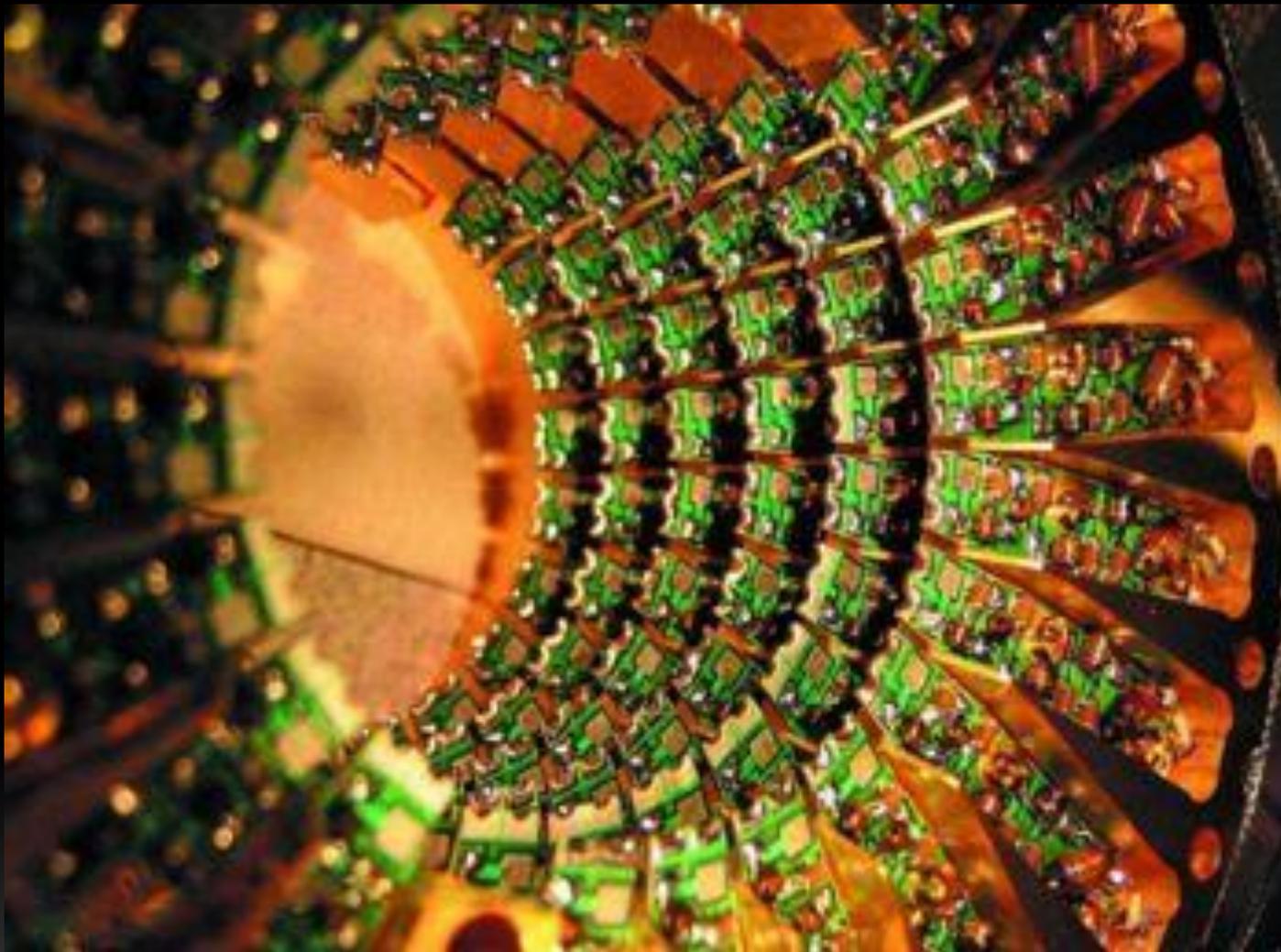


Что такое квантовый компьютер

Квантовый компьютер — вычислительное устройство, которое использует явления квантовой суперпозиции и квантовой запутанности для передачи и обработки данных.



Так выглядит рабочий узел квантового компьютера изнутри. Температура процессорной зоны должна быть близка к абсолютному нулю.

Возможное применение.

Благодаря огромной скорости разложения на простые множители, квантовый компьютер позволит расшифровывать сообщения, зашифрованные асимметричным криптографическим алгоритмом RSA. До сих пор этот алгоритм считается сравнительно надёжным, так как эффективный способ разложения чисел на простые множители для классического компьютера в настоящее время неизвестен. Для того, например, чтобы получить доступ к кредитной карте, нужно разложить на два простых множителя число длиной в сотни цифр. Даже для самых быстрых современных компьютеров выполнение этой задачи заняло бы в сотни раз больше времени, чем возраст Вселенной. Благодаря алгоритму Шора эта задача становится вполне осуществимой, если квантовый компьютер будет построен.

Применение идей квантовой механики уже открыли новую эпоху в области криптографии, так как методы квантовой криптографии открывают новые возможности в области передачи сообщений. Прототипы систем подобного рода находятся на стадии разработки.

Возможность квантовой телепортации.

Алгоритм телепортации реализует точный перенос состояния одного кубита (или системы) на другой. В простейшей схеме используются 3 кубита: телепортируемый кубит и запутанная пара, один кубит которой находится на другой стороне. Отметим, что в результате работы алгоритма первоначальное состояние источника разрушится — это пример действия общего принципа невозможности клонирования — невозможно создать точную копию квантового состояния, не разрушив оригинал. Не получится скопировать произвольное состояние, и телепортация — замена этой операции.

Телепортация позволяет передавать квантовое состояние системы с помощью обычных классических каналов связи. Таким образом, можно, в частности, получить связанное состояние системы, состоящей из подсистем, удалённых на большое расстояние.

Главные технологии для квантового компьютера:

- 1.Твердотельные квантовые точки на полупроводниках: в качестве логических кубитов используются либо зарядовые состояния (нахождение или отсутствие электрона в определённой точке) либо направление электронного и/или ядерного спина в данной квантовой точке. Управление через внешние потенциалы или лазерным импульсом.
- 2.Сверхпроводящие элементы (джозефсоновские переходы, СКВИДы и др.). В качестве логических кубитов используются присутствие/отсутствие куперовской пары в определённой пространственной области. Управление: внешний потенциал/магнитный поток.
- 3.Ионы в вакуумных ловушках Пауля (или атомы в оптических ловушках). В качестве логических кубитов используются основное/возбуждённое состояния внешнего электрона в ионе. Управление: классические лазерные импульсы вдоль оси ловушки или направленные на индивидуальные ионы + колебательные моды ионного ансамбля.
- 4.Смешанные технологии: использование заранее приготовленных запутанных состояний фотонов для управления атомными ансамблями или как элементы управления классическими вычислительными сетями.

Вывод

- Квантовый компьютер это сложная технология, и ее реализация требует ресурсов пока что недоступных на данный момент времени.
- С его помощью можно расшифровать любую шифровку от паролей в интернете до банковских карт и тд.
- Телепортация кубитов (информации) на любые расстояния.
- Уже в наши дни есть экспериментальные прототипы квантовых компьютеров, которые могут выполнять простейшие алгоритмы в этой сложной системе

