МОСКОВСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ ИМЕНИ М.В. ЛОМОНОСОВА
ФАКУЛЬТЕТ ВЫЧИСЛИТЕЛЬНОЙ МАТЕМАТИКИ И КИБЕРНЕТИКИ
КАФЕДРА СУПЕРКОМПЬЮТЕРОВ И КВАНТОВОЙ ИНФОРМАТИКИ

Моделирование релятивистской системы квантового распределения ключей

Введение в дипломную работу

Студент 523 группы
Большаков Роман

Научный руководитель
профессор Молотков С.Н.

Москва
2014

Содержание

1 Классическая криптография

Задача передачи секретной информации известна человечеству с самых ранних времён. Из основных типов сведений, для которых может быть важна их секретная передача, можно выделить следующие:

- важная государственная информация,
- информация, содержащая военные секреты,
- коммерческие данные,
- личная конфиденциальная информация.

Исход большого количества военных кампаний и финансовый успех многих корпораций всегда был напрямую связан в том числе с умением передавать информацию без её утечки к третьим лицам, что говорит о существенной ценности развития технологий секретной передачи данных.

1.1 Симметричные и асимметричные криптосистемы

Традиционно для шифрования информации используются два подхода: симметричные криптосистемы и асимметричные. В симметричных методах шифрования применяется один и тот же ключ как для шифрования, так и для расшифрования данных. Обе стороны коммуникации должны знать этот ключ и хранить его в секрете. При асимметричном шифровании используется два ключа: открытый и закрытый. Открытый ключ передается по незащищенному каналу и используется для проверки электронной подписи и шифрования сообщения. Закрытый ключ используется для расшифрования сообщений и генерации электронной подписи.

Асимметричные криптосистемы имеют ряд преимуществ перед симметричными:

- не нужно предварительно передавать секретный ключ по надежному каналу,
- этот секретный ключ известен только одной стороне,
- пару ключей можно долгое время не менять.

Однако есть и серьезные недостатки, которые не позволяют полностью перейти на использование асимметричных систем:

- в алгоритм сложно внести изменения,
- ключи имеют большую длину,
- по сравнению с симметричными криптосистемами процесс шифрования и расшифрования медленнее на порядки,
- требуются значительно большие вычислительные мощности для функционирования асиметричной криптосистемы.

1.2 Стойкость симметричного шифрования

Итак, главное свойство симметричных шифров — в них используется один и тот же ключ k для шифрования и расшифрования сообщения. Это можно обозначить как

$$C = E_k(m), m = D_k(C),$$

где E — шифрующая функция,

- D — расшифровывающая функция,
- m — исходное сообщение,
- C — шифротекст.

Приведем теоретическое обоснование стойкости одного из наиболее важного метода шифрования — одноразового блокнота [1]. Введем обозначения:
$\mathbb{M}$ — множество всевозможных открытых текстов M,
$\mathbb{C}$ — множество шифротекстов C,
$\mathbb{K}$ — множество ключей K.

На каждом из указанных множество введена вероятность выбора соответствующего элемента. Для возможности однозначного расшифрования сообщения, требуется $|\mathbb{C}| \geq |\mathbb{M}|$. Кроме того, целесообразно полагать, что выбор ключа не должен зависеть от передаваемого сообщения: $p(M = m, K = k) = p(M = m)p(K = k)$.

Пытаясь вскрыть шифр, Ева имеет задачу нахождения исходного сообщения m по его шифротексту c. Вероятность решить эту задачу равна

$$p(M = m|C = c) = \frac{p(M = m)p(C = c|M = m)}{p(C = c)}.$$

Цель Алисы и Боба состоит в том, чтобы шифротекст давал как можно меньше информации об исходном сообщении.

Криптосистема называется абсолютно стойкой, если для всех открытых текстов m и всех шифротекстов c выполняется

$$p(C = c|M = m) = p(M = m).$$

Если пары сообщения из M и соответствующего ему шифротекста из C – статистически независимые случайные величины, то такая криптосистема обладает **совершенной криптостойкостью**.

Пусть сообщения M и ключи K являются независимыми случайными величинами. Это значит, что совместное распределение $P_{mk}(M, K)$ равно произведению отдельных распределений:

$$P_{mk}(M, K) = P_m(M) \cdot P_k(K).$$

Пусть $C = E_K(M)$ — шифрованный текст, $M = D_K(C)$ — расшифрованный текст. Можно найти $P_c(C)$, $P_{mck}(M, C, K)$.

Оценим энтропию открытого текста M с учетом статистической независимости M и C:

$$H(M) = H(M|C) \leq H(MK|C) = H(K|C) + H(M|CK) = H(K|C) \leq H(K).$$

Так как энтропия открытого текста при заданном шифротексте и известном ключе равна нулю, то $H(M|CK) = 0$. В результате получаем

$$H(M) \leq H(K).$$

С другой стороны, энтропия открытого текста $H(M)$ характеризует минимальную длину последовательности для описания случайной величины M (открытого сообщения), а $H(K)$ характеризует минимальную длину последовательности для описания ключа. Получилось, что совершенная криптостойкость возможна только тогда, когда длина ключа не меньше, чем длина шифруемого сообщения, то есть

$$H(M) \leq H(K).$$

Таким образом, приходим к теореме Шеннона:

Теорема 1. *Симметричная криптосистема, заданная набором*

$$(\mathbb{M}, \mathbb{C}, \mathbb{K}, E_k(\cdot), D_k(\cdot)),$$

где $|\mathbb{M}| = |\mathbb{C}| = |\mathbb{K}|$*, является абсолютно стойкой тогда и только тогда, когда выполнены условия:*

1. *вероятности использования всех ключей равны:* $p(K = k) = 1/|\mathbb{K}|, \forall k \in \mathbb{K}$*,*
2. *для каждой пары сообщения* $m \in \mathbb{M}$ *и шифротекста* $c \in \mathbb{C}$ *существует только один ключ* $k \in \mathbb{K}$ *такой, что* $E_k(m) = c$*.*

1.3 Криптосистема Вернама

Приведем пример системы с совершенной криптостойкостью.

Пусть сообщение представлено двоичной последовательностью длины N:

$$m = (m_1, m_2, \cdots, m_N).$$

Распределение вероятностей сообщений $P_m(m)$ может быть любым. Ключ также представлен двоичной последовательностью $k = (k_1, k_2, \cdots, k_N)$ той же длины, но с равномерным распределением $P_k(k) = \frac{1}{2^N}$ для всех ключей.

Шифрование в криптосистеме Вернама осуществляется путем покомпонентного суммирования по модулю 2 последовательностей открытого текста и ключа:

$$C = M \oplus K = (m_1 \oplus k_1, m_2 \oplus k_2, \cdots, m_N \oplus k_N).$$

Легальный пользователь знает ключ и осуществляет расшифрование: $M = C \oplus K = (m_1 \oplus k_1, m_2 \oplus k_2, \cdots, m_N \oplus k_N)$.

После выполнения этих операций ключ перестает использоваться, что объясняет другое название шифра Вернама — **одноразовый блокнот**.

Основная задача, к которой приводит использование симметричных криптосистем: как секретно передать секретный ключ? Если в нашем распоряжении имеется надежный канал, то отпадает и необходимость использовать какое бы то ни было шифрование. В противном случае, в предположении о неограниченных вычислительных и иных возможностях злоумышленника (единственное условие: должны соблюдаться законы природы), задача распределения ключей оказывается неразрешимой в классической физике. Однако с помощью квантовой физики можно предъявить такой протокол распределения ключей, что какими бы возможностями не обладал злоумышленник (с учетом того же условия), легитимные пользователи либо получат общий секретный ключ, который не будет известен злоумышленнику, либо любое вторжение злоумышленника в канал связи будет приводить к детектированию подслушивания.

2 Основные понятия квантовой теории информации

2.1 Квантовые состояния

При проведении первых опытов над элементарными частицами было обнаружено, что их поведение очень сложно увязать с имевшимися на тот момент представлениями о физических явлениях. Это привело к тому, что после формулировки новых законов, описывающих поведение элементарных частиц, это часть физики стали называть квантовой теорией, а сложившуюся на тото момент физическую картину мира — классической.

2.1.1 Волновая функция и чистые состояния

Одно из главных отличий квантовой теории от классической проявляется в самом определении квантовой частицы и её состояния. Представление о квантовой частице, как о некотором теле, имеющем определенные физические характеристики вроде координаты, размера или массы, оказалось в корне неверным, так как для некоторых частиц не удавалось даже понять, в какой точке пространства они в принципе находятся. Зато оказалось возможным предсказать, как эти частицы будут себя вести. Трудность заключалась в том, что объяснить поведение частиц удалось только после окончательного отказа от попыток вычислить «традиционные» характеристики системы. Это привело к тому, что состояние элементарных частиц и их систем стали представлять с помощью «волновой функции».

Введем понятие *чистого квантового состояния*. Таким состоянием будем называть вектор в гильбертовом пространстве $\mathcal{H}$ с единичной нормой. Под нормой вектора понимается корень его скалярного квадрата.

Будем обозначать вектор состояния, соответствующий состоянию ψ, как $|\psi\rangle$. Сопряжённый вектор, соответствующий состоянию ψ, будем обозначать как $\langle\psi|$. Скалярное произведение векторов $|\psi\rangle$ и $\langle\psi|$ будем обозначать как $\langle\phi|\psi\rangle$, а образ вектора $|\psi\rangle$ под действием оператора $\mathcal{F}$ будем обозначать $\mathcal{F}\,|\psi\rangle$. Подобные обозначения в целом согласуются с обозначениями обычной линейной алгебры, но более удобны в квантовой механике, так как позволяют более наглядно и коротко называть используемые векторы.

Если мы рассмотрим два различных состояния, то суперпозиции (всевозможные линейные комбинации) пары соответствующих им векторов дадут двумерное линейное комплексное пространство. При рассмотрении квантовой системы, состоящей из двух подсистем, пространство состояний строится в виде тензорного произведения.

Для каждого чистого квантового состояния $|\psi\rangle$ можно определить соответствующий ему оператор $\rho_\psi = |\psi\rangle\langle\psi|$, называемый оператором плотности. Этот оператор имеет единичный след, ранг 1 и действует как проектор на чистое состояние $|\psi\rangle$.

2.1.2 Изменение состояний во времени

Одним из ключевых законов квантовой механики является уравнение Шрёдингера, описывающее изменение квантовых состояний во времени. Традиционно это уравнение записывается как

$$i\hbar\frac{d\,|\psi\rangle}{dt} = H\,|\psi\rangle\,,$$

где $\hbar$ — постоянная Планка. Эрмитов оператор H называется гамильтонианом системы, и именно он оказывает влияние на её эволюцию.

Так как существует соответствие между унитарными и эрмитовыми операторами [2]

$$U = e^{iH},$$

то уравнение Шрёдингера может быть переписано:

$$|\psi'\rangle = U\,|\psi\rangle\,.$$

Такой вид оказывается более удобным, так как он означает, что любая эволюция квантовой системы может быть представлена как действие унитарного преобразования.

2.1.3 Принцип суперпозиции квантовых состояний

Квантовая суперпозиция — это суперпозиция состояний, которые не могут быть реализованы одновременно с классической точки зрения, это суперпозиция альтернативных (взаимоисключающих) состояний.

Если функции Ψ_1 и Ψ_2 являются допустимыми волновыми функциями, описывающими состояние квантовой системы, то их линейная суперпозиция, $\Psi_3 = c_1\Psi_1 + c_2\Psi_2$, также описывает какое-то состояние данной системы. Если измерение какой-либо физической величины $\hat{f}$ в состоянии $|\Psi_1\rangle$ приводит к определённому результату f_1 , а в состоянии $|\Psi_2\rangle$ – к результату f_2 , то измерение в состоянии $|\Psi_3\rangle$ приведёт к результату f_1 или f_2 с вероятностями $|c_1|^2$ и $|c_2|^2$ соответственно.

2.1.4 Кубиты

Простейшим примером нетривиального квантового объекта является система с двумя базисными состояниями. Физическими примерами таких систем могут быть фотоны с соответствующими направлениями поляризации или направления спина электрона. В этом случае соответствующее гильбертово пространство будет двумерным, его обозначают $\mathcal{H}^2$. Если не важна конкретная физическая природа двухуровневой системы, её состояния обозначают как $|0\rangle$ и $|1\rangle$. Такую систему называют *кубитом* по аналогии с классическим битом.

Произвольное чистое состояние кубита можно записать как

$$|\psi\rangle = \cos\alpha\,|0\rangle + \sin\alpha\,|1\rangle\,.$$

2.2 Измерения

Именно процедура измерений квантовых состояний отличает квантовый случай проведения опытов от классического и дает возможность применения квантовой криптографии. Важднейшим отличием квантовой механики от классической является то, что в общем случае *измерение квантовой системы меняет её исходное состояние*

2.2.1 Квантовые наблюдаемые

В любом экмперименте можно выделить две его стадии: приготовление состояния ρ и его измерение M. Измерение не обязано давать точно предсказуемый результат, в общем случае результат измерения — это статистический набор исходов $\{x\}$ с ссответствующими вероятностями $\mu_\rho(x)$. Естесственно требовать, чтобы для статистических ансамблей квантовых состояний результаты их наблюдения также были бы статистическими смесями результатов наблюдения соответствующих отдельных состояний ансамбля. Такое требование называется требованием аффинности:

$$\mu_\rho(x) = \sum_i p_i \mu_{\rho_i}(x), \rho = \sum_i p_i \rho_i.$$

Этого требования достаточно для следующего утверждения [3].

Теорема 2. *Пусть $\rho \to \mu_\rho$ — аффинное отображение множества квантовых состояний в вероятностные распределения на конечном множестве X. Тогда существует семейство эрмитовых операторов $\{M_x\}$ такое, что*

$$M_x \geq 0, \sum_{x \in X} M_x = I, \mu_\rho(x) = \operatorname{Tr} \rho M_x$$

Эта теорема говорит о том, что измерение квантовой системы можно связать с набором положительных эрмитовых операторов, сумма которых равна единичному оператору. В этом случае вероятность каждого из исходов равно следу произведения состояния и оператора, соответствующего данному исходу. Это приводит к определению квантовой наблюдаемой.

Определение 1. *Квантовая наблюдаемая со значениями из множества X — набор эрмитовых операторов $\{M_x\}_{x \in X}$ таких, что*

$$M_x \geq 0, \sum_{x \in X} M_x = I.$$

Такой набор операторов называют разложением единицы.

Из теоремы следует, что при измерении состояния ρ, описываемом разложением единицы $\{M_x\}$, вероятность получить каждый из исходов x равна

$$\Pr(x|\rho) = \operatorname{Tr} M_x \rho,$$

а для чистого состояния $|\psi\rangle$ в силу свойст следа эта вероятность выражается более просто:

$$\Pr(x|\rho_\psi) = \langle\psi| M_x |\psi\rangle .$$

2.2.2 Коллапс волновой функции

Важным законом квантовой механики является коллапс волновой функции, или редукция. Это свойство означает переход состояния послед измерения в одно из собственных состояний оператора измерения. Так, при измерении $\{M_i\}$ и получении результата i исходное состояние будет преобразовано в

$$\rho'_i = \frac{\sqrt{(M_i)}\rho\sqrt{(M_i)}}{\operatorname{Tr} M_i \rho}.$$

Это одно из важнейших для квантовой криптографии свойств, поскольку оно говорит о том, что попытки измерить систему ведут к помехам. Из этого следует, что попытки перехвата информации всегда можно детектировать по ошибкам на приёмной стороне.

2.2.3 Невозможность достоверного различения неортогональных состояний

Невозможность достоверного различения неортогональных квантовых состояний [4] — важный результат, на котором также во многом основывается секретность протоколов квантовой криптографии.

Этот результат можно сформулировать следующим образом: для чистых состояний $|\psi_0\rangle$ и $|\psi_1\rangle$ таких, что $\langle\psi_0|\psi_1\rangle = \cos\alpha \neq 0$, не существует измерения $\{M_0, M_1\}$, которое давало бы точный результат, то есть соответствовало бы условиям

$$\begin{aligned} \langle\psi_0| M_0 |\psi_0\rangle = 1, \quad \langle\psi_1| M_0 |\psi_1\rangle = 0, \\ \langle\psi_0| M_1 |\psi_0\rangle = 0, \quad \langle\psi_1| M_1 |\psi_1\rangle = 1. \end{aligned} \tag{1}$$

Докажем это утверждение. Допустим, такое измерение существует. Рассмотрим представление $|\psi_1\rangle$ как линейной комбинации состояния $|\psi_0\rangle$ и его норированного ортогонального дополнения $\left|\psi_0^\perp\right\rangle$:

$$|\psi_1\rangle = a\,|\psi_0\rangle + b\left|\psi_0^\perp\right\rangle, \quad |a^2| + |b^2| = 1.$$

Так как $|\psi_0\rangle$ и $|\psi_1\rangle$ неортогональны, то $0 < |a| < 1,\ 0 < |b| < 1$. Из условий на операторы очевидно следует, что $\sqrt{M_1}\,|\psi_0\rangle = 0$, а значит,

$$\sqrt{M_1}\,|\psi_1\rangle = \sqrt{M_1}a\,|\psi_0\rangle + \sqrt{M_1}b\left|\psi_0^\perp\right\rangle = \sqrt{M_1}b\left|\psi_0^\perp\right\rangle,$$

из чего следует, что равенство в (1) можно записать как

$$\langle\psi_1|\,M_1\,|\psi_1\rangle = |b^2|\left\langle\psi_0^\perp\right|M_1\left|\psi_0^\perp\right\rangle \le |b^2|,$$

что противоречит (1) в силу $|b| < 1$. Полученное противоречие доказывает невозможность различения неортогональных состояний.

2.2.4 Четкие и нечеткие наблюдаемые

Обычно под наблюдаемой подразумевают только ортогональное разложение единицы. Такие наблюдаемые будем называть *четкими наблюдаемыми* [3]. В то же время требование взамной ортогональности всех операторов не является обязательным, а в некоторых случая выгоднее пользоваться наблюдаемыми, в которых не все операторы ортогональны друг другу, в целях получения максимального количества информации. Такие наблюдаемые называются нечеткими.

На первый взгляд нечеткие наблюдаемые просто смешивают вероятности разных исходов и не могут принести дополнительной пользы. Однако это не так. Рассмотрим пример, как нечеткая наблюдаемая может помочь различить неортогональные состояния $|\phi\rangle$ и $|\psi\rangle$:

$$\langle\phi|\psi\rangle = \cos\eta.$$

Одно из возможных измерений для такой пары состояний принято называть «измерение с тремя исходами», и оно использует три результата: $\{0, 1, ?\}$. Соответствующие эрмитовы операторы равны

$$\begin{aligned} M_0 &= \frac{\left|\psi^\perp\right\rangle\left\langle\psi^\perp\right|}{1+\cos\eta} = \frac{I - |\psi\rangle\langle\psi|}{1+\cos\eta}, \\ M_1 &= \frac{\left|\phi^\perp\right\rangle\left\langle\phi^\perp\right|}{1+\cos\eta} = \frac{I - |\phi\rangle\langle\phi|}{1+\cos\eta}, \\ M_? &= I - M_0 - M_1. \end{aligned} \tag{2}$$

Несложно обнаружить, что

$$\operatorname{Tr} M_0\,|\psi\rangle\langle\psi| = \langle\psi|\,M_0\,|\psi\rangle = \frac{\left\langle\psi|\psi^\perp\right\rangle\left\langle\psi^\perp|\psi\right\rangle}{1+\cos\eta} = 0,$$

и аналогично $\operatorname{Tr} M_1\,|\phi\rangle\langle\phi| = 0$. Это значит, что при применении такого измерения нет шансов получить исход 0 при измерении состояния $|\phi\rangle$, а при измерении состояния $|\psi\rangle$ не может получиться исход 1. Это значит, что такое измерение позволяет различать неортогональные состояния без ошибок. Цена этого — некоторая вероятность (равная $\cos\eta$) получить несовместный исход «?», который соответствует уклонению от ответа.

2.3 Составные квантовые системы

Рассмотрение квантовых систем из нескольких частиц может привести к интересным свойствам, которые не встречаются в классическом случае. Еще в переписке Эйнштейна, Подольского и Розена [5] были отмечены необычные свойства составных квантовых систем, которые противоречили локальности: получалось, что действия над одной подсистемой могут мгновенно оказывать влияние на другую подсистему вне зависимости от расстояния между ними.

2.3.1 Тензорное произведение

Для начала определим, в каком пространстве находятся составные квантовые системы.

Рассмотрим наиболее простой случай двух кубитов. Интуитивно понятно, что возможны 4 варианта их совместного состояния:

- оба кубита в состоянии $|0\rangle$;
- первый кубит в состоянии $|0\rangle$, второй – в состоянии $|1\rangle$;
- первый кубит в состоянии $|1\rangle$, второй – в состоянии $|0\rangle$;
- оба кубита в состоянии $|1\rangle$.

Именно эти четыре вектора и будут являться базисными в пространстве двух кубитов.

Формально это описывается следующим образом. Если есть пространства $\mathcal{H}_1$ и $\mathcal{H}_2$ с размерностями d_1 и d_2 и ортонормированными базисами $\{e_i\}$ и $\{f_i\}$, то можно определить пространство с базисом $\{e_i \otimes f_j\}$, $i = \overline{1, d_1}$, $j = \overline{1, d_2}$. Если ввести на этом пространстве скалярное произведение

$$\langle e_i \otimes f_j | e_m \otimes f_n \rangle = \langle e_i | e_m \rangle \cdot \langle f_j | f_n \rangle$$

и продолжить его по линейности на остальные векторы, то в результате получим гильбертово пространство, называемое тензорным произведением $\mathcal{H}_1$ и $\mathcal{H}_2$, обозначаемое $\mathcal{H}_1 \otimes \mathcal{H}_2$.

Тензорное произведение операторов $A_1 \in \mathcal{S}(\mathcal{H}_1)$ и $A_2 \in \mathcal{S}(\mathcal{H}_2)$ — оператор $A_1 \otimes A_2$ в пространстве $\mathcal{H}_1 \otimes \mathcal{H}_2$, который действует по закону

$$(A_1 \otimes A_2) |e_1 \otimes e_2\rangle = (A_1 |e_1\rangle) \otimes (A_2 |e_2\rangle).$$

Встает вопрос о том, всякое ли состояние в пространстве $\mathcal{H}_1 \otimes \mathcal{H}_2$ можно задать как тензорное произведение состояний из частичных пространств $\mathcal{H}_1$ и $\mathcal{H}_2$. Ответ на него отрицателен. Классическим контрпримером является состояние в пространстве двух кубитов, называемое ЭПР:

$$|\psi_{EPR}\rangle = \frac{|00\rangle + |11\rangle}{\sqrt{2}}.$$

Легко видеть, что это состояние невозможно представить в виде тензорного произведения одночастичных состояний:

$$|\psi_{EPR}\rangle \neq (a_1 |0\rangle + b_1 |1\rangle) \otimes (a_2 |0\rangle + b_2 |1\rangle).$$

2.3.2 Частичный оператор плотности и частичные измерения

После определения тензорного произведения операторов плотности возникает необходимость определить обратную операцию, с помощью которой можно было бы по состоянию

$\rho_1 \otimes \rho_2 \in \mathcal{H}_1 \otimes \mathcal{H}_2$ получить исходные операторы $\rho_1 \in \mathcal{H}_1$ и $\rho_2 \in \mathcal{H}_2$. Такая операция называется взятием частичного следа и определяется следующим образом:

$$\mathrm{Tr}_{\mathcal{H}_2} \rho_{12} = \sum_{i,j,k} |e_i\rangle \langle e_j| \langle e_i \otimes f_k| \rho_{12} |e_j \otimes f_k\rangle .$$

Аналогично для частичного следа по первому подпространству:

$$\mathrm{Tr}_{\mathcal{H}_1} \rho_{12} = \sum_{i,j,k} |f_i\rangle \langle f_j| \langle e_k \otimes f_i| \rho_{12} |e_k \otimes f_j\rangle .$$

По определению этой операции видно, что:

$$\mathrm{Tr}_{\mathcal{H}_2} \rho_1 \otimes \rho_2 = \rho_1,$$

$$\mathrm{Tr}_{\mathcal{H}_1} \rho_1 \otimes \rho_2 = \rho_2.$$

Рассмотрим теперь ситуацию, когда квантовое состояние распределено между двумя участниками, один из которых производит измерение над своей подсистемой. Такое действие называют частичным измерением.

При измерении одной подсистемы над второй не производится активных действий, поэтому в разложении единицы, описывающем общее измерение, все операторы, соответствующие второй подсистеме, будут тождественными. Например, если перый участник применяет измерение $\{\langle 0| |0\rangle , \langle 1| |1\rangle\}$, то в составной системе это измерение будет выглядеть так:

$$M_0 = |0\rangle \langle 0|_1 \otimes I_2, \qquad M_1 = |1\rangle \langle 1|_1 \otimes I_2.$$

Стоит заметить, что несмотря на тождественные операторы в правой части, измерение первой подсистемы в общем случае влияет на состояние второй подсистемы.

2.3.3 Квантовая запутанность

Квантовая запутанность — квантовомеханическое явление, при котором квантовые состояния двух или большего числа объектов оказываются взаимозависимыми. Такая взаимозависимость сохраняется, даже если эти объекты разнесены в пространстве за пределы любых известных взаимодействий, что находится в логическом противоречии с принципом локальности. Например, можно получить пару фотонов, находящихся в запутанном состоянии, и тогда если при измерении спина первой частицы спиральность оказывается положительной, то спиральность второй всегда оказывается отрицательной, и наоборот.

Рассмотрим состояние ЭПР в пространстве двух кубитов

$$|\psi_{EPR}\rangle = \frac{|00\rangle + |11\rangle}{\sqrt{2}}$$

и посмотрим, что будет, если провести измерение над первой подсистемой. При выпадении исхода 0 начальное состояние перейдет в

$$\frac{\sqrt{M_0} |\psi_{EPR}\rangle \langle \psi_{EPR}| \sqrt{M_0}}{\langle \psi_{EPR}| M_0 |\psi_{EPR}\rangle} = |00\rangle \langle 00| ,$$

что соответствует чистому состоянию $|00\rangle$. Аналогично при исходе 1 начальное состояние перейдет в $|11\rangle$. Это говорит об удивительном факте: измерение одной части квантового состояния может изменять все состояние в целом.

Это свойство имеет место не для произвольных квантовых состояний, а только для запутанных. Запутанные состояния определяются как состояния в составном пространстве, которые нельзя представить в виде тензорного произведения состояний в каждом из частичных пространств.

Для состояний, которые не являются запутанными, подобное свойство не имеет места: измерение одной подсистемы никак не влияет на состояние второй.

2.3.4 Невозможность клонирования квантовых состояний

В квантовой криптографии важен еще один результат из теории составных квантовых систем. Выше было показано, что неортогональные квантовые состояния нельзя достоверно различить. Здесь будет показано, что такие состояния нельзя и клонировать [6] — например, чтобы собрать более полную статистику результатов измерений.

Преобразование U, клонирующее произвольное чистое состояние $|\psi\rangle$, можно описать так:

$$U\,|\psi\rangle \otimes |A\rangle = |\psi\rangle \otimes |\psi\rangle\,,$$

где $|A\rangle$ — исходное состояние вспомогательной системы.

Чтобы показать невозможность такого преобразования, достаточно рассмотреть его действие на базисные состояния $|0\rangle$ и $|1\rangle$:

$$\begin{aligned} U\,|0\rangle \otimes |A\rangle &= |0\rangle \otimes |0\rangle\,, \\ U\,|1\rangle \otimes |A\rangle &= |1\rangle \otimes |1\rangle\,, \end{aligned} \tag{3}$$

а также на состояние $\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$. В силу линейности оператора U и соотношений 3 должно выполняться

$$U(\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \otimes |A\rangle) = \frac{1}{\sqrt{2}}(|0\rangle \otimes |0\rangle + |1\rangle \otimes |1\rangle).$$

С другой стороны, по определению U должно получаться

$$U(\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \otimes |A\rangle) = \frac{1}{2}(|0\rangle + |1\rangle) \otimes (|0\rangle + |1\rangle).$$

Полученное противоречие доказывает невозможность клонирования произвольных квантовых состояний. Стоит отметить, что клонировать состояния из ортогонального набора можно: для этого достаточно их измерить и приготовить состояние, соответствующее результату измерения.

3 Базовые протоколы квантового распределения ключей

К 1984 году основная часть описанных результатов уже была известна, и их оказалось достаточно для того, чтобы сформулировать принципы квантовой криптографии и предоставить доводы в пользу секретности такого способа распределения ключей.

Основные факты квантовой теории информации, на которых основывается квантовая криптография — связанные между собой утверждения о невозможности клонирования произвольных квантовых состояний и о невозможности достоверного различения неортогональных состояний. В сочетании эти результаты дают тот факт, что попытки различения квантовых состояний из неортогонального набора ведут к помехам, а значит, действия перехватчика могут быть детектированы по величине ошибки на приемной стороне.

Важно заметить, что квантовая криптография не делает никаких предположений о характере действий подслушивателя и объеме доступных ему ресурсов: предполагается, что перехватчик может обладать любыми ресурсами и делать все возможные действия в рамках известных на сегодняшний день законов природы. Это существенно отличает квантовую криптографию от классической, которая опирается на ограничения в вычислительной мощности подслушивателя.

3.1 Протокол BB84

Неформально принцип действия всех протоколов квантовой криптографии можно описать следующим образом. Передающая сторона (Алиса) на каждом шаге посылает одно из состояний из неортогонального набора, а принимающая сторона (Боб) производит такое измерение, что после дополнительного обмена классической информацией между сторонами они должны иметь битовые строки, полностью совпадающие в случае идеального канала и отсутствия перехватчика. Ошибки в этих строках могут говорить как о неидеальности канала, так и о действиях подслушивателя. При величине ошибки, превышающей некоторый предел, действие протокола прерывается, иначе же легитимные пользователи могут извлечь полностью секртеный ключ из этих частично совпадающих битовых строк.

3.1.1 Общая схема протокола

Протокол BB84 [7] использует два базиса:

$$\begin{aligned} + : \left|0^{+}\right\rangle = |0\rangle\,, \quad \left|1^{+}\right\rangle = |1\rangle\,, \\ \times : \left|0^{\times}\right\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle), \quad \left|1^{\times}\right\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle). \end{aligned} \tag{4}$$

На этапе приготовления состояний Алиса случайным образом выбирает один из указанных базисов, а затем случайно выбирает значение бита: 0 или 1, и в соответствии с этим выбором посылает один из четырех сигналов. При посылке каждого из этих сигналов Алиса запоминает свой выбор базиса и выбор бита, что приводит к появлению на ее стороне двух случайных битовых строк.

Боб, получая каждый из присланных Алисой сигналов, производит над ним одно из двух измерений случайным образом. Каждое из них способно дать достоверный резлуьтат из-за ортогональности состояний внутри каждого базиса:

$$\begin{aligned} M_0^{+} = \left|0^{+}\right\rangle\left\langle 0^{+}\right|, \qquad M_1^{+} = \left|1^{+}\right\rangle\left\langle 1^{+}\right|, \\ M_0^{\times} = \left|0^{\times}\right\rangle\left\langle 0^{\times}\right|, \qquad M_1^{\times} = \left|1^{\times}\right\rangle\left\langle 1^{\times}\right|. \end{aligned} \tag{5}$$

В результате он получает две строки: с выбором базисов и с исходами этих измерений.

Итак, после передачи всех состояний и проведения измерений Алиса и Боб имеют по две строки каждый. Теперь происходит согласование базисов: по открытому каналу Алиса и Боб объявляют друг другу свои строки с выбором базисов. Те посылки, в которых базисы не совпали, выбрасываются. Если базис Алисы совпал с базисом Боба, то в случае отсутствия помех в канале связи результаты в их битовых строках на соответствующей позиции также будут совпадать, поэтому после этапа согласования в случае идеального канала и отсутствия действий со стороны перехватчика Алиса и Боб обладают одними и теми же битовыми строками.

Но если в канале были ошибки или перехватчик пытался подслушать информацию, битовые строки Алисы и Боба могут не совпадать, поэтому для проверки они должны согласованно раскрыть примерно половины своих битовых строк. Согласно центральной предельной теореме, ошибка в раскрытой битовой последовательности дает достаточно точную оценку ошибки во всей последовательности, и по ней можно достаточно точно оценить вероятность ошибки в оставшихся позициях. Если величина ошибки оказывается больше некоторой величины (параметра протокола), передача данных прекращается: это означает, что перехватчик обладает слишком большой информацией о ключе. В противном случае перед Алисов и Бобом стоит задача получения общего секретного ключа, которую можно разбить на два этапа: сначала производится коррекция ошибок [8], после чего у Алисы и Боба оказываются совпадающие битовые строки; затем происходит усиление секретности [9], которое ставит своей

целью исключить информацию о ключе, которая могла попасть к перехватчику в результате действий над состояниями или в ходе коррекции ошибок. В конечном итоге у перехватчика не должно остаться информации об общей битовой строке Алисы и Боба.

3.1.2 Стойкость протокола

При предложении протокола BB84 его стойкость была показана только на интуитивном уровне: попытка Евы измерить передаваемые состояния влечет к их разрушению, что приводит к ошибкам на приемной стороне. Однако только измерениями посылаемых сигналов действия Евы не ограничиваются. Более того, непросто рассчитать информацию, способную попасть к Еве при всех возможных действиях с ее стороны. Однако оказалось, что можно доказать стойкость протокола BB84, не прибегаю к оценкам информационных величин для всех возможных атак Евы. В 2000 году было показано [10], что секретность квантовой криптографии можно свести к свойствам квантовых кодов коррекции ошибок: если ошибки, возникающие в квантовом канале связи, можно достоверно исправить, то можно добиться и секретной передачи данных. Это дает критическую величину ошибки, до которой возможно секретное распределение ключей.

Доказательство стойкости протокола проще всего провести, введя несколько дополнительных протоколов. Так, стойкость введенного первым ЭПР-протокола [11] легко вытекает из теории квантовых измерений, а последовательным изменением некоторых действий легитимных пользователей он может быть сведен к более строго описанному протоколу BB84 без нарушения исходной секретности [12, 13].

Схема протокола, рассмотренная в [13], незначительно отличающаяся от описанной выше, использует для коррекции ошибок и усиления секретности свойства CSS-кодов, который не являются оптимальными. Теоретическая оценка на величину ошибки q, которую можно исправить в квантовом канале, дается границей Шеннона: $1 - 2h(q) > 0$. Достижение этой границы сводится к использованию случайных классических кодов. Теоретический предел ошибки, до которой возможно секретное распределение информации, равен примерно 11%, а именно корню уравнения $1 - 2h(q) = 0$.

3.1.3 Стратегии подслушивателя

Итак, утверждается, что при величине ошибки на приемной стороне менее 11% возможна секретная передача данных. В то же время не говорится о том, каким образом протокол теряет секретность при большей величине ошибки. В этом разделе рассмотрены некоторые схемы атаки, на одной из которых достигается теоретический предел ошибки на приемной стороне.

3.1.3.1 Прием-перепосыл

Наиболее простой сценарий действий Евы — измерение передаваемого по квантовому каналу состояния с дальнейшим пересылом получившегося результата дальше. Именно таким образом прослушиваются классические каналы. В квантовом случае такая стратегия не работает.

Если Ева стремится произвести те же действия, что производит у себя Боб, то, не знаю исходного состояния, она сталкивается с нерешаемой проблемой различения состояний из неортогонального набора. Применяя случайным образом одно из измерений

$$\begin{aligned} + : M_0^+ = \left|0^+\right\rangle \left\langle 0^+\right|, \quad M_1^+ = \left|1^+\right\rangle \left\langle 1^+\right|, \\ \times : M_0^\times = \left|0^\times\right\rangle \left\langle 0^\times\right|, \quad M_1^\times = \left|1^\times\right\rangle \left\langle 1^\times\right| \end{aligned} \tag{6}$$

к посланному состоянию, в половине случаев Ева будет неверно укадывать базис. В силу свойства несмещенности базисных состояний при неверно угаданном базисе вероятность ошибки евы состоавляет 50%, то есть Ева не получает полезной информации о сигнале.

Но это не все проблемы Евы. Неверно угаданный базис при проведении измерения вследствие коллапса волновой функции неизбежно приведет к тому, что Бобу будет послано ошибочное состояние. При применении измерения "$+$" вне зависимости от исходного состояния дальше будет послано одно из состояний набора $\{|0^+\rangle, |1^+\rangle\}$, аналогично с диагональным базисом "$\times$". Измеряя эти состояния в «верном» для них базисе, Боб получит ошибку, по которой действия Евы будут обнаружены.

Величину ошибки на приемной стороне можно вычислить так. Допустим, Ева подвергала атаке не все состояния, а только их часть, атакуя каждый сигнал с вероятностью p. Тогда доля $1-p$ сигналов приходит к Бобу без ошибки (а Еве приходится просто угадывать значение бита в таких посылках, что вносит в ее ошибку вклад, равный $(1-p)/2$). Для посылок, атакованных Евой, существует два равновероятных развития событий:

- Ева верно угадала базис, значит, точно получила информацию и не внесла возмущения.
- Ева ошиблась в выборе базиса. Тогда с вероятностью $1/2$ она получила ошибочный результат. Кроме того, совершенно точно она передала ошибочное состояние Бобу, что приводит к появлению ошибки на его стороне, вероятность которой также равна $1/2$.

Вероятность каждого из этих сценариев равна $p/2$, и нетрудно видеть, что доля ошибок на приемной стороне будет равна $p/4$, а доля ошибок у Евы составит

$$\frac{1}{2} - \frac{p}{4}.$$

Это значит, что при всех значениях параметра p, меньших единицы, Ева имеет больше ошибок, чем Боб, и тогда ее информация о ключе строго меньше. При $p = 1$ доли ошибок у Боба и Евы совпадают и равны 25%. Так как ошибка Боба однозначно связана с параметром p, то 25% — пороговая величина ошибки для такой атаки, до которой возможно секретное распределение ключей.

3.1.3.2 Коллективная атака

Критическая ошибка индивидуального подслушивания, равная 25% превосходит теоретический порог в 11%. Возникает вопрос, как Еве нужно изменить схему атаки, чтобы добиться лучших результатов? Оказывается, что слабая сторона индивидуальной атаки — в проведении измерений над каждым передаваемым состоянием по отдельности. Из свойства супераддитивности классически-квантового канала [3] следует, что выгоднее проводить измерение над всей последовательностью полученных состояний сразу. В [14] показано, что критическая ошибка Q_c для коллективной атаки равна корню уравнения $1 - h(Q_c) = h(Q_c)$, что совпадает с полученным выше теоретическим пределом.

3.2 Протокол B92

Протокол BB84 является первым и наиболее изученным протоколом квантовой криптографии. Однако попытки его техничесокй реализации столкнулись с рядом технических трудностей (о них ниже), в результате чего Ева может провести перехват информации, невозможный при строгой реализации всех принципов протокола BB84. Появилась необходимость разработки протоколов, способдных противостоять Еве и на современном уровне развития технологий.

В протоколе BB84 при отсутствии действий перехватчика и помех в канале вероятность ошибки на приемной стороне до согласования базисов составляет 25%. Это вызвано использованием строго зафиксированной конфигурации двух пар базисных векторов. Цель протокола B92 [4] состоит в возможности изменения этого параметра в зависимости от, например, длины канала или его качества. В ряде случаев это позволяет добиться большей скорости передачи данных.

На каждом шаге протокола B92 Алиса посылает Бобу одно из двух неортогональных состояний $|\psi_0\rangle$, $|\psi_1\rangle$, где $\langle\psi_0|\psi_1\rangle = \cos\eta$ — основной параметр протокола. На стороне Боба производится измерение с тремя исходами

$$\begin{aligned} M_0 &= \frac{I - |\psi_1\rangle\langle\psi_1|}{1+\cos\eta}, \\ M_1 &= \frac{I - |\psi_0\rangle\langle\psi_0|}{1+\cos\eta}, \\ M_? &= I - M_0 - M_1. \end{aligned} \tag{7}$$

Посылки, в которых был получен несовместный исход, отбрасываются.

После передачи всех сообщений Алиса и Боб, так же как в BB84, согласованно раскрывают часть своих битовых последовательностей и оценивают число ошибок. Если их оказалось больше некоторой величины, выполнение протокола прерывается, иначе из оставшейся части можно получить полностью секретный ключ. Стойкость протокола относительно наиболее эффективной атаки Евы (коллективной) была исследована в [15].

3.3 Проблемы практических реализаций

Несмотря на заявления о теоретической секретности указанных протоколов, на практике возникают различные трудности. Первая из них — в настоящее время не существует строго однофотонного источника. Современные лазеры выдают так называемые когерентные состояния:

$$|\alpha\rangle = e^{-\frac{\mu}{2}} \sum_{n=0}^{\infty} \frac{\alpha^n}{\sqrt{n!}} |n\rangle = e^{-\frac{\mu}{2}} (|0\rangle + \alpha\,|1\rangle + \frac{\alpha^2}{2}\,|2\rangle + \cdots),$$

где $\mu = |\alpha|^2$ — среднее число фотонов, $|0\rangle \equiv |vac\rangle$ — вакуумное состояние с числом фотонов 0. Значение параметра μ находится в районе 0.1-0.2, что дает вероятность вакуумного состояния примерно 0.9, вероятность, что в посылке будет ровно один фотон –0.09, ровно два фотона — 0.009 и т. д.

Проблема неоднофотонных источников дополняется второй — помехи и потери в квантовом канале связи. Эти два фактора дают возможность провести атаку с расщеплением фотонов [16]. Вкратце, Ева может определить число фотонов в посылке. Если их более одного, то она отщепляет себе один фотон, а оставшуюся часть отправляет Бобу. Если фотон в посылке ровно один, эта посылка блокируется и Бобу ничего не посылается, таким образом имитируется потеря посылки из-за плохого качества канала. После передачи всех состояний у Евы будут храниться фотоны на каждую из принятых Бобом посылок. После раскрытия базисов она проводит соответствующие измерения и полностью знает секретный ключ, не вызвав при этом никаких ошибок на приемной стороне.

Однако, даже если в распоряжении Алисы имеется строго однофотонный источник, то при наличии потерь в канале Ева все равно может узнать [17] секретный ключ и остаться незамеченной следующим образом. Над каждой посылкой проводится измерение с тремя исходами. Если был получен совместный результат, Ева точно знает, какое состояние приготовила Алиса, поэтому может приготовить такое же и послать его Бобу. В случае несовместного результата посылка блокируется. Такая стратегия не производит никаких ошибок на приемной стороне.

3.4 Релятивистское квантовое распределение ключей

Возникает принципиальный вопрос: существуют ли такие протоколы квантового распределения ключей, которые обеспечивают безусловную секретность при не строго однофотонном источнике и произвольных потерях в канале связи? Ответ на этот вопрос: да, существуют. Но для их построения недостаточно опираться исключительно на законы квантовой механики, как это делают все базовые протоколы (BB84 [7], B92 [4], SARG04 [18]. decoy-state [19], phase-time coding [20]).

Все эти протоколы не используют тот факт, что фотоны движутся с предельно возможной скоростью света. В релятивитской схеме квантового распределения ключей всё взаимодействие происходит в пространстве-времени Минковского, и существенно используется ограничение специальной теории относительности на невозможность движения со скоростями больше скорости света. Основная идея релятивистской схемы состоит в том, чтобы «растянуть» информацию и в пространстве, и во времени. Для того, чтобы Ева смогла получить эту информацию, ей придется собрать все части вместе, так как по отдельности они абсолютно бесполезны. Для такого сбора потребуется некоторое время. После получения данных эту информацию потребуется снова разнести в пространстве-времени, на что так же потребуется время. В итоге Ева будет вызывать детектируемые задержки.

Учет фундаментальных ограничений, накладываемых специальной теорией относительности, приводит к тому, что возможна передача секретных ключей на любые расстояния через открытое пространство даже при не строго однофотонном источнике и любых потерях в канале связи.

Список литературы

1. Vernam G. Cipher printing telegraph system for secret wire and radio telegraphic communications // Journal of American Institute of Electrical Engineers. 1926. Т. 45. С. 109–115.
2. Nielsen Michael A, Chuang Isaac L. Quantum computation and quantum information. Cambridge university press, 2010.
3. А.С. Холево. Квантовые системы, каналы, информация. МЦНМО, 2010.
4. Bennett Charles H. Quantum cryptography using any two nonorthogonal states // Physical Review Letters. 1992. Т. 68, № 21. С. 3121.
5. Einstein A., Podolsky B., Rosen N. Can Quantum-Mechanical Description of Physical Reality Be Considered Complete? // Phys. Rev. 1935. Т. 47, № 10. С. 777–780.
6. Wootters W. K., Zurek W. H. A single quantum cannot be cloned // Nature. 1982. oct. Т. 299, № 5886. С. 802–803.
7. Bennett Charles H, Brassard Gilles [и др.]. Quantum cryptography: Public key distribution and coin tossing // Proceedings of IEEE International Conference on Computers, Systems and Signal Processing / New York. Т. 175. 1984. С. 8.
8. Brassard Gilles, Salvail Louis. Secret-Key Reconciliation by Public Discussion. // EUROCRYPT / под ред. Tor Helleseth. Т. 765 из *Lecture Notes in Computer Science*. Springer, 1993. С. 410–423.
9. Generalized privacy amplification. / Charles H. Bennett, Gilles Brassard, Claude Crépeau [и др.] // IEEE Transactions on Information Theory. 1995. Т. 41, № 6. С. 1915–1923.
10. Shor Peter W, Preskill John. Simple proof of security of the BB84 quantum key distribution protocol // Physical Review Letters. 2000. Т. 85, № 2. С. 441.
11. Ekert Artur K. Quantum cryptography based on Bell's theorem // Physical review letters. 1991. Т. 67, № 6. С. 661–663.
12. Lo Hoi-Kwong, Chau H. F., Ardehali M. Efficient Quantum Key Distribution Scheme and a Proof of Its Unconditional Security. // J. Cryptology. 2005. Т. 18, № 2. С. 133–165.
13. Baigneres Thomas. Quantum Cryptography: On the Security of the BB84 Key-Exchange Protocol: Tech. Rep.: : 2003.
14. Molotkov SN, Timofeev AV. Explicit attack on the key in quantum cryptography (BB84 protocol) reaching the theoretical error limit Q c 11% // JETP Letters. 2007. Т. 85, № 10. С. 524–529.
15. Molotkov S.N. On a collective attack on the key in quantum cryptography on two nonorthogonal states // Journal of Experimental and Theoretical Physics Letters. 2004. Т. 80, № 8. С. 563–567.
16. Acín Antonio, Gisin Nicolas, Scarani Valerio. Coherent-pulse implementations of quantum cryptography protocols resistant to photon-number-splitting attacks // Physical Review A. 2004. Т. 69, № 1. С. 012309.
17. Dusek Miloslav, Jahma Mika, Lütkenhaus Norbert. Unambiguous state discrimination in quantum cryptography with weak coherent states. 2000. С. Physical Review A.

18. Quantum cryptography protocols robust against photon number splitting attacks for weak laser pulses implementations / Valerio Scarani, Antonio Acin, Gregoire Ribordy [и др.] // Phys. Rev. Lett. 2004. Т. 92. С. 057901.

19. Hwang W. Y. Quantum Key Distribution with High Loss: Toward Global Secure Communication // Phys. Rev. Lett. 2003. August. Т. 91, № 5. С. 057901.

20. Kronberg DA, Molotkov SN. Security of a two-parameter quantum cryptography system using time-shifted states against photon-number splitting attacks // Journal of Experimental and Theoretical Physics. 2009. Т. 109, № 4. С. 557–584.