Кожухівський Андрій Дмитрович
доктор тех. наук, професор, професор кафедри Систем та технологій кібербезпеки

Квантовий алгоритм пошуку в несортованій базі даних

Одним з добре відомих класичних алгоритмів є алгоритм пошуку деякого обраного елемента з великого набору N елементів в сортованій базі даних, який можна визначити, наприклад, методом дихотомії. Цей алгоритм входить в якості підпрограми у велетенське число різноманітних програм. З фізичної точки зору це відповідає пошуку білої кулі серед N - 1 чорних куль, що лежать в урні. Зрозуміло, не можна підглядати, а можна тільки виймати кулі по черзі і тоді розглядати їх, визначаючи, вийняли потрібну кулю або ні. Біла куля буде знайдена класичним алгоритмом з вірогідністю 1/2 після $N/2$ спроб. Чи існує алгоритм пошуку, що дозволяє знайти потрібний елемент за менше число спроб? Несподівано виявилось, що такий алгоритм існує. Саме такий, але вже квантовий алгоритм пошуку був запропонований Гровером. Важливість існування такого алгоритму в тому, що він демонструє переваги квантових обчислень над класичними. Тому обговоримо цей алгоритм детальніше.

Нехай серед $N = 2^n$ елементів треба вибрати один. Розпочнемо з того, що кожному елементу x_i зіставимо певний стан n кубітів виду $|\dots,0,0,\dots,1,0,1,\dots,1\rangle$. Таких станів рівно $N = 2^n$. Тому одному елементу можна зіставити рівно один стан. Тоді завдання зводиться до пошуку одного стану, що відповідає шуканому елементу серед 2^n станів. Для того, щоб можна було виділити шуканий елемент від інших елементів x_i , $i \neq 0$, він повинен відрізнятися від них. Іншими словами, шуканий елемент повинен мати властивість, що відрізняє його від інших елементів. У фізичному прикладі це був колір кулі. З нормальної точки зору існування такої властивості означає існування функції $C(x)$, такої, що $C(x_0) = 1$, а $C(x_i) = 0$, якщо $i \neq 0$. Тоді можна припустити, що можна побудувати квантову схему, яка в стані розрізняти шуканий стан кубітів від інших станів. Якщо не вдаватися до внутрішнього устрою такої схеми, то її дію можна зображувати, як на наведеному в презентації рисунку. Важливо відмітити, що дія цієї схеми оборотна і, отже, такий унітарний оператор може бути побудований. Часто така схема називається оракулом.