

УДК 004.75:339.722

Ковальов І.Є.¹, Воскобойник В.О.²

¹ студ. гр. РТ-819 НУ «Запорізька політехніка»

² канд. техн. наук, проф. НУ «Запорізька політехніка»

ЯК ЗМІНИТЬСЯ КРИПТОГРАФІЯ ПІСЛЯ ПОЯВИ КВАНТОВИХ КОМП'ЮТЕРІВ

Не зважаючи на те, що реально працюючого квантового комп'ютера ще створено, криптоаналітики стверджують, що квантові комп'ютери несуть дуже великий ризик навіть для найсучасніших методів криптографії. Це пояснюється тим, що квантові комп'ютери здатні збільшити свої обчислювальні потужності в експоненціальному розмірі, використовуючи квантові біти (кубіти) в якості елементної бази.

Кубіти здатні одночасно представляти різні можливі стани, проміжні між 0 і 1 - це явище називається суперпозицією, а також впливати на біти в просторі, використовуючи принцип квантової заплутаності.

За допомогою цих явищ, машина з 300 кубітами здатна представляти більше значень, ніж кількість атомів в спостережуваного Всесвіту.

Для більшого розуміння, порівняємо класичні біти з квантовими: якщо маючи 8 класичних бітів можна отримати одне з 256 значень, то 8 квантових бітів можуть представляти собою одночасно 256 значень і тому кожен новий кубіт подвоює кількість можливих значень (що добре видно на рисунку 1), саме за рахунок цього і підіймається його потужність обчислень.

І постає важливе питання: що потрібно зробити, щоб уникнути загрози витоку величезного об'єму інформації, тому що, хакери спробують використовувати квантові алгоритми в своїх цілях, оскільки вони можуть допомогти їм набагато швидше пробиватися через алгоритми шифрування.

Один з алгоритмів, опублікований Ловом Гровером з AT & T Bell Labs, допомагає квантовим комп'ютерам набагато швидше шукати варіанти вирішення рівняння. Ще один алгоритм, опублікований в 1994 році Пітером Шором, допомагає за допомогою квантових комп'ютерів неймовірно швидко знаходити прості множники цілих чисел. Це загрожує безпеці, так як більшість традиційних криптосистем спирається на факторизації цілих чисел або завдання дискретного логарифмування.

Вчені шукають алгоритми шифрування, які будуть стійкими навіть до квантових комп'ютерів.

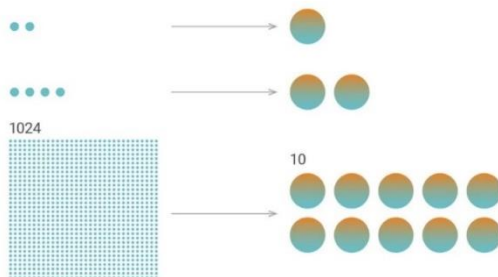


Рисунок 1 – співвідношення необхідної кількості бітів до кубітів

У останніх наукових роботах вказується, що комп'ютер з 20 млн. кубітів зможе впоратися з алгоритмом RSA всього за 8 годин, в той час як класичний комп'ютер буде це робити декілька сотень років. Прогрес квантових обчислень непередбачуваний і стрибок в створенні квантового комп'ютера може бути зроблений коли завгодно, тому важливо вже мати якісь рішення для протидії квантовим комп'ютерам.

Основна проблема на шляху створення квантових комп'ютерів – це елементна база. В якості кубіту є перспективним застосування стабілізованих фотонів як універсальних частин, спроможних використовувати своє призначення в обробці інформації. Проблема в тому, що через деякий час кубіт втрачає свої дані і цей час дуже-дуже малий. Через це, сучасні перспективні прототипи працюють при температурі - 273,13 градусів за Цельсієм (0.02 Кельвіни).

Аналіз сучасних алгоритмів шифрування показує, що методи криптографії в квантовій електроніці потребують збільшення розмірів цифрових ключів для значного збільшення кількості варіантів підтвердження дійсності користувачів. Так, просте подвоєння розміру ключа з 128 до 256 біт збільшує кількість можливих варіантів, які доведеться перебрати квантової системі, що використовує алгоритм Гровера. Тому є доцільним використовувати підхід на базі більш складних функцій з потайним входом для протидії алгоритму Шора.

Враховуючи вище сказане, слід відзначити, що важливість цього напрямку пов'язана з тим, що технології криптографії мають перспективу подальшого вдосконалення та впровадження в безліч галузей діяльності.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Roger A. Grimes, Cryptography Apocalypse: Preparing for the Day When Quantum Computing Breaks Today's Crypto. Видавництво «ДМК Прес», 2020. –290 с.