УДК 681.3.06

ВЛАДИСЛАВ ВЛАДИСЛАВОВИЧ ГУДІЛІН

курсант 2 курсу факультету №4 Харківського національного університету внутрішніх справ

ВОЛОДИМИР МИХАЙЛОВИЧ СТРУКОВ

кандидат технічних наук, доцент, професор кафедри інформаційних технологій та кібербезпеки факультету №4 Харківського національного університету внутрішніх справ

ПРОБЛЕМИ ЗАХИСТУ ЗАШИФРОВАНИХ ДАНИХ В ЕПОХУ КВАНТОВИХ ТЕХНОЛОГІЙ

На сьогоднішній день більша частина інформації, яка передається по відкритих каналах передачі даних, шифрується з впровадженням криптографічних систем з відкритим ключем. Принцип роботи даних систем полягає у використанні двох ключів. Відкритий ключ кореспондента використовується при шифруванні вихідного повідомлення. Він публікується у відкритому доступі. Закритий або секретний ключ вживають при розшифровці отриманого повідомлення. З кінця 70-х років XX століття найбільш використовуваною системою з відкритим ключем є алгоритм RSA. Стійкість алгоритму RSA ґрунтується на тому, що факторизація великих чисел – дуже складна математична задача, для розв’язання якої до сих пір не існує достатніх обчислювальних потужностей, а також ефективного алгоритмічного рішення. Саме тому криптографічна система з відкритим ключем довгий час вважалася однією з найнадійніших систем шифрування [1].

Однак в 1994 році американський вчений Пітер Шор розробив квантовий алгоритм факторизації (алгоритм Шора). Отриманий квантовий алгоритм, на відміну від класичних алгоритмів, справляється із завданням факторизації за поліноміальний час. Виходячи з цього факту алгоритм Шора може бути використаний для злому RSA. Суть алгоритму полягає в зведенні задачі

факторизації до пошуку періоду деякої функції. Якщо відомий її період, то факторизація здійснюється за допомогою алгоритму Евкліда за реальний час на класичному комп'ютері. Таким чином, підхід Шора включає в себе дві частини: класичну і квантову. Квантова частина займається пошуком періоду функції, а класична частина спочатку готує цю функцію, а потім перевіряє період, знайдений квантовою частиною. Якщо період знайдений правильно, то задача буде вирішена. Таким чином, Пітер Шор показав, що досить потужний квантовий комп'ютер може з легкістю зламати алгоритм RSA, і це викликало шок серед спеціалістів з інформаційної безпеки.

Вважалося, що для злому RSA-шифрування, на якому побудовані сьогодні майже всі системи, що передають і зберігають конфіденційну інформацію, необхідний квантовий комп'ютер з мільярдом кубітів. Однак нещодавно дослідження квантових обчислень, проведене Крейгом Гідні з Google і Мартіном Екерой з Королівського інституту в Стокгольмі, відкрило більш ефективний метод злому систем шифрування і на порядок скоротило вимоги до ресурсів. Вони довели, що для злому знадобиться всього 20 млн кубіт і вісім годин роботи. Крім того, вони підрахували, що пристрої з 20 млн кубіт, що неможливі сьогодні, можуть стати реальністю через 25 років [2].

Прогрес в області створення квантового комп'ютера йде швидше ніж передбачалося. Кращого результату у розробці квантового комп’ютера домоглася компанія IBM, яка за допомогою квантового комп'ютера з п'яти кубітів змогла розкласти на множники число 15. Канадська компанія D-Wave випускає квантові комп'ютери з тисячі кубітів, з якими експериментують в Google і NASA. Однак машина D-Wave – не універсальний квантовий комп'ютер, і її перевага в порівнянні з класичними комп'ютерами багатьма оскаржується. Поряд з успіхами компаній IBM і Google, наукові групи з Гарварда та університету Меріленду практично одночасно реалізували дві нові системи для квантових обчислень з 51 і 53 кубітами.

Отже, зі збільшенням загроз шифрування даних за допомогою традиційного алгоритму RSA, слід впроваджувати нові підходи шифрування інформації. Спеціалісти пропонують застосувати квантову та постквантову криптографію. Перший підхід – постквантова криптографія пропонує нові алгоритми шифрування, які базуються на математичних задачах, що представляють складність для злому як «класичними», так і квантовими комп'ютерами. На цей момент в сфері постквантової криптографії ведуться наукові дослідження з пошуку таких алгоритмів, виконуються перевірки існуючих рішень і пілотні проекти їх реалізації. Однак до сих пір на ринку відсутні єдині визнані стандарти постквантового шифрування, які довели свою ефективність. Можлива ситуація, при якій з розвитком квантових комп'ютерів обраний алгоритм вже не забезпечить необхідний рівень захисту, і його доведеться міняти. Тому важливо вибрати оптимальний алгоритм відразу. Інша особливість постквантової криптографії – це високі вимоги до обчислювальних ресурсів. З одного боку, дані алгоритми можна реалізувати практично в будь-якому програмному коді, з іншого боку – при зростанні обсягів даних, що захищаються, потужності наявного обладнання може виявитися недостатньо.

Другий підхід – квантова криптографія, яка для забезпечення секретності інформації використовує основні закони квантової механіки. У квантовій криптографії можна виділити наступні основні напрямки: технології квантової передачі даних, технології квантового розподілу ключів, квантове шифрування, технології квантової цифрового підпису, технології квантового хешування. Математично було доведено, що квантові канали передачі даних є найбезпечнішими, що дозволяє отримати новий рівень захисту інформації. Носієм інформації, яка зашифрована з використанням законів квантової механіки, в даному випадку буде квантовий об'єкт, наприклад, фотон. Згідно фундаментальним законам квантової фізики вимір квантового об'єкта або будь-який інший вплив на нього призводить до зміни його стану. З цього випливає, що

спроба перехопити повідомлення або прослуховування каналу призведе до зміни стану фотона, що відразу ж стане відомо одержувачу. Складність перехоплення та розшифрування інформації полягає у поляризації фотона. Поляризація використовується, як для шифрування так і для дешифрування. Наприклад, фотони, що поляризовані по вертикалі, можуть кодувати одиницю, а по горизонталі – нуль. Виміряти поляризацію можна тільки один раз, після чого стан незворотньо змінюється. Квантові канали передачі даних є основою для реалізації алгоритмів квантового розподілу ключів – головного напрямку розвитку квантової криптографії. Технологія квантового розподілу ключів дозволяє розподіляти ключі між віддаленими користувачами по відкритих каналах зв'язку, ґрунтуючись на законах квантової фізики. Технологія квантового розподілу ключів будується на неможливості копіювання невідомого квантового стану, неможливості прослухати сигнал, неможливості абсолютно надійно розрізнити два різних стани [3].

Квантова криптографія є цілком працюючою технологією. Наприклад, швейцарська приватна компанія ID Quantigue забезпечувала захист даних при пересиланні результатів підрахунку голосів на виборах в Швейцарії за допомогою квантової криптографії. Перешкодою для повсюдного застосування квантової криптографії є обмежена відстань, на яке можна передавати фотони. Проходячи через оптичне волокно, половина фотонів втрачається кожні 10-15 км, що робить передачу ключа на відстань більше 200-300 км практично неможливою. Але Китай запропонував вирішити цю проблему, запустивши квантовий супутник. Супутник проводить сеанси квантового зв’язку зі станціями, що розташовані на Землі, поки пролітає над ними. Це дозволяє суттєво збільшити відстань при передачі даних у зашифрованому стані між віддаленими точками.

Таким чином, з розвитком квантових технологій всі традиційні асиметричні та симетричні алгоритми шифрування стають все менш надійними. Так, для

вирішення цієї масштабної задачі державним та приватним установам слід спрямувати увагу на впровадження постквантової та квантової криптографії.

Список використаних джерел:

1. Simon Singh The Code Book. Doubleday. 1999. 416 с.
2. How to factor 2048 bit RSA integers in 8 hours using 20 million noisy qubits by Craig Gidney and Martin Ekera. URL: https://www.researchgate.net/publication/333338015_How_to_factor_2048_bit_RSA_integers_in_8_hours_using_20_million_noisy_qubits.
3. Willi-Hans Steeb, Yorick Hardy Problems and Solutions in Quantum Computing and Quantum Information (third edition). World Scientific. Singapore. 2011.