Технічні науки

УДК: 004.051

Середа Дар'я Антонівна

студентка

Харківського національного університету радіоелектроніки

Середа Дарья Антоновна

студентка

Харьковского национального университета радиоэлектроники

Sereda Daria

Student of the

Kharkiv National University of Radio Electronics

Квасняк Катерина Миколаївна

студентка

Харківського національного університету радіоелектроніки

Квасняк Екатерина Николаевна

студентка

Харьковского национального университета радиоэлектроники

Kvasniak Kateryna

Student of the

Kharkiv National University of Radio Electronics

Науковий керівник:

Олійник Олександр Олександрович

асистент кафедри ПІ

Харківський національний університет радіоелектроніки

КВАНТОВІ ОБЧИСЛЕННЯ ТА КРИПТОГРАФІЯ
КВАНТОВЫЕ ВЫЧИСЛЕНИЯ И КРИПТОГРАФИЯ
QUANTUM COMPUTING AND CRYPTOGRAPHY

Анотація. *Досліджено теоретичні питання щодо впливу квантових комп'ютерів на криптографію.*

Ключові слова: *квантовий комп'ютер, асиметричне шифрування, криптографія, безпека даних, кубіти, ключ, пост-квантова.*

Аннотация. *Исследованы теоретические вопросы о влиянии квантовых компьютеров на криптографию.*

Ключевые слова: *квантовый компьютер, ассиметричное шифрование, криптография, безопасность данных, кубиты, ключ, пост-квантовая.*

Summary. *Theoretical questions about the influence of quantum computers on cryptography have been studied.*

Key words: *quantum computer, asymmetric encryption, cryptography, data security, qubits, key, post-quantum.*

Квантові комп'ютери можуть бути дуже корисними для наукових розробок завдяки новому та швидкому способу виконання обчислень. Однак, як тільки вони будуть доступні, вони можуть порушити криптографію, що використовується в даний час, і підірвати захист (особистих) даних.

Фізичні закони квантової механіки дозволяють створити альтернативний метод для обробки інформації сучасними комп'ютерами. У той час як традиційні комп'ютери використовують біти (0 або 1), квантові комп'ютери використовують квантові біти або кубіти, які одночасно можуть бути комбінацією $|0\rangle$ і $|1\rangle$.

Можливий спектр значень, які може приймати один кубіт, найкраще зображено поверхнею сфери Блоха на рисунку 1. Сфера Блоха – це геометричне зображення кубіта. Кожний з кубітів може приймати значення

кожної точки на поверхні, що описується двома кутами φ і θ. Полюсними точками є $|0\rangle$ або $|1\rangle$.

У той час як біти допускають два дискретних значення, кубіти можуть зберігати точку в двовимірному континуумі, поверхню сфери. Квантові обчислення можуть скористатися перевагами цих потужніших кубітів і виконувати операції не тільки для визначеного значення $|0\rangle$ або $|1\rangle$, а й для всіх можливих суперпозицій одночасно [1]. Отже, квантові обчислення досягають переваги в ефективності перед бінарними обчисленнями для окремих завдань. Деякі завдання були б здійсненні лише завдяки такому підвищенню ефективності, якби було доступне відповідне апаратне забезпечення квантового комп'ютера.

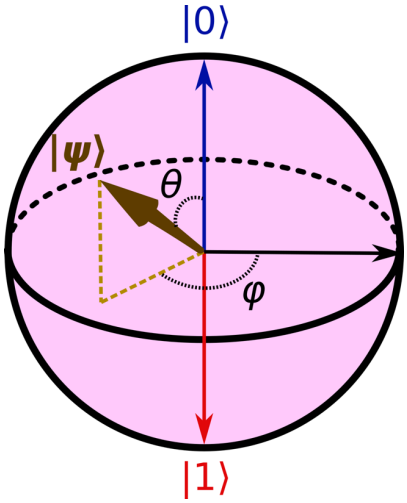

Рис. 1. Сфера Блоха

Існує багато причин, чому квантові обчислення можуть мати значний вплив на захист даних з точки зору безпеки даних і конфіденційності комунікацій. Однією з причин є можливість зламати криптографічний алгоритм. Квантові обчислення можуть зламати безліч алгоритмів сучасної класичної криптографії.

Криптографія з відкритим ключем, також відома як асиметричне шифрування, є методом шифрування даних з використанням криптографічних протоколів, заснованих на алгоритмах. Для цього потрібні

два окремих ключі, приватний і відкритий ключ. Алгоритм Rivest-Sharmir-Adleman (RSA) — це криптографічна система, яка використовується для криптографії з відкритим ключем і зазвичай використовується під час надсилання конфіденційних даних через Інтернет. Алгоритм RSA дозволяє шифрувати повідомлення як відкритими, так і закритими ключами, щоб їх конфіденційність і автентичність залишалися незмінними.

Квантові комп'ютери дозволили би криптографічним системам з відкритим ключем піддаватися небезпеці з боку зломників, якщо вони мали би достатньо потужний квантовим комп'ютер, який міг би здійснити розшифровку без попереднього знання приватного ключа. Ураженими могли би бути, наприклад, цифрові підписи, важливі Інтернет-протоколи, такі як HTTPS (TLS), необхідні для безпечного перегляду, онлайн-банкінг, інтернет-магазини, тощо [2]. Приклад такого квантового комп'ютера представлено на рисунку 2.

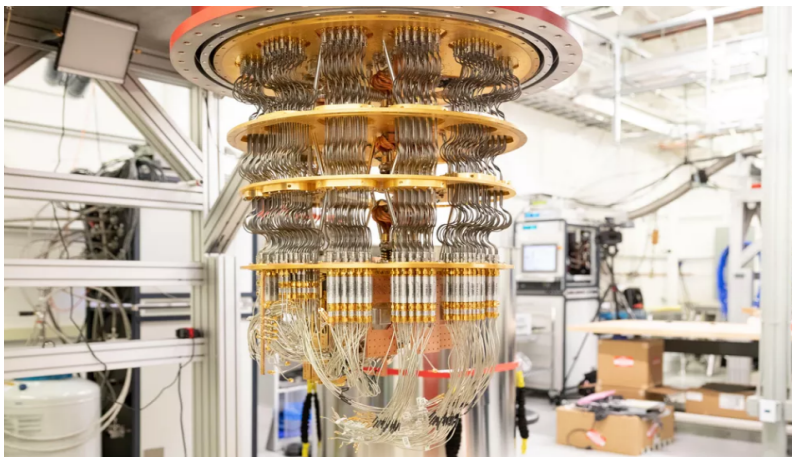

Рис. 2. Квантовий комп'ютер

Квантові обчислення також можуть мати негативні наслідки для гарантії безпеки симетричних криптографічних систем, таких як Advanced Encryption Standard (AES). Асиметрична (наприклад, RSA) і симетрична (наприклад, AES) криптографія часто використовуються разом, наприклад, із використанням HTTPS. Симетрична криптографія потребує практичних

способів конфіденційного обміну приватними ключами. Щоб гарантувати безпеку даних, обмін приватними ключами повинен залишатися безпечним. Але ключові методи обміну, які використовуються сьогодні на практиці, засновані на проблемах, які можуть поставити під загрозу квантові обчислення. Щоб гарантувати конфіденційність даних, весь обмін ключами повинен залишатися безпечним.

Пост-квантова криптографія або квантово-безпечна криптографія відноситься до криптографії, на безпеку якої, як вважають, не впливають квантові комп'ютери. Це досягається використанням дуже різних математичних будівельних блоків, які включають математичні операції, які квантові комп'ютери не можуть вирішувати ефективніше, ніж інші комп'ютери [3].

Проте пост-квантова криптографія, ймовірно, буде мати недоліки в продуктивності та буде потребувати більших обчислювальних ресурсів, наприклад, для шифрування і розшифрування даних, та більше мережевих ресурсів для обміну довгими ключами та сертифікатами. Пост-квантова криптографія ще не стандартизована. Національний інститут США Standards and Technology (NIST) працює над стандартом для пост-квантової криптографії та планує опублікувати проект з першим алгоритмом у 2022 чи 2024 році. Після стандартизації алгоритми буде необхідно інтегрувати зі стандартними інтернет-протоколами, такими як HTTPS [4].

Станом на 2020 рік прототипи (нестандартизованої) пост-квантової криптографії доступні для тестування у вигляді вихідного коду, програмних бібліотек (наприклад, для OpenSSL), хмарних сервісів (наприклад, Amazon AWS і Cloudflare) і споживчого програмного забезпечення (наприклад, Google Chrome). За оцінками, повний перехід на практиці може зайняти навіть 15-20 років. Організації повинні враховувати, як довго їм потрібно гарантувати абсолютну конфіденційність даних і захист від ретроспективного розшифрування.

Виходячи з того, що ми знаємо сьогодні, в осяжному майбутньому квантовий комп'ютер не представляє безпосередньої загрози. Можливо, знадобляться десятиліття, щоб створити придатний для використання квантовий комп'ютер, який може виконувати відомі алгоритми. Але для даних, які повинні залишатися в безпеці дуже довго, ця невизначеність створює проблему, яка може вимагати раннього переходу до постквантової криптографії.

Література

1. Jack D. Hidary Quantum Computing: An Applied Approach. 2020. P. 1265.
2. Quantum computers could crack today's encrypted messages. That's a problem // Cnet: [Веб-сайт]. URL: https://www.cnet.com/tech/computing/quantum-computers-could-crack-todays-encrypted-messages-thats-a-problem/ (дата звернення: 30.11.2021).
3. Валиев К. А. Квантовые компьютеры: можно ли их сделать «большими»? // УФН. 1999. Т. 169. С. 691-694.
4. Steane A. M., Rieffel E. G. Beyond Bits: The Future of Quantum Information Processing // IEEE Computer. January 2000. P. 38-45.