2] є відносно новим протоколом VPN, який порушує традицію проектування цих протоколів на основі IPsec і натомість будує їх із сучасними системами та єдиним вибором, уникаючи узгодження між вузлами-учасниками. Постквантовий дизайн WireGuard [3] використовує систему Classic McEliece для довгострокових ключів і Saber для ефемерних ключів. Їхня конструкція виграє від коротких зашифрованих текстів, які надає Classic McEliece, а також високої швидкості генерації ключів і компактного розміру ключа та зашифрованого тексту Saber, не стикаючись із витратами на надсилання великих ключів Classic McEliece. Це дозволяє протоколу підтримувати розмір пакетів UDP у межах 1280 байт.

2.2. Використання постквантової криптографії для VPN. У 2018 році ETSI опублікував [4] аналіз і порівняння використання постквантових систем у VPN. У документі надано детальний опис протоколу Internet Key Exchange (IKE), типової основи для VPN, побудованих на IPsec, Transport Layer Security (TLS), що використовується для транспортування, протоколу Media Access Control Security (MACsec), який іноді використовується для захисту комунікацій. для останньої милі між маршрутизатором і клієнтом і, нарешті, протокол Secure Shell (SSH). Для кожного з цих протоколів проаналізовано вимоги до замінників, а також для комбінованих (гібридних) систем і надано рекомендації.

2.3. Дослідження, що аналізують постквантові системи для TLS. Кілька публікацій торкалися протоколу TLS. Бібліотека Open Quantum Safe (liboqs) дуже спростила створення прототипів, надаючи системи, вмонтовані у форк OpenSSL.

Остання версія TLS – 1.3; досліджує постквантові системи аутентифікації. Зовсім недавно Cloudflare опублікував дослідження [5] про вплив розмірів підписів і сертифікатів постквантових систем на TLS. У цьому дослідженні також розглядалися проблеми автентифікації.

3. Поняття безпеки

Загальноприйнятим очікуванням є те, що квантові комп'ютери загрожують лише безпеці криптографії з відкритим ключем (PKC), а точніше основним схемам PKC, таким як шифрування, KEM і схеми підпису. Однак це здебільшого базується на вже наявних знаннях про атаки, які загрожують цим схемам, тоді як атаки на інші схеми та протоколи наразі невідомі. Поширеним підходом у сучасній криптографії є зменшення поверхні атаки проти математичної безпеки протоколу чи системи, щоб порушити безпеку її основних будівельних блоків за допомогою доказів безпеки. Будівельними блоками в цьому випадку можуть бути або математичні проблеми, такі як проблема RSA або проблема LWE, або це можуть бути KEM, схеми підписів або геш-функції, для яких ми вже встановили безпеку іншим доказом або криптоаналізом. Поняття безпеки, яке ми очікуємо від KEM – це безпека IND-CCA.

3.1. Квантові криптоаналітики. Для наведених вище понять безпеки це означає, що ми повинні вважати, що криптоаналітик є квантовим алгоритмом. Хоча це, звичайно, впливає на складність вирішення математичних завдань, що використовуються, на багато доказів безпеки ця зміна не впливає.

У пост-квантовому випадку ми вважаємо, що криптоаналітики мають доступ до квантового комп'ютера. Оскільки геш-функції є відкритими функціями, це означає, що криптоаналітик може запускати їх на своєму квантовому комп'ютері і, отже, може запитувати їх про суперпозиції входів або навіть заплутані квантові стани. Ця здатність не може бути відображена у звичайному ROM. Отже, був запропонований QROM (квантоводоступний ROM) [6]. У QROM криптоаналітикам надається саме ця додаткова здатність

Перше питання при перегляді існуючих моделей безпеки полягає в тому, чи слід надавати противнику квантовий доступ до наданих оракулів і, якщо так, то до яких. У цьому контексті квантовий доступ до оракула для функції f відноситься до здатності робити запит із суперпозицією вхідних даних для f та отримувати відповідну суперпозицію виходів f. Більш формально, оракул квантової суперпозиції для функції $f: X \to Y$ визначається як унітарне перетворення

$$U_f : \sum_{x\in X, y\in Y} a_{x,y} |x,y\rangle \to \sum_{x\in X, y\in Y} a_{x,y} |x, y \oplus f(x)\rangle, \quad (1)$$

де $\oplus$ відноситься до порозрядного xor. Слід зазначити, що з урахуванням класичного опису f цей квантовий оракул може бути реалізований за допомогою стандартних методів.

Висновки. Таким чином в роботі наведено поточний стан розробки та стандартизації постквантових алгоритмів. Окрім проблем інтерфейсу та швидкості, проблема заміни доквантових систем на постквантові полягає в тому, що це повільний процес, який вимагає років обговорень в органах стандартизації, які контролюють системи. Навіть якщо вибір NIST буде прийнято без змін і ці органи почнуть працювати ще до оголошення повних специфікацій нових стандартів, ще кілька років дані будуть захищені суто доквантовими системами. Для усунення ризиків можна використовувати гібридну систему; тобто розгорнути постквантову криптографію сьогодні як додатковий рівень разом із доквантовою криптографією, а не розгортати її як заміну доквантової криптографії. Однак гібридні системи можуть бути більшою проблемою продуктивності за іншими показниками вартості.

Література

[1] *Robert J. McEliece. A public-key cryptosystem based on algebraic coding theory, 1978. JPL DSN Progress Report. Available at: http://ipnpr.jpl.nasa.gov/progress_report2/42-44/44N.PDF.*

[2] *Jason A. Donenfeld. WireGuard: Next generation kernel network tunnel. In ISOC Network and Distributed System Security Symposium/ 2017. The Internet Society, February/March 2017.*

[3] *Andreas Hülsing, Kai-Chun Ning, Peter Schwabe, Florian Weber, and Philip R. Zimmermann. Post-quantum WireGuard. Cryptology ePrint Archive, Report 2020/379, 2020. Available at: https://eprint.iacr.org/2020/379.*

[4] *ETSI Technical Report. Quantum-safe virtual private networks. ETSI TR 103, 2018. Available: https://www.etsi.org/deliver/etsi_tr/103600_103699/103617/01.01.01_60/tr_103617v010101p.pdf.*

[5] *Bas Westerban. Sizing up post-quantum signatures, 2201. https://blog.cloudflare.com/sizing-up-post-quantum-signatures/.*

[6] *Dan Boneh, Özgür Dagdelen, Marc Fischlin, Anja Lehmann, Christian Schaffner, and Mark Zhandry. Random oracles in a quantum world. In Dong Hoon Lee and Xiaoyun Wang, editors, Advances in Cryptology – ASIACRYPT 2011, volume 7073 of Lecture Notes in Computer Science, pages 41– 69. Springer, Heidelberg, December 2011.*

Current state of standardization of post-quantum cryptography

Yelyzaveta Ostrianska, Yurii Gorbenko

The paper provides an overview and analysis of the current state of standardization of post-quatic cryptography. The development of quantum computers threatens the security of cryptographic algorithms used today. To counter this threat, the field of post-quantum cryptography was launched. But deploying new cryptographic systems takes a lot of time and effort. Thus, policymakers and system owners must be prepared. Currently, standards bodies continue to standardize protocols built using pre-quantum systems that cannot withstand quantum attacks. To such protocols, it is advisable to exchange the concept of hybrid systems (double encryption, double KEM, double signatures, etc.). However, this is not in the current plan. Therefore, it is possible to obtain post-quantum integration when developing new standards or updating existing ones.

Отримано 14.03.23