Квантовая информация и квантовая оптика

С.П.Кулик (кафедра квантовой электроники)

Часть 1. Общие принципы квантовых вычислений.

Введение

Квантовая информация - это новая область науки и технологии, сочетающая в себе разделы физики, математики, кибернетики и инженерии. Ее целью является выяснение роли фундаментальных законов физики, открытых в XX веке в процессах получения, передачи и обработки информации. Сейчас ясно, что теория классической информации не всегда может адекватно ответить на вопрос, как информация может быть использована в реальном (физическом) - т.е. в квантовом мире. Некоторые выводы теории квантовой информации могут быть представлены как обобщение классической теории в тех случаях, когда информация передается и хранится с помощью квантовых состояний, а не в форме классических битов.

Рис.1. Современное соотношение области применимости теорий классической и квантовой информации на фоне современных информационных технологий.

С 1959 года, когда был создана первая микросхема, был выработан эмпирический закон (закон Мура[1]), согласно которому число транзисторов в кристалле одной интегральной схемы в течение первых 15 лет удваивалось каждый год, а затем и до сих пор такое удвоение происходит за 1.5 года. Если первые кремниевые микросхемы имели размеры элементов в плоскости кристалла порядка десятков микрон, то современные образцы характеризуются размерами порядка 100 нм, а контроль осуществляется с точностью порядка 10 нм.

Согласно закону Мура, менее чем через 20 лет размеры интегральной схемы станут порядка атомных, а, следовательно, законы их функционирования будут определяться законами микромира, т.е. квантовой механикой. При этом с неизбежностью придется учитывать, что объекты микромира ведут себя совершенно необычно с точки зрения классического мира. Таким образом, до сих пор квантовые эффекты, связанные с малостью

[1] Существует много интерпретаций закона Мура – за каждые полтора года: удваивается производительность микропроцессоров; удваивается тактовая частота микропроцессоров; удваивается вычислительная мощность компьютера; удваивается плотность транзисторов на чипе; стоимость чипа падает вдвое; и др. В 2003 году Гордон Мур подсчитал, что количество транзисторов, ежегодно поставляемых на рынок в мире, достигло 10^{19}. Это в сто раз больше, чем количество муравьев на Земле...

размеров различных устройств, воспринимались как преграда на пути к миниатюризации электронных устройств. Квантовая информатика призвана выяснить, как использовать фундаментальные квантовые свойства.

Важным аспектом в мотивации квантовых информационных технологий является то, что благодаря техническому прогрессу экспериментаторы получили доступ к единичным квантовым объектам и научились контролировать эти объекты с высокой точностью.

К настоящему времени, пожалуй, единственным практическим приложением квантовой информатики является ***квантовая криптография***. В этой области уже разработаны и реализованы алгоритмы, использующие свойства квантовых объектов - невозможность клонирования состояния и измерения без возмущения. Основное преимущество квантовых криптографических протоколов - даже не абсолютная их секретность (в классической криптографии существуют безусловно секретные ключи), а то, что сам факт подслушивания становится известным для пользователей, а надежность передачи информации не уменьшается, если уровень вносимых при передаче ошибок не превышает определенного уровня.

Однако теоретически возможны и другие приложения теории квантовой информации, например – ***квантовый компьютер***. Это физическое устройство, выполняющее логические операции над квантовыми состояниями путем унитарных (т.е. сохраняющих энергию) преобразований, не нарушающих квантовые суперпозиции в процессе вычислений.

Для чего нужен квантовый компьютер? Рассмотрим, например, математическую проблему факторизации больших чисел - т.е. разложения произвольного числа на простые множители. Эта задача непосредственно связана с криптографией, где секретные ключи формируются именно посредством такого алгоритма.

Математики твердо верят, хотя они и не доказали это, что для факторизации числа с N десятичными разрядами любому классическому компьютеру требуется число шагов, которое растет экспоненциально с N. Иначе говоря, добавление одного десятичного разряда к числу в общем случае умножает время, необходимое для его факторизации, на постоянный множитель. Конкретно, время растет с ростом длины N факторизуемого числа как $\exp\left(N^{1/3}\right)$.

Так, задача вычисления произведения двух простых чисел 521 и 809 не вызывает проблем. Однако, обратная задача - нахождение простых сомножителей числа 421489 потребует заетного времени – т.н. задача класса NP.

Таким образом, при увеличении числа разрядов задача быстро становится неразрешимой. Наибольшее число, которое было разложено на простые множители в качестве математического соревнования, т.е. число, чьи простые множители были втайне выбраны математиками, чтобы составить задачу для других математиков, состояло из 129 разрядов. Если же число разрядов окажется порядка 1000, то никто не знает, как решить эту задачу. Если же будет создан квантовый компьютер, то квантовый алгоритм факторизации (П.Шора) позволит реализовать эту операцию за долю секунды. Невыполнимость факторизации лежит в основе наиболее надежных на сегодняшний день методов шифрования (в частности системы RSA - Rivest, Shamir, Adleman), которая используется для защиты электронных

банковских счетов. Когда будет построена машина для квантовой факторизации, все такие криптографические системы станут абсолютно бесполезны.

Кубиты

Кубит (q-бит, от quantum bit – квантовый бит) - это минимальная единица передаваемой или хранимой квантовой информации, аналогичная биту в классической информации.

Математически кубит – это вектор в двумерном гильбертовом пространстве. Он задается набором двух базисных векторов $|0\rangle$ и $|1\rangle$, которые аналогичны значениям нуля и единицы классического бита. Кубит отличается от классического бита тем, что может находиться в состоянии произвольной суперпозиции базисных векторов $|S\rangle = \alpha|0\rangle + \beta|1\rangle$, где α и β – комплексные числа, удовлетворяющие условию $|\alpha|^2 + |\beta|^2 = 1$. Если учесть, что общая фаза волновой функции несущественна, то состояние кубита задается двумя вещественными параметрами, например, сферическими координатами точки (θ, φ). Такие состояния удобно визуализировать при помощи сферы Блоха (Рис.2).

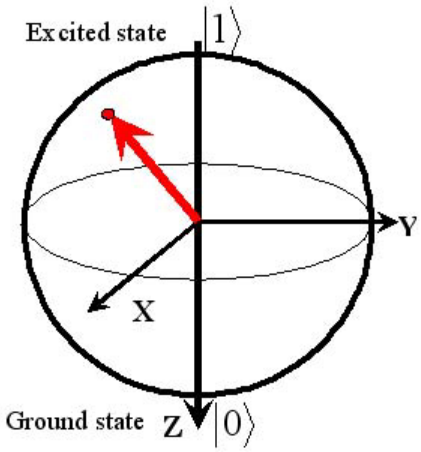

Рис.2. Изображение состояния двухуровневой системы на сфере Блоха.

Таким образом, нельзя сказать, что кубит представлен либо вектором $|0\rangle = (1,0)$, либо вектором $|1\rangle = (0,1)$ – это лишь две возможности из бесконечного многообразия состояний. Хотя состояние кубита описывается волновой функцией и строго определено, отдельные измерения дают вероятностные результаты. Вероятность измерить кубит в состояниях $|0\rangle$ и $|1\rangle$ равна $|\alpha|^2$ и $|\beta|^2$, соответственно. Преобразования, совершаемые над кубитом, описываются линейными операторами.

С физической точки зрения кубит представляет собой чистое состояние квантового объекта, имеющего всего два различных состояния. Такую систему в квантовой механике называют ***двухуровневой***. Типичным примером двухуровневой системы является атом, который может находиться только на двух энергетических уровнях – основном E_g и возбужденном E_e (считается, что остальные уровни энергии атома находятся слишком

далеко, и вероятность перехода на них пренебрежимо мала). Это же пространство состояний (в терминах теории групп оно называется *SU(2)*-пространством) описывает также спин электрона, равный 1/2, и поляризацию фотона.

Физические преобразования над кубитами осуществляются путём воздействия на соответствующие степени свободы физического объекта. Например, поляризационные кубиты преобразуются при помощи фазовых пластинок, состояние электрона в двухуровневом атоме задается приложением импульса резонансного электромагнитного поля определенной длительности и амплитуды, и.т.д.

Несколько кубитов могут образовывать т.н. перепутанные состояния[2], для которых волновая функция не сводится к прямому произведению волновых функций отдельных кубитов. Вообще говорят, что квантовая система состоит из *n* кубитов, если ее гильбертово пространство имеет размерность 2^n, и при этом имеется 2^n взаимно ортогональных квантовых состояний. Заметим, что *n* классических битов могут представлять 2^n различных состояний.

Далее, говоря о двух ортогональных состояниях единичного кубита, мы будем пользоваться обозначениями: $\{|0\rangle,|1\rangle\}$. Если речь пойдет о состояниях конкретной системы, например, поляризации света, то будем пользоваться другими обозначениями, такими как $\{|H\rangle,|V\rangle\}$ - это будет ясно из контекста. В общем случае 2^n взаимно ортогональных состояний *n* кубитов можно представить в виде вектора $\{|i\rangle\}$, где i - это *n*-разрядное двоичное число. Например, для трех кубитов $n=3$: $\{|000\rangle,|001\rangle,|010\rangle,|011\rangle,|100\rangle,|101\rangle,|110\rangle,|111\rangle\}$ - всего 2^3 состояний.

В чем же состоит отличие между когерентной суперпозицией $|S\rangle=\alpha|0\rangle+\beta|1\rangle$, и смесью (между чистым состоянием и смешанным)? Дело в том, что для чистого состояния $|S\rangle$ всегда можно указать базис, в котором значение кубита строго определено, т.е. является собственным. Для смешанного состояния такого базиса не существует. Например, рассмотрим чистое состояние

$$|S\rangle=\frac{1}{\sqrt{2}}\left(|0\rangle+|1\rangle\right). \qquad (1)$$

При измерениях в базисе $|0\rangle$ и $|1\rangle$, очевидно, что состояния нуля и единицы будут обнаружены с вероятностью 50%. Однако если в качестве базисных использовать состояния $|+45\rangle=\frac{1}{\sqrt{2}}\left(|0\rangle+|1\rangle\right)$ и $|-45\rangle=\frac{1}{\sqrt{2}}\left(|0\rangle-|1\rangle\right)$, то состояние (1) уже строго определено и не

[2] Перепутывание - (“запутывание”, “сцепленность”, “переплетение” - от немецкого verschrankung) - это квантовая разновидность корреляции, не имеющей классического аналога. Грубо говоря, две подсистемы являются перепутанными, когда их совместное состояние более определено и менее стохастично, чем состояние любой из подсистем.

флуктуирует при измерениях. Легко убедиться, что новые базисные состояния $|+45\rangle$ и $|-45\rangle$ - ортогональны: $\langle +45|-45\rangle = 0$.

Утверждение об однозначности измерения значения кубита в новом базисе доказывается следующим образом. Применим к кубиту (1) преобразование вида:

$$\begin{aligned} \hat{H}|0\rangle &= \frac{1}{\sqrt{2}}\left(|0\rangle + |1\rangle\right), \\ \hat{H}|1\rangle &= \frac{1}{\sqrt{2}}\left(|0\rangle - |1\rangle\right). \end{aligned} \qquad (2)$$

Тогда $\hat{H}|S\rangle = \frac{1}{2}\left(|0\rangle + |1\rangle + |0\rangle - |1\rangle\right) = |0\rangle$. Таким образом, получается, что измерение кубита в новом базисе всегда будет давать ноль. Преобразование $\hat{H}$ называется ***преобразованием Адамара***.

Прямая аналогия рассмотренным преобразованиям – преобразования поляризации света в оптике. Если степень поляризации равна единице (в общем случае - эллиптическая), то всегда можно с помощью фазовой пластинки, действие которой описывается унитарным преобразованием *SU(2)*

$$\hat{D} = \begin{pmatrix} t & r \\ -r^* & t^* \end{pmatrix}, \; t = \cos\delta + i\sin\delta\cos 2\chi, \; r = i\sin\delta\sin 2\chi, \qquad (3)$$

привести это состояние к линейной поляризации (горизонтальной *H* или вертикальной *V*). Этого, очевидно, нельзя сделать с неполяризованным светом.

Говоря об основных этапах эволюции квантовых состояний, в том числе кубитов, выделим три ее компоненты: приготовление, (унитарное) преобразование и измерение.

Приготовление состояний

Рассмотрим процедуру приготовления квантового состояния. Современная лабораторная техника позволяет поместить одиночный атом в ловушку и охладить его до сверхнизких температур, при этом он переходит в основное состояние $|g\rangle$. Пусть в момент времени $t_0 = 0$ на него действует короткий лазерный импульс с известными амплитудой и длительностью. Лазерное излучение с большой точностью можно рассматривать классически. Частота лазера приблизительно попадает в резонанс с боровской частотой перехода $\omega_0 = \left(E_e - E_g\right)/\hbar$ между $|g\rangle$ и одним из возбужденных $|e\rangle$ состояний атома. Согласно теории атом под действием лазерного импульса переходит в известное состояние $|\psi\rangle = a|g\rangle + b|e\rangle$, где коэффициенты *a* и *b* определяются "площадью" лазерного импульса - произведением амплитуды на длительность. Вероятность перехода на возбужденный уровень под действием внешнего монохроматического поля дается формулой Раби:

$$P = \left[\frac{\Omega}{\tilde{\Omega}}\sin\left(\tilde{\Omega}t/2\right)\right]^2, \qquad (4)$$

где $\Omega \equiv \left|\vec{d}_0 \vec{E}_0\right| / \hbar$ - частота Раби, d_0 – дипольный момент атома, E_0 – амплитуда поля, $\tilde{\Omega} = \sqrt{\Omega^2 + (\omega - \omega_0)^2}$ - т.н. отстройка частоты. Эта формула показывает, что квантовая система под действием резонансного возмущения $\left(\omega \to \omega_0,\ \tilde{\Omega} \to \Omega\right)$ периодически переходит с нижнего уровня на верхний и обратно (рис.3). Время полного перехода в возбужденное состояние $|e\rangle$, согласно (4), составляет:

$$\frac{t\Omega}{2} = \frac{\pi}{2} \Rightarrow t_\pi = \frac{\pi}{\Omega} = \frac{\pi\hbar}{d_0 E_0}. \qquad (5)$$

Лазерный импульс такой длительности называют π-импульсом. Формула Раби дает рецепт приготовления двухуровневой системы в заданном состоянии. Например, для перевода системы из основного состояние в когерентное $|\psi\rangle = \frac{1}{\sqrt{2}}\left(|g\rangle + |e\rangle\right)$ необходимо подействовать на нее т.н. $\pi/2$-импульсом, при котором $\frac{t\Omega}{2} = \frac{\pi}{4} \Rightarrow t_{\pi/2} = \frac{\pi}{2\Omega} = \frac{\pi\hbar}{2d_0 E_0}$.

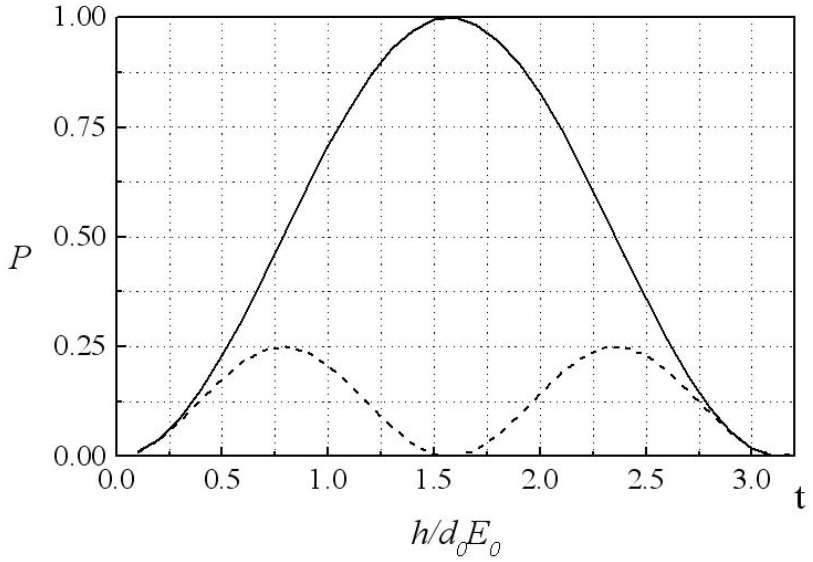

Рис.3. Эволюция двухуровневой системы под действием классического заданного поля. Пунктиром отложена зависимость вероятности перехода от времени в нерезонансном случае, когда $\omega - \omega_0 = \sqrt{3}\Omega$.

Таким образом, атом в момент окончания лазерного импульса приготавливается в любом наперед заданном состоянии. В дальнейшем состояние эволюционирует в соответствии с уравнением Шредингера: $|\psi\rangle = a|g\rangle + b|e\rangle \exp(-i\omega_0 t)$.

Отметим, что описанная процедура приготовления состояния не является измерением чего-либо, так что эти процедуры не эквивалентны, как это часто полагают. Существенным допущением явилось классическое описание лазерного поля, которое играет роль заданной внешней силы, действующей на атом. Как и при описании измерения, на стадии

приготовления необходимо "рукой" установить разумную границу между классическим и квантовым мирами.

Здесь мы пренебрегли взаимодействием атома с невозбужденными, вакуумными модами поля, что допустимо в случае достаточно короткого лазерного импульса. Учет этого взаимодействия привел бы к спонтанному излучению фотона (точнее, волнового пакета со средней частотой ω_0 и экспоненциально убывающей амплитудой), т.е. к релаксации квантовой системы. Отображающая состояние точка на сфере Блоха будет при этом двигаться по спирали от одного полюса к другому. В результате достаточно долгой релаксации атом с большой вероятностью снова оказывается в основном состоянии, а поле - в однофотонном состоянии.

Квантовые логические элементы

Этот раздел посвящен вопросам преобразования квантовых состояний. Будем называть логическим элементом (ЛЭ) умозрительное или реальное устройство, при помощи которого производятся преобразования. Математически они описывается соответствующими операторами. Таким образом, унитарные логические операции над кубитами выполняются с помощью ЛЭ (введены Давидом Дойчем в 1985-1989 гг.)

Например, рассмотрим следующее преобразование кубита $\hat{P}$: $|0\rangle \xrightarrow{P} |0\rangle$, $|1\rangle \xrightarrow{P} \exp(i\omega t)|1\rangle = \exp(i\theta)|1\rangle$ (фазовращатель). Тогда состояние кубита (по прошествии времени t) после действия операции $P(\theta)$:

$$\hat{P}(\theta) = \begin{pmatrix} 1 & 0 \\ 0 & e^{i\theta} \end{pmatrix} \tag{6}$$

изменится. В другом виде это можно записать так:

$$\hat{P}(\theta) = |0\rangle\langle 0| + \exp(i\theta)|1\rangle\langle 1|. \tag{7}$$

Перечислим некоторые основные квантовые ЛЭ:

1. $\hat{I} \equiv |0\rangle\langle 0| + |1\rangle\langle 1| \Rightarrow \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ - тождественное преобразование (8)

2. $\hat{X} \equiv |0\rangle\langle 1| + |1\rangle\langle 0| \Rightarrow \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ - ЛЭ “НЕ” (9)

3. $\hat{Z} \equiv \hat{P}(\pi) \Rightarrow \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$, (10)

4. $\hat{Y} \equiv \hat{X}\hat{Z} \Rightarrow \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$, (11)

5. $\hat{H} \equiv \frac{1}{\sqrt{2}}\left[\left(|0\rangle + |1\rangle\right)\langle 0| + \left(|0\rangle - |1\rangle\right)\langle 1|\right] \Rightarrow \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$ - ЛЭ Адамара (12)

Все они – т.н. одно-кубитовые операции, которые действуют на единичный кубит. Поскольку их действие можно описать действием некоторых гамильтонианов в уравнении

Шредингера, то все они являются унитарными операциями. Таким образом, мы будем говорить о логических операциях (ЛО) и о ЛЭ, с помощью которых эти операции выполняются. Ниже мы рассмотрим подробно физический аналог операции Адамара $\hat{H}$. Напомним, что для классических битов существует только две ЛО: операции "тождественного преобразования" и отрицания "НЕ". В квантовом случае, при операции "НЕ" состояния $|0\rangle$ и $|1\rangle$ меняются местами, т.е. существует прямая аналогия с классикой. Поскольку такая операция представляется оператором Паули $\hat{\sigma}_x$, то она часто обозначается символом $\hat{X}$. То же относится и к обозначениям $\hat{Z}$ и $\hat{Y}$.

Рассмотрим подробнее ЛО Адамара для случая, когда имеется две пространственные моды (а не поляризационные, как было выше) – т.н. «пространственный» кубит (рис.4). Из вида преобразования (12) следует, что частица, падающая на один из двух входов делителя BS, может с одинаковой вероятностью оказаться как в верхнем, так и в нижнем выходном пучке. Если на входе состояние - кубит $|S\rangle_{in} = \alpha|0\rangle_{in} + \beta|1\rangle_{in}$ (т.е. вероятности обнаружить частицу (фотон) на верхнем и на нижнем входе делителя, соответственно, равны $|\alpha|^2$ и $|\beta|^2$), то после делителя состояние преобразуется к виду:

$$|S\rangle_{out} = \hat{H}|S\rangle_{in} = \frac{1}{\sqrt{2}}\{(\alpha+\beta)|0\rangle_{out} + (\alpha-\beta)|1\rangle_{out}\}. \qquad (13)$$

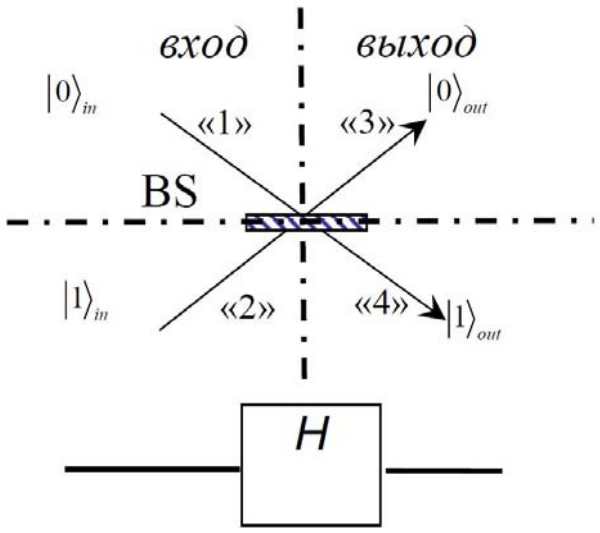

Рис.4. Реализация операции Адамара в случае «пространственного кубита»

Отсюда сразу следует, что амплитуда вероятности найти частицу в верхнем плече теперь равна $\alpha+\beta$, а в нижнем $\alpha-\beta$. Так, если $\alpha=0$ или $\beta=0$ (входное состояние частицы достоверно известно - либо сверху, либо снизу), то имеется одинаковая вероятность обнаружить ее в любом из выходных плечей. Однако, если $\alpha=\beta$, то частица обязательно будет обнаружена в верхнем плече и никогда - в нижнем! Заметим, что в данном примере речь идет о четырех пространственных модах. Две из них - входные и две - выходные. Два

ортогональных входных состояния обозначены как $|0\rangle_{in}$ и $|1\rangle_{in}$. Аналогичным образом можно рассматривать другие моды, например, поляризационные.

Следующий важный этап рассмотрения одно-кубитовых ЛЭ - последовательность нескольких ЛЭ. Если два преобразователя Адамара стоят последовательно, то физически это эквивалентно действию интерферометра с фиксированной (нулевой) фазовой задержкой между двумя плечами (рис.5):

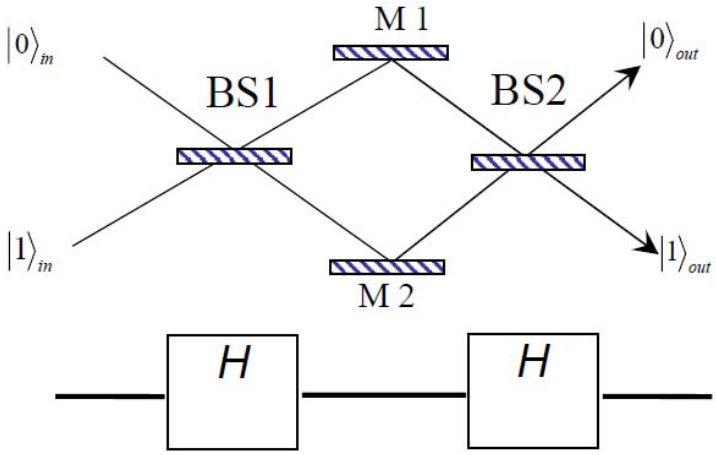

Рис.5. Интерферометр Маха-Цандера, реализованный на двух ЛЭ Адамара.

В данном случае зеркала (M1 и M2) нужны только для того, чтобы перенаправить пучки. Действие интерферометра как последовательность двух ЛЭ Адамара представляется в виде:

$$|S\rangle_{out} = \hat{H}\hat{H}|S\rangle_{in} = \hat{H}\left[\frac{1}{\sqrt{2}}\left\{(\alpha+\beta)|0\rangle_{out} + (\alpha-\beta)|1\rangle_{out}\right\}\right] = |S\rangle_{in} \qquad (14)$$

Результат прямо следует из того факта, что двойное действие преобразования Адамара есть тождественное преобразование - на выходе интерферометра воспроизводится входное состояние. В частном случае, когда на входе имеется только одно состояние ($\alpha = 1$, $\beta = 0$), согласно (14) на выходе частица будет обнаружена в верхнем плече, хотя внутри интерферометра эта частица имеет одинаковые вероятности оказаться в каждом из плеч. Дело в том, что выходные амплитуды вероятностей определяются относительной фазой, набегающей в интерферометре. В классической оптике этот эффект изучен детально и не вызывает удивления. Оказывается, что с массивными частицами, поведение которых можно описывать волнами де-Бройля, дело происходит точно также.

На языке теории квантовой информации рассмотренный эффект формулируется так. В лабораторном базисе ($|0\rangle$ и $|1\rangle$) кубит на выходе интерферометра имеет определенное значение, если и только если кубит на входе имеет определенное значение. Внутри интерферометра результат измерения состояния кубита в лабораторном базисе максимально не определен, так как его состояние представляет равновесовую суперпозицию базисных состояний: $|S\rangle = \hat{H}|S\rangle_{in} = \frac{1}{\sqrt{2}}\{|0\rangle \pm |1\rangle\}$.

Действие двух операций Адамара можно дополнить ЛЭ “фазовращатель” (6). Как видно, его действие состоит в том, чтобы вносить сдвиг фаз у одного из пучков (будем считать, что это происходит в нижнем пучке, хотя это не важно - важна только относительная фаза): $\hat{P}(\theta)|0\rangle = |0\rangle$, $\hat{P}(\theta)|1\rangle = \exp\{i\theta\}|1\rangle$.

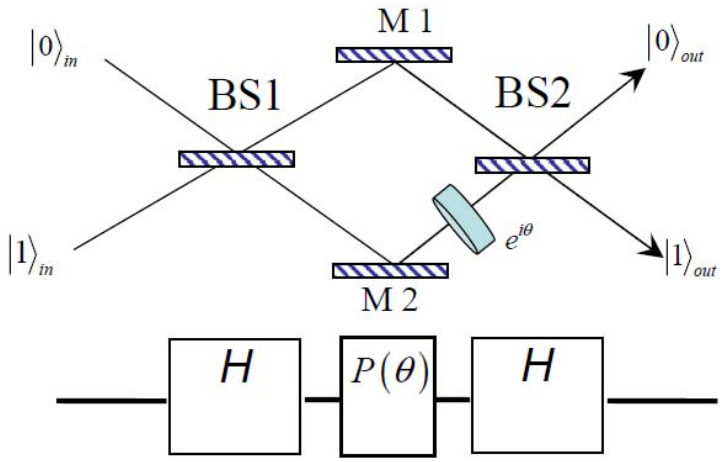

Рис.6. Интерферометр Маха-Цандера с регулируемой фазовой задержкой, как последовательность трех ЛЭ: $\hat{H}$, $\hat{P}(\theta)$, $\hat{H}$.

Значит, выходной кубит можно вычислить, применяя последовательность трех логических операций:

$$|S\rangle_{out} = \hat{H}\hat{P}(\theta)\hat{H}|S\rangle_{in} \qquad (15)$$

Например, если на входе имеется только один пучок, $\alpha = 1$, $\beta = 0$, т.е. $|S\rangle_{in} = |0\rangle$, то состояние кубита на выходе окажется:

$$|S\rangle_{out} = \hat{H}\hat{P}(\theta)\hat{H}|S\rangle_{in} = \frac{1}{2}\left\{\left[e^{i\theta}+1\right]|0\rangle + \left[e^{i\theta}-1\right]|1\rangle\right\}. \qquad (16)$$

Из этого выражения видно, что если $\theta = 0$, то значение кубита $|S\rangle_{out} = |0\rangle$, а если $\theta = \pi$, то $|S\rangle_{out} = |1\rangle$. Таким образом ЛЭ $\hat{H}\hat{P}(\theta)\hat{H}$ может переключать состояние кубита между двумя значениями. Из (16) видно, что вероятность того, что кубит имеет значение $|0\rangle$, равна $P_0 = \cos^2(\theta/2)$, а вероятность того, что он имеет значение $|1\rangle$, равна $P_1 = \sin^2(\theta/2)$.

Квантовая интерференция

Согласно принципу суперпозиции, если квантовый бит может находиться в каждом из ортогональных состояний, то он может находиться и в состоянии их когерентной суперпозиции. Такие состояния, в которых физическая величина может одновременно принимать два значения, не имеют аналога при классическом описании. Чтобы понять это, рассмотрим простейший мысленный эксперимент. Его схема показана на рисунке 7. В

качестве частиц будем рассматривать однофотонные состояния, которые достаточно хорошо можно приготавливать в эксперименте.

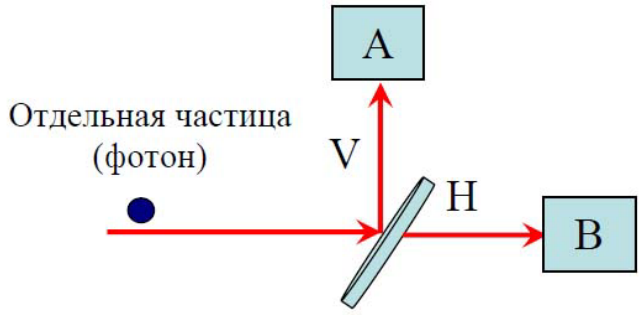

Рис.7. Прохождение отдельной частицы через поляризационный светоделитель.

Фотоны падают на поляризационный светоделитель, которое отражает вертикально поляризованную компоненту вверх, и пропускает горизонтально поляризованную компоненту. При прохождении светоделителя фотон не расщепляется пополам: энергия (частота) фотонов в выходных плечах светоделителя не меняется (светоделитель – линейный прибор). Если свет на входе поляризован под углом 45°, т.е. исходное состояние фотонов содержит равновесовой вклад этих двух ортогональных состояний, то светоделитель случайно распределяет фотоны в оба плеча – в среднем половина частиц пойдет вверх, а другая половина – вправо. Однако с точки зрения квантовой механики это не очень корректное утверждение – на самом деле нет смысла утверждать, что фотон находится или в плече H, или в плече V. Чтобы продемонстрировать это, рассмотрим другой эксперимент.

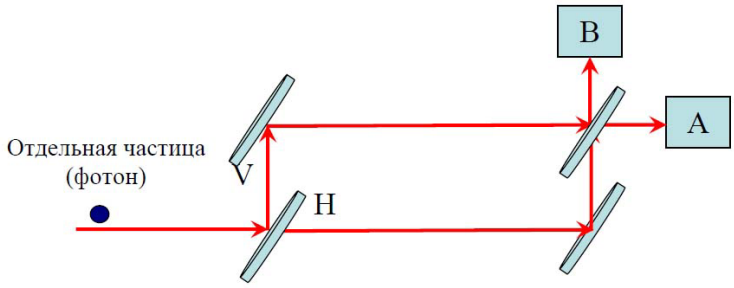

Рис.8. Однофотонная интерференция в интерферометре Маха-Цандера

На рисунке 8 изображена оптическая схема, представляющая собой последовательное соединение двух поляризационных светоделителей, так, чтобы выходные плечи первого служили бы входными плечами для второго. Такой интерферометр называется интерферометром Маха-Цандера. Будем считать, что длины плеч внутри интерферометра равны с точностью до долей длины волны, так что относительная фаза между ними много меньше $\pi/2$.

Предположим, что фотон, который с вероятностью 50% попадает в одно из двух плеч, попадает в плечо H. Но тогда, казалось бы, он точно так же с равной вероятностью распределится в одно из двух плеч и на втором светоделителе, как это было рассмотрено в предыдущем примере. Следовательно, два детектора A и B будут давать отсчеты с

одинаковой частотой. Те же рассуждения можно привести для случая, когда после первого делителя фотон направляется по пути V. Таким образом, если фотон двигался бы по строго определенным путям внутри интерферометра - неважно, вдоль какого - каждый из детекторов срабатывал бы одинаково часто - в половине всех случаев. Эксперимент и расчет показывает, что это не так. А именно, когда оптические пути в интерферометре одинаковы, фотон всегда попадает в детектор A и никогда - в B. Более того, известно, что если перекрыть любой из путей движения фотонов, оба детектора начинают давать одинаковое количество отсчетов, причем, каждый, в среднем, в четыре раза реже, чем количество фотонов на входе. Рассуждая в терминах фотонов - неделимых частиц - можно прийти к выводу, что фотон должен в некотором смысле находиться в обоих плечах одновременно при движении через интерферометр. Так, если открыты оба плеча, фотон немедленно узнает о том, что он не должен попасть в B. Иногда говорят о том, что фотону B доступна некая информация, которая распространяется вдоль другого пути со скоростью света, отражаясь от зеркал так же, как и сам фотон. Часто этому свойству квантовой интерференции приписывается существование двойников, которые оказывают влияние на движение частиц, причем касается это не только фотонов, но и других массивных частиц (нейтронов, α-частиц, электронов), с которыми проводятся интерференционные опыты.

Основы теории измерения

Формально квантовая механика описывает внутреннее состояние системы с помощью вектора состояния $|\psi\rangle = \sum_j \psi_j |\phi_j\rangle$ (где $|\phi_j\rangle$ - базисные вектора), имеющего единичную длину в линейном пространстве, определенном на поле комплексных чисел (гильбертово пространство). В этом пространстве определено скалярное произведение векторов:

$$\langle\varphi|\psi\rangle \equiv \sum_j \varphi_j^* \psi_j , \qquad (17)$$

где символ «*» означает комплексное сопряжение. Каждое физическое измерение *M*, которое может быть выполнено над системой, соответствует разложению гильбертова пространства системы на ортогональные подпространства, причем на каждое подпространство приходится по одному результату измерений. Таким образом, число возможных исходов измерений ограничено размерностью *d* гильбертова пространства. Соответственно при наиболее полных измерениях гильбертово пространство раскладывается на *d* одномерных подпространств.

Пусть $\hat{M}_k$ является проекционным оператором в *k*-ое подпространство измерения *M*. Тогда тождественный оператор *I* есть просто сумма проекционных операторов:

$$\hat{I} \equiv \hat{M}_1 + \hat{M}_2 + ... + \hat{M}_d . \qquad (18)$$

Из определения вектора состояния следует, что если система, находящаяся в состоянии $|\psi\rangle$, подвергается измерению *M*, ее поведение становится вероятностным. Исход *k*-ого измерения описывается вероятностью $\left|\hat{M}_k |\psi\rangle\right|^2$, которая на векторном языке соответствует квадрату длины проекции вектора состояния в подпространство M_k. После измерения

система переходит в новое состояние (постулат редукции фон Неймана) $\hat{M}_k|\psi\rangle\big/\left|\hat{M}_k|\psi\rangle\right|$, которое является просто единичным вектором в направлении проекции старого вектора состояния в подпространство M_k. Согласно этому постулату, измерение оставляет вектор состояния неизменным (т.е. результат измерения является предопределенным, детерминированным), только если начальный вектор состояния лежал целиком в одном из ортогональных подпространств, характеризующих измерение.

Гильбертово пространство отдельного фотона в двуплечевом интерферометре является двухмерным пространством ($d=2$). То же имеет место для поляризации единичного фотона. Следовательно, поляризационное состояние фотона полностью может быть описано с помощью линейной комбинации, скажем, двух единичных векторов $|0\rangle=(1,0)\equiv|H\rangle$ и $|1\rangle=(0,1)\equiv|V\rangle$. Проекционные операторы в базисе $|0\rangle$, $|1\rangle$ - это операторы $\hat{M}_0=|0\rangle\langle 0|$, $\hat{M}_1=|1\rangle\langle 1|$. Например, фотон, линейно поляризованный под углом α к горизонтальному направлению, описывается вектором $\psi=(\cos\alpha,\sin\alpha)$. Измеряя такой фотон в вертикально-горизонтальном (лабораторном базисе) получим горизонтально поляризованный фотон с вероятностью $\cos^2\alpha$ и вертикально поляризованный фотон с вероятностью $\sin^2\alpha$. В этом смысле два вектора $|0\rangle$ и $|1\rangle$ представляют собой разложение двухмерного гильбертова пространства в два ортогональных одномерных пространства. Эти два вектора будем назвать линейным прямоугольным базисом.

Альтернативным базисом того же гильбертова пространства является т.н. диагональный базис, образованный векторами $d_1=1/\sqrt{2}\,(1,1)\equiv|+45^0\rangle$ и $d_2=1/\sqrt{2}\,(1,-1)\equiv|-45^0\rangle$.

Определение. Два (рассмотренных) базиса называются ***сопряженными*** (conjugated, mutually unbiased), если каждый вектор одного базиса имеет проекции одинаковой длины на все вектора другого базиса. Это означает, что система, приготовленная в некоем состоянии, представленном векторами одного базиса, будет вести себя совершенно случайным образом, будучи измеренной в сопряженном базисе. Математически это требование записывается как

$$\left|\langle\varphi_i|\psi_j\rangle\right|^2=\frac{1}{2} \qquad (19)$$

В общем случае в знаменателе выражения (19) должна стоять размерность гильбертова пространства.

Действительно, проецируя (измеряя) фотон, находящийся в состоянии $|\psi_{in}\rangle\equiv|1\rangle$ на состояние $|\psi_{out}\rangle\equiv\frac{1}{\sqrt{2}}\{|0\rangle+|1\rangle\}$, получаем, что результат будет происходить с вероятностью

$$\left|\langle\psi_{out}|\psi_{in}\rangle\right|^2=\left|\frac{1}{\sqrt{2}}\{\langle 0|+\langle 1|\}|1\rangle\right|^2=\frac{1}{2}.$$

Часть 2. Квантовая криптография. Квантовое распределение ключа

Квантовая криптография (КК) - это интердисциплинарная область знания, технологии и техники, в которой решается задача об обеспечении легитимных пользователей идентичными случайными последовательностями символов посредством передачи квантовых состояний. Такие последовательности представляют собой основу для криптографических ключей, с помощью которых шифруется закрытая информация. Поэтому иногда квантовую криптографию называют квантовым распределением ключей (Quantum Key Distribution). КК основана на соотношении неопределенностей Гейзенберга: наблюдаемые величины, которым в квантовой механике ставятся в соответствие некоммутирующие операторы, не имеют общего набора собственных векторов, и не могут быть одновременно измерены. Таким образом, в основе КК лежат законы природы, а не вычислительные или любые другие возможности легитимных пользователей или злоумышленников. КК является составной частью квантовой связи (quantum communication).

По сложившейся традиции, особенно в англоязычной литературе, участников процесса кодирования/декодирования называют Алисой и Бобом (рис.9). Кроме того, в криптографии рассматривается некий злоумышленник или подслушиватель (eavesdropper) Ева, который владеет современными вычислительными ресурсами, полностью осведомлен об используемых криптографических методах, алгоритмах, протоколах, и т.д. и пытается каким-либо образом скомпрометрировать их. Под компрометацией понимается несанкционированное чтение закрытой информации, ее модификация и т.д. Все эти действия подслушивателя Евы называются криптографической атакой.

Рис.9. Схема общения между участниками протоколов КК.

Теорема о запрете клонирования: неизвестное квантовое состояние нельзя копировать.

Под копированием понимается процедура, при которой каждому входному состоянию ставится в соответствие два идентичных ему выходных состояния. Унитарность эволюции квантово-механических систем делает такой процесс возможным только при искажении копируемого состояния. Более того, чем больше информации о состоянии извлекается в процессе копирования, тем большее искажение вносится в исходное состояние. Эта теорема лежит в основе квантовой криптографии. Действительно, искажение состояния приводит к

статистическим ошибкам, проявляющимися на определенном этапе выполнения протокола квантовой криптографии. Анализ этих ошибок позволяет легитимным пользователям сделать вывод о несанкционированном вторжении в линию связи и либо исправить их, либо прервать сеанс связи.

Кодирование информации в квантовых состояниях впервые было предложено в работах Стефана Визнера, а также Чарльза Беннета и Жиля Брассарда. Их идея состояла в том, что пассивный подслушиватель не может достоверно различить неортогональные квантовые состояния (назовем их $|\psi\rangle$ и $|\varphi\rangle$), если он не знает базиса, в котором те были приготовлены. На этом этапе проявляется принципиальное отличие между классическими и квантовыми состояниями. Действительно, предположим, что Ева настраивает свой измеряющий прибор в неком исходном состоянии $|m\rangle$. Ее цель – различить состояния $|\psi\rangle$ и $|\varphi\rangle$, не возмущая их. Ее действия будут описываться следующими унитарными преобразованиями над входными состояниями:

$$|\psi\rangle|m\rangle \xrightarrow{U} |\psi\rangle|m_1\rangle, \tag{1}$$

$$|\varphi\rangle|m\rangle \xrightarrow{U} |\varphi\rangle|m_2\rangle. \tag{2}$$

Унитарность сохраняет скалярное произведение, поэтому

$$\langle\psi|\varphi\rangle U^{\dagger}U\langle m|m\rangle = \langle\psi|\varphi\rangle\langle m_1|m_2\rangle, \tag{3}$$

откуда следует, что

$$\langle m_1|m_2\rangle = 1. \tag{4}$$

Соотношение (4) означает, что конечное состояние измерительного прибора Евы одно и то же. Ева не возмутила квантовых состояний, но она и не получила никакой информации о них, в силу (4). Можно рассмотреть и более общее измерение, когда Ева возмущает своим прибором исходные состояния:

$$|\psi\rangle \to |\psi'\rangle,\ |\varphi\rangle \to |\varphi'\rangle \tag{5}$$

Тогда в результате ее действий:

$$|\psi\rangle|m\rangle \to |\psi'\rangle|m_1\rangle, \tag{6}$$

$$|\varphi\rangle|m\rangle \to |\varphi'\rangle|m_2\rangle. \tag{7}$$

И опять, в силу унитарности, получаем:

$$\langle\psi|\varphi\rangle = \langle\psi'|\varphi'\rangle\langle m_1|m_2\rangle. \tag{8}$$

Наилучшая ситуация с точки зрения Евы возникает, когда скалярное произведение $\langle m_1|m_2\rangle$ принимает минимальное значение. Это происходит при условии

$$\langle\psi'|\varphi'\rangle = 1, \tag{9}$$

(так как $\langle\psi|\varphi\rangle = const \neq 0$). При этом она получает максимальную возможность различить два состояния своего прибора, но два исходно неортогональных состояния становятся неразличимыми (9).

К.Шеннон рассматривал шифрование (кодирование) как отображение исходного

сообщения в криптограмму - зашифрованное сообщение:

$$C = F_i(M), \tag{10}$$

где C - криптограмма (от coding), F_i - отображение, M - исходное сообщение (от message), i - индекс, соответствующий конкретному используемому ключу. Рассмотрим простейший шифр, в котором исходный алфавит сообщения совпадает с множеством знаков ключа и множеством знаков криптограммы. Пусть кодирование выполняется путем замены знаков исходного сообщения на знаки криптограммы в зависимости от очередного значения символа ключа, который выбирается из случайной последовательности чисел от 0 до 39. Тогда сообщение, ключ и криптограмма представляются в виде последовательности знаков одного и того же алфавита. Например, будем использовать простой алфавит заглавных букв русского языка, пробела и нескольких знаков препинания:

А	Б	В	…	Э	Ю	Я		.	,	!	?	;
00	01	02		31	32	33	34	35	36	37	38	39

Таблица 1. Соответствие символов алфавита числам от 00 до 39

Допустим, мы хотим зашифровать сообщение “КОД ВЕРНАМА”. Запишем его в верхней строке вспомогательной таблицы. Ниже укажем соответствующие численные символы из верхней таблицы. В третью строку поместим случайную выборку из сорока чисел от 00 до 39. В последней строке поместим результат суммирования символов второй и третьей строки по модулю 40:

К	О	Д		В	Е	Р	Н	А	М	А
10	14	04	34	02	05	16	13	00	12	00
15	04	13	28	11	09	38	30	02	24	05
25	18	17	22	13	14	14	03	02	36	05

Таблица 2. Пример кодирования сообщения «КОД ВЕРНАМА» (первая строка), представленного набором чисел (вторая строка), последовательность случайных чисел (третья строка), и результат его кодирования (четвертая строка).

Например, четвертый символ “пробел” в сообщении имеет числовой код “34”. Соответствующее случайное число, выпавшее на этот символ, оказалось “28”. Тогда $34 + 28 = 62 = 40 + 22$, следовательно, остаток при суммировании по модулю “40” равен 22. Таким образом, шифрование и дешифрование по рассмотренному алгоритму можно записать в виде:

$$M + k \left(mod\, 40\right) = C. \tag{11}$$

$$C - k \left(mod\, 40\right) = M. \tag{12}$$

Этот способ шифрования был изобретен Жильбером Вернамом. Клод Шеннон показал, что если ключ действительно случайный, имеет такую же длину, как и само сообщение, и не

используется более одного раза, то такая одноразовая передача сообщения абсолютно защищена. Примечательно, что результат не зависит от вычислительной мощности, доступной криптоаналитику. Шифры такого рода называются безусловно стойкими. Рассмотренный пример относится к криптосистемам, использующим равновероятный случайный ключ, имеющий длину, равную длине сообщения. Они называются одноразовыми блокнотами. Несмотря на обеспечение безусловной секретности, на практике такие системы получили ограниченное применение, поскольку требуют передачи ключа большого объема для каждого нового сообщения. А для длинных ключей процедура их управления, включающая их генерацию, передачу и хранение крайне усложняется. Другим недостатком кода Вернама является тот факт, что ключ должен использоваться лишь один раз. Так при повторном использовании Ева может, записывая и сравнивая отдельные части криптограммы, восстановить как фрагменты открытого текста, так и сам ключ. Кроме того, чисто из физических соображений, классические состояния физических объектов могут быть измерены сколь угодно точно и без их возмущения. Поэтому в рамках классических физических представлений невозможно обеспечить секретное распределение ключа через открытый канал связи, т.к. нельзя гарантировать обнаружение попыток пассивного подслушивания. Поэтому криптограммы с одноразовыми ключами не получили широкого применения.

Таким образом, существующие одноключевые криптографические протоколы обеспечивают хорошую защищенность при условии решения проблемы распределения ключа. Однако у этих систем существует две принципиальные проблемы*:*

1. как осуществить распределение ключей по защищенному каналу;
2. как осуществить аутентификацию секретного ключа (т.н. проблема первого общения).

Первая из проблем имеет два способа ее решения. Первый - математический - достигается с помощью т.н. двухключевых протоколов или криптографии с открытым ключом. Второй способ - физический - реализуется с помощью квантовой криптографии.

Итак, квантовая криптография позволяет решить одну из проблем классической криптографии, а именно - распределение ключей с последующим шифрованием в режиме одноразового блокнота. Тем самым, обеспечивается безусловная секретность при обмене информацией между легитимными пользователями. При этом, как уже говорилось, для обеспечения безусловной секретности необходимо удовлетворить трем условиям:

- сообщение шифруется ключом, который представляет собой случайную последовательность символов, например, нулей и единиц;
- длина ключа должна быть не меньше длины сообщения;
- ключ используется только один раз.

Кроме квантового канала связи, по которому передающая и принимающая стороны обмениваются квантовыми состояниями – либо по волоконной оптической линии связи, либо через атмосферу, важно, что неотъемлемым атрибутом КК является т.н. «открытый» канал связи. Открытым называется канал, если передаваемая по нему информация может быть доступна любому участнику протокола, в том числе злоумышленнику. Важным условием

использования открытого канала в КК является невозможность изменить передаваемую по нему информацию. Таким каналом может выступать, например, интернет.

Протокол BB84.

Под протоколом понимается совокупность действий (таких как инструкции, команды, вычисления, алгоритмы), выполняемых в заданной последовательности двумя или более легитимными субъектами с целью достижения некоего результата.

Известно несколько протоколов распределения ключей на основе дискретных квантовых состояний. Наиболее известный из них - BB84. В нем используется два (или, в общем случае, три) взаимно-несмещенных базиса, состоящих из пары ортогональных состояний. Они образованы парами ортогональных поляризационных векторов: в лабораторном базисе: $\left(\left|\updownarrow\right\rangle \equiv \left|V\right\rangle, \left|\leftrightarrow\right\rangle \equiv \left|H\right\rangle\right)$, в диагональном базисе: $\left(\left|\swarrow\right\rangle \equiv \frac{1}{\sqrt{2}}\left\{\left|H\right\rangle + \left|V\right\rangle\right\}, \left|\nwarrow\right\rangle \equiv \frac{1}{\sqrt{2}}\left\{\left|H\right\rangle - \left|V\right\rangle\right\}\right)$. Полная формализация достигается, если состояниям, соответствующим вертикальной и горизонтальным поляризациям света, сопоставить векторы в т.н. вычислительном базисе: $\left|H\right\rangle \to \left|1\right\rangle, \left|V\right\rangle \to \left|0\right\rangle$. Протокол включает следующие этапы, которые проиллюстрированы в таблице 3:

1. Вводится синхронизация между действиями Алисы и Боба, т.е. каждый из них знает наверняка, в какой момент времени посылается состояние;

2. Алиса выбирает случайный массив битов (чередование 0 или 1 в моменты, оговоренные синхронизационным протоколом);

3. Алиса выбирает случайную последовательность (поляризационных) базисов – чередование либо лабораторного, либо диагонального;

4. Алиса посылает Бобу последовательность фотонов, кодируя поляризацию каждого фотона, исходя из массива битов и поляризационного базиса: каждый фотон имеет определенную поляризацию и описывается одним из четырех базисных векторов. Например, единице соответствуют состояния $\left|\updownarrow\right\rangle$, $\left|\nwarrow\right\rangle$, а нулю – состояния $\left|\leftrightarrow\right\rangle$ и $\left|\swarrow\right\rangle$ в лабораторном и диагональном базисах, соответственно.

5. Боб принимает (измеряет) посланные Алисой фотоны в одном из двух базисов. Причем выбор базиса – случаен. Боб интерпретирует результаты своих измерений в бинарном представлении, т.е. пользуясь тем же правилом, что и Алиса: «0» - $\left|\leftrightarrow\right\rangle, \left|\swarrow\right\rangle$ и «1» - $\left|\updownarrow\right\rangle, \left|\nwarrow\right\rangle$. Заметим, что, как следует из теории измерений, Боб полностью теряет информацию о состоянии фотона, поляризованного в лабораторном базисе, измеряя его в диагональном базисе и, наоборот. Следовательно, Боб получает достоверную информацию о состоянии фотонов только в половине всех случаев – когда выбранный им базис совпал с базисом Алисы, т.е. когда измерение дает детерминированный результат. Если подслушивания не было, то в оставшейся половине случаев Алиса и Боб имеют некоррелированные результаты. Следовательно, в среднем, Боб получает массив битов с

25%-ым содержанием ошибок. Этот массив называется сырым ключом. Кроме того, будем учитывать тот факт, что часть фотонов теряется при передаче. Практически, уровень технических ошибок в квантовых протоколах на сегодняшний день составляет несколько процентов (в отличие от уровня 10^{-9}, достижимого в современных оптотелекоммуникационных линиях связи). Этот уровень называется Quantum Bit Error Rate (QBER).

6. Происходит обсуждение результатов измерений по открытому каналу связи, причем и Алиса и Боб предполагают, что их могут подслушать, но не перехватить или изменить результаты. Сначала они определяют, какие из фотонов были зарегистрированы Бобом. Затем, определяют, в каких случаях Боб угадал базис: Боб сообщает базис, в котором производилось измерение, но не сообщает сам результат. Оставляются только те события, для которых базисы Алисы и Боба совпали. При этом теряется 50% информации – когда Боб неверно угадал базис. Алиса и Боб считают, что в случаях, когда Боб угадал базис, биты, закодированные соответствующими фотонами, переданы правильно. Заметим, что по открытому каналу информация о самой случайной последовательности битов, посылаемых Алисой, не передается – вывод делается только на основе теории квантовых измерений. Каждый из переданных таким образом фотонов в правильном базисе несет один бит информации, а именно был ли он поляризован вертикально или горизонтально в лабораторном базисе или под углами $\pm 45^0$ - в диагональном базисе. В итоге у Боба остается более короткий массив битов, который называется просеянным ключом.

7. Затем Алиса и Боб проверяют, были ли попытки подслушивания во время распределения ключа. Для этого они сравнивают некоторые биты, которые, как они считают, были распределены правильно, по открытому каналу связи. Позиции битов по шкале синхронизационного протокола должны выбираться случайно, но одинаково, скажем, сравнивая каждый третий бит. Если осуществлялось подслушивание, то с вероятностью 50% биты Алисы и Боба, которые должны были совпадать, различаются. Использованные для сравнения биты выбрасываются из исходной последовательности, и она сокращается. Если сравнение не обнаруживает разницы, то Алиса и Боб делают вывод, что распределение ключа произошло с высокой степенью надежности (существует некоторая вероятность не обнаружить подслушивания, но при этом у подслушивателя окажется мало информации).

8. Последний шаг протокола квантовой криптографии состоит в том, чтобы, используя классические алгоритмы, исправить ошибки (error correction) и уменьшить информацию, доступную Еве. Последняя процедура называется усилением секретности (privacy amplification). Простейшая процедура коррекции ошибок состоит в следующем. Алиса случайно выбирает пары битов и производит над ними логическую операцию XOR. Боб выполняет такую же операцию над соответствующими своими битами. Если результат совпадает, они сохраняют первый из двух битов и уничтожают второй – поскольку сама процедура происходит по открытому каналу и результат доступен Еве. Если результаты отличаются – оба бита выкидываются (на практике используется более сложный алгоритм). После этой процедуры Алиса и Боб имеют одинаковые копии ключа, но у Евы все же может

остаться некоторая информация о нем, поэтому вступают в силу протоколы усиления секретности. Эти классические протоколы работают следующим образом. Алиса опять выбирает случайно пары битов и вычисляет их сумму по модулю 2 (XOR). Но в отличие от процедуры коррекции ошибок, она не сообщает это значение. Она лишь оглашает, какие биты были выбраны, например, под номерами 103 и 539. Затем Алиса и Боб заменяют два бита на результат операции XOR. Таким образом, Алиса и Боб укорачивают свои ключи. Если Еве доступна лишь часть информации о двух битах, то ее информация о результате выполнения операции XOR будет еще меньше. Итак, если вероятность ошибок не превосходит некоторой критической величины (в нерелятивистских схемах предел, по-видимому, составляет 11%, что определяется потерями в оптическом волокне), то далее возможна коррекция ошибок в нераскрытой части при помощи классических кодов и дальнейшее сжатие ключа для получения результирующего секретного ключа.

9. Включается абсолютно стойкий протокол одноразового блокнота через открытый канал связи.

10. Весь протокол повторяется каждый раз при необходимости посылки очередного сообщения.

Заметим, что на практике для передачи квантовых битов и обмена классическими сообщениями можно использовать один и тот же канал связи.

Вкратце рассмотрим, что происходит при попытке подслушивателя (Евы) извлечь часть информации. Рассмотрим простейшую атаку «перехват-пересылка» в протоколе BB84. Эта атака сводится к тому, что Ева случайно выбирает один из двух измерительных базисов, производит измерение и перепосылает Бобу то состояние, которое она измерила. В половине случаев она правильно угадывает базис, производит адекватное измерение, и перепосылает соответствующее «правильное» состояние Бобу. В этом случае подслушатель остается незамеченным и извлекает всю информацию о состоянии. Однако в другой половине случаев Ева неправильно выбирает базис и, следовательно, посылает «неправильное» состояние, которое будучи измерено в «правильном» базисе даст ошибку с вероятностью $0.5*0.5=0.25$. Эта ошибка выявляется после процедуры сравнения базисов. Как видно, она более чем в два раза превышает критический уровень этого протокола 0.11.

К проблемам квантовой криптографии следует отнести наличие потерь в оптических элементах, флуктуации их параметров под внешним воздействием, присутствие темновых отсчетов в используемых однофотонных детекторах и др. Технический способ решения этих проблем состоит в использовании элементов криптографической системы более высокого качества. Физический путь состоит в разработке новых протоколов, обладающих более высоким уровнем критической ошибки.

Основная литература

1. Д.Боумейстер, А.Экерт, А.Цайлингер, Физика квантовой информации. Москва, Постмаркет, 2002.-376с., ил.

2. М.Нильсен, И.Чанг, Квантовые вычисления и квантовая информация. Москва, Мир, 2006.-824с., ил.

ПЕРЕДАЧА КВАНТОВЫХ ДАННЫХ																			
АЛИСА																			
Случайная последовательность битов у Алисы	**0**	**1**	**1**	**0**	**1**	**1**	**0**	**0**	**1**	**0**	**1**	**1**	**0**	**0**	**1**	**1**	**0**	**1**	**0**
Базис, случайно выбираемый Алисой	**D**	**R**	**D**	**R**	**R**	**R**	**R**	**R**	**D**	**D**	**R**	**D**	**D**	**D**	**R**	**D**	**R**	**R**	**D**
Состояние, которое посылает Алиса	⤢	↕	⤡	↔	↕	↕	↔	↔	⤡	⤢	↕	⤡	⤢	⤢	↕	⤡	↔	↕	⤢
БОБ																			
Базис, случайно выбираемый Бобом	**R**	**D**	**D**	**R**	**R**	**D**	**D**	**R**	**D**	**R**	**D**	**D**	**D**	**D**	**R**	**R**	**R**	**D**	**D**
Биты, регистрируемые Бобом (***сырой ключ***)	**1**	**0**	**1**	**0**	**1**	**1**	**0**	**0**	**1**	**1**	**1**	**1**	**0**	**0**	**1**	**0**	**0**	**0**	**0**
Учет технических потерь	**1**	×	**1**	×	**1**	**1**	**0**	**0**	×	**1**	**1**	**1**	×	**0**	**1**	×	**0**	**0**	**0**
ОТКРЫТОЕ ОБСУЖДЕНИЕ																			
Боб сообщает базис, в котором зарегистрирован бит	**R**		**D**		**R**	**D**	**D**	**R**	×	**R**	**D**	**D**	×	**D**	**R**	×	**R**	**D**	**D**
Алиса сообщает, какой базис совпадает с ее базисом	**-**		**Да**		**Да**	**-**	**-**	**Да**	**-**	**-**	**-**	**Да**	**Да**	**Да**	**Да**		**Да**	**-**	**Да**
Предварительная распределенная информация - ***просеянный ключ***			**1**		**1**			**0**				**1**		**0**	**1**		**0**		**0**
КОРРЕКЦИЯ ОШИБОК																			
Боб сообщает случайно выбранные биты					**1**										**1**		**0**		
Алиса сравнивает их с соответствующими своими					**Да**										**Да**		**Да**		
ИТОГ																			
Распределенный ключ			**1**					**0**				**1**		**0**					**0**

Таблица 3. Протокол BB84 (нет подслушивания, без усиления секретности)