Отцова Е. А.
ВлГУ, ИВТ, ИМ-101

КВАНТОВЫЕ КОМПЬЮТЕРЫ, ПЕРЕВЕРНУВШИЕ МИР

ВВЕДЕНИЕ

Как это часто бывает с великими идеями, сложно выделить первооткрывателя. По-видимому, первым обратил внимание на возможность разработки квантовой логики венгерский математик И. фон Нейман. Однако в то время ещё не были созданы не то что квантовые, но и обычные, классические, компьютеры. А с появлением последних основные усилия ученых оказались направлены в первую очередь на поиск и разработку для них новых элементов (транзисторов, а затем и интегральных схем), а не на создание принципиально других вычислительных устройств.

Ещё в начале 1980-х г. лауреат Нобелевской премии по физике Ричард Фейман (82) заметил, что определённые квантово-механические операции нельзя в точности переносить на классический компьютер. Это наблюдение натолкнуло на мысль, о том, что вычисления будут более продуктивными, если они будут производиться при помощи квантовых операций.

Например, ученые, занимающие квантовыми исследованиями пришли к выводу, что практически невозможно напрямую рассчитать состояние эволюционирующей системы, состоящей всего лишь из нескольких десятков взаимодействующих частиц, например молекулы метана (CH_4). Объясняется это тем, что для полного описания сложной системы необходимо держать в памяти компьютера экспоненциально большое (по числу частиц) количество переменных. Возникла парадоксальная ситуация: зная уравнение эволюции, зная с достаточной точностью все потенциалы взаимодействия частиц друг с другом и начальное состояние системы, практически невозможно вычислить ее будущее, даже если система состоит лишь из 30 электронов в потенциальной яме, а в распоряжении имеется суперкомпьютер с оперативной памятью, число битов которой равно числу атомов в видимой области Вселенной(!). И в то же время, для исследования динамики такой системы можно просто поставить эксперимент с 30 электронами, поместив их в заданные потенциал и начальное состояние.

На это, в частности, обратил внимание русский математик Ю. И. Манин, указавший в 1980 году на необходимость разработки теории квантовых вычислительных устройств. В 1980-е годы эту же проблему изучали американский физик П. Бенев, явно показавший, что квантовая система может производить вычисления, а также английский ученый Д. Дойч, теоретически разработавший универсальный квантовый компьютер, превосходящий классический аналог.

Однако создание квантовых компьютеров и машин, в которых используются квантовые операции, оказалось очень сложным, поэтому это направление развивалось крайне медленно. НО так продолжалось только до 1994 года – когда Питер Шор, удивив мир, описал квантовый алгоритм разложения целых чисел на множителя за полиномиальное время.

ЗНАЧЕНИЕ ОТКРЫТИЯ

Всем известно, что скромный продукт фирмы RSA Data Security, Inc., названный так в честь его авторов – американских математиков Ривеста, Шамира и Адельмана, встроен в большинство продаваемых операционных систем, а также во множество других приложений, используемых в различных устройствах – от смарткарт до сотовых телефонов.

Алгоритм RSA – самый распространенный метод шифрования с открытым ключом. Причем для создания пары открытого и закрытого ключей используется следующая важная гипотеза. Если имеется два больших (требующих более сотни десятичных цифр для своей записи) *простых* числа M и K, то найти их произведение N=MK не составит большого труда (для этого даже не обязательно иметь компьютер: достаточно аккуратный и терпеливый человек сможет перемножить такие числа с помощью ручки и бумаги). А вот решить обратную задачу, то есть, зная большое число N, разложить его на простые множители M и K (так называемая *задача факторизации*) – практически невозможно!

Для проверки справедливости гипотезы о практической сложности разложения на множители больших чисел проводились и до сих пор еще проводятся специальные конкурсы. Рекордом считается разложение всего лишь 155-значного (512-битного) числа. Вычисления велись

параллельно на многих компьютерах в течение семи месяцев 1999 года. Если бы эта задача выполнялась на одном современном персональном компьютере, потребовалось бы примерно 35 лет машинного времени! Расчеты показывают, что с использованием даже тысячи современных рабочих станций и лучшего из известных на сегодня вычислительных алгоритмов одно 250-значное число может быть разложено на множители примерно за 800 тысяч лет, а 1000-значное - за 10^{25}(!) лет. (Для сравнения возраст Вселенной равен ~10^{10} лет.)

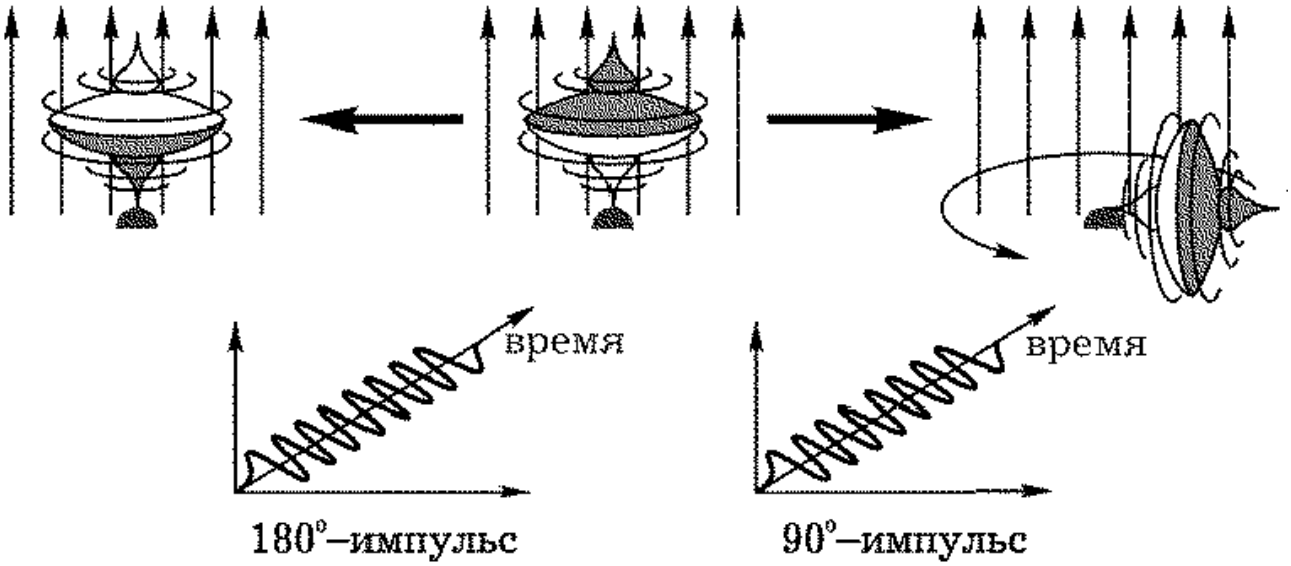
Поэтому криптографические алгоритмы, подобные RSA, оперирующие достаточно длинными ключами, считались абсолютно надежными и использовались во многих приложениях.

Оказывается, используя законы квантовой механики, можно построить такие компьютеры, для которых задача факторизации (и многие другие!) не составит большого труда. Согласно оценкам, квантовый компьютер с памятью объемом всего лишь около 10 тысяч квантовых битов способен разложить 1000-значное число на простые множители в течение всего нескольких часов

В это время теория квантовых компьютеров и квантовых вычислений утвердилась в качестве новой области науки.

КВАНТОВАЯ ИНФОРМАЦИЯ

Основная ячейка квантового компьютера – квантовый бит, q-бит. Это квантовая частица, имеющая два базовых состояния, которые обозначаются $|0\rangle$ и $|1\rangle$. Двум значениям q–бита могут соответствовать, например, направления вверх и вниз спина атомного ядра.



В отличии от классического бита, q-бит может находиться в состоянии суперпозиции, то есть одновременно в состоянии 1 и 0. Обычное классическое толкование этой ситуации – это изображение оси спинов частиц под углом 90° к постоянному магнитному полю.

Если один q-бит находится в суперпозиции двух состояний 0 и 1, то 2 q-бита могут находиться в суперпозиции четырех состояний: 00, 01, 10, 11.

Если имеется классический и квантовый регистры, импульс, который можно рассматривать как вычислительную операцию для классического регистра, изменит m переменных. Если же это квантовый регистр, то тот же импульс может одновременно преобразовать 2^m переменных. Таким образом, квантовый регистр, в принципе, способен обрабатывать информацию в 2^m / m раз быстрее по сравнению со своим классическим аналогом.

Этим и объясняется экспоненциальное увеличение скорости вычислений по сравнению с классическими компьютерами.

Состояния суперпозиции называют запутанными состояниями, для которых существует парадокс ЭПР. Заключается в том, что с помощью ЭПР пары можно распространять сигналы быстрее скорости света.

КВАНТОВЫЕ АЛГОРИТМЫ

В 1996 году коллега Шора по работе в Lucent Technologies Лов Гровер предложил квантовый алгоритм быстрого поиска в неупорядоченной базе данных. Если для обнаружения произвольной записи среди N записей с вероятностью успеха 50% классическим методом требуется в среднем N/2 обращений, то квантовому методу Гровера для достижения той же вероятности достаточно числа обращений, пропорционального квадратному корню из N. Например, если вы ищете имя в неотсортированном списке из 100 млн. разных имен, то классическому алгоритму, чтобы найти его с вероятностью 50/50, придется проверить 50 млн. имен. Квантовому компьютеру, исполняющему алгоритм Гровера, для той же цели потребуется всего 10 тыс. обращений к базе данных. 5000-кратное ускорение.

ПОСТРОЕНИЕ КВАНТОВОГО КОМПЬЮТЕРА

Ученые проводят эксперименты для построения КК с использованием ядерного магнитного резонанса (ЯМР).

ЯМР оперирует с квантовыми частицами в ядрах внутри молекул жидкости. Частицы со спином действуют как крошечные магнитики и будут выстраиваться вдоль приложенного внешнего магнитного поля. Две противоположные ориентации соответствуют двум квантовым состояниям с различными энергиями, которые составляют q-бит. Можно сказать, что параллельный спин соответствует числу 1 и антипараллельный – 0.

В дополнение к этому ЯМР использует переменные электромагнитные поля. Прикладывая переменное поле на правильной частоте, определенные спины можно заставить перевернуться в другое состояние. Это особенность позволяет переориентировать ядерные спины по желанию. Например, протоны (ядра водорода), помещенные в магнитное поле с напряженностью 10 тесла, можно заставить изменить направление спина, прикладывая магнитное поле, осциллирующее с частотой 400 МГц – то есть на радиочастотах.

Группа исследователей из Гарвардского и Массачусетского университетов в качестве эксперимента использовали хлороформ $CHCl_3$.

Прототипы квантовых компьютеров существуют уже сегодня. Правда, пока что экспериментально удается собирать лишь небольшие регистры, состоящие всего из нескольких квантовых битов. Группа, возглавляемая американским физиком И. Чангом (IBM), объявила о сборке 5-битового квантового компьютера. Несомненно, это большой успех. Квантовые системы еще не способны обеспечить надежные вычисления, так как они либо недостаточно управляемы, либо очень подвержены влиянию шумов.

АЛЬТЕРНАТИВА

Предлагается собирать квантовые регистры из миниатюрных сверхпроводниковых колец. Каждое кольцо выполняет роль q-бита, а состояниям 0 и 1 соответствуют направления электрического тока в кольце - по часовой стрелке и против нее. Переключать такие q-биты можно магнитным полем.

Два варианта размещения q-битов в полупроводниковых структурах. В первом случае роль q-бита выполняет электрон в системе из двух потенциальных ям, создаваемых напряжением, приложенным к мини-электродам на поверхности полупроводника. Состояния 0 и 1 - положения электрона в одной из этих ям. Переключается q-бит изменением напряжения на одном из электродов. В другом варианте q-битом является ядро атома фосфора, внедренного в определенную точку полупроводника. Состояния 0 и 1 - направления спина ядра вдоль либо против внешнего магнитного поля. Управление ведется с помощью совместного действия магнитных импульсов резонансной частоты и импульсов напряжения.

СПИСОК ИСПОЛЬЗУЕМЫХ ИСТОЧНИКОВ

1. IEEE Spectrum, February 2001: The Topsy Turvy World of Quantum Computing *by Justin Mullins*.
2. Человек и компьютер, Февраль 2001: Федичкин Л. Квантовые компьютеры.
3. Н. Гершенфелд, И. Чанг Квантовые вычисления с молекулами, 1998.