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

Моделирование релятивистской системы квантового распределения ключей

Дипломная работа

Студент 523 группы
Большаков Роман

Научный руководитель
профессор Молотков С.Н.

Москва
2015

Оглавление

Введение

Квантовое распределение ключей (QKD) — концепт секретного распределения ключей, основанный на фундаментальных законах квантовой механики. Квантовая криптография [**?**, **?**, 1–4] приобрела популярность за обещание абсолютной секретности против подслушивания. «Абсолютной» понимается в том смысле, что секретность гарантирована фундаментальными запретами квантовой механики (на копирование неизвестного квантового состояния и невозможности достоверной различимости неортогональных квантовых состояний) [**?**,**?**,**?**,5], а не нашими технологическими возможностями. Достоверная неразличимость неортогональных квантовых состояний приводит к тому, что любые попытки вторжения в канал связи с целью получения информации о передаваемых состояниях вызывают их неизбежное возмущение, что ведет к ошибкам на приемной стороне и детектированию подслушивателя. Если ошибка на приемной стороне не превосходит некоторой критической величины[1], то ошибки могут быть исправлены через аутентичный открытый классический канал связи. В результате последующего сжатия (хеширования [**?**]) очищенного ключа возникает секретный ключ, известный только двум легитимным пользователям.

Однако, *практические* схемы реализации QKD — серьезный вызов для ученых, так как все реализации так или иначе отличаются от теоретических моделей. Две основные проблемы всех существующих реализаций, ни одна из которых не может быть эффективно устранена: *1*) любой существующий в настоящее время источник фотонов имеет ненулевую вероятность испустить два или более фотонов одновременно, в то время как в теории нужен ровно один [6, 7], и *2*) наличие потерь в квантовом канале связи.

[1] Величина критической ошибки определяется конкретным протоколом

В реальной ситуации неоднофотонность источника вместе с потерями в квантовом канале связи приводит к тому, что все базовые протоколы распредения ключей: BB84, B92, SARG04, decoy-state (с состояниями-ловушками), phase-time (фазово-временное кодирование) оказываются неустойчивыми относительно PNS атаки (атака с расщеплением по числу фотонов) и не гарантируют секретность ключей, если длина квантового канала связи превышает некоторую критическую величину.

Протоколы используются как в оптоволоконных системах квантовой криптографии, так и в системах, работающих через открытое пространство. Конечной целью работ по квантовой криптографии в открытом пространстве является создание глобальной системы распределения ключей на большие расстояния через низкоорбитальные спутники. При передаче ключей через открытое пространство могут быть использованы протоколы, стойкость которых базируется на запретах только квантовой механики, применяемые в оптоволоконных системах квантовой криптографии. Однако при не строго однофотонном источнике квантовых состояний и потерях в канале связи дальность передачи секретных ключей при помощи таких протоколов ограничена [2]. В принципе можно сформулировать протоколы, дальность которых не ограничена, но при этом неизбежно требуются априорное знание величины потерь и их контроль в канале связи. Если для оптоволоконных систем такой подход может оказаться достаточным, то для открытого пространства он неприемлем, поскольку априорно потери в канале связи неизвестны и могут меняться в течение передачи ключей. По-видимому, при неоднофотонном источнике и больших априорно не известных потерях, одних только фундаментальных запретов квантовой механики недостаточно для формулировки протоколов, гарантирующих секретность ключей.

Возникает принципиальный и практически важный вопрос о том, существуют ли протоколы квантового распределения ключей, которые обеспечивают безусловную секретность ключей при не строго однофотонном источнике и произвольных потерях в квантовом канале связи. Ниже будет предъявлен такой протокол. Данный протокол, кроме ограничений квантовой механики на различимость квантовых состояний, использует дополнительные ограничения, диктуемые специальной теорией относительности.

Глава 1

Основы квантового распределения ключей

1.1 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.

1.1.1 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 передаётся по незащищённому 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 надёжному 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.

1.1.2 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 [8]. Введем обозначения:
$\mathbb{M}$ — множество всевозможных открытых текстов M,

$\mathbb{C}$ — множество шифротекстов C,

$\mathbb{K}$ — множество ключей K.

На каждом из указанных множеств 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 (этим именем в дальнейшем будем называть злоумышленника, перехватчика, подслушивателя) 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 (этими именами будем называть легитимных пользователей протокола) 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* $E_k(m) = c$.

1.1.3 Криптосистема Вернама

Приведём 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 путём 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 перестаёт 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 надёжный 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.

1.2 Основные понятия квантовой теории информации

1.2.1 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, эту часть физики стали называть квантовой теорией, а сложившуюся на тот момент физическую картину мира — классической.

1.2.1.1 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 $\langle\phi|$ 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 $|\psi\rangle$.

1.2.1.2 Смешанные состояния

С помощью операторов плотности вводится общее понятие квантового состояния. *Смешанным квантовым состоянием* называется статистическая смесь нескольких чистых состояний:

$$\rho = \sum_i p_i |\psi_i\rangle\langle\psi_i|, \quad p_i \geq 0 \forall i, \quad \sum_i p_i = 1. \tag{1.1}$$

Очевидно, что след смешанного состояния равен единице. Также несложно показать его положительную определенность:

$$\langle\varphi|\rho|\varphi\rangle = \sum_i p_i |\langle\varphi|\psi_i\rangle|^2 \geq 0 \ \forall |\varphi\rangle \in \mathcal{H}. \tag{1.2}$$

Как известно, любой эрмитов оператор A имеет спектральное разложение

$$A = \sum_i \lambda_i |\lambda_i\rangle\langle\lambda_i|, \tag{1.3}$$

где собственные значения λ_i вещественны, а собственные векторы $|\lambda_i\rangle$ ортогональны и нормированны. Это означает, что любой положительный эрмитов оператор с единичным следом можно назвать оператором плотности некоторого квантового состояния: из положительной определенности (1.2) следует положительность всех собственных значений (которые

интерпретируются как вероятностные веса), а из условия единичного следа — то, что сумма собственных значений равна единице. В итоге это значит, что такая их комбинация может трактоваться как статистическая смесь, что приводит в общему определению квантового состояния.

Определение 1. *Квантовое состояние — положительный эрмитов оператор в гильбертовом пространстве с единичным следом.*

Квантовые состояния образуют выпуклое множество $\mathcal{S}(\mathcal{H})$ в пространстве операторов $\mathcal{H}$. Крайними точками этого множества являются чистые состояния, описывающиеся операторами ранга 1.

1.2.1.3 Изменение состояний во времени

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

$$i\hbar\frac{d\left|\psi\right\rangle}{dt} = H\left|\psi\right\rangle, \tag{1.4}$$

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 [9]:

$$U = e^{iH}, \tag{1.5}$$

то уравнение (1.4) может быть переписано следующим образом:

$$\left|\psi'\right\rangle = U\left|\psi\right\rangle. \tag{1.6}$$

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

1.2.1.4 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.

1.2.1.5 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

$$|\psi\rangle = \cos\alpha\,|0\rangle + \sin\alpha\,|1\rangle\,. \tag{1.7}$$

1.2.2 Измерения

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

1.2.2.1 Квантовые наблюдаемые

В любом эксперименте 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 соответствующими вероятностями $\mu_\rho(x)$. Естественно 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:

$$\mu_\rho(x) = \sum_i p_i \mu_{\rho_i}(x), \quad \rho = \sum_i p_i \rho_i, \tag{1.8}$$

где p_i — вероятности, с которыми каждое состояние входит в ансамбль состояний. Этого требования достаточно для следующего утверждения [10].

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*

$$M_x \geq 0, \quad \sum_{x \in X} M_x = I, \quad \mu_\rho(x) = \operatorname{Tr} \rho M_x. \tag{1.9}$$

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 равна следу произведения состояния и оператора, соответствующего данному исходу. Это приводит к определению квантовой наблюдаемой.

Определение 2. *Квантовая наблюдаемая со значениями из множества X — набор эрмитовых операторов $\{M_x\}_{x \in X}$ таких, что*

$$M_x \geq 0, \quad \sum_{x \in X} M_x = I. \tag{1.10}$$

Такой набор операторов называют разложением единицы.

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

$$\Pr(x|\rho) = \operatorname{Tr} M_x \rho, \tag{1.11}$$

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

$$\Pr(x|\rho_\psi) = \langle\psi| M_x |\psi\rangle . \tag{1.12}$$

1.2.2.2 Коллапс волновой функции

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

$$\rho'_i = \frac{\sqrt{M_i}\rho\sqrt{M_i}}{\operatorname{Tr} M_i \rho}. \tag{1.13}$$

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.

1.2.2.3 Невозможность достоверного различения неортогональных состояний

Невозможность достоверного различения неортогональных квантовых состояний [11] — 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

$$\begin{aligned} \langle\psi_0| M_0 |\psi_0\rangle = 1, \quad \langle\psi_1| M_0 |\psi_1\rangle = 0, \\ \langle\psi_0| M_1 |\psi_0\rangle = 0, \quad \langle\psi_1| M_1 |\psi_1\rangle = 1. \end{aligned} \tag{1.14}$$

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

$$|\psi_1\rangle = a |\psi_0\rangle + b \left|\psi_0^\perp\right\rangle, \quad |a^2| + |b^2| = 1. \tag{1.15}$$

Так как $|\psi_0\rangle$ и $|\psi_1\rangle$ неортогональны, то $0 < |a| < 1$, $0 < |b| < 1$. Из условий (1.14) на операторы очевидно следует, что $\sqrt{M_1} |\psi_0\rangle = 0$, а значит,

$$\sqrt{M_1} |\psi_1\rangle = \sqrt{M_1} a |\psi_0\rangle + \sqrt{M_1} b \left|\psi_0^\perp\right\rangle = \sqrt{M_1} b \left|\psi_0^\perp\right\rangle, \tag{1.16}$$

из чего следует, что последнее равенство в (1.14) можно записать как

$$\langle\psi_1| M_1 |\psi_1\rangle = |b^2| \left\langle\psi_0^\perp\right| M_1 \left|\psi_0^\perp\right\rangle \leq |b^2|, \tag{1.17}$$

что противоречит (1.14) в силу $|b| < 1$. Полученное противоречие доказывает невозможность различения неортогональных состояний.

1.2.2.4 Чёткие и нечёткие наблюдаемые

Обычно под наблюдаемой подразумевают только ортогональное разложение единицы. Такие наблюдаемые будем называть *чёткими наблюдаемыми* [10]. В то же время требование взаимной ортогональности всех операторов не является обязательным, а в некоторых случаях выгоднее пользоваться наблюдаемыми, в которых не все операторы ортогональны друг другу, в целях получения максимального количества информации. Такие наблюдаемые называются *нечёткими*.

На первый взгляд нечёткие наблюдаемые просто смешивают вероятности разных исходов и не могут принести дополнительной пользы. Однако это не

так. Рассмотрим пример, как нечёткая наблюдаемая может помочь различить неортогональные состояния $|\varphi\rangle$ и $|\psi\rangle$: $\langle\varphi|\psi\rangle = \cos\eta \neq 0$.

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

$$\begin{aligned} M_0 &= \frac{\left|\psi^\perp\right\rangle\left\langle\psi^\perp\right|}{1+\cos\eta} = \frac{I - |\psi\rangle\langle\psi|}{1+\cos\eta}, \\ M_1 &= \frac{\left|\varphi^\perp\right\rangle\left\langle\varphi^\perp\right|}{1+\cos\eta} = \frac{I - |\varphi\rangle\langle\varphi|}{1+\cos\eta}, \\ M_? &= I - M_0 - M_1. \end{aligned} \tag{1.18}$$

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

1.2.3 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 [12] были отмечены необычные свойства составных квантовых систем, которые противоречили принципу локальности: получалось, что действия над одной подсистемой могут мгновенно оказывать влияние на другую подсистему вне зависимости от расстояния между ними.

1.2.3.1 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

$$\langle e_i \otimes f_j | e_m \otimes f_n \rangle = \langle e_i | e_m \rangle \cdot \langle f_j | f_n \rangle \tag{1.19}$$

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

$$(A_1 \otimes A_2)\,|e_1 \otimes e_2\rangle = (A_1\,|e_1\rangle) \otimes (A_2\,|e_2\rangle). \tag{1.20}$$

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:

$$|\psi_{EPR}\rangle = \frac{|00\rangle + |11\rangle}{\sqrt{2}}. \tag{1.21}$$

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

$$|\psi_{EPR}\rangle \neq (a_1 |0\rangle + b_1 |1\rangle) \otimes (a_2 |0\rangle + b_2 |1\rangle). \tag{1.22}$$

1.2.3.2 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:

$$\mathrm{Tr}_{\mathcal{H}_2} \rho_{12} = \sum_{i,j,k} |e_i\rangle \langle e_j| \langle e_i \otimes f_k| \rho_{12} |e_j \otimes f_k\rangle . \tag{1.23}$$

Аналогично для частичного следа по первому подпространству:

$$\mathrm{Tr}_{\mathcal{H}_1} \rho_{12} = \sum_{i,j,k} |f_i\rangle \langle f_j| \langle e_k \otimes f_i| \rho_{12} |e_k \otimes f_j\rangle . \tag{1.24}$$

По определению этой операции видно, что:

$$\begin{aligned} \mathrm{Tr}_{\mathcal{H}_2} \rho_1 \otimes \rho_2 &= \rho_1, \\ \mathrm{Tr}_{\mathcal{H}_1} \rho_1 \otimes \rho_2 &= \rho_2. \end{aligned} \tag{1.25}$$

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 первый участник применяет измерение $\{|0\rangle \langle 0| , |1\rangle \langle 1|\}$, то в составной системе это измерение будет выглядеть так:

$$M_0 = |0\rangle \langle 0|_1 \otimes I_2, \qquad M_1 = |1\rangle \langle 1|_1 \otimes I_2. \tag{1.26}$$

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

1.2.3.3 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 (1.21) в пространстве двух кубитов

$$|\psi_{EPR}\rangle = \frac{|00\rangle + |11\rangle}{\sqrt{2}} \tag{1.27}$$

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

$$\frac{\sqrt{M_0}\,|\psi_{EPR}\rangle\,\langle\psi_{EPR}|\,\sqrt{M_0}}{\langle\psi_{EPR}|\,M_0\,|\psi_{EPR}\rangle} = |00\rangle\,\langle 00|\,, \tag{1.28}$$

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 всё 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.

1.2.3.4 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 [13] — например, чтобы собрать более полную статистику результатов измерений.

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

$$U\,|\psi\rangle \otimes |A\rangle = |\psi\rangle \otimes |\psi\rangle\,, \tag{1.29}$$

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

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

$$\begin{aligned} U\,|0\rangle \otimes |A\rangle &= |0\rangle \otimes |0\rangle\,, \\ U\,|1\rangle \otimes |A\rangle &= |1\rangle \otimes |1\rangle\,, \end{aligned} \tag{1.30}$$

а также на состояние $\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$. В силу линейности оператора U и соотношений (1.30) должно выполняться

$$U(\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \otimes |A\rangle) = \frac{1}{\sqrt{2}}(|0\rangle \otimes |0\rangle + |1\rangle \otimes |1\rangle). \tag{1.31}$$

С другой стороны, по определению U (1.29) должно получаться

$$U(\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \otimes |A\rangle) = \frac{1}{2}(|0\rangle + |1\rangle) \otimes (|0\rangle + |1\rangle). \tag{1.32}$$

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.

1.3 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 (1.2.3.4) и о невозможности достоверного различения неортогональных состояний (1.2.2.3). 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 приёмной 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.

1.3.1 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 секретный ключ из этих частично совпадающих битовых строк.

1.3.1.1 Общая схема протокола

Протокол BB84 [14] использует два базиса:

$$\begin{aligned} + &: \left|0^{+}\right\rangle = |0\rangle\,, \quad \left|1^{+}\right\rangle = |1\rangle\,, \\ \times &: \left|0^{\times}\right\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle), \quad \left|1^{\times}\right\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle). \end{aligned} \tag{1.33}$$

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 четырёх 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:

$$\begin{aligned} M_0^{+} &= \left|0^{+}\right\rangle\left\langle 0^{+}\right|, \qquad M_1^{+} = \left|1^{+}\right\rangle\left\langle 1^{+}\right|, \\ M_0^{\times} &= \left|0^{\times}\right\rangle\left\langle 0^{\times}\right|, \qquad M_1^{\times} = \left|1^{\times}\right\rangle\left\langle 1^{\times}\right|. \end{aligned} \tag{1.34}$$

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 Алисой и Бобом стоит задача получения общего секретного ключа, которую можно разбить на два этапа: сначала производится коррекция ошибок [15], после чего у Алисы и Боба оказываются совпадающие битовые строки; затем происходит усиление секретности [16], 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.

1.3.1.2 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 приёмной стороне. Однако только измерениями посылаемых сигналов действия Евы не ограничиваются. Более того, непросто рассчитать информацию, способную попасть к Еве при всех возможных действиях с её стороны. Однако оказалось, что можно доказать стойкость протокола BB84, не прибегая к оценкам информационных величин для всех возможных атак Евы. В 2000 году было показано [17], 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 даёт 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 [18] 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 [19, 20].

Схема протокола, рассмотренная в [20], 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 $1 - 2h(q) = 0$.

1.3.1.3 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.

Прием-перепосыл

Наиболее простой сценарий действий Евы — измерение передаваемого по квантовому каналу состояния с дальнейшей пересылкой 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 зная исходного состояния, она сталкивается с нерешаемой проблемой различения состояний из неортогонального набора. Применяя случайным образом одно из измерений (1.34) к посланному состоянию, в половине случаев Ева будет неверно угадывать 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 "$\times$" будет послано одно из состояний набора $\{|0^\times\rangle, |1^\times\rangle\}$. Измеряя эти состояния в «верном» для них базисе, Боб получит ошибку, по которой действия Евы будут обнаружены.

Величину ошибки на приёмной 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 её 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 приёмной стороне будет равна $p/4$, а доля ошибок у Евы составит

$$\frac{1}{2} - \frac{p}{4}. \tag{1.35}$$

Это значит, что при всех значениях параметра p, меньших единицы, Ева имеет больше ошибок, чем Боб, и тогда её 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.

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 [10] следует, что выгоднее проводить измерение над всей последовательностью полученных состояний сразу. В [21] 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.

1.3.2 Протокол B92

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

В протоколе BB84 при отсутствии действий перехватчика и помех в канале вероятность ошибки на приёмной стороне до согласования базисов составляет 25%. Это вызвано использованием строго зафиксированной конфигурации двух пар базисных векторов. Цель протокола B92 [11] 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 (1.18)

$$\begin{aligned} M_0 &= \frac{I - |\psi_1\rangle\langle\psi_1|}{1+\cos\eta}, \\ M_1 &= \frac{I - |\psi_0\rangle\langle\psi_0|}{1+\cos\eta}, \\ M_? &= I - M_0 - M_1. \end{aligned} \tag{1.36}$$

Посылки, в которых был получен несовместный исход $M_?$, 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 [22].

1.3.3 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*:

$$|\alpha\rangle = e^{-\frac{\mu}{2}} \sum_{n=0}^{\infty} \frac{\alpha^n}{\sqrt{n!}} |n\rangle = e^{-\frac{\mu}{2}} (|0\rangle + \alpha\,|1\rangle + \frac{\alpha^2}{2}\,|2\rangle + \cdots), \tag{1.37}$$

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.

Параметр α, описывающий когерентное состояние, изменяется с оптической частотой ($\approx 10^{15}$ Гц), фаза параметра $\alpha = |\alpha|e^{i\theta}$ в каждой посылке распределена случайным образом на интервале $[0; 2\pi]$, поэтому само по себе такое состояние никакой информации не несет. В самом деле, матрица плотности когерентного

состояния есть усреднение по фазе:

$$\rho = \overline{|\alpha\rangle \otimes \langle\alpha|} = \int_0^{2\pi} \frac{d\theta}{2\pi} |\sqrt{\mu}e^{i(\varphi+\theta)}\rangle \ \langle\sqrt{\mu}e^{-i(\varphi+\theta)}| = e^{-\mu} \sum_{n=0}^{\infty} \frac{\mu^n}{n!} |n\rangle\langle n|, \ \forall\varphi \quad (1.38)$$

Проблема неоднофотонных источников дополняется второй — помехи и потери в квантовом канале связи. Эти два фактора дают возможность провести атаку с расщеплением по числу фотонов [23]. 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 приёмной стороне.

Однако, даже если в распоряжении Алисы имеется строго однофотонный источник, то при наличии потерь в канале Ева все равно может узнать [24] 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 приёмной стороне и оставляет подслушивателя незамеченным.

1.3.4 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 [14], B92 [11], SARG04 [25]. decoy-state [26], phase-time coding [27]).

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 для соблюдения протокола, на что так же потребуется время. В итоге Ева будет вызывать детектируемые задержки прихода состояний.

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.

Глава 2

Релятивистский протокол распределения ключей

В этой главе будет описан протокол квантового распределения ключей через открытое пространство, не требующий синхронизации часов между сторонами и существенным образом использующий ограничения релятивистской механики. Вначале будет дана общая идея протокола, обоснование его секретности, затем приведены некоторые технические подробности.

2.1 Общая идея

1) Алиса и Боб контролируют области пространства, необходимые для приготовления и измерения протяженных квантовых состояний.
2) Расстояние L между Алисой и Бобом всем известно и является параметром протокола. Алиса и Боб имеют часы, но не имеют общего начала отсчета времени (часы не синхронизированы).
3) Алиса передает серию состояний. Отправка посылки происходит в один из двух моментов времени внутри интервала ΔT, в какой именно — выбирается случайно (рис 2.2). Посылка представляет собой протяженное классическое состояние, состоящее из пары интенсивных когерентных пакетов, разделенных пространственно-временным интервалом l_{pac}, длина которого определяется исходя из свойств среды, в которой производится

передача[1]: $|\alpha_c\rangle_1 \otimes |\alpha_c\rangle_2$ (индексы «1» и «2» отвечают пакетам, локализованным в моменты времени 1 и 2, рис 2.1); среднее число фотонов в состоянии $\mu_c = |\alpha_c|^2 \gg 1$. Момент времени $t_{A,i}$ посылки состояния в канал связи Алисой фиксируется по её часам.

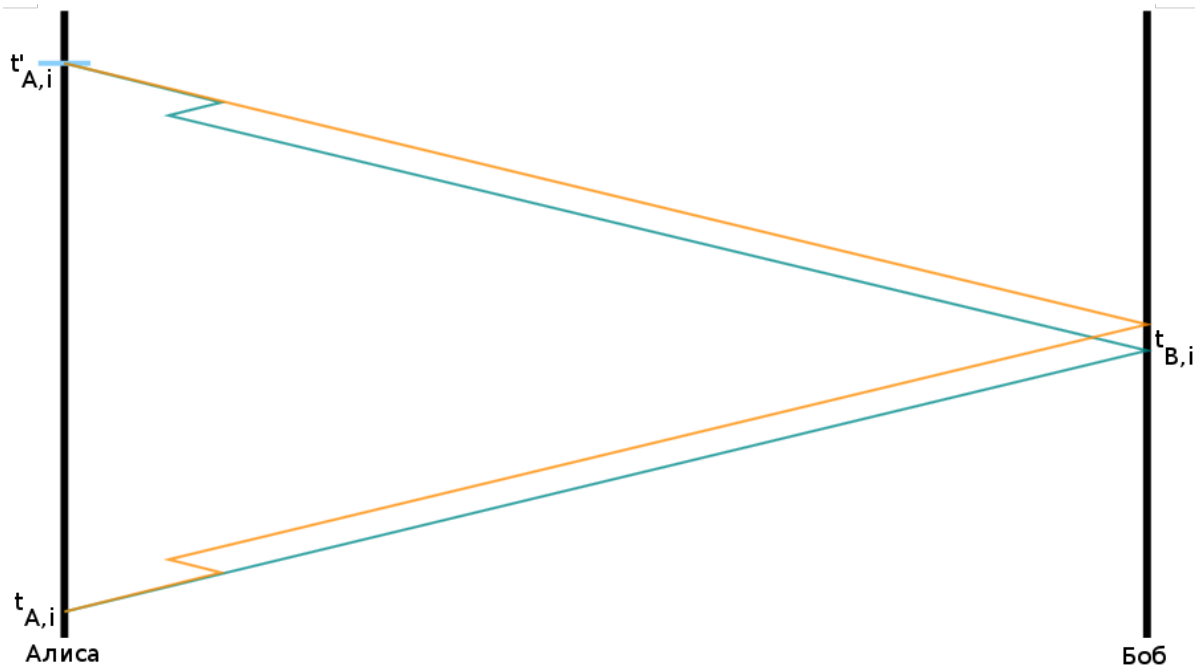

Рисунок 2.1: Пространственно-временная диаграмма, поясняющая процесс приготовления, преобразования и распространения протяженных квантовых состояний.

4) На приемной стороне работает аппаратура Боба в ждущем режиме. Момент прихода $t_{B,i}$ каждой i-й посылки фиксируется быстрым классическим детектором. Классический сигнал ослабляется до квазиоднофотонного уровня, на заднюю из «половинок» случайным образом навешивается фаза с помощью фазового модулятора. Полученное состояние $|\alpha\rangle_1 \otimes |e^{i\varphi_B}\alpha\rangle_2$ ($\mu = |\alpha|^2 < 1$) возвращается обратно Алисе [2]. Кодирование осуществляется на стороне Боба. Выбору логического 0 в ключе отвечает значение относительной фазы у двух импульсов $\varphi_B = \varphi_0$, а логической 1 — $\varphi_B = \varphi_1$.
5) Алиса, зная расстояние L и время отправки $t_{A,i}$ по своим часам своего состояния в канал связи, рассчитывает время прихода квантового

[1] Для передачи в воздухе пакеты должны быть разделены не менее, чем 1 метром пространства (см. приложение **??**)

[2] Все задержки на стороне Боба, связанные с обработкой, заранее известны. Их величина непринципиальна и считается включенной в моменты $t_{A,B,i}$ и $t'_{A,B,i}$.

состояния от Боба $t'_{A,i}$. В нужный момент включая фазовый модулятор, преобразует пришедшее состояние, случайным образом и независимо от Боба изменяя относительную фазу одной из «половинок»: $|\alpha\rangle_1 \otimes |e^{i\varphi_B}\alpha\rangle_2 \to |\frac{\alpha}{2}\rangle_1 \otimes |\frac{(e^{i\varphi_B}-e^{i\varphi_A})\alpha}{2}\rangle_2$ ($\varphi_A = \varphi_0$ или $\varphi_A = \varphi_1$), и производит измерения *только в определенном временном окне*. Если $\varphi_A \neq \varphi_B$, то возникает отсчет в детекторе, а если $\varphi_A = \varphi_B$, то отсчета не возникает в силу деструктивной интерференции. В результате отсчета Алиса достоверно знает, какой бит ключа посылал Боб.

6) После проведения серии посылок стороны обмениваются интервалами времени между соседними посылками (рис 2.2), которые каждый фиксировал по своим часам, и сравнивают их между собой. Подсчитывается доля их несовпадений η. Соседние посылки, интервалы между которыми не совпали, Алиса и Боб отбрасывают.
7) Далее часть оставшейся последовательности раскрывается и сравнивается для оценки вероятности ошибки. Если ошибка меньше критической, происходит исправление ошибок через открытый классический канал связи и сжатие очищенного ключа. В результате возникает секретный ключ, известный только Алисе и Бобу.

Нужно заметить, что Алиса и Боб не должны следить за средним числом долетевших посылок. Потери в канале связи не входят в критерий секретности ключей (§2.4).

2.2 Секретность протокола относительно различных атак

Протокол релятивистского квантового распределения ключей преследует две цели: первое, предоставить само распределение ключей и, второе, синхронизировать часы между Алисой и Бобом. Важную роль в обеспечении секретности играют релятивизм вкупе с протяженностью состояния, а также посылка Алисой состояний в случайные моменты времени. Рассмотрим возможные действия Евы в отсутствие какого-либо компонента из этих двух.

2.2.1 Необходимость протяженности состояния и ограничений СТО

Поясним, почему для получения информации о ключе необходимо иметь доступ к двум «половинкам» состояния, локализованным во временных окнах 1 и 2.

Информация о ключе заключена в относительной фазе двух состояний, $|\alpha\rangle_1$ и $|e^{i\varphi_B}\alpha\rangle_2$. Из (1.38) видно, что информация о фазе при доступе только к одной половинке полностью теряется. Таким образом, чтобы получить состояние, которое зависит от относительной фазы φ_B, несущей информацию о ключе, злоумышленнику необходимо иметь доступ к двум половинкам состояния.

В нерелятивистской квантовой криптографии возможны следующие атаки.

– Атака «прием-перепосыл»: Ева в каждой посылке измеряет состояния, затем в зависимости от исхода измерения посылает свои состояния.
– Коллективная атака: Ева готовит в каждой посылке свое состояние (анциллу), которое при помощи унитарного преобразования запутывается с информационным состоянием. Анцилла остается в квантовой памяти для дальнейших коллективных измерений сразу над всей последовательностью, а модифицированное состояние направляется к Алисе (Бобу).

В релятивистском случае обе атаки приводят к задержкам и к вероятности ошибки 50% в каждой посылке.

Причина состоит в следующем. Для различения матриц плотности и получения информации о ключе, $\rho(\varphi_B = \varphi_0)$ и $\rho(\varphi_B = \varphi_1)$, которые нелокальны в пространстве-времени (локализованы во временных окнах 1 и 2), необходимо иметь доступ к двум половинкам одновременно.

Любое унитарное преобразование, сводящее две разделенные в пространстве-времени Минковского половинки состояний, требует конечного времени (ситуация поясняется на рис. 2.3). Более формально, время, необходимое для сведения половинок вместе, диктуется фундаментальными ограничениями специальной теории относительности. Данное время равно высоте прошлой части светового конуса, накрывающего обе половинки (рис

2.3). После сведения половинок вместе Ева может делать либо унитарные преобразования состояния, либо измерения с определенным исходом.

Затем ей снова необходимо приготовить протяженное в пространстве-времени состояние. На это также требуется конечное время, равное высоте будущей части светового конуса. Однако при этом исходные состояния, которые распространяются со скоростью света, окажутся уже сдвинутыми в пространстве-времени по отношению к новому состоянию Евы. Поскольку Алиса делает преобразования и измерения только в определенном временном окне (рис 2.1), вторая половинка состояния не успеет прибыть и не будет участвовать в преобразованиях. Вместо истинного состояния $|\frac{e^{i(\varphi_B-\varphi_A)}\alpha}{2}\rangle_2$ в центральном временном окне 2 окажется состояние $|\frac{e^{i\varphi_B}\alpha}{2}\rangle_2$ (см. рис. 2.1 и формулу (1.38)). Такое состояние даст вероятность ошибки 50%, поскольку оно не зависит от выбора фазы Алисы.

Конечно, Ева может заранее приготовить первую половинку состояния, сделать преобразования, сводящие половинки состояний Боба вместе, провести UM-измерения и в случае определенного исхода приготовить вторую половинку с нужной фазой. В этом случае задержек и ошибок на стороне Алисы не будет. Однако из-за неортогональности состояний неизбежно будут неопределенные исходы, при которых Ева не знает состояния (она может только пытаься случайно угадать фазу). Однако при угадывании на стороне Алисы вероятность ошибки составит все те же 50%. При неопределенном исходе Ева уже не сможет блокировать свою заранее приготовленную половинку из-за ограничений специальной теории относительности.

2.2.2 Необходимость посылки состояния в случайный момент

Поясним, почему Алиса должна посылать свои состояния в случайные и известные только ей моменты времени. Поскольку часы у Алисы и Боба не синхронизированы, Боб не знает, когда он получит состояния от Алисы. Если б Алиса посылала состояния в регулярные и известные всем моменты времени, то Ева могла бы действовать следующим образом.

Ева заранее, до прихода к себе состояния от Алисы, посылает к Бобу состояние, аналогичное состоянию Алисы (которое не несет никакой

информации о ключе и каждый раз одинаково). Затем, получив назад от Боба свое ослабленное когерентное состояние, уже несущее информацию о ключе, она делает измерения с определенным исходом [2]. Поскольку состояния неортогональны, Ева может с некоторой вероятностью получить как определенный исход, так и неопределенный. Если получен определенный исход, то Ева однозначно знает передаваемый бит ключа. Тот факт, что на такое измерение требуется конечное время, для Евы не важен, поскольку она заранее посылает свои состояния и поэтому имеет необходимый запас времени. При определенном исходе Ева готовит свое состояние, аналогичное теперь уже известному состоянию Боба, и посылает его в нужный момент времени, после регистрации классического состояния Алисы, чтобы не вызвать задержки измерений у Алисы. Исходное состояние Алисы, которое приходит к ней позднее, Ева блокирует.

Если же Евой получен неопределенный исход, то Ева ничего не посылает Алисе и блокирует приход ее состояния к Бобу. Потеря состояния списывается на потери в канале связи, которые не контролируются и могут быть любыми. При такой стратегии Ева знала бы весь ключ и не производила задержек и ошибок на стороне Алисы.

При посылке Алисой состояний в случайные моменты времени, а затем сравнении моментов прихода состояний в соседних посылках к Бобу такая стратегия не работает, поскольку посылка Евой состояния к Бобу в неправильный момент времени неизбежно приведет к ее обнаружению. Такие посылки отбрасываются. Пусть доля таких посылок есть η. Если Алиса выбирает случайные моменты посылки из двух возможностей, то вероятность угадывания Евой составляет 1/2. В асимптотическом пределе большого числа посылок из доли η Ева знает значения бита в половине этих посылок, где она угадала правильный момент и при этом не произошло сбоя момента прихода состояния к Бобу.

Как видно из анализа выше, для детектирования любых попыток подслушивания в данном протоколе важны как ограничения квантовой механики на принципиальную неразличимость неортогональных квантовых состояний,

так и ограничения специальной теории относительности на предельную скорость передачи каких бы ни было физических состояний, как квантовых, так и классических.

Ограничения специальной теории относительности принципиальны для детектирования атаки с UM-измерениями. Все протоколы нерелятивистской квантовой криптографии без контроля затухания становятся несекретными при определеленных потерях, поскольку Ева при UM-измерениях не производит ошибок и знает весь ключ, начиная с критической величины потерь [2]. В даннном случае ошибки неизбежны из-за нехватки времени (релятивистское ограничение) и неортогональности квантовых состояний (квантовомеханический запрет на достоверную различимость неортогональных состояний).

2.3 Технические подробности приготовления и измерения состояний

Алиса активирует лазер (рис. 2.4) в определенный момент времени и получает на выходе интенсивное когерентное состояние, локализованное в интервале l_{pac}. Интерферометр Алисы состоит из двух симметричных светоделителей и задержки по одному плечу между ними. В плече с задержкой также установлен фазовый модулятор, но при первом проходе он не используется и на состояния не влияет.

Симметричный светоделитель вводится как оператор $\hat{U}_{50/50}$, действующий на два когерентных состояния на входе следующим образом:

$$\hat{U}_{50/50}\begin{bmatrix}|\alpha\rangle\\|\beta\rangle\end{bmatrix} = \begin{bmatrix}\frac{1}{\sqrt{2}}(|\alpha\rangle + |\beta\rangle)\\\frac{1}{\sqrt{2}}(|\alpha\rangle - |\beta\rangle)\end{bmatrix}. \tag{2.1}$$

То есть в один выход светоделителя направляется сумма входных состояний, в другой — их разность.

Если на входе светоделителя только одно состояние (второе вакуумное), то это состояние «расщепится» и в оба выхода светоделителя отправятся

одинаковые части:

$$\hat{U}_{50/50}\begin{bmatrix}|\alpha\rangle\\0\end{bmatrix}=\begin{bmatrix}\frac{|\alpha\rangle}{\sqrt{2}}\\\frac{|\alpha\rangle}{\sqrt{2}}\end{bmatrix}. \tag{2.2}$$

Если эти «половинки» одновременно достигнут входа второго светоделителя, то, согласно определению, в верхний выход отправится исходное состояние $|\alpha\rangle$, в нижнем не будет ничего:

$$\hat{U}_{50/50}\begin{bmatrix}\frac{|\alpha\rangle}{\sqrt{2}}\\\frac{|\alpha\rangle}{\sqrt{2}}\end{bmatrix}=\begin{bmatrix}\frac{1}{\sqrt{2}}(\frac{|\alpha\rangle}{\sqrt{2}}+\frac{|\alpha\rangle}{\sqrt{2}})\\\frac{1}{\sqrt{2}}(\frac{|\alpha\rangle}{\sqrt{2}}-\frac{|\alpha\rangle}{\sqrt{2}})\end{bmatrix}=\begin{bmatrix}|\alpha\rangle\\0\end{bmatrix}. \tag{2.3}$$

При прохождении через интерферометр локализованное состояние Алисы преобразуется в состояние из двух половинок, разделенных интервалом l: $|\alpha_c\rangle_1\otimes|\alpha_c\rangle_2$. Затем состояние через линзовую систему направляется в канал связи. Приготовление протяженного состояния из локализованного требует конечного времени (рис 2.1).

На приемной стороне Боба классическое состояние вводится в волоконную часть. Через светоделитель состояние поступает на классический детектор, по импульсу тока на котором оценивается интенсивность состояния и записывается его время прилета. Затем сигнал отражается от фарадеевского зеркала, в зависимости от сигнала на детекторе ослабляется и становится равным $|\alpha\rangle_1\otimes|\alpha\rangle_2$. При прохождении второй половинки ослабленного состояния через фазовый модулятор на последний подается импульс напряжения и «навешивается» относительная фаза. Получившееся состояние $|\alpha\rangle_1\otimes|e^{i\varphi_B}\alpha\rangle_2$ направляется к Алисе.

Поскольку Алиса знает время приготовления своего состояния и расстояние L между передающей и приемной станциями, при обратном проходе она активирует фазовый модулятор в момент прохождения первой половины состояния по нижнему, более длинному, плечу интерферометра. Из-за разности хода на втором светоделителе интерферируют передняя, из нижнего плеча, и задняя, из верхнего плеча интерферометра, половинки. Таблица 2.1 отражает последовательное преобразование состояний по оптическому тракту.

Верхний и нижний входы BS	Верхнее и нижее плечо BS после PM	Верхний и нижний выход BS
$\|\alpha\rangle_1 \otimes \|e^{i\varphi_B}\alpha\rangle_2 \otimes \|vac\rangle_3$	$\|\frac{\alpha}{\sqrt{2}}\rangle_1 \otimes \|\frac{e^{i\varphi_B}\alpha}{\sqrt{2}}\rangle_2 \otimes \|vac\rangle_3$	$\|\frac{\alpha}{2}\rangle_1 \otimes \|\frac{(e^{i\varphi_B}+e^{i\varphi_A})\alpha}{2}\rangle_2 \otimes \|\frac{\alpha}{2}\rangle_3$
$\|vac\rangle_1 \otimes \|vac\rangle_2 \otimes \|vac\rangle_3$	$\|vac\rangle_1 \otimes \|\frac{e^{i\varphi_A}\alpha}{\sqrt{2}}\rangle_2 \otimes \|\frac{\alpha}{\sqrt{2}}\rangle_3$	$\|\frac{\alpha}{2}\rangle_1 \otimes \|\frac{(e^{i\varphi_B}-e^{i\varphi_A})\alpha}{2}\rangle_2 \otimes \|\frac{\alpha}{2}\rangle_3$

Таблица 2.1: Преобразование состояний по оптическому тракту на пути от Боба к Алисе

На входе лавинного фотодетектора в центральном временном окне 2 состояние равно $|\frac{(e^{i\varphi_B}-e^{i\varphi_A})\alpha}{2}\rangle_2$. При обратном проходе состояния в плече лазера являются холостыми.

Далее, если Боб выбрал $\varphi_B = \varphi_0$, а Алиса выбрала также $\varphi_A = \varphi_0$ (или $\varphi_B = \varphi_1$ и $\varphi_A = \varphi_1$), то отсчета в детекторе не будет из-за деструктивной интерференции. В противоложном случае, когда Боб выбрал $\varphi_B = \varphi_0$, а Алиса выбрала $\varphi_A = \varphi_1$ (и аналогично $\varphi_B = \varphi_1$ и $\varphi_A = \varphi_0$), будет отсчет. Таким образом, Алиса по отсчету детектора знает бит, выбранный Бобом.

Следует отметить, что данная схема является реализацией двух измерений, которые Алиса выбирает случайно путем выбора фазы. Фактически данное измерение реализует проекцию на состояние $|e^{i\varphi_B}\alpha\rangle_2 \ {}_2\langle e^{i\varphi_B}\alpha|$ и на его ортогональное дополнение $I - |e^{i\varphi_B}\alpha\rangle_2 \ {}_2\langle e^{i\varphi_B}\alpha|$.

2.4 Длина секретного ключа

Получим длину секретного ключа при атаке с измерениями с определенным исходом (UM). Для этого требуется найти оптимальные измерения для различения матриц плотности $\rho(\varphi_B = \varphi_0)$ и $\rho(\varphi_B = \varphi_1)$, минимизирующие ошибку неопределенного (inconclusive — ?) исхода. Поскольку действие любого квантового преобразования только уменьшает различимость квантовых состояний, так как расстояние между ними уменьшается, то вероятность неопределенного исхода для чистых состояний меньше. Эта ситуация отвечает тому, что фаза α как бы известна Еве. Таким образом, дальнейшие оценки оказываются в пользу Евы, так как завышают ее информацию. Как известно, в случае неортогональных чистых состояний минимально возможная вероятность

неопределенного исхода при их различении равна

$$Pr\{?\} = {}_2\langle e^{i\varphi_0}\alpha | e^{i\varphi_1}\alpha\rangle_2 = e^{-2\mu \sin^2 \frac{\varphi}{2}},\ \varphi = \varphi_0 - \varphi_1.$$

Соответственно, вероятность определенного исхода $Pr\{OK\} = 1 - Pr\{?\}$

Пусть доля посылок, которые подслушивает Ева, составляет δ. Ошибка на приемной стороне Алисы равна

$$Q\left(\frac{1}{2}\delta Pr\{?\}\right) = 0 \cdot \delta Pr\{OK\} + \frac{1}{2}\delta Pr\{?\} + 0 \cdot (1-\delta).$$

Взаимная информация Алиса-Боб после исправления ошибок и взаимная информация Алиса(Боб)-Ева равны

$$\begin{aligned} I(A;B) &= 1 - h\left(\frac{1}{2}\delta Pr\{?\}\right), \\ I(A;E) &= \delta(1 - Pr\{?\}). \end{aligned}$$

Критическая величина ошибки, до которой возможно секретное распределение ключей, и длина секретного ключа R в битах на посылку определяются из условия $I(A;B) = I(A;E)$ [28]:

$$R\left(\frac{1}{2}\delta Pr\{?\}\right) = 1 - h\left(\frac{1}{2}\delta Pr\{?\}\right) - \delta(1 - Pr\{?\}).$$

Обсудим теперь последнюю, так называемую прозрачную атаку Евы со светоделителем. Данная атака не приводит ни к задержкам измерений, ни к ошибкам на стороне Алисы, но не дает полной информации о ключе. В этом месте для секретности ключей опять важна неортогональность состояний Боба.

Ева использует асимметричный светоделитель, отводит состояния от Боба и сохраняет их в квантовой памяти. Когерентные состояния преобразуются на светоделителе самоподобным образом (остаются когерентными, но с другой α, зависящей от коэффициента деления). При отсчете детектора Алиса достоверно знает бит Боба. Для этих посылок Ева делает коллективные измерения над всей последовательностью в своей квантовой памяти (отбрасывая посылки, где у Алисы не было отсчета). Информация Евы ограничена фундаментальной

границей Холево на доступную классическую информацию, которую можно извлечь из ансамбля квантовых состояний [29]. При этом максимум достигается в том случае, когда Ева отводит себе целиком состояния Боба. Таким образом, взаимная информация Алиса-Боб и взаимная информация Алиса-Ева при такой атаке равны

$$\begin{aligned} I(A;B) &= 1, \\ I(A;E) &\leq \chi(\rho) = S(\rho), \end{aligned}$$

$$\rho = \frac{1}{2}(\rho_0 + \rho_1),\ \rho_{0,1} = (|\alpha\rangle_1 \otimes |e^{i\varphi_{0,1}}\alpha\rangle_2)({}_2\langle e^{i\varphi 0,1}\alpha| \otimes {}_1\langle\alpha|),$$

где $S(\rho) = -Tr\{\rho\log(\rho)\}$ — энтропия фон Неймана. Окончательно для длины секретного ключа имеем

$$\begin{aligned} R &= I(A;B) - I(A;E) = 1 - C(\varepsilon), \\ C(\varepsilon) &= -\left(\frac{1-\varepsilon}{2}\right)\log\left(\frac{1-\varepsilon}{2}\right) - \left(\frac{1+\varepsilon}{2}\right)\log\left(\frac{1+\varepsilon}{2}\right), \end{aligned}$$

где $\varepsilon = \exp(-2\mu\sin^2[\frac{\varphi_0-\varphi_1}{2}])$, $C(\varepsilon)$ — классическая пропускная способность квантового канала связи Боб-Ева, которая в данном случае совпадает с энтропией фон Неймана.

Возможна также комбинация различных атак Евы. В этом случае длина финального секретного ключа

$$R\left(\frac{1}{2}\delta Pr\{?\}\right) = 1 - \frac{\eta}{2} - h\left(\frac{1}{2}\delta Pr\{?\}\right) - \delta(1 - Pr\{?\}) - C(\varepsilon).$$

Поскольку Алиса и Боб не знают доли подслушиваемых посылок δ, и Алиса видит только ошибку Q, удобней привести длину ключа как функцию наблюдаемой ошибки. Зависимости длины секретного ключа R от наблюдаемой ошибки приведены на рис. 2.5a, а зависимость R от среднего числа фотонов при заданной наблюдаемой ошибке показаны на рис. 2.5b. Значение параметра η (доли посылок с угадыванием момента времени приготовления состояния Алисы) положено $\eta = 0$ (данная доля известна из сравнения сбоев моментов прихода состояний к Алисе). Как видно из рис. 2.5, протокол обеспечивает достаточно большую критическую ошибку (до 35%, рис. 2.5a). Кроме того,

среднее число фотонов при $Q = 0$ формально может быть любым (рис 2.5b). Длина ключа нигде не обращается в нуль, но, естественно, падает с ростом μ как $\sim e^{-2\mu}$. Подчеркнем еще раз принципиальный момент: в отличие от любых нерелятивистских протоколов квантовой криптографии потери в канале связи вообще не входят в длину секретного ключа, что является следствием фундаментальных запретов специальной теории относительности.

2.5 Обработка полученного ключа

Любой протокол квантового распределения частей состоит из двух частей: квантовой и классической [1]. Квантовая часть включает в себя собственно передачу квантовых состояний, манипуляции над ними и измерения, и проводится с использованием квантового канала связи. Классическая часть проводится через открытый аутентичный классический канал (то есть такой, который злоумышленник может прослушивать, но не может изменить передаваемые данные) и включает в себя коррекцию ошибок и усиление секретности.

2.5.1 Коррекция ошибок

Результатом квантовой части является так называемый «сырой» ключ на обеих сторонах квантового канала. Этот ключ должен быть очищен от всех ошибок, неизбежно возникающих в процессе. Ошибки могут быть как внутренними (из-за низкой эффективности самого протокола), так и внешними, исходящими как от физических недостатков используемой аппаратуры, так и от действий подслушивателя. Внутренние ошибки исправить проще, что обычно и делается по ходу протокола путем передачи через открытый канал информации о начальном состоянии. К примеру, в протоколе BB84 [14] половина от всей переданной последовательности состояний будет измерена Бобом в базисе, не совпадающим с тем, в каком их готовила Алиса. Это приведет к тому, что 50% полученных бит в итоге не войдут в секретный ключ. В реальности же, оставшиеся биты все еще будут подвержены ошибкам, возникших либо со стороны аппаратуры, либо из-за действий злоумышленника, что в принципе

неразличимо. В дальнейшем будет предполагаться, что используемая аппаратура идеальна, а все ошибки возникают исключительно из-за воздействия Евы.

В [15] продемонстрировано существование оптимального, хоть и не эффективного, протокола, оставляющего минимальное количество информации подслушивателю. На практике же стандартом де-факто для всех протоколов квантового распределения ключей является протокол коррекции ошибок *Cascade*.

2.5.1.1 Протокол Cascade

1) Работа протокола происходит в несколько проходов, число которых определяется сторонами до начала процесса. У каждой из сторон имеется своя битовая строка: $A = A_1, \ldots, A_n$ и $B = B_1, \ldots, B_n$ (где $B_i, A_i \in \{0, 1\}$) у Алисы и Боба соответственно.
2) На каждом проходе i Алиса и Боб выбирают значение k_i и случайную функцию $f_i : [1..n] \to [1..\lceil \frac{n}{k_i} \rceil]$. Биты, чья позиция находится в множестве $K_j^i = \{l \mid f_i(l) = j\}$ формируют блок j в проходе i. Таким образом, строка каждого из участников перемешивается случайно выбранным образом и разбивается на блоки размера k_i.
3) Алиса посылает Бобу четности каждого блока текущего прохода:

$$a_j = \bigoplus_{l \in K_j^i} A_l,\ 1 \leq j \leq \left\lceil \frac{n}{k_i} \right\rceil$$

4) Боб вычисляет свои b_j таким же образом и сравнивает их с полученными a_j.
5) Множество блоков, в которых содержится нечетное число ошибок, обозначим $\mathcal{E}$. Изначально в это множество заносятся блоки, четности которых не совпали: $(b_j \neq a_j)$.
6) Если $\mathcal{E} \neq \emptyset$, выбирается блок наименьшего размера из $\mathcal{E}$, иначе проход считается завершенным.
7) Для выбранного блока проводится дихотомический поиск ошибки:
   a) Алиса посылает Бобу четность первой половины бит указанного блока.

б) Боб сравнивает полученные данные со своими. Если четности не совпали, то в первой половине блока находится нечетное число ошибок; если совпали — во второй.

в) Процесс повторяется с той половиной блока, о которой теперь известно, что в ней находится нечетное число ошибок.

г) В конце концов будет найдена одна позиция, значения строк в которой у Алисы и Боба различаются.

8) В результате поиска Боб обнаружит позицию l такую, что $B_l \neq A_l$ и исправит свое значение.

9) Все блоки K_v^u для $1 \leq u < i$ такие, что $l \in K_v^u$ (то есть содержащие в себе только что исправленную позицию) будут теперь иметь нечетное число ошибок. Обозначим множество этих блоков за $\mathcal{K}$

10) Множество $\mathcal{E}$ изменяется следующим образом: для каждого блока $K \in \mathcal{K}$, если $K \in \mathcal{E}$, происходит его удаление из $\mathcal{E}$, в противном случае блок K добавляется к $\mathcal{E}$. Формально говоря, $\mathcal{E}' = \mathcal{E} \bigtriangledown \mathcal{K} = (\mathcal{E} \cup \mathcal{K}) \setminus (\mathcal{E} \cap \mathcal{K})$.

11) Дальнейшее выполнение продолжается с шага 6 и множеством $\mathcal{E}'$ в качестве $\mathcal{E}$.

На практике обычно используется 4 прохода, размеры блоков в каждом следующем проходе удваиваются, а начальный размер блока выбирается из соображений максимизации количества исправленных ошибок в первом проходе, что зависит от предполагаемой величины ошибок p.

2.5.2 Усиление секретности

После коррекции ошибок Алиса и Боб имеют одинаковую строку W из n бит, о которой подслушивателю Еве известна некоторая информация, описываемая вероятностным распределением $P_{W|V=v}$ над всеми n-битными строками, где v обозначает конкретное значение случайной величины V, представляющей собой сумму всей её (Евы) информации. Для примера, Ева может узнать некоторые биты или косвенную информацию о них во время квантовой части протокола, некоторые во время исправления ошибок (четности блоков) или найти какой-то более изощренный способ узнать некоторую информацию о строке W. Алиса и Боб имеют представление о том, сколько примерно информации может быть

доступно злоумышленнику, то есть о распределении $P_{W|V=v}$, но они не знают наверняка, к каким битам их строки относится эта информация. Используя открытый аутентичный канал (свободный для прослушивания, но сообщения в котором невозможно модифицировать или несанкционированно вставить), они хотят договориться о такой функции $g : \{0,1\}^n \to \{0,1\}^r$, что Ева, несмотря на ее частичное знание о строке W и полном знании о функции g, не будет знать практически ничего о $g(W)$. Этот процесс преобразует частично секретную n-битную строку W в высокосекретную, но более короткую, r-битную строку $g(W)$, которая уже может использоваться как секретный ключ.

Метод, которым выбирается функция g, был предложен Беннетом в работе [30] и заключается в выборе конкретной функции случайным образом из заранее известного универсального семейства хеш-функций (введены Картером и Вегманом в [31]), отображающих n-битные строки в r-битные.

Определение 3. *Семейство $\mathcal{F}$ функций $\mathcal{A} \to \mathcal{B}$ называется универсальным, если*

$$\Pr[f(x_1) = f(x_2)] < \frac{1}{|B|} \quad \forall x_1, x_2 \in \mathcal{A} : x_1 \neq x_2,$$

а f выбирается из $\mathcal{F}$ в соответствии с равномерным распределением.

В [16] было показано, что энтропия Реньи (определение ниже) распределения вероятности Евы о строке W дает нижнюю границу размера r секретного ключа, который возможно получить из W с помощью универсального хеширования.

Определение 4. *Пусть X — случайная величина из алфавита $\mathcal{X}$ с распределением вероятности P_X. Вероятностью коллизии $P_c(X)$ называется вероятность того, что X примет одно и то же значение дважды в двух независимых экспериментах:*

$$P_c(X) = \sum_{x \in X} P_X(x)^2. \tag{2.4}$$

Определение 5. *Энтропия Реньи порядка 2 (или просто «энтропия Реньи») случайной величины X определяется как*

$$R(X) = -\log P_c(X). \tag{2.5}$$

Определение 6. *Условная энтропия Реньи $R(X|Y)$ определяется как*

$$R(X|Y) = \sum_y P_Y(y) R(X|Y=y) = -\sum_y P_Y(y) \log P_c(X|y). \tag{2.6}$$

Иначе говоря, $R(X)$ может быть выражена как $R(X) = -\log E[P_X(X)]$, где $E[\cdot]$ обозначает математическое ожидание. Энтропия Шеннона $H(X)$ аналогичным образом выражается как $H(X) = -E[\log P_X(X)]$. Из неравенства Йенсена (см [**?**]) очевидным образом следует следующее утверждение.

Утверждение 1. *Энтропия Реньи ограничена сверху энтропией Шеннона:*

$$R(X) \leq H(X),$$

причем равенство достигается тогда и только тогда, когда P_X является равномерным распределением над алфавитом $\mathcal{X}$ или его подмножеством.

Аналогично имеем $H(X|Y) \geq R(X|Y)$. Следует заметить, что энтропия Реньи, как и энтропия Шеннона, всегда положительна.

Следующая теорема является основным результатом, полученным в работе [16]:

Теорема 3. *Пусть X — случайная величина в алфавите $\mathcal{X}$ с вероятностым распределением P_X и энтропией Реньи $R(X)$. Кроме того, пусть G — случайная величина, отвечающая случайному выбору (внутри равномерного распределения) члена универсального семейства хеш-функций, отображающих $\mathcal{X} \to \{0,1\}^r$. Тогда*

$$H(G(X)|G) \geq R(G(X)|G) \geq r - \frac{2^{r-R(X)}}{\ln 2}. \tag{2.7}$$

Необходимо обратить внимание, что G является случайной величиной, и что энтропия $H(G(X)|G)$ есть среднее по всем возможным выборам функции g. Может случиться так, что $H(G(X)|G=g) = H(g(X))$ значительно отличается от r для некоторой функции g, но такая функция g может быть выбрана лишь с пренебрежимо малой вероятностью.

Эта теорема применяется и к условным вероятностным распределениям, таким как описанное выше $P_{W|V=v}$. Если известно, что энтропия Реньи

информации Евы $R(W|V = v)$ составляет как минимум t бит, и Алиса с Бобом выбирают $S = G(W)$ как их секретный ключ, тогда

$$R(S|G,V = v = R(G(W)|G,V = v) \geq r - \frac{2^{r-t}}{\ln 2}. \tag{2.8}$$

Величина $H(S|G,V = v)$ имеет следующий информационный смысл: это количество бит, которое не хватает Еве, чтобы полностью узнать ключ S, если она имеет конкретную информацию о ключе v, в среднем по всем хеш-функциям g универсального семейства G.

Ключ S будет действительно практически секретным, так как $H(S|G,V = v) \geq R(S|G,V = v)$, и, следовательно, $H(S|G,V = v)$ сколько угодно близко к максимальному значению. Более точно, если $r < t$, то общая информация Евы о ключе S уменьшется экспоненциально с фактором $t - r$.

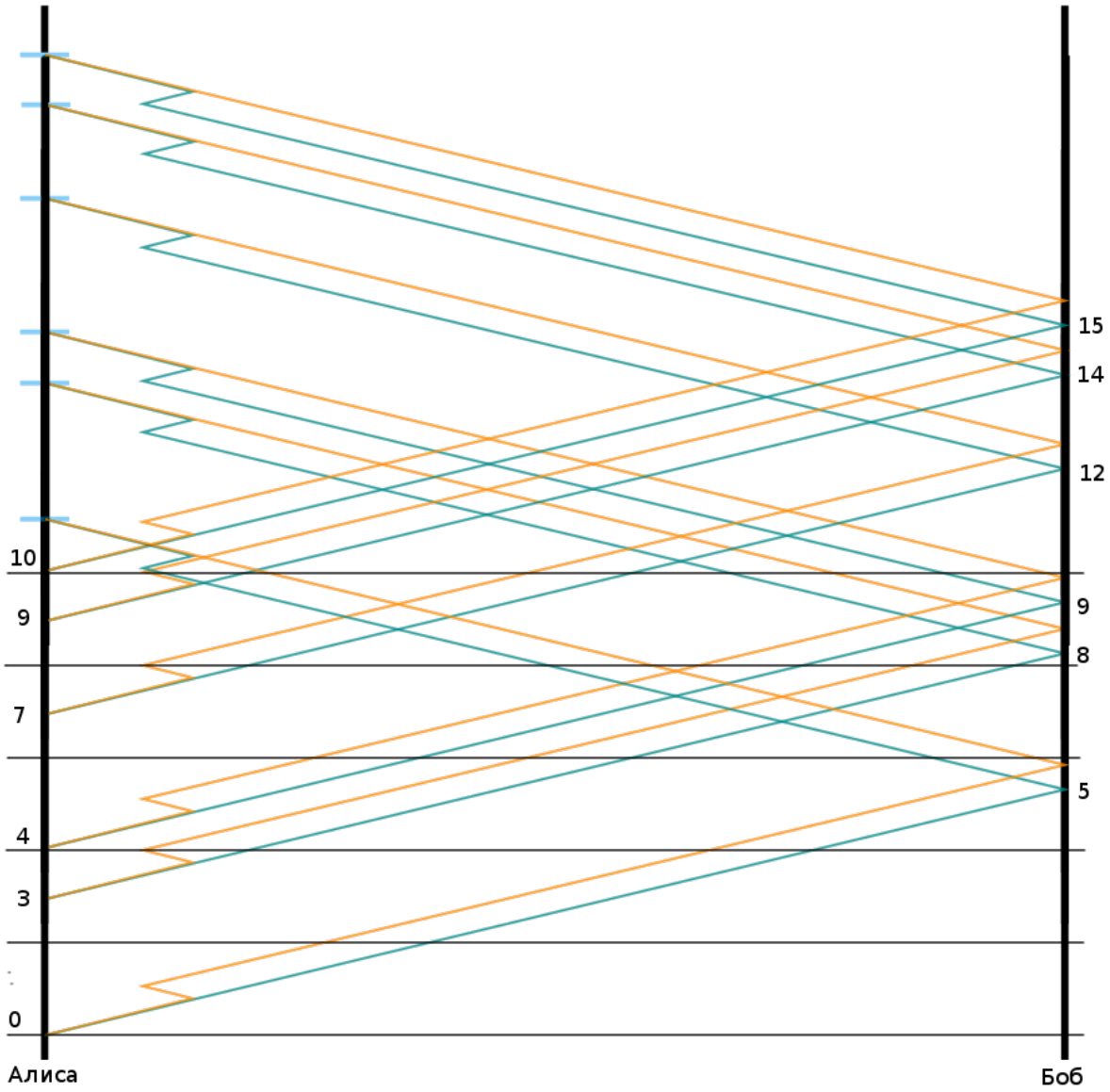

Рисунок 2.2: Пространственно-временная диаграмма, поясняющая посылку классических и прием квантовых состояний в случайные моменты. Слева и справа от вертикальный осей числами обозначены моменты посылки и приема состояний.

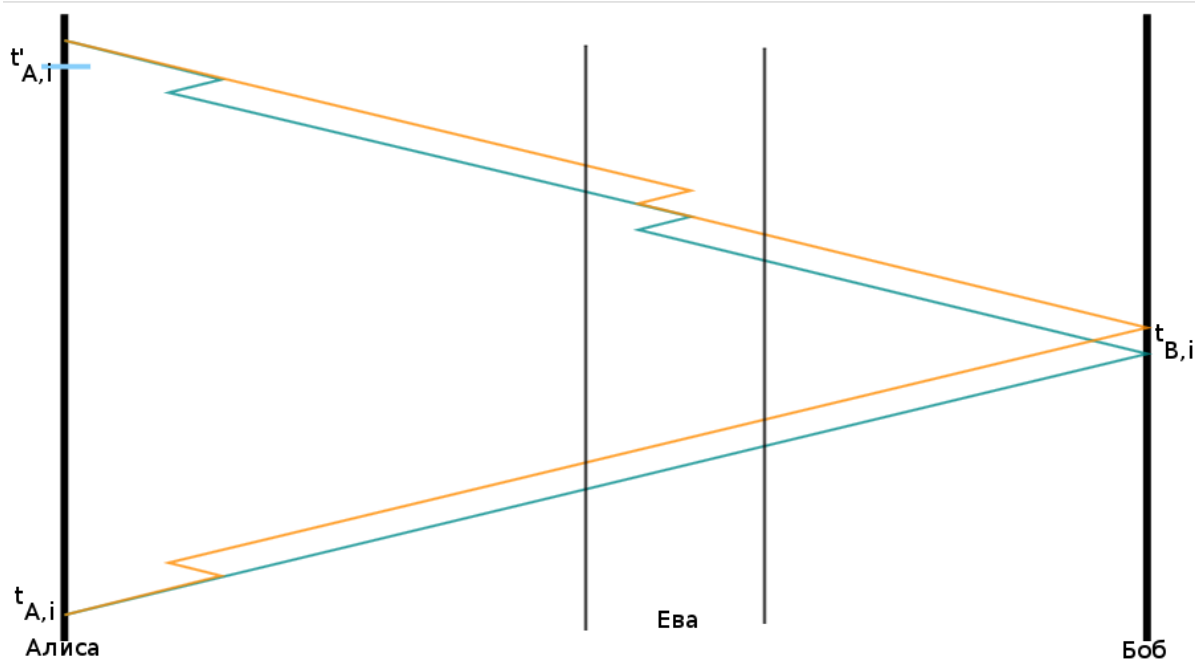

Рисунок 2.3: Пространственно-временная диаграмма, поясняющая причину задержек по времени протяженных состояний при подслушивании Евой

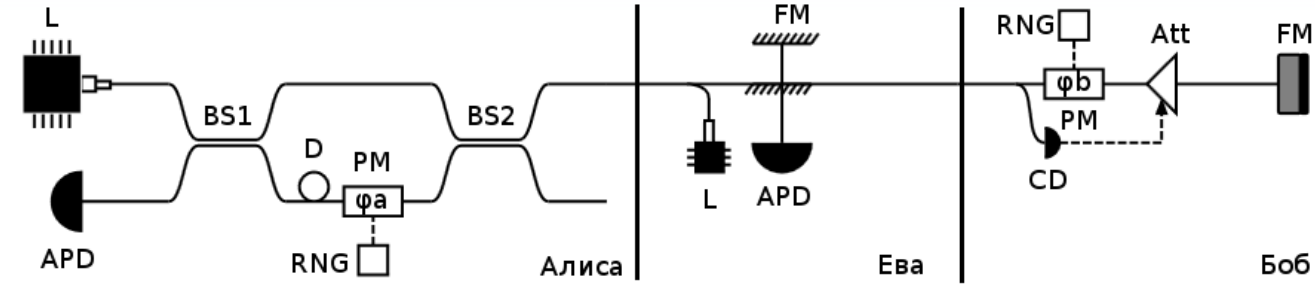

Рисунок 2.4: Двухпроходная оптическая схема приготовления, преобразования и детектирования состояний. L — лазер, APD — лавинный стробируемый однофотонный детектор, BS1, BS2 –интерферометр с разностью хода по нижнему и верхнему плечу, D — задержка в плече интерферометра, PM — фазовый модулятор, RNG — генератор случайных чисел, CD — быстрый классический детектор, Att — управляемый аттенюатор, FM — фарадеевское зеркало

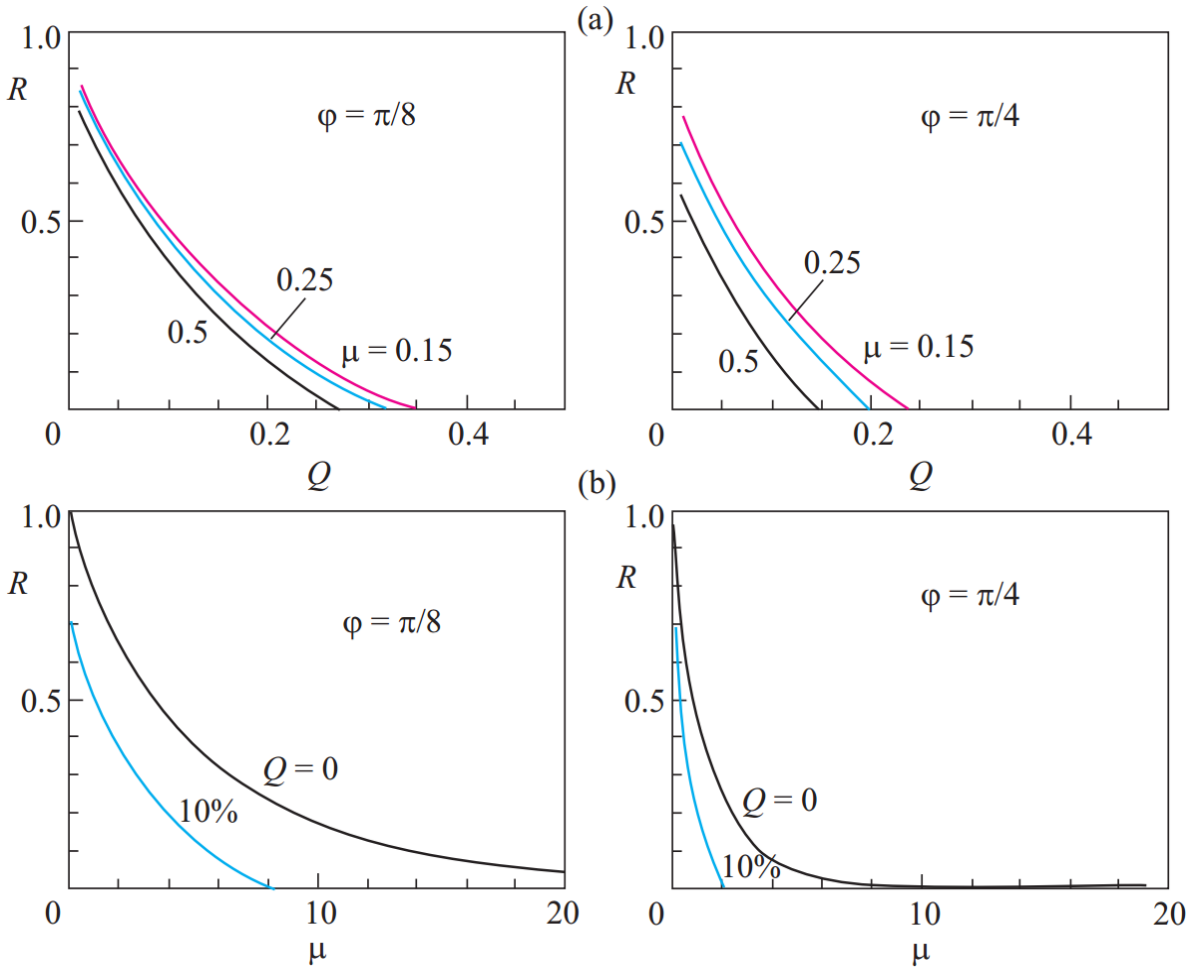

Рисунок 2.5: Зависимость длины секретного ключа R от наблюдаемой ошибки (a) и среднего числа фотонов (b)

Список литературы

1. Quantum cryptography / N. Gisin, G. Ribordy, W. Tittel [и др.] // Rev. Mod. Phys. 2002. March. Т. 74, № 1. С. 145–195.
2. The security of practical quantum key distribution / Valerio Scarani, Helle Bechmann-Pasquinucci, Nicolas J Cerf [и др.] // Reviews of Modern Physics. 2009. Т. 81, № 3. С. 1301.
3. Hughes Richard, Nordholt Jane. Refining quantum cryptography // Science. 2011. Т. 333, № 6049. С. 1584–1586.
4. Lam PK, Ralph TC. Quantum cryptography: Continuous improvement // Nature Photonics. 2013. Т. 7, № 5. С. 350–352.
5. Dieks DGBJ. Communication by EPR devices // Physics Letters A. 1982. Т. 92, № 6. С. 271–272.
6. Lounis Brahim, Moerner WE. Single photons on demand from a single molecule at room temperature // Nature. 2000. Т. 407, № 6803. С. 491–493.
7. Benjamin Simon. Single photons" on demand" // Science. 2000. Т. 290, № 5500. С. 2273–2274.
8. 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.
9. Nielsen Michael A, Chuang Isaac L. Quantum computation and quantum information. Cambridge university press, 2010.
10. А.С. Холево. Квантовые системы, каналы, информация. МЦНМО, 2010.

11. Bennett Charles H. Quantum cryptography using any two nonorthogonal states // Physical Review Letters. 1992. Т. 68, № 21. С. 3121.

12. 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.

13. Wootters W. K., Zurek W. H. A single quantum cannot be cloned // Nature. 1982. oct. Т. 299, № 5886. С. 802–803.

14. 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.

15. 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.

16. Generalized privacy amplification. / Charles H. Bennett, Gilles Brassard, Claude Crépeau [и др.] // IEEE Transactions on Information Theory. 1995. Т. 41, № 6. С. 1915–1923.

17. 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.

18. Ekert Artur K. Quantum cryptography based on Bell's theorem // Physical review letters. 1991. Т. 67, № 6. С. 661–663.

19. 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.

20. Baigneres Thomas. Quantum Cryptography: On the Security of the BB84 Key-Exchange Protocol: Tech. Rep.: : 2003.

21. 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.

22. 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. T. 80, № 8. C. 563–567.

23. Acín Antonio, Gisin Nicolas, Scarani Valerio. Coherent-pulse implementations of quantum cryptography protocols resistant to photon-number-splitting attacks // Physical Review A. 2004. T. 69, № 1. C. 012309.

24. Dusek Miloslav, Jahma Mika, Lütkenhaus Norbert. Unambiguous state discrimination in quantum cryptography with weak coherent states // Physical Review A. 2000.

25. 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. T. 92. C. 057901.

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

27. 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. T. 109, № 4. C. 557–584.

28. Renner Renato. Security of Quantum Key Distribution. 2006. jan. URL: http://arxiv.org/abs/quant-ph/0512258v2; http://arxiv.org/pdf/quant-ph/0512258v2.

29. Holevo A.S. An introduction to quantum information theory // MCCME (Publishing House of Moscow Independent University). 2002.

30. Bennett Charles H, Brassard Gilles, Robert Jean-Marc. Privacy amplification by public discussion // SIAM journal on Computing. 1988. T. 17, № 2. C. 210–229.

31. Carter Larry, Wegman Mark N. Universal Classes of Hash Functions // Journal of Computer and System Sciences. 1979. T. 18, № 2. C. 143–154.