Бочко О.О. *— рецензент Бритов О.А.*
ННК "ІПСА" НТУУ "КПІ"

Алгоритм Шора

Алгоритм Шора – це квантовий алгоритм факторизації (розкладання числа на прості множники), що дозволяє розкласти число N за час $O((\log N)3)$, витративши $O(\log N)$ місця. Алгоритм складається з двох частин. Перша частина алгоритму перетворює задачу факторингу на задачу знаходження періоду функції, і може бути реалізована класично. Друга частина знаходить період за допомогою квантового перетворення Фур'є, і відповідальна за квантове прискорення алгоритму.

Значимість алгоритму полягає в тому, що при використанні досить потужного квантового комп'ютера, він зробить можливим злом криптографічних систем з відкритим ключем. Приміром, RSA використовує відкритий ключ N, що є добутком двох великих простих чисел. Один зі способів зламати шифр RSA – знайти множники N. При досить великому N це практично неможливо зробити, використовуючи відомі класичні алгоритми. Так як алгоритм Шора працює тільки на квантовому комп'ютері, в даний час не існує технічних засобів, що дозволяють за поліноміальний час від довжини числа розкласти достатньо велике число на множники. Алгоритм Шора у свою чергу, використовуючи можливості квантових комп'ютерів, здатний призвести факторизації числа за поліноміальний час. Це може поставити під загрозу надійність більшості криптосистем з відкритим ключем, заснованих на складності проблеми факторизації чисел.

Алгоритм Шора заснований на можливості швидко обчислити власні значення унітарного оператора з високою точністю, якщо можна ефективно обчислювати будь-які його ступеня. Взявши в якості такого оператора множення на x за модулем N (цей оператор діє в $2n$-мірному просторі, де, перетворюючи базисний вектор, що відповідає числу a, в базисний вектор, що відповідає числу $xa \pmod N$), ми зможемо обчислити таке n, що $xn = 1 \pmod N$, що дозволяє (з високою ймовірністю) N розкласти на множники на звичайному комп'ютері.

Як і інші алгоритми для квантових комп'ютерів, алгоритм Шора імовірнісний: він дає вірну відповідь з високою ймовірністю. Імовірність помилки може бути зменшена при повторному використанні алгоритму. Алгоритм може бути модифікований так, що відповідь, отримана за поліноміальний час, буде вірна з одиничною ймовірністю. Алгоритм Шора був розроблений Пітером Шором в 1994 році. Через сім років, в 2001 році, його працездатність була продемонстрована групою фахівців IBM. Число 15 було розкладено на множники 3 і 5 за допомогою квантового комп'ютера з 7 кубіта (кубіт – квантовий розряд або найменший елемент для зберігання інформації в квантовому комп'ютері).

В листопаді 2007 року компанія D-Wave провела демонстрацію роботи зразка 28-кубітного комп'ютера та анонсувала плани про створення 1024-кубітного комп'ютера в найближчому майбутньому. Враховуючи вищезгадані факти, можна очікувати на революційні зміни в сфері криптографії, оскільки квантові алгоритми, зокрема алгоритм Шора, може кардинально понизити рівень криптостійкості популярних нині систем шифрування інформації.

Література

1. *Kilin S. Ya.* Quanta and information / Progress in optics. – 2001. – Vol. 42. – P. 1–90.
2. К.А. Валиев, А.А. Кокин: "Квантовые компьютеры: надежды и реальность". Москва, Ижевск: Регулярная и хаотическая динамика, 2004. – 320 с.