УДК 004.056
С. Пащак
(Тернопільський національний технічний університет імені Івана Пулюя)

ПЕРСПЕКТИВНІ МЕТОДИ ТА ЗАСОБИ ПОСТКВАНТОВОГО ТА КВАНТОВОГО ЗАХИСТУ ІНФОРМАЦІЇ

S. Pashchak

PROMISING METHODS AND TOOLS FOR POST-QUANTUM AND QUANTUM INFORMATION SECURITY

Важко уявити сучасний світ без ІКС, які в свою чергу спираються на засоби криптографії. Проте, існує низка загроз які ставлять під сумнів стійкість поширених криптографічних систем, тому поява постквантових і квантових систем ставить собі мету розробку систем які не мають такого недоліку.

Постквантова криптографія (Post-quantum cryptography, PQC) є криптографічними способами шифрування та підписання інформації, які є стійкими до атак на базі квантових алгоритмів. Amazon, IBM та Microsoft пропонує своїм користувачам використовувати постквантові алгоритми для захисту даних[1], і не дивно, бо ще у 2021 році у Китаї розробили квантовий комп'ютер який виконує деякі задачі у 10^{24}-рази швидше ніж звичайний комп'ютер[2].

У випадку із квантовою криптографією(Quantum cryptography, QC), безпека базується не на математичних властивостях, а на законах квантової механіки. Якщо постквантову систему можна реалізувати просто змінивши код, для реалізації квантового шифрування потрібні технології рівня провідних лабораторій світу та великого бюджету[3]. Тому сьогодні цей інструмент доступний хіба, що науковій та військовій галузі.

Квантова криптографія, наразі володіє тільки інструментом квантового розподілу ключа(QKD), різняться тільки методи.

В свою чергу зараз перевірені та сертифіковані алгоритм постквантового криптографії такі:

- шифрування з відкритим ключем та встановлення ключів;
- генерація цифрового підпису[4].

Взаємне застосування постаквантових та квантових алгоритмів захисту, теоретично, призводить до існування найбільш захищених ІКС. Наразі, невідомо таких гібридних систем але деякі сервіси вже частково перейшли на системи PQC, дехто це робить в цілях реклами, а дехто заради безпеки. У деяких конкретних випадках, це не несе додаткових витрат, як-от алгоритм Kyber при однаковому розмірі ключа є швидшим за буд-який ECC алгоритм[5], але мають більший розмір ключів та шифру Проте, NIST вже оголосив нових кандидатів, які можливо розв'яжуть дану проблему. Тому подальші дослідженні і впровадження, є дуже перспективним, як у академічному так і комерційному плані.

Література

1. Amazon, IBM Move Swiftly on Post-Quantum Cryptographic Algorithms Selected by NIST URL: https://www.darkreading.com/cyber-risk/amazon-ibm-move-swiftly-on-post-quantum-cryptographic-algorithms-selected-by-nist
2. Two of World's Biggest Quantum Computers Made in China URL: https://spectrum.ieee.org/quantum-computing-china
3. Measurement-Device-Independent Quantum Key Distribution URL: https://journals.aps.org/prl/pdf/10.1103/PhysRevLett.108.130503
4. Post-Quantum Cryptography URL: https://csrc.nist.gov/Projects/post-quantum-cryptography/selected-algorithms-2022
5. Kyber and Post-Quantum Crypto - How does it work? URL: https://pretalx.c3voc.de/media/rc3-2021-cwtv/submissions/UGZY8B/resources/Kyber_and_Post-Quantum_Crypto_-_CCC_pR5OKou.pdf