Эссе студента 912 группы
Зайдуллина М.Г.
на тему

«Квантовая криптография»

1.Предисловие

Данная работа представляет собой попытку сделать краткий обзор новых направлений науки, разрабатывающих способы хранения, передачи и обработки информации используя законы квантовой механики. Область эта очень обширна, что не позволяет сделать в этой работе сделать даже краткого обзора всех теоретических основ, на которых строится квантовая теория информации и алгоритмов. Так как наш обзор предполагает быть кратким, в него не будут включены детальные описания каких-либо алгортимов квантовых вычислений и количество математических выкладок будет сведено к минимуму. Больше будут рассматриваться практические вопросы применения квантовой механики в работе с информацией.

2.Введение

В последние годы интерес к тому, что принято называть «квантовыми компьютерами», необычайно возрос. Важность этой бурно развивающейся области в применении к теории защиты информации безусловна, чего стоит только возможность (пока только теоретическая) находить простые сомножители больших составных чисел за полиномиально зависящее от длины числа время. А ведь на том факте, что с использованием современных компьютеров и алгоритмов эта задача решается только за экспоненциально возрастающее время, основаны самые распространенные сейчас алгоритмы шифрования и электронной подписи. Квантовые вычисления позволяют решать с полиномиальной сложностью некоторые важные задачи, которые на классических машинах требуют экспоненциально сложных алгоритмов решения. Будут рассмотрены различные способы физической реализации квантовых компьютеров; вопрос этот чрезвычайно важен и интересен, так как еще в начале 90-х годов прошлого века многие авторитетные ученые сомневались в реализуемости квантовых вычислений «во плоти», а не только на бумаге.

Квантовая память, которая использует для хранения информации квантовые характеристики атомов, ядер или других квантовых частиц и систем, была успешно реализована несколько лет назад. Хотя на первый взгляд кажется, что память на квантовых принципах построить гораздо проще по сравнению с квантовым вычислителем, все же сейчас объемы, достигнутые в экспериментах, относительно малы – десятки и сотни бит. Основные проблемы стоящие на пути повышения объемов – слабая помехозащищенность, а так же необходимость разработки эффективных алгоритмов чтения и коррекции ошибок.

На важной особенности квантовых систем, состоящей в том, что акт измерения состояния системы всегда изменяет ее, основан механизм передачи информации по открытому каналу с очень высокой стойкостью к прослушиванию. Будет описано несколько успешно реализованных экспериментов по передачи информации на относительно большие расстояния, в которых в качестве носителя используются поляризованные фотоны. Самое важное практическое применение квантовых каналов связи – квантовое распределение ключей, которое решает многие проблемы классичесих алгоритмов распределения ключей.

3.Квантовые вычисления

Все классические вычислительные машины, начиная от «аналитической машины» Чарльза Беббиджа и кончая современными суперкомпьютерами, как бы они ни отличались по скорости и своим возможностям основаны на одних и тех же принципах. Информация в

этих машинах хранится и обрабатывается в виде нулей и единиц. Все операции работают с четко определенными массивами бит, в которых каждый бит обязательно имеет одно из двух состояний, результат операции всегда однозначно определяется входными данными. Для всех классических компьютеров чаще всего используется простая математическая модель – машина Тьюринга, по своей сути очень простое устройство. Даже работу современного процессора, содержащего десятки миллионов транзисторов, выполняющих триллионы элементарных логических операций в секунду, можно смоделировать на машине Тьюринга и количество вычислений, необходимых для решения одной и той же задачи процессору и модели, будет связано полиномиально. На машине Тьюринга эффективно решается очень широкий класс задач, как чисто математических, так и задач моделирования различных процессов классической физики. Под эффективносью обычно понимается, что затраты на решение задачи зависят полиномиально от сложности задачи (т.е объема входных данных – длины чисел, количества моделируемых частиц и т.д.) Однако существуют задачи, для которых не найдены эффективные алгоритмы решения на классических компьютерах. Пример, имеющий огромную важность для современной криптографии – невозможность (правда недоказанная строго математически) быстро найти простые множители составного большого числа. Самые быстрые современные алгоритмы решают эту задачу за $\exp(const*n^{1/3})$ шагов, где n – число знаков в двоичной записи числа. Очень широко используемые сейчас алгоритмы цифровой подписи и шифрования с открытым ключем, основывают всю свою надежность на этом факте. Считается, что даже очень хорошо оснащенному технически противнику, желающему взломать шифр, потребуется на это слишком много времени, чтобы попытка взлома имела практический смысл. В другой области – проблеме поиска информации по какому-то шаблону, например, в базе данных, самые общие существующие алгоритмы по сути не отличаются от простого перебора, что практически чрезвычайно неэффективно, так как объемы современных хранилищ информации сами по себе возрастают экспоненциально из года в год.

Самая широкая область, в которой современные компьютеры бессильны – моделирование квантовых систем. Для простоты рассмотрим систему из n частиц, каждая из которых может иметь спин либо +1/2, который кодируется нулем, либо –1/2, который кодируется единицей. Базисными состояниями системы будет набор из 2^n векторов. Согласно квантовой механике в процессе измерения мы обнаружим систему в одном из этих состояний. Однако между измерениями система находится в состоянии суперпозиции нескольких базисных состояний. Это новое состояние описывается набором из 2^n комплексных чисел - амплитуд, каждое из которых (вернее его квадрат) определяет вероятность обнаружить систему в процессе измерения в соответствующем базисном состоянии. Любое изменение системы со временем или в процессе взаимодествия с другими системами описывается унитарным оператором, который представим в виде матрицы из 2^n*2^n элементов и описывает преобразование 2^n мерного вектора амплитуд. Таким образом, чтобы смоделировать на классическом компьютере один акт воздействия оператора на систему, потребуется сделать $O(2^{2n})$ операций. А если учесть, что для моделирования изменения системы за большой промежуток времени, может потребоваться перемножение матриц операторов, то становится понятна огромная сложность в моделировании квантовых систем, макроскопических размеров. Сам же процесс квантового преобразования системы существенно нелокален, то есть состояние одного кубита при преобразовании влияет на все остальные кубиты, то есть сверхпаралеллизм заложен саму физическую основу квантового компьютера.

Понятно, что ограниченность применения классических компьютеров обусловлена тем, что в основе их работы лежит классическая механика, и скорее всего невозможность эффективно решать на них некоторые классы задач, есть их коренное свойство, которое нельзя обойти, не перейдя к совершенно другим принципиальным основам. Впервые идеи

использовать квантовые системы для вычислений встречаются в работах Ричарда Фейнмана и некоторых других, менее именитых, ученых в 70-х годах прошлого века. Первой задачей для ученых стала необходимость разработать теоретическую модель квантовых вычислителей, подобную машине Тьюринга, принципы которой в столь же малой степени зависели бы от конкретной физической реализации модели. В 1985 году Д.Дойч предложил свою математическую модель – квантовую машину Тьюринга, а 1989 году - аналогичную, но более простую в использовании – модель квантовых схемы. Квантовая схема – это простейшее, базовое, преобразование пары элементов (спинов) в системе, описываемое парой номеров элементов и шестнадцатью комплексными числами. Любое сложное преобразование системы можно свести к последовательности применения квантовых схем, которые представляют собой некии прообраз программы для квантового компьютера. Для конкретной реализации компьютера мы должны уметь записывать в регистры (наборы квантовых ячеек, информация в которых обычно представляется в виде направления спина) данные, проводить над ними операции и считывать результат. Так как для практической реализации квантовые схемы не очень удобны, разрабатываются более конкретные и не такие общие базовые преобразования, аналогичные базовым логическим элементам в классических компьютерах. Существуют различные интересные квантовые логические элементы, выполняющие с классической точки зрения очень нетривиальные операции.

Очевидно, что квантовые компьютеры могут эффективно моделировать квантовые системы, что потенциально в будущем позволит использовать их для моделирования свойств таких существенно квантовых систем, как кристаллы или сверхмалые элементы будущих наноустройств. Самая «широкоизвестная» особенность квантовых компьютеров – это способность решать задачу разложения числа на простые множители за полиномиальное время. В 1994 году П.Шор придумал квантовый алгоритм, позволяющий разложить число за $n^3(\log n)^{const}$ шагов. Это открытие вызвало всплеск бурных эмоций в рядах защитников информации, однако огромные сложности в практической реализации квантовых компьютеров, способных разложить на множители хотя бы число 15, позволяют пользователям шифровальных алгоритмов быть спокойными еще как минимум десяток лет. В конце 2001 года в исследовательском центре IBM в Альмадене был реализован компьютер выполняющий на семи кубитах (квантовых битах) операция разложения по алгоритму Питера Шора числа 15 на множители 3 и 5. Количество кубит в реализуемых до сегодняшнего времени компьютерах пока не превосходит двух десятков. По слухам, ученые из того центра готовят компьютер с существенно улучшенными характеристиками, которые позволят ему найти сомножители числа 56. Еще одной задачей, для которой существует хороший алгоритм решения на квантовом компьютере, является поиск в неупорядоченной базе данных. Однако тут выбор нужного элемента происходит за $\sqrt{n}$ шагов против n шагов на классическом компьютере, то есть выигрыш не такой принципиальный. Стоит заметить, что на этом список известных полезных квантовых алгоритмов заканчивается, но не потому, что их больше не существует, а потому, что теория квантовых вычислений находится еще на ранней стадии своего развития и пока нет никакого формализованного алгоритма для построения квантовых алгоритмов. Можно сказать, что открытие Питером Шором его алгоритма есть большая удача (гениям всегда везет).

Сложности, встающие на пути исследователей, пока не позволяют строить большие компьютеры. Среди них основную роль играют слабая помехозащищенность системы кубит, необходимость в сложных методах коррекции ошибок (теория квантовых кодов, позволяющих понижать вероятность появленя неустранимых ошибок, довольно хорошо разработана), и, разумеется, невероятная техническая сложность создания самой системы кубит, сохранения ее постоянной конфигурации и организации механизмов надежной записи и считывания информации. Опять же Шором разработана схема эффективной

коррекции ошибок. Так как на самом деле любой унитарный оператор может быть реализован с какой-то не абсолютной точностью, то в процессе преобразований накапливаются погрешности. Схема Шора обеспечивает возможность сколь угодно длинных вычислений, при условии, что каждый из применяемых унитарных операторов реализован с погрешностью ниже пороговой. На данный момент предлагается несколько способов физической реализации квантовых компьютеров.

Первый подход – использовать энергетические уровни (включая тонкую и сверхтонкую структуру) атомов и ионов. Положительная сторона этого подхода в том, что довольно легко управлять положением атомов и ионов используя лазеры, резонаторы и магнитные поля, а также легко приготовить необходимое начальное состояние системы. Однако большую проблему представляет сложность организации взаимодействия отдельных частиц и целенаправленного воздействия на пару и более атомов из-вне. Это направление экспериментальной физики сейчас бурно развивается и, похоже, имеет большое будущее.

Другой подход – использование ядерных спинов и ядерного магнитного резонанса для изменения и измерения. Несложная реализуемость произвольных унитарных операторов при помощи определенных импульсов магнитного поля была показана даже при комнатной температуре. Однако для приведения системы в начальное состояние необходимо охладить ее до сверхнизких температур, при которых резко усиливаются нежелательные взаимодействия между отдельными атомами и молекулами. Сложно реализовать воздействие на какой-то определенный спин, если в системе ядер с такими спинами несколько, что связано с невозможностью фокусировать магнитное поле в необходимом пространстве.

Использование в качестве кубитов сверхпроводящих гранул, единственной степенью свободы которых при сверхнизких температурах является заряд, два разных значения которого и принимаются за базисные состояния, считается перспективным направлением. Взаимодействие гранул легко происходит посредством джозефсоновских контактов. Единственная сложность состоит с невозможности на текущем уровне развития техники изменять состояние отдельной гранулы.

Автор известной книги по квантовым вычислениям А.Китаев придумал использовать в качестве кубитов анионы, особые квази-частицы, возбуждения, в двумерной электронной жидкости, находящейся в магнитном поле. Анионы, которые можно использовать в квантовых компьютерах (так называемые неабелевы анионы), пока существуют лишь на бумаге. Однако возможность их существования и использования в качестве кубитов позволяет обойти существенный недостаток других систем – погрешность реализации унитарных операторов. Системы анионов по самой своей природе таковы, что при преобразованиях их свойства меняются абсолютно четко. Сами же преобразования осуществляются посредством перемещения анионов. По этой причие квантовый компьютеры на основе анионов называют топологическими.

Напоследок скажем пару слов об изветных квантовых алгоритмах. Вдаваться в математику, как уже упоминалось, возможности нет, но попытки автора полнстью описать алгоритмы без использования сухих формул не увенчались успехом. Задача поиска в неструктурированной базе данных сводится к известной задаче об «оракуле». Предполагается, что у нас есть черный ящик, или оракул, которому на вход X подается какая-то управляющая информация, а на вход Y пробные данные, в ответ на которые оракул сообщает соответствуют ли они предикату задаваемому входом X или нет. В классическом варианте ответ оракула есть либо «истина», либо «ложь» и для нахождения такого y, при котором предикат истинен, необходим перебор всех возможных значений y. Квантовый вариант оракула по сути есть оператор U_x, действующий на вход Y и выдающий $|y\rangle$, если предикат истинен и $-|y\rangle$ иначе. Для быстрого нахождения такого y, при котором предикат истинен, по определенному правилу строится новый оператор V,

зависящий от всех возможных значений входных данных и их количества. Воздействие произведения операторов UV на вектор, представляющий собой сумму всех возможных состояний входа, грубо говоря, поворачивает этот вектор в гиперплоскости в направлениий вектора правильного ответа y_0. После определенного количества таких умножений мы получим вектор y_0.

Алгоритмы разложения числа на множители и вычисления дискретного логарифма, были придуманы Шором и работают, в отличие от известных классических алгоритмов, за полиномиальное время. Алгоритм нахождения делителей сводится к нахождению периода числа относительно другого (периодом двух чисел a и b, таких, что (a,b)=1 и a<b, назвается такое число t, при котором $a^t=1(\mathrm{mod} b)$, и которое записывается как $per_b(a)$). Квантовый алгоритм нахождения периода используется в классическом вероятностном алгоритме, в котором вероятность найти делитель за одну итерацию равна $1-1/2^{k-1}$, где k – число различных простых делителей исходной числа. Сам алгоритм нахождения периода вообще говоря лишь частично квантовый, унитарные преобразования в нем используются при нахождении последовательности собственных числе оператора умножения вычета на произвольное число a, и уже из последовательности различных собственных чисел вычисляется с определенной вероятностью период.

3.Квантовое распределение ключей.

Алгоритмы с открытым ключем, в которых любой может зашифровать данные используя общеизвестный ключ и только автор этого ключа может расшифровать сообщение (или наоборот) основаны на недоказанной сложности задач типа разложения числа на простые множители и дискретного логарифмирования. В отличие от них, алгоритмы шифрования, использующие для кодирования сообщений секретные ключи, например DES, являются по сути очень устойчивыми к криптоатакам, однако перед установкой нормального процесса обмена кодированными сообщениями, обе стороны должны заполучить в свое распоряжение секретный ключ, который должен быть известен только этим сторонам. Возникает потребность в безопасном распределении ключей, которая сейчас решается с помощью нескольких способов, начиная от использования почты и курьеров и заканчивая известным алгоритмом Диффи-Хелмана. Существующие алгоритмы, хоть и считаются надежными, подверженными многим недостаткам, которые способны решить квантовые алгоритмы распределения ключей. Основная проблема классического распределения ключей состоит в возможности перехвата теоретическим противником секретного ключа в момент его передачи, сохранение и повторная посылка его исходному получателю. Таким образом противник может остаться незамеченным, узнать ключ и получить доступ к зашифрованным данным. Попытка решить эту проблему сделана в алгоритме Диффи-Хелмана, в котором каждая из сторон генерирует свой секретный ключ, шифрует его определенным образом и пересылает по открытому каналу связи. В итоге каждая из сторон имеет свой ключ и зашифрованный ключ другой стороны, из которых они получают секретный ключ, который и используется для шифрования информации. Надежность алгоритма основывается на сложности нахождения полученного в результате такого обмена секретного ключа по двум переданным открытым ключам. Но теоретически невозможность решения этой задачи за практически приемлемое время не доказана, к тому же вполне возможно, что задача дискретного логарифмирования (на сложности классических алгоритмов решения которой и основан протокол Диффи-Хелмана) будет в будущем эффективно решена с использованием квантовых компьютеров и алгоритма Шора.

Надежность квантовых алгоритмах передачи секретных данных базируется не на изощренных математических преобразованиях, а на законах физики, которые теоретически невозможно обойти. Главное свойство квантовых систем состоит в невозможности определить состояние системы не изменив ее, то есть до измерения

система находилась не обязательно в том же состоянии, в котором она было до него. Этот факт делает при определенном устройстве квантового канал невозможным для потенциального противника, прослушивающего канал остаться незамеченным. Принцип неопределенности Гейзенберга, а также теорема Белла активно используются в современных разработках. Существует два основных типа протоколов надежной передачи данных по квантовому каналу, первый основан использует пары частиц, находящихся в связанных состояниях, а второй поляризованные фотоны. Насколько известно автору, практически реализован только второй способ, однако экспериментально с помощью первого способа можно передать несколько бит информации, но и эти биты требуют огромных технических и эмоциональных затрат.

Первый известный протокол, использующий поляризацию фотонов для передачи данных – BB84, был разработан в Монреальском институте Чарльзом Беннеттом и Жилем Брассардом. Дадим краткое описание этого протокола. В литературе по криптографии общепринятым считается обозначение двух сообщающихся сторон Бобом и Алисой, причем Алиса передает, а Боб получает информацию. Потенциальный же враг, злобно подслушивающий канал, зовется Евой. Предполагается, что Алиса может генерировать частицы, могущие иметь два состояния в одном из двух неортогональных базисов. К примеру, это могут быть фотоны поляризованные под углом 0^o (кубит «0») и 90^o («1») или 45^o и 135^o градусов к вертикали, или это могут быть электроны со спином направленным верх или вниз в одном из базисов и влево или вправо в другом базисе. Причем если мы измеряем значение кубита не в том базисе, в котором он поляризован, то он с равной вероятностью примет значение 0 или 1. Алиса произвольным образом генерирует последовательность кубит со случайной поляризацией (одной из четырех), а Боб принимает эти кубиты в случайно выбранном базисе (каждый кубит в произвольном базисе). Так как базис Боба не всегда совпадает с базисом, в котором был поляризован кубит, то в среднем четверть кубит будут измерены неверно. Это слишком большой процент для стандартных алгоритмов исправления ошибок, однако протокол BB84 предполагает, что после окончания процесса передачи Боб сообщает Алисе договариваются по открытому каналу связи о том, в каком базисе он измерял кубиты, а Алиса отвечает ему какие из этих измерений были правильные. Неправильно полученные кубиты отсеиваются, а из правильных формируется по строке кубиту Алисы и Боба, которые в случае нормальной, без вмешательства Евы, передачи должны быть идентичными. Если Ева прослушивает канал, пытаясь остаться незамеченной, то ей нужно получать кубиты в каком то из базисов, а затем посылать Бобу кубиты в том состоянии, которое она измерила. Иначе она поступить не может, так как существует теорема о запрете клонирования квантовых состояний. Это важнейшее отличие квантовых систем от классических и делает возможными идеально (если не учитывать шумы) защищенные каналы связи. Так как в половине случаев ее базис не будет совпадать с тем, в котором генерировала кубиты Алиса, то она испортит четверть кубит из тех, что Боб с Алисой считают правильными. Для проверки ненарушенности канала связи им достаточно сравнить части сообщений, если процент ошибок не превышает некторого предела, то канал связи не был подслушан и применяются стандартные алгоритмы коррекции ошибок. Таким образом вероятность, что Ева останется незамеченной чрезвычайно мала. Кроме того, алгоритмы коррекции ошибок учитывают возможность того, что Ева подслушала лишь часть передаваемого сообщения и таким образом процент внесенных ей ошибок уложился в пределы нормы. Они разрабатываются так, чтобы доля правильной информации от конечного варианта ключа, которой обладает Ева уменьшилась (privacy amplification). Существует несколько более поздних модификаци этого алгоритма, направленных на уменьшение процента ошибок и количества полезной информации, которую теоретически может получить Ева. Используются так же системы не с четырьмя, а с двумя, но не ортогональными поляризациями, а так же с шестью состояниями в трех различных базисах. Подробно рассматривать их не имеет смысла.

В теории все выглядит красиво, однако на практике возникают определенные трудности. Данный протокол все равно не стоек к атакам, при которых Ева полностью изолирует Боба от процесса общения и играет для Алисы его роль. Возникают определенные трудности с физической реализацией канала и процесса генерации фотонов. В реальности в канале всегда есть затухания и возможно даже помехи. До недавнего времени техника не позволяла управляемо генерировать строго по одному фотону с требуемой поляризацией. Наличие же в одном передаваемом кубите даже двух кубитов оставляет Еве теоретическую возможность перехватить один из фотонов, не влияя на другой. Это лишь несколько улучшит ее положение, так как она все равно не знает в каком базисе испускала фотоны Алиса. Однако, если ей будет доступно более одного фотона, она сможет послать их на измерители обоих базисов и таким образом и остаться незамеченной и получить всю правильную информацию. Автор слышал о реализации квантового канала, в котором принцип неопределенности применяется не в отношении поляризаций, а к средней фазе и средней амплитуде пачки фотонов, которые тоже нельзя измерить одновременно. Измерение фазы меняет амплитуду и наоборот. Таким образом запрет на наличие более одного фотона на кубит отпадает. Однако о теоретических основах этого протокола автор сказать ничего не может.

Существенным шагом вперед в теории квантовой коммуникации стала выдвинутая в 1991 году Артуром Экертом идея использовать для передачи пары частиц, находящихся в так называемом связанном состоянии. В этих состояниях проявляются нелокальные свойства квантового мира. Фотоны (в связанных состояниях могут находиться любые частицы), возникшие при определенных условиях (например при распаде обычной частицы) и разнесенные на макроскопические состояния, продолжают сохранять в некотором роде информационную связь. Если измерить поляризацию одного из фотонов, то второй мгновенно примет соответствующее измеренной у первого фотона значение поляризации. Этот парадокс нелокальности впервые описали Эйнштейн, Подольский и Розен в 1935 году. Впоследствии он привел к открытию Беллом его известных неравенств, которые сильнейшим образом повлияли на развитие квантовой физики и квантовой теории информации и коммуникации. Споры о влиянии этих неравенств на глубокую интерпретацию квантовой механики не утихают до сих пор.

Экерт предложил генерировать связанную пару частиц в независимом источнике и послыть по частице из каждой пары Алисе и Бобу. Каждый из них измеряет поляризацию или спин частицы в своем произвольном (одном из двух, как в протоколе BB84) базисе, затем источник сообщает, в каком базисе генерировались частицы. Если базисы Алисы и Боба соответствуют базису источника, то они сохраняют измеренный кубит. Видно, что протокол практически идентичен предыдущему. Очень интересным, но пока теоретическим способом передачи информации с использованием связанных состояний является следующая схема. Боб генерирует пару частиц в связанном состоянии, одну из которых посылает Алисе, а одну сохраняет в строгой неприкосновенности у себя. Алиса, используя особый квантовый оператор совершает над своей частицей одно из четырех действий: не изменяет ее, поворачивает на 180^{o} градусов относительно оси X, или оси Y, или оси Z. При этом она не измеряет ее спина. Полученную частицу она посылает обратно Бобу, который подает свою частицу и частицу Алисы на другой квантовый вентиль, который совершает измерение того преобразования, которое сделала Алиса, иногда это называют «измерением Белла». Таким образом с помощью одной частицы было передано 2 бита информации. Сейчас модель «измерителя Белла» существует только в теории.

Квантовая теория коммуникации является на сегодняшний день самой активно разрабатываемой темой в квантовой теории информации. В ее основу положен сложный математический аппарат классической теории информации с существенными дополнениями, обусловленными квантовой механикой. Насколько известно автору, до сих пор не существует конечного ответа о степени защищенности квантовых каналов связи.

На сегодняшний день уже проведено несколько экспериментов по передаче сообщений через квантовые каналы связи. Использовались модификации алкоритма BB84. Рекорд по дальности передачи данных принадлежит шведским исследователям, которые передали ключ на расстояние порядка 60 километров через оптоволокно. В одном из недавних экспериментов, проведенных в Германии компанией QinetiQ, информация передавалась направленным пучком по воздуху на расстояние 23 километра. Потери фотонов при этом были очень большими, поэтому каждый отдельный фотон четко регистрировался и записывалось точное время его регистрации. Используя эту информацию, стороны затем выясняли какие фотоны были приняты правильно, а какие прилетели со стороны, то есть представляли собой шум.

3.1.Краткое описание основных протоколов связи по квантовым каналам и виды атак на них.

Краткое описание процесса коммуникации по протоколу BB84.

1. Алиса посылает последовательность фотонов в одном из 4-х состояний в двух ортогональных базисах. Вероятность появления каждого из состояний равна одной четвертой.
2. Боб измеряет состояние фотонов в одном из двух ортогональных базисов, базисы выбираются равновероятно. Он заранее договорился с Алисой какие состояния считаются «1», а какие «0».
3. По обычному открытому каналу связи Боб сообщает Алисе какой базис он использовал для измерения в каждом конкретном случае.
4. Алиса сообщает о всех случаях, когда Боб использовал тот же базис, в котором посылала фотон она.
5. Все измерения, в которых базисы не совпадали, отбрасываются. Остальные данные считаются правильными и интерпретируются как последовательность битов.
6. Алиса и Боб проверяют наличие прослушивания (об этом подробнее дальше).

Протокол BB92:

1. Алиса посылает фотоны в одном из двух неортогональных состояний с равной вероятностью.
2. Боб измеряет состояние фотонов используя проекцию на одно из подпространств, ортогональных первоначальным состояниям. Подпространства так же выбираются равновероятно. Если Алиса послала фотон в состоянии 1, а Боб измеряет его состояние, спроецировав на подпространство ортогональное этому состоянию, то он стопроцентно не зарегестрирует пришествия фотона. Если же он выберет другой подпространство, то с определенной вероятностью он получит ненулевой результат и будет знать в каком из состояний Алиса послала фотон.
3. Боб по открытому каналу сообщает Алисе в каких измерениях он получил положительный результат.
4. Все остальные данные отбрасываются, а оставшиеся трактуются как последовательность битов, в которой единице соответствует одно из состояний, а нулю другое.
5. Проверка наличия прослушивания.

Протокол EPR:

1. Выбираются три неортогональных состояния такие, что вероятности обнаружить фотон, испущенный в одном из состояний, в проекции на каждое из других состояний равны. Так, если используется поляризация, эти состояния будут поляризациями под углом 0, $\pi/3$, $2\pi/3$.
2. Источник света генерирует пары связанных фотон, находящихся равновероятно в одном из этих трех состояний.

3. Алиса и Боб измеряют приходящие фотон одновременно и независимо. Каждый произвольно и равновероятно выбирает в проекции на какое состояние пытаться измерить фотон.
4. Алиса записывает детектирование фотона как «1», а отсутствие как «0». Боб делает наоборот.
5. По открытому каналу они сообщают друг другу в каком из базисов они измеряли приход фотона. Из тех измерений, в которых базисы совпадали, формируется ключ. Из оставшихся измерений формируется вспомогательный ключ, который используется для детектирования подслушивания.

Надежность этих трех основных протоколах основана на том факте, что при прямом измерении состояния фотонов, которое будет делать гипотетический подслушиватель, он будет изменять это состояние и таким образом влиять на уровень ошибок в полученных Бобом сообщениях. Если уровень ошибок превышает определенный порог (а в третьем протоколе если удовлетворяется неравенство Белла) , значит канал прослушивался. Однако этот вид прослушивания (так называемый непрозрачный или opaque) является самым простым и неэффективным. Существует несколько других алгоритмов, которые дают возможность Еве получить определенную часть достоверной инфомации и остаться незамеченной. При этом законы квантовой механики все равно ведут к тому, что Ева влияет на исходную информацию. Чем больше полезной инфомации получает Ева, тем больше она влияет на канал.

Алгоритм полупрозрачного подслушивания без связывания:

1. Алиса и Боб используют состояния А и Б для передачи соответственно нуля и единицы. Это могут быть и неортогональные состояния.
2. Ева производит пробный фотон В.
3. Ева перехватывает фотон Алисы и производит над своим пробным фотоном и перехваченным унитарное преобразовние.
4. Состояние перехваченного фотона при этом немного меняется и он посылается Бобу.
5. Состояние пробного фотона так же меняется и содержит теперь часть информации о состоянии перехваченного фотона.
6. Ева использует пробный фотон для измерения состояния в соответствующих базисах, информацию о которых она может получить из переговоров Боба и Алисы по открытому каналу.

Это так называемое слабое подслушивание, при котором шпион может получить только малую часть информации оставаясь незамеченным. Относительный размер правильной информации, полученной Евой, определяется как используемым протоколом, так и уровнем шума в канале. О пользе такого подслушивания и о точных выражениях, определяющих возможную долю украденной информации, автор не находит возможным распространятся в силу ограничения временных ресурсов.

Алгоритм полупрозрачного подслушивания со связыванием идентичен предыдущему за тем исключением, что выбирается такое унитарное преобразование, что после него пробный и перехваченный фотоны оказываются в связанном состоянии. При этом Ева не производит измерений своего пробного фотона до того, как Боб произведет измерение своего. Благодаря связыванию доля общей информации этой пары увеличивается и Ева может получить больше полезной информации дменьше возмущая исходную.

Интересную возможность получения информации о фотоне без нарушения его состояния дает индуцированное излучение. Если фотон поместить в соответствующую его энергии среду предварительно накачанного лазера, то он будет индуцировать испускание

фотонов точно такой же поляризации и фазы. Однако вследствие спонтанного излучения в выходном пучке фотонов будет доля «неправильных». Теоретически показано, что эта доля не может быть уменьшена ниже 1/6. Это вносит довольно большие ошибки в измерения как Боба, так и самой Евы, к тому же перед ней встает трудность отделения одного фотона для отправления к Бобу.

Теоремы квантовой механики запрещают точное измерение произвольной системы без изменения ее состояния. Существует возможность так называемого квантового неразрушающего измерения (quantum non-demolition measurement, QND), но, во-первых, измерить возможно далеко не все (например возможно детектирование фотонов без их поглощения), а во-вторых, неразрушающее не значит ненарушающее. Таким образом теоретически невозможно прослушать квантовый канал, получив всю информацию и оставшись незамеченным. Любое вмешательство продуцирует ошибки в измерениях Боба.

4.Квантовая память.

Квантовый компьютер как реальная машина требует для своей работы возможность хранить информацию в памяти. По сути реализация квантовой памяти мало отличается от самого квантового компьютера – те же кубиты, те же способы считывания и записи состояний. Однако значительными отличиями квантовой памяти является необходимость сохранять записанные кубиты на длительный промежуток времени. Задача чрезвычайно сложна, так как квантовый состояния очень легко нарушаются реагируя с окружающей средой и тепловыми колебаниями, влияние которых нельзя свести к нулю. Весной прошлого года в Гарвардском университете был успешно проведен эксперимент, в котором информация была записана и считана из квантовых ячеек памяти. Роль ячеек играли атомы рубидия, квантовое состояние записывалось и считывалось лазерным лучем. Записанная информация была прочитана без помех, что до сих пор не удавалось в других экспериментах. Однако время жизни квантового состояния было очень мало – порядка одной миллисекунды, что требует очень частого восстановления состояния. К квантовой памяти применяютсе те же алгоритмы кодирования для исправления ошибок, что и в квантовым компьютерах и в квантовых каналах связи. На самом деле разработка устойчивых к ошибкам квантовых механизмов храниения, чтения и записи данных и составляет большую часть работ, касающихся квантовой памяти. Самими новыми и интересными алгоритмами исправления ошибок можно считать так называемые поверхностные коды, которые были введены А.Китаевым. Они работают на множестве кубитов организованных в двухмерную матрицу. На пальцах эти алгоритмы объяснить невозможно, а математическое описание слишком обширно.

Интересное теоретическое направление развития квантовой памяти недавно описал в своей работе швейцарский ученый Карло Тругенбергер. Он считает, что необходимо разрабатывать такие алгоритмы работы квантовой памяти, которые будут подобны запоминанию образов в человеческом мозгу. По его мнению это повзолит существенно повысить устойчивость к ошибкам и емкость квантовой памяти, используя тот факт, что в квантовую память можно записывать не только набор конретных нулей или единиц, а суперпозицию любых базисных состояний.

Литература:

1. А.Китаев, А.Шень, М.Вялый.Классические и квантовые вычисления. 1999.
2. Nicolas Gisin, Gregoire Ribordy, Wolfgang Tittel and Hugo Zbinden. Quantum cryptography. (December 12, 2001; submitted to Reviews of Modern Physics)
3. Nicolas Gisin, Renato Renner, Stefan Wolf. Quantem key agreement.

4. Eric Dennis, Alexei Kitaev, Andrew Landahl and John Preskill. Topological quantum memory. (Received 25 October 2001; accepted for publication 16 May 2002)
5. An Introduction to Quantum Key Distribution. Stephen J.Wiesner. National University of Singapore. 10.2002.
6. Proposal of an experimental scheme for realising a translucent eavesdropping on a quantum cryptographic channel . M.Genovese. Instituto Elettrotecnico Nazionale Galileo Ferraris. 12.2000.
7. Interferometry with Faraday mirrors for quantum cryptography. H.Zbinden, J.D.Gautier, N.Gisin, B.Huttner, A.Muller, W.Tittel. University of Geneva. 04.1997

А также материалы сайтов:

www.osp.ru

www.qubit.org

www.nature.com

www.membrana.ru

www.computerra.ru

www.newscientist.com

www.cryptome.org