УДК 004.38

ДОСЛІДЖЕННЯ ЗАСТОСУВАННЯ МЕТОДІВ ПОСТ-КВАНТОВОЇ КРИПТОГРАФІЇ ДЛЯ РОЗПОДІЛЕНИХ СИСТЕМ АВТОРИЗАЦІЇ

Нікітченко Б.Ю.
Науковий керівник – к.т.н., доц. Лановий О.Ф.
Харківський національний університет радіоелектроніки, каф. ПІ
м. Харків, Україна
тел.: +38(096) 022-02-59, email: bohdan.nikitchenko@nure.ua.

This work discusses quantum computers and their impact on modern cryptography. It explains how quantum computers can exponentially speed up decryption, which is a serious threat to encryption systems based on algorithms such as RSA, discrete logarithm, and Diffie-Hellman. Post-quantum cryptography (PQC) is suggested as a solution, and several PQC solutions such as lattice-based cryptography, code-based cryptography, and hash-based signatures are proposed. The work also mentions quantum key distribution (QKD) as another solution to the existing cryptography problem.

Квантові комп'ютери – це системи, які використовують властивості квантових станів для виконання обчислень. У сучасних комп'ютерах і КПК дані представлені в бітах у вигляді 0 або 1, але у квантових комп'ютерах 0 і 1 існують одночасно в різних комбінаціях в один і той же час. Здатність існувати одночасно в один і той самий час називається суперпозицією [1].

Криптографія з відкритим ключем (PKC) є основою сучасної безпечної взаємодії в Інтернеті. Криптографія з відкритим ключем є асиметричною, тобто використовує два ключі: один – публічний, який є спільним для всіх, а інший - приватний, який використовується системою для підтвердження своєї ідентичності. Клієнт надсилає повідомлення одержувачу, генеруючи хеш повідомлення і шифруючи його за допомогою відкритого ключа. Сервер використовує свій ключ, приватний ключ, щоб розшифрувати повідомлення, яке може бути розшифроване лише відповідним приватним ключем і не може бути розшифроване жодним іншим ключем, навіть у випадку атаки на посередника.

Ключі, як відкритий, так і закритий, є простими числами. У випадку асиметричного ключа беруться два простих числа, p і q, які складають приватний ключ. Їх добуток p – q є відкритим ключем. Для невеликих чисел p і q буде легко знайти його прості множники. Наприклад, якщо в якості відкритого ключа було задано число 15, то розкладання 15 на прості числа дає 3 і 5. Однак, якщо це число має 200 або 400 цифр, розкласти його на прості числа буде складно для будь-якого сучасного класичного комп'ютера, і на це підуть мільйони або трильйони років.

Складність факторизації простих чисел дозволила криптографії з відкритим ключем працювати протягом багатьох десятиліть без проблем. Але квантові комп'ютери можуть досягти експоненціального прискорення

розшифровки більшості алгоритмів криптографії з відкритим ключем, таких як алгоритм RSA, алгоритм дискретного логарифмування та алгоритм Діффі-Хеллмана, що становить серйозну загрозу для систем шифрування, заснованих на цих алгоритмах.

Для того, щоб вирішити проблеми, пов'язані з квантовими алгоритмами, постквантова криптографія буде спрямована на те, щоб ускладнити квантовим комп'ютерам злам цифрових підписів.

Було запропоновано кілька рішень для постквантової криптографії (PQC), таких як криптографія на основі решітки, кодова криптографія, багатовимірна поліноміальна криптографія та підписи на основі хешу.

Поки тривають активні дослідження, спрямовані на пошук рішення для існуючої криптографії, було запропоновано ще одне абсолютно інше рішення: Квантовий розподіл ключів (QKD) [2]. У мережі, коли дві сторони спілкуються через захищений канал, зловмисник все ще може переглянути зашифрований текст. Завдяки QKD можна виявити підслуховувач ще до того, як він надішле будь-яку захищену інформацію, і одразу ж припинити комунікацію між двома сторонами. Коли підслуховувач втручається, він впливає на квантовий стан, і таким чином дві сторони дізнаються про зміну.

Квантовий розподіл ключів – це процес безпечної передачі симетричних ключів під час виконання алгоритмів PQC. Для класичних систем обмін секретними симетричними ключами через ненадійне середовище буде проблематичним у квантовий час. QKD намагається вирішити цю проблему. Насправді, існують різні алгоритми розподілу ключів з використанням схем з відкритим ключем, які не є RSA або ECC, але QKD пропонує гарантії безпеки, засновані на законах фізики. Крім того, він буде стійким до квантових атак. Причиною цього є те, що QKD досягається шляхом кодування даних з використанням квантових станів світла, які неможливо зламати зловмиснику [2].

В епоху PQC додатки повинні мати можливість працювати з більш ніж одним криптографічним алгоритмом для обробки як квантових, так і класичних шифрів. Використання механізмів гібридних ключів дозволить новим додаткам захиститися від квантових загроз, зберігаючи при цьому традиційні стандарти. Зрештою, організаціям необхідно підготуватися до нових стандартів шифрування.

Список використаних джерел:

1. Azure.Microsoft Superposition, and entanglement https://azure.microsoft.com/en-us/resources/cloud-computing-dictionary/what-is-a-qubit/#introduction

2. QKD quantum key distribution (2022, листопад) https://www.techtarget.com/searchsecurity/definition/quantum-key-distribution-QKD