Министерство образования и науки Российской Федерации
Федеральное агентство по образованию
ГОУ ВПО Владимирский государственный университет
Кафедра информационных систем и информационного менеджмента

Доклад
«Квантовые компьютеры»

Выполнил:
ст. гр. ИМ-204
Денисов П.И.
Проверил:
Огрызков С.А.

Владимир 2005

Введение

Цивилизация развивалась по мере того, как люди открывали новые способы использования различных физических ресурсов, таких как материалы, силы и машины. В 20-м веке, когда изобретение компьютеров позволило выполнять сложную обработку данных вне человеческого мозга, в этот список была добавлена информация. История компьютерной технологии состоит из последовательности скачков от одной физической реализации к другой – от шестеренок к реле, от реле к электронным лампам, от ламп к транзисторам, от транзисторов к интегральным схемам и так далее. Современная техника литографии позволяет сжать логические элементы и провода до размеров микронов на поверхности кремниевого ЧИПа. При этом технология неизбежно достигнет точки, когда логические элементы станут настолько малыми, что они будут состоять всего из нескольких атомов. На расстояниях масштаба атомных размеров материя подчиняется законам квантовой механики, которые значительно отличаются от законов классической физики, определяющих свойства обычных логических элементов. Так что, если компьютеры будут становиться все меньше, то в будущем новая, квантовая технология должна заменить собой или добавиться к тому, что есть сейчас.

Еще в начале 80-х годов XX века Ричард Фейман в своей работе отметил, что определенные квантовые эффекты не могут быть эффективно смоделированы на классических компьютерах. Это наблюдение привело к рассуждениям, что возможно обычные вычисления можно выполнить более эффективно, если использовать эти квантовые эффекты. Однако построение квантовых компьютеров – вычислительных машин, использующих подобные квантовые эффекты, казалось делом сложным. К тому же никто не был уверен, что использование квантовых эффектов ускорит вычисления, и поэтому область квантовых вычислений прогрессировала весьма слабо. И только в 1994 году, когда Питер Шор удивил всех, описав полиномиальный квантовый алгоритм для разложения целых чисел на множители, квантовым вычислениям было уделено должное внимание. Это открытие привело к суматохе, как среди экспериментаторов, которые стали пытаться построить квантовый компьютер, так и среди теоретиков, пытающихся разработать другие квантовые алгоритмы. Дополнительный интерес к этому вопросу

был подстегнут изобретением квантовой передачи ключей шифрования и более позже сообщениями об экспериментальных успехах квантовой телепортации и демонстрацией двухбитового квантового компьютера.

Основы квантовых вычислений

Чтобы разобраться, чем же квантовые компьютеры так сильно отличаются от классических, нужно обратить внимание на единицу хранения информации – бит. Бит – это физическая система, которая может находиться в одном из двух возможных состояний, соответствующим логическим значениям – да или нет, истина или ложь, либо просто 0 или 1.

Например, в цифровых компьютерах, напряжение между пластинами конденсатора представляет бит информации: заряженный конденсатор соответствует 1, а незаряженный соответствует 0. Один бит информации можно также представить двумя разными поляризациями светового луча или двумя электронными состояниями атома. Однако, если возьмем атом в качестве физического бита, то квантовая механика скажет, что кроме двух различных электронных состояний, атом также может находиться в когерентной суперпозиции этих двух состояний. Это значит, что атом находится в каждом из состояний 0 и 1.

Попробуем отразить одиночный фотон от полу-посеребренного зеркала, т.е. от зеркала, которое отражает ровно половину падающего на него света, в то время как вторая половина проходит сквозь него (Рисунок 1).

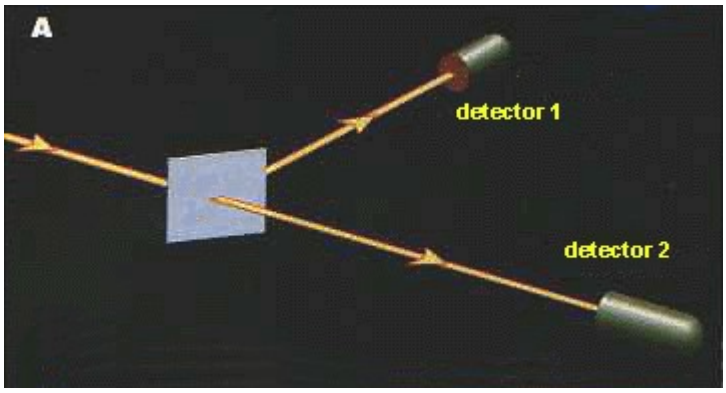

Рисунок 1

Где окажется фотон после того, как он столкнулся с зеркалом – в отраженном луче или в прошедшем луче? Казалось бы, разумно ответить, что фотон будет или в одном, или в другом луче с одинаковой вероятностью. То есть, можно было бы предположить, что фотон случайно выберет один из двух возможных путей. В самом деле, так и происходит. Если разместим два фотодетектора за полу-отражающим зеркалом, на пути каждого из двух лучей, мы с равной вероятностью зарегистрируем фотон в одном из детекторов: или в детекторе 1, или в детекторе 2.

Означает ли это, что после полу-посеребренного зеркала фотон путешествует или в отраженном, или в прошедшем луче с вероятностью 50%? Нет, это не так. В действительности фотон отправляется «обоими путями сразу». Это можно продемонстрировать, если соединить оба луча при помощи двух полностью отражающих зеркал и еще одного полу-отражающего. Дополнительное полу-отражающее зеркало поставим в точке встречи двух лучей, а фотодетекторы разместим на продолжении каждого из двух лучей (Рисунок 2).

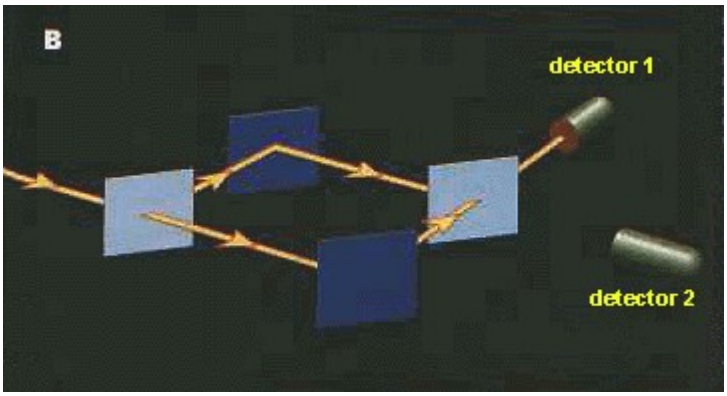

Рисунок 2

При помощи такой установки можно наблюдать поистине удивительное явление квантовой интерференции.

Если бы фотон просто с вероятностью 50% выбирал один или другой путь после полупрозрачного зеркала, то каждый из детекторов на выходе из установки мог бы обнаружить фотон с той же вероятностью 50%. Однако, этого не происходит. Если два возможных пути в точности равны по длине, то оказывается, что фотон со 100% вероятности попадает в детектор 1, и никогда в детектор 2! Фотон явно принуждают попасть в детектор 1! Поэтому, представляется неизбежным, что фотон должен, в некотором смысле, пройти по обоим путям сразу. Если поместить поглощающий экран на пути одного из лучей (любого), то снова окажется, что фотон может попасть в любой из детекторов 1 или 2 (Рисунок 3).

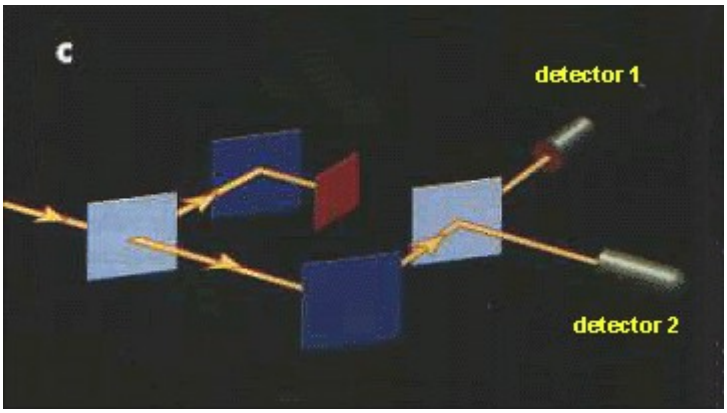

Рисунок 3

Если блокировать один из путей, то фотон может попасть в детектор 2; при обоих открытых путях фотон как-то знает, что ему не разрешено оказаться в детекторе 2, так что фотон должен был как-то «прощупать» оба пути. Поэтому совершенно корректно говорить о том, что между двумя полу-прозрачными зеркалами фотон перемещается по обоим путям сразу: по пути прошедшего и отраженного лучей. Выражаясь техническим языком, можно сказать, что фотон находится в когерентной суперпозиции двух состояний: состояния отраженного луча и состояния прошедшего луча. Точно также и атом может быть приготовлен в суперпозиции двух различных электронных состояний. В общем случае произвольная квантовая двух-уровневая система может быть приготовлена в суперпозиции своих двух логических состояний 0 и 1. Такая система называется кубитом (quantum bit). В каждый данный момент времени кубит кодирует одновременно 1 и 0.

Теперь разовьем идею суперпозиции состояний несколько далее. Рассмотрим регистр, составленный из трех физических битов. Любой классический регистр такого типа может в любой момент хранить одно из восьми различных значений. То есть, регистр может находиться только в одном из восьми возможных конфигураций: 000, 001, 010, ... 111. Квантовый регистр, составленный из трех кубитов, может хранить в любой момент все 8 чисел в квантовой суперпозиции (Рисунок 4).

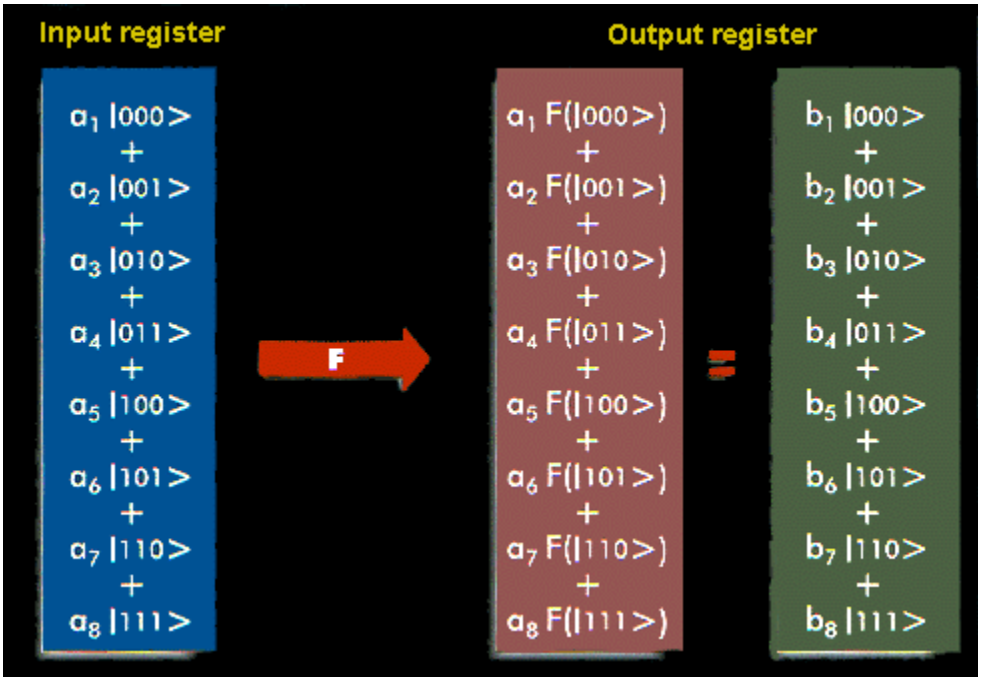

Рисунок 4

Все восемь чисел физически наличествуют в кубите, и это не более удивительно, чем одиночный кубит, одновременно хранящий значения 0 и 1. Если будем добавлять кубиты в регистр, то увеличим его емкость экспоненциально, то есть, 3 кубита могут хранить 8 различных чисел одновременно, 4 кубита могут хранить 16 разных чисел, и так далее. В общем случае L кубитов могут хранить 2^L чисел одновременно. Далее, как только регистр приготовлен в суперпозиции разных чисел, мы можем выполнять математические операции сразу над ними всеми. Например, если кубиты - это атомы, то правильно настроенные лазерные импульсы воздействуют на атомные электронные состояния и заставляют начальную суперпозицию чисел изменяться к некоторой другой суперпозиции. Во время такого изменения обрабатывается каждое число в суперпозиции, и таким образом мы производим массовые параллельные вычисления, но только в одном элементе квантового компьютера. Это означает, что квантовый компьютер может всего за один вычислительный шаг выполнять одну и ту же вычислительную операцию над 2^L разных входных числах, закодированных в когерентной суперпозиции L кубитов. Чтобы выполнить такую же работу, любой классический компьютер должен повторять одно и то же вычисление 2^L раз. Или же надо использовать 2^L отдельных процессоров, работающих параллельно. Другими словами, квантовый компьютер предлагает огромный выигрыш в использовании вычислительных ресурсов, таких как время и память.

Но все это звучит как просто еще один вид чисто технологического прогресса. Может показаться, что классические компьютеры могут делать все то же самое, что и квантовые, просто за большее время и используя больший объем памяти. Дело, однако, в том, что классическим компьютерам требуется экспоненциально больше времени или памяти, чтобы сравняться в производительности с квантовыми компьютерами, а это, в самом деле, слишком много, так как экспоненциальный рост - это очень быстрый рост, он быстро исчерпывает доступные ресурсы времени и ли памяти. Давайте подробнее рассмотрим этот вопрос.

Чтобы решить какую-нибудь определенную задачу, компьютер следует точной последовательности инструкций, которые можно механически применить к любой задаче данного типа и гарантированно получить решение. Определение такой последовательности инструкций называется алгоритм. В качестве примера алгоритмов можно привести процедуры сложения и умножения целых чисел, которым обучают в начальной школе. Если механически применять эти процедуры, можно получить правильное решение для любой пары целых чисел. Некоторые алгоритмы быстрые (например, умножение), другие очень медленные (например, разложение на множители, игра в шахматы). Рассмотрим, например, следующую задачу разложения на множители.

? x ? = 29083

Сколько времени займет у вас, используя бумагу и карандаш, найти два целых числа, которые можно вписать в пустующие места этого уравнения (существует единственное решение)? Возможно, около часа. Решение обратной задачи,

127 x 129 = ?,

опять же, при помощи бумаги и карандаша, займет меньше минуты. А все потому, что мы знаем быстрые алгоритмы для умножения, но нам неизвестен в равной мере быстрый алгоритм для разложения на множители. Под «быстрым» или «медленным» алгоритмом принято понимать не то, сколько реального времени уходит на выполнение алгоритма, а то, значительно ли увеличивается время выполнения алгоритма, если его применять к большим числам. Указанный выше стандартный метод из учебника для перемножения чисел требует довольно немного дополнительной работы, когда переходим от умножения трехзначных чисел к тридцатизначным числам. Для сравнения, разложение тридцатизначного числа на

множители, используя простейший метод пробного деления, примерно в 10^{13} раз дольше, чем разложение трехзначного числа. То есть, увеличение разрядности числа увеличивает использование вычислительных ресурсов в гигантских масштабах. Самое большое известное число, которое разложили на множители, состояло из 129 разрядов.

Квантовый компьютер IBM

Учёные IBM создали самый мощный квантовый компьютер и заставили его работать. IBM продемонстрировала использование созданного в лабораториях компании семикубитового квантового компьютера для факторизации чисел по так называемому алгоритму Шора. Хотя решённая им задача вряд ли способна поразить воображение, это самое сложное вычисление за всю историю квантовых компьютеров.

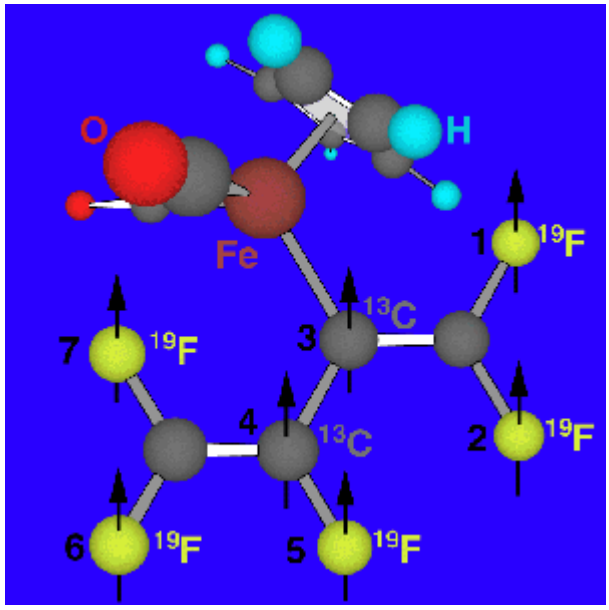

Рисунок 5. Семикубитовая молекула, лежащая в основе квантового компьютера IBM

Компьютер, созданный группой учёных из IBM и Станфордского университета, представляет собой пробирку с миллионами (10^{18}) молекул, имеющих семь ядерных спинов. Основой данного квантового компьютера являются специально созданные исследователями молекулы, состоящие из пяти атомов фтора и двух атомов углерода. Эти молекулы программировались при помощи радиосигналов, а информация считывалась при помощи метода ядерного магнитного резонанса (NMR).

Была выполнена простейшая реализация алгоритма Шора – алгоритма разложения числа на простые множители, разработанного специально для квантовых компьютеров в 1994 году сотрудником AT&T Питером Шором. Она раскладывает на простые множители число 15 и требует для работы 7 кубитов. Во время эксперимента были успешно найдены числа 3 и 5 как множители числа 15.

В отличие от обычных алгоритмов факторизации числа, для которых увеличение длины числа на один разряд примерно удваивает время работы

алгоритма, время работы алгоритма Шора увеличивается на определенное постоянное значение. Поэтому алгоритм Шора может быть эффективно применен для факторизации больших чисел, что может повлечь фундаментальные изменения в криптографических алгоритмах, так как криптостойкость многих из них основана на том, что невозможно эффективно раскладывать большие числа на простые множители. Факт, что квантовый компьютер можно использовать и в криптографии или для взлома шифров, привлекает Управление национальной безопасности США и Министерство обороны, которые финансируют работы Стэнфорда по созданию квантового компьютера.

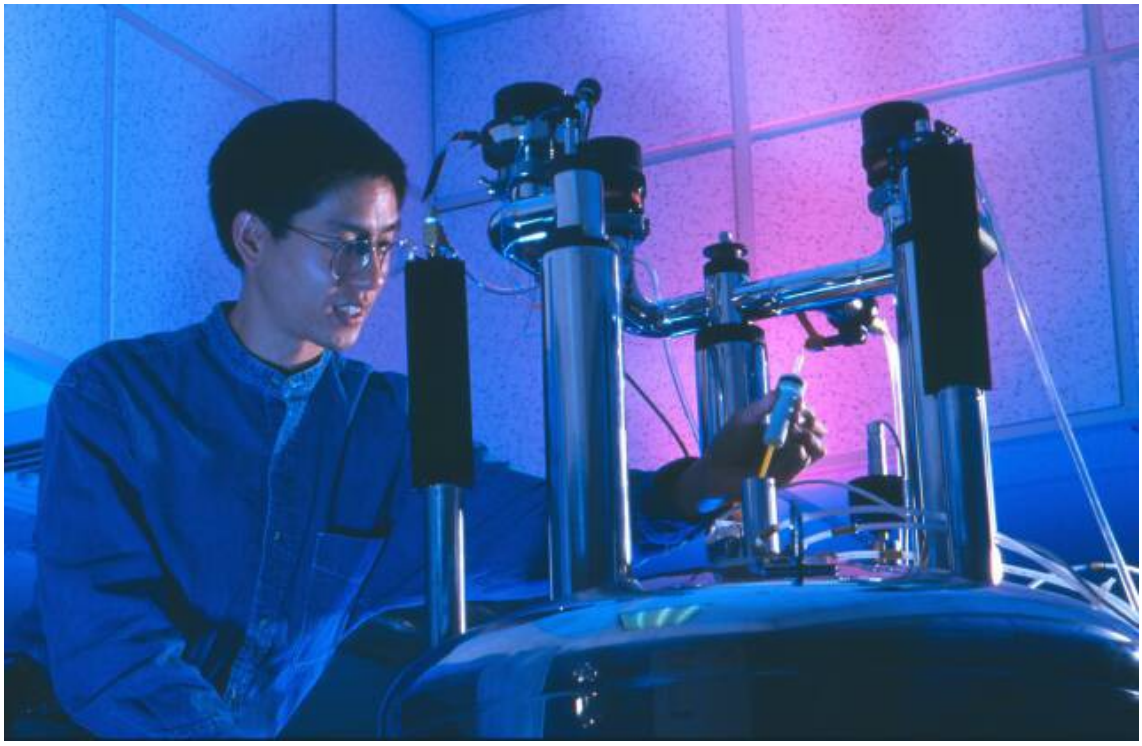

Рисунок 6. **Доктор Айзек Чуанг помещает колбу, содержащую устройство на ЯМР-сканер**

«Несмотря на тривиальность этой задачи, для ее решения требуется беспрецедентный контроль в процессе работы наиболее сложного на сегодняшний день квантового компьютера», — отметил менеджер отдела информационной физики IBM Research Нэбил Эймер (Nabil Amer).

«Этот результат укрепляет растущее понимание того, что однажды квантовые компьютеры смогут решать задачи, которые столь сложны, что для поиска их решения даже самым мощным суперкомпьютерам и миллионов лет окажется мало», - добавил Нейбил Эймер.

Джон Прескилл (John Preskill), профессор теоретической физики и директор Института квантовой информатики при компании CalTech (Пасадена, штат Калифорния), подчеркнул, что данный эксперимент продвинул квантовую вычислительную технику на шаг вперед, позволив выявить характер возможных ошибок. «Сложность создания мощных квантовых компьютеров отчасти связана с тем, что они в большой степени подвержены ошибкам, - пояснил Прескилл. - Чтобы дать квантовым вычислениям путевку в жизнь, мы должны понять характер этих ошибок».

Представление о потенциале квантовых компьютеров дает следующая информация: по словам Прескилла, самым быстродействующим из современных компьютеров – суперкомпьютерам – требуется около месяца, чтобы разложить на простые множители число из 130 цифр, а разложение числа из 200 цифр — вообще непосильная для них задача. Квантовому же компьютеру она по плечу, но для этого он должен содержать тысячи квантовых разрядов, или атомов, а не семь, как компьютер IBM, который пока справляется только с двухзначными числами.

«Со временем квантовый компьютер можно будет использовать для таких целей, как поиск в базах данных; с его помощью, например, может быть значительно ускорен поиск в вебе. Но такие компьютеры вряд ли станут применяться для более прозаических задач типа редактирования текстов», - говорит руководитель группы ученых из IBM, Стэнфордского университета и Университета Калгари Исаак Чуанг.

За гранью закона Мура Современная технология микропроцессоров, которые становятся все более микроскопическими и в то же время более мощными, подчиняется эмпирическому закону Мура, который, как ожидается, будет оставаться справедливым еще примерно десятилетие. Но эта технология – литография – не позволит создать микропроцессоры размером с молекулу, поэтому ученые ищут другие конструкции, использующие генетические методы и другие тонкие технологии. «Примерно на рубеже 2020 годов, когда элементы примут размеры атомов и молекул, закончится действие закона Мура и начнется эпоха квантовой вычислительной техники» – говорит Исаак Чуанг. Атомы и молекулы и есть базовые элементы квантового компьютера.

Правда, пока не ясно, когда можно будет построить такой компьютер. Исаак Чуанг утверждает, что в ближайшие два года появятся более мощные квантовые компьютеры, использующие до десяти атомов.

Области применения

Квантовая теория – одно из самых перспективных направлений науки на сегодняшний день. И одно из самых загадочных. Для того, чтобы понимать квантовую физику, необходимо забыть обо всём том, о чём вас учили в школе. Забыть о том, что вы видели в жизни. Кванто-механический мир – это абсолютно другая вселенная, абсолютно другие законы, абсолютно другая жизнь. Нигде в мире нет аналогов тому, что происходит на уровне электронов. Именно поэтому технологии, которые даёт нам практическое применение этой науки, так потрясают наше воображение! Принципиально новые компьютерные технологии с невообразимой мощностью вычислений, абсолютно достоверные каналы передачи закодированной информации, мгновенное перемещение материальных объектов на расстоянии (телепортация) – уже известные и разрабатываемые в данный момент направления этой науки.

Квантовая связь и криптография

Из обширной области разработки квантовых методов связи и криптографии рассмотрим последствий создания квантовых компьютеров и систем связи для двух современных наиболее популярных криптосистем: для системы с открытым ключом (RSA система, Rivest, Sharnir, Adieman, 1977) и системы с ключом одноразового пользования (Vernam, 1935).

В основе системы RSA лежит предположение о том, что решение математической задачи о разложении больших чисел на простые множители на классических компьютерах невозможно; оно требует экспоненциально большого числа операций и астрономического времени.

Квантовый алгоритм Шора дает возможность вычислить простые множители больших чисел за практически приемлемое время и взломать шифры RSA криптосистем. 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 $\sim 10^{10}$ лет.), в то время как 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.

Для криптосистем с ключом одноразового пользования квантовые методы связи оказываются хорошей новостью: они позволяют обнаружить наличие подслушивания при передаче ключа. Эта возможность основана на квантовом принципе неопределенности Гейзенберга, который гласит, что измерение изменяет состояние измеряемой квантовой системы. Пусть ключ передается по световолокну с помощью фотонов, и информация закодирована в поляризации фотонов. Тогда подслушивание заключается в перехвате и измерении поляризации пересылаемых фотонов; после измерения они пересылаются адресату. При наличии подслушивания адресат обнаружит, что 25% фотонов приходят к нему с "неправильной" поляризацией. Если этих ошибок нет, то передача ключа не подслушивается, и им можно пользоваться. Таким образом, квантовые методы обеспечивают гарантированную секретность ключа одноразового пользования. Эксперименты по передаче ключа выполнены на расстояния до 40 км.

Квантовые каналы связи дают и другие возможности.

1. С помощью одного кубита можно передавать 2 бита информации ("плотное квантовое кодирование").
2. Возможна передача неизвестного квантового состояния («квантовая телепортация») по классическому каналу, если абоненты связи предварительно поделили коррелированную пару квантовых частиц. Потенциальные возможности применения этих феноменов еще не выяснены.

Нерешенные проблемы на пути построения квантовых компьютеров

Среди нерешенных проблем отметим:

- в настоящее время отсутствует практическая разработка методов квантовых измерения состояний отдельного ядерного спина или их малых групп;
- не изучено влияние неидеальности управляющих кубитами импульсных последовательностей и многоуровневой сверхтонкой структуры энергетического спектра на декогерентизацию квантовых состояний;
- не разработаны способы подавления декогерентизации, определяемой шумами в электронной измерительной системе;
- не опробованы квантовые методы коррекции ошибок для многокубитовых систем.

Будущее квантовых компьютеров

Можно ожидать, что в будущем появятся также комбинированные варианты твердотельных квантовых компьютеров, использующих, например, в одной структуре и ядерные спины, и квантовые точки с электронными спинами, а также комбинированные методы обращения к кубитам, такие как двойной электрон-ядерный магнитный резонанс, динамическая поляризация ядерных спинов и оптическое детектирование ядерного магнитного резонанса.

Таким образом, весьма возможно, что в перспективе квантовые компьютеры будут изготавливаться с использованием традиционных методов микроэлектронной технологии и содержать множество управляющих электродов, напоминая современный микропроцессор. Для того чтобы снизить уровень шумов, критически важный для нормальной работы квантового компьютера, первые модели, по всей видимости, придется охлаждать жидким гелием. Вероятно, первые квантовые компьютеры будут громоздкими и дорогими устройствами, не умещающимися на письменном столе и обслуживаемыми большим штатом системных программистов и наладчиков оборудования в белых халатах. Доступ к ним получат сначала лишь государственные структуры, затем богатые коммерческие организации. Но примерно так же начиналась и эра обычных компьютеров.

А что же станет с классическими компьютерами? Отомрут ли они? Вряд ли. И для классических, и для квантовых компьютеров найдутся свои сферы применения. Хотя, по всей видимости, соотношение на рынке будет все же постепенно смещаться в сторону последних.

Внедрение квантовых компьютеров не приведет к решению принципиально не решаемых классических задач, а лишь ускорит некоторые вычисления. Станет возможна квантовая связь – передача кубитов на расстояние, что приведет к возникновению своего рода квантового Интернета. Квантовая связь позволит обеспечить защищенное (законами квантовой механики) от подслушивания соединение всех желающих друг с другом. Ваша информация, хранимая в квантовых базах данных, будет надежнее защищена от копирования, чем сейчас. Фирмы, производящие программы для квантовых компьютеров, смогут уберечь их от любого, в том числе и незаконного, копирования.

Заключение

Окончательный вывод о том, какие из вариантов окажутся в конце концов реализованными в полномасштабном квантовом компьютере сейчас сделать пожалуй не представляется возможным. Для этого предстоит преодолеть еще много уже известных и еще неизвестных трудностей. Однако, в любом случае появление квантовых компьютеров будет означать революцию не только в вычислительной технике, но также и в технике передачи информации, в организации принципиально новых систем связи типа квантового Интернета и может быть началом развития новых пока неизвестных областей Науки и Техники.

Новая техника XXI века рождается путем синтеза новых идей в математике, физике, информатике, технологии. Исключительные возможности квантовых компьютеров будут способствовать и еще более глубокому пониманию физических законов в Природе. Построение квантовых компьютеров было бы еще одним подтверждением принципа неисчерпаемости Природы: Природа имеет средства для осуществления любой корректно сформулированной задачи.

Приложение 1. Хронология теории квантовых компьютеров

14 декабря 1900 г. День рождения квантовой теории	Немецкий физик и будущий нобелевский лауреат Макс Планк доложил на заседании Берлинского физического общества о фундаментальном открытии квантовых свойств теплового излучения. В физике родилось понятие кванта энергии и среди других фундаментальных постоянных поля вилась постоянная Планка (h = 1,38062*10-23Дж/К).
1925 г.	В.Гайзенберг предложил матричный вариант квантовой механики
1926 г.	Э.Шредингер сформулировал волновое уравнение для описания движения электрона во внешнем поле. Э.Ферми и П.Дирак получили квантово-статистическое распределение для электронного газа, учитывающее при заполнении отдельных квантовых состояний квантовый принцип, сформулированный тогда же В.Паули.
1928 г.	Ф.Блох выполнил анализ квантово-механической задачи о движении электрона во внешнем периодическом поле, создаваемом атомными остатками в кристаллической решетке. Этот анализ показал, что электронный энергетический спектр в кристаллическом твердом теле имеет зонную структуру. Это привело к существенным изменениям представлений о Природе вообще и о твердом теле, в частности.
1980 – 1982 гг. Теория квантовых компьютеров	Советский математик Ю.И.Маниный опубликовал новую идею о квантовых вычислениях, и которая стала активно обсуждаться лишь после опубликования в 1982 году статьи американского физика-теоретика нобелевского лауреата Р.Фейнмана.
1995 г.	Первый прототип квантового компьютера на основе ионов, захваченных ионными ловушками, предложен австрийскими физиками И.Цираком и П.Цоллером.
1996 г.	Разработка квантового алгоритма поиска данных в неотсортированной базе данных (Лов Гровер, AT&T Bell Labs, США).
1998 г.	Создание первого в мире квантового компьютера - прародителя ЭВМ нового поколения (Айзек Чуанг, фирма IBM; Нейл Гершенфельд, Массачусетский технологический институт, США) с использованием двух атомов молекулы хлороформа (атом водорода и атом углерода)
1999 г.	В NEC Fund.Res.Lab. в Японии был создан первый твердотельный кубит.
Август 2000 г.	Создание первого в мире квантового компьютера (Айзек Чуанг, фирма IBM; Нейл Гершенфельд, Массачусетский технологический институт, США) с использованием пяти атомов
Декабрь 2001 г.	Создание первого в мире квантового компьютера (Айзек Чуанг, фирма IBM; Нейл Гершенфельд, Массачусетский технологический институт, США) с использованием семи атомов. Компьютер реализовал факторизации чисел по алгоритму Шора. Создание уникального светодиода, способного испускать единичный фотон (Кембриджский университет, Великобритания, совместно со специалистами компании Toshiba).