МОСКОВСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ ИМЕНИ М.В. ЛОМОНОСОВА
ФАКУЛЬТЕТ ВЫЧИСЛИТЕЛЬНОЙ МАТЕМАТИКИ И КИБЕРНЕТИКИ

Большаков Роман

Релятивистская квантовая криптография

Курсовая работа

Научный руководитель
профессор Молотков С.Н.

Москва
2014

Содержание

Введение

Квантовое распределение ключей (QKD) — концепт секретного распределения ключей, основанный на фундаментальных законах квантовой механики. Квантовая криптография [1–6] 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) [1, 7–9], 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 [10]) 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 [11, 12], и *2*) наличие потерь в квантовом канале связи.

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 [4]. 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 кванто-

[1] Величина критической ошибки определяется конкретным протоколом

вой механики на различимость квантовых состояний, использует дополнительные ограничения, диктуемые специальной теорией относительности.

1 Основные особенности протокола релятивистского квантового распределения ключей

Обычная, нерелятивистская, квантовая криптография основывается на фундаментальных принципах квантовой механики, однако, не привязана к элементарным частицам или другим физическим обхектам, которые несут передаваемые квантовые состояния. В описываемом протоколе *релятивистской* квантовой криптографии это должна быть безмассовая частица, движущаяся со скоростью света, например, фотон. Это имеет значение, если принять во внимание пространственно-временную структуру коммуникации в пространстве Минковского, обращающейся к невозможности передать информацию быстрее, чем со скоростью света. Эта явная связь с пространством-временем совершенно игнорируется в обычных протоколах квантового распределенеия ключей.

Описываемый протокол основан на протяженных по времени когерентных квантовых состояниях. Благодаря их протяженной природе, проведенная атака «прием-перепосыл» неизбежно повлечет детектируемые задержки. Таким образом, детектирование действий подслушивателя может быть проведено учетом как ошибок, так и задержек сигнала. Это автоматически делает протокол полностью невосприимчивым к произвольным большим потерям в квантовом канале связи и создает потенциал для его использования в системах земля-спутник для создания глобального сервиса распределения ключей.

Так как задержки сигнала играют критическую роль в релятивистском подходе, протокол жизнеспособен только в каналах связи на открытом пространстве, расположенных по линии взгляда, где не существует более короткого пути меж двух сторон, и сигнал распространяется со скоростью света. Важно заметить, что протокол терпим к наличию воздуха на пути света, что немного задерживает сигнал по сравнению со скоростью света; это приводит лишь к необходимости достаточной протяженности по времени передаваемых квантовых состояний. В типичных условиях необходима протяженность примерно на 1 нс на каждый километр в воздухе.

Несмотря на то, что отслеживание точного времени требует, в общем случае, внешней синхронизации часов, описываемый протокол берет заботу о синхронизации между Алисой и Бобом на себя, никаких других схем внешней синхронизации не нужно. В то же время протоколу необходимо априорное знание расстояния между сторонами коммуникации, что требуется, например, если подслушиватель Ева пытается замедлить любую передачу между Алисой и Бобом.

Итак, основные особенности протокола включают в себя: *1*) протяженность квантовых состояний не обязана быть столь же большой, какова длина канала связи; она только лишь должна компенсировать задержки в канале относительно идеального канала со скоростью передачи равной скорости света в вакууме; *2*) так как релитявистские принципы позволяют провести синхронизацию часов, внешние схемы синхронизации не требуются; *3*) протокол предоставляет безусловную секретность ключа даже при использовании обычных слабых лазерных импульсов при сколь угодно больших потерях в канале связи; практические ограничения на потери определяются только темновыми шумами используемого детектора.

2 Общая идея релятивистского квантового распределения ключей через открытое пространство без синхронизации часов

- Алиса и Боб контролируют области пространства, необходимые для приготовления и измерения протяженных квантовых состояний.

- 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).

- Происходит передача серии состояний Алисой. Каждая посылка происходит в случайный момент времени внутри интервала ΔT. Достаточно, чтобы Алиса случайно выбирала один из двух моментов посылки сигнала внутри интервала ΔT (рис 1). Алиса готовит протяженное классическое состояние, состоящее из пары интенсивных когерентных пакетов, разделенных интервалом $l > l_{pac}$ (l_{pac} — ширина пакета, см. ниже): $|\alpha_c\rangle_1 \otimes |\alpha_c\rangle_2$ (индексы «1» и «2» отвечают пакетам, локализованным в моменты времени 1 и 2, рис 2); среднее число фотонов в состоянии $\mu_c = |\alpha_c|^2 \gg 1$. Временное разрешение проводится с точностью до ширины пакета l_{pac} (интервалы времени, меньшие l_{pac}/c, считаются нулевыми). Момент времени $t_{A,i}$ посылки состояния в канал связи Алисой фиксируется по своим часам.

- Аппаратура Боба на приемной стороне работает в ждущем режиме. При помощи быстрого классического детектора Боб фиксирует момент прихода состояния в каждой i-й посылке $t_{B,i}$. Далее классический сигнал ослабляется до квазиоднофотонного уровня, и при помощи фазового модулятора на одну из «половинок» (заднюю) случайным образом навешивается фаза. Состояние $|\alpha\rangle_1 \otimes |e^{i\varphi_B}\alpha\rangle_2$ ($\mu = |\alpha|^2 < 1$) направляется обратно к Алисе [2]. Значение относительной фазы у двух импульсов $\varphi_B = \varphi_0$ отвечает выбору логического 0 в ключе, а $\varphi_B = \varphi_1$ — логической 1. Кодирование осуществляется на стороне Боба.

- Алиса, зная расстояние L и время отправки $t_{A,i}$ по своим часам своего состояния в канал связи, знает время прихода квантового состояния от Боба $t'_{A,i}$, преобразует состояния, случайно и независимо от Боба изменяет 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 результате Алиса знает, какой бит ключа посылал Боб.

- После проведения серии посылок Боб сообщает Алисе интервалы времени между соседними посылками (рис 1), которые он фиксировал по своим часам. Алиса сравнивает их со своими интервалами времени между посылками по своим часам. Подсчитывается доля их несовпадений η. Соседние посылки, интервалы между которыми не совпали, Алиса и Боб отбрасывают.

- Далее часть последовательности Алисой и Бобом раскрывается и сравнивается для оценки вероятности ошибки. Если ошибка меньше критической, то происходит исправление ошибок через открытый классический канал связи. Затем происходит сжатие очищенного ключа. В результате возникает секретный ключ, известный только Алисе и Бобу.

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

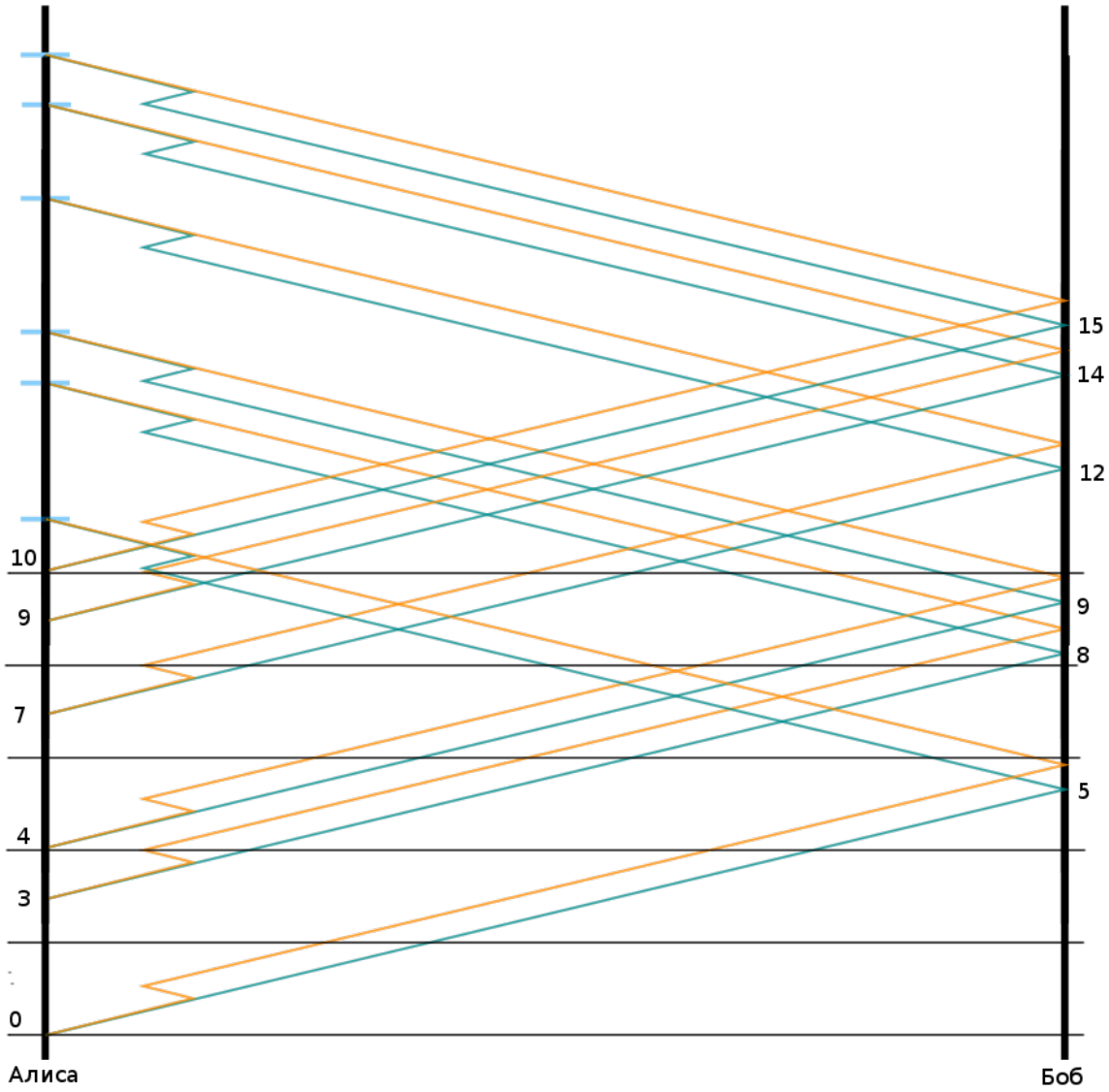

Рисунок 1: Пространственно-временная диаграмма, поясняющая посылку классических и прием квантовых состояний в случайные моменты. Слева и справа с помощью «0» и «1» обозначены моменты посылки и приема состояния

Отметим, что Алиса и Боб не должны следить за средним числом долетевших посылок. Потери в канале связи, как будет показано позднее, вообще не входят в критерий секретности ключей.

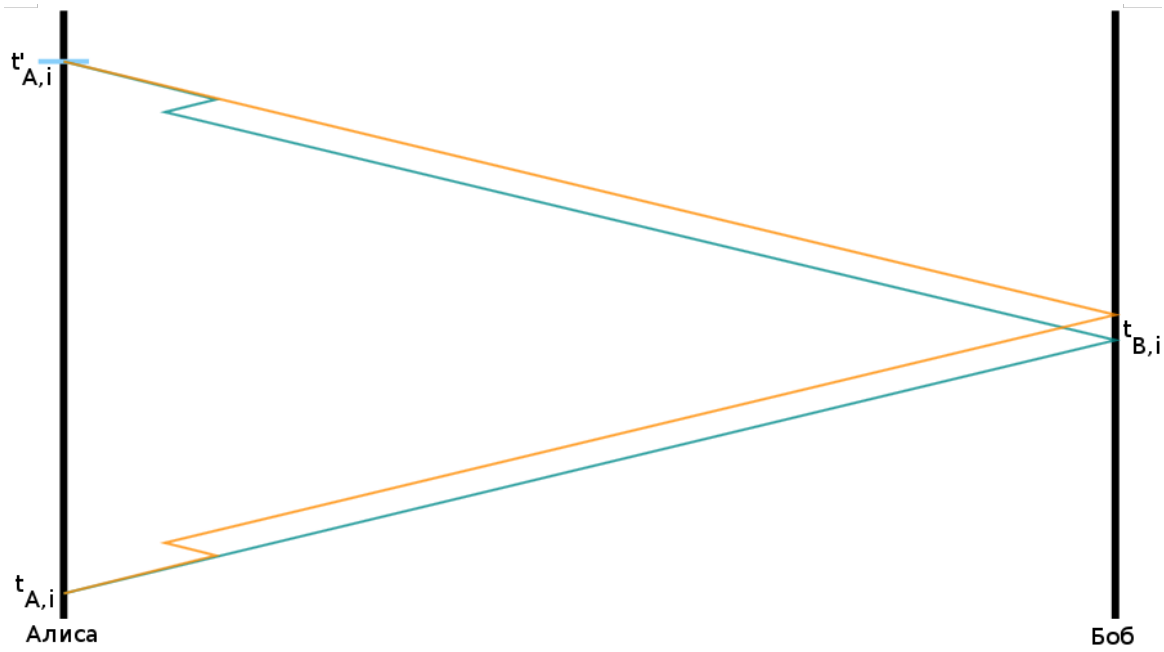

Рисунок 2: Пространственно-временная диаграмма, поясняющая процесс приготовления, преобразования и распространения протяженных квантовых состояний

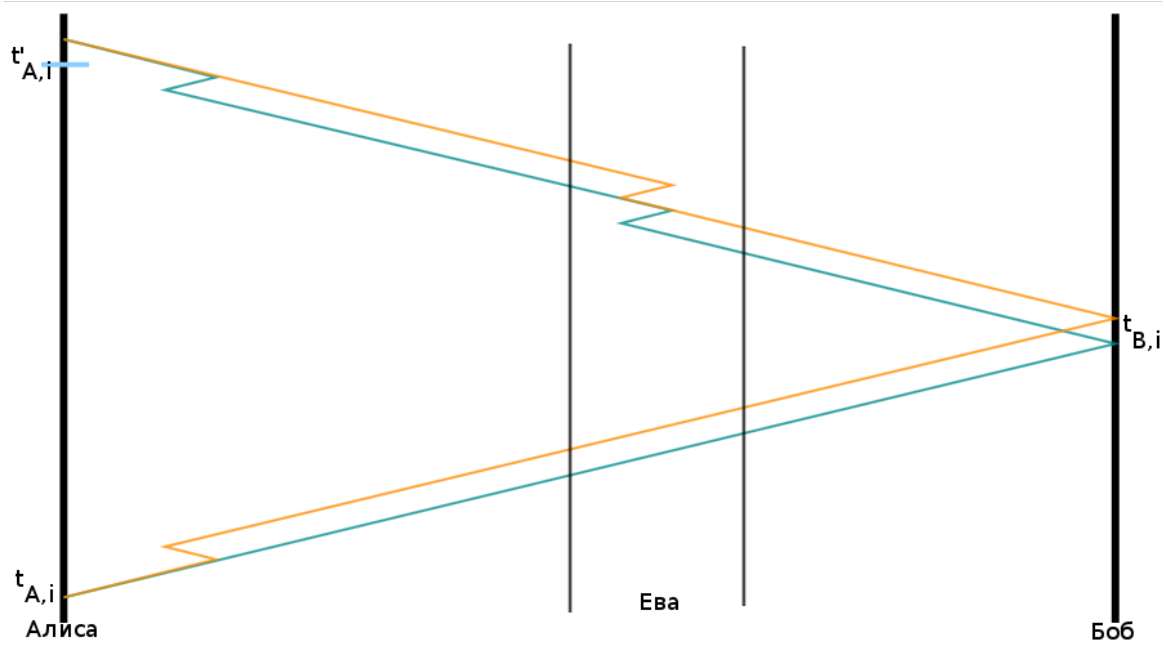

Рисунок 3: Пространственно-временная диаграмма, поясняющая причину задержек по времени протяженных состояний при подслушивании Евой

3 Технические подробности приготовления и измерения состояний

Алиса активирует лазер (рис. 4) в определенный момент времени и получает на выходе интенсивное когерентное состояние, локализованное в интервале l_{pac}. При прохождении через интерферометр локализованное состояние 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).

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.

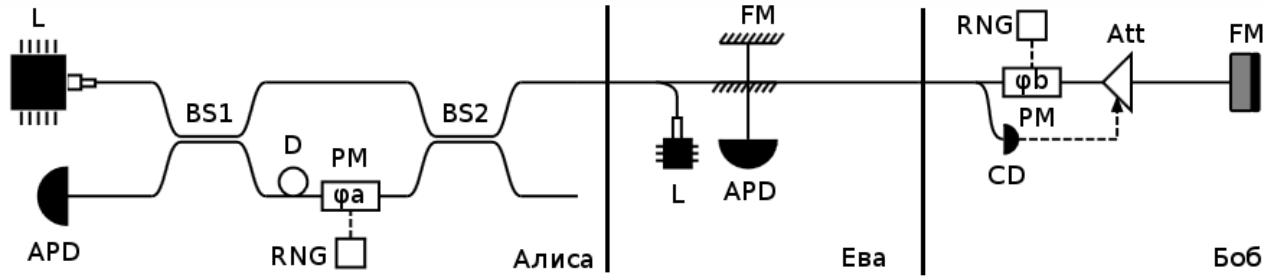

Рисунок 4: Двухпроходная оптическая схема приготовления, преобразования и детектирования состояний. L — лазер, APD — лавинный стробируемый однофотонный детектор, BS1, BS2 —интерферометр с разностью хода по нижнему и верхнему плечу, D — задержка в плече интерферометра, PM — фазовый модулятор, RNG — генератор случайных чисел, CD — быстрый классический детектор, Att — управляемый аттенюатор, FM — фарадеевское зеркало

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 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 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 $I - |e^{i\varphi_B}\alpha\rangle_2\ {}_2\langle e^{i\varphi_B}\alpha|$.

4 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.

4.1 Необходимость протяженности состояния и релятивизма

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 $|e^{i\varphi_B}\alpha\rangle_2$. Поскольку параметр α, описывающий когерентное состояние в шредингеровской картине, изменяется с оптической частотой ($\approx 10^{15}$ Гц), фаза параметра $\alpha = |\alpha|e^{i\theta}$ в каждой посылке случайно распределена на интервале $[0; 2\pi]$. Поэтому при доступе только к одной половинке (причем любой) Ева видит состояние, которое описывается матрицей плотности

$$\rho_i = \int_0^{2\pi} \frac{d\theta}{2\pi} |\sqrt{\mu}e^{i(\varphi_{iB}+\theta)}\rangle_i \, {}_i\langle\sqrt{\mu}e^{-i(\varphi_{iB}+\theta)}| = e^{-\mu}\sum_{n=0}^{\infty}\frac{\mu^n}{n!}|n\rangle_i \, {}_i\langle n| \tag{1}$$

$$i = 1, 2, \ \sqrt{\mu} = |\alpha|, \ \varphi_{0B} = \varphi_B, \ \varphi_{1B} = 0.$$

Из (1) видно, что информация о фазе при доступе только к одной половинке полностью теряется.

При доступе к двум половинкам состояние, которое видит Ева, уже зависит от относительной фазы φ_B, несущей информацию о ключе. Действительно,

$$\rho(\varphi_B) = \int_0^{2\pi} \frac{d\theta}{2\pi} |\sqrt{\mu}e^{i(\varphi_B+\theta)}\rangle_1 \, {}_1\langle\sqrt{\mu}e^{-i(\varphi_B+\theta)}| \otimes |\sqrt{\mu}e^{i\theta}\rangle_2 \, {}_2\langle\sqrt{\mu}e^{-i\theta}| =$$

$$e^{-2\mu}\sum_{n,k,n',k'=0}^{\infty} e^{i\varphi_B(n-n')}\frac{\mu^{\frac{n+k-n'-k'}{2}}}{\sqrt{n!k!n'!k'!}}|k\rangle_1 \otimes |n\rangle_2 \, {}_2\langle n'| \otimes \, {}_1\langle k'|\delta_{n+k,n'+k'}. \tag{2}$$

Таким образом, для получения информации о ключе необходим 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. 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 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), 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 и формулу (1)). 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 пытаться 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.

4.2 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 [4]. 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 [4]. В даннном случае ошибки неизбежны из-за нехватки времени (релятивистское ограничение) и неортогональности квантовых состояний (квантовомеханический запрет на достоверную различимость неортогональных состояний).

5 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 $I(A;B) = I(A;E)$ [13]:

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

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 [14]. 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. 5a, а зависимость R от среднего числа фотонов при заданной наблюдаемой ошибке показаны на рис. 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. 5, протокол обеспечивает достаточно большую критическую ошибку (до 35%, рис. 5a). Кроме того, среднее число фотонов при $Q = 0$ формально может быть любым (рис 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.

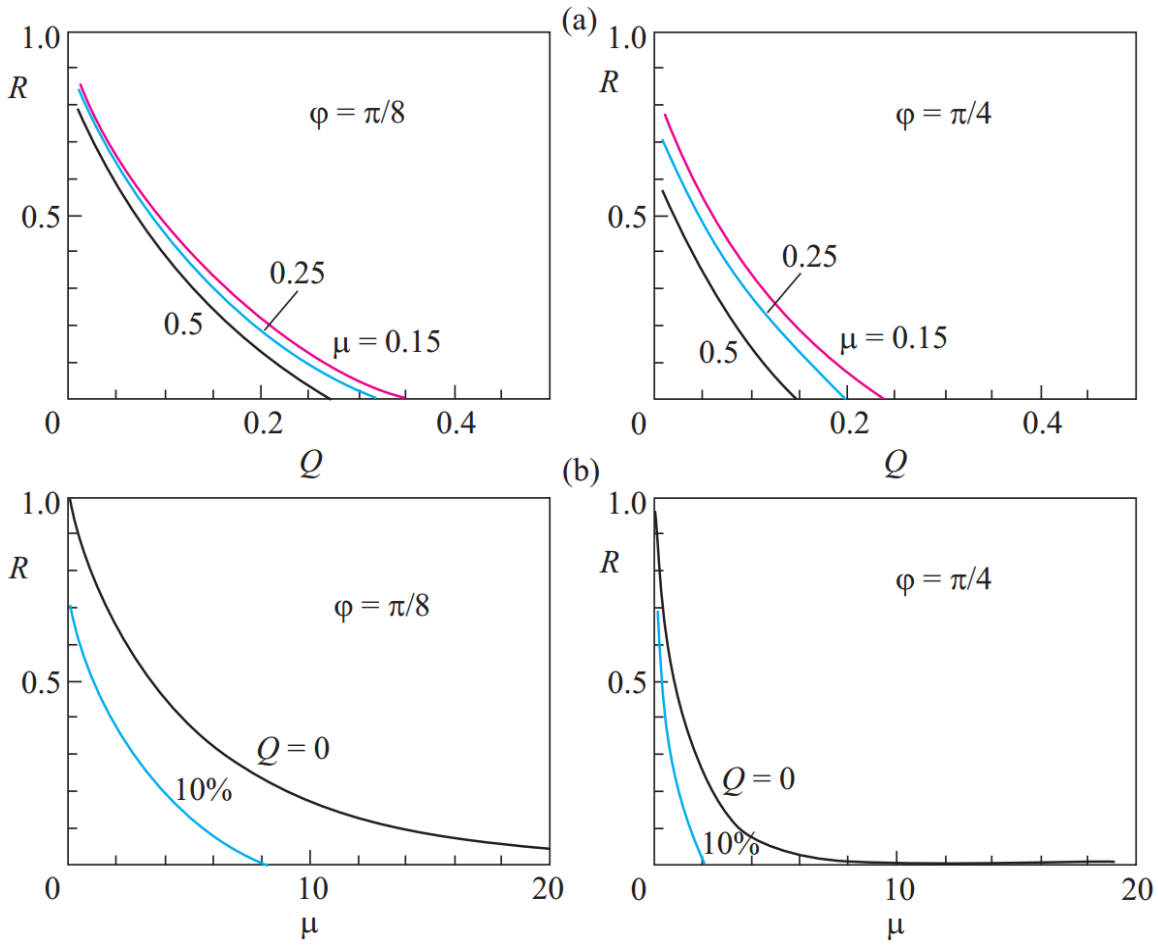

Рисунок 5: Зависимость длины секретного ключа R от наблюдаемой ошибки (a) и среднего числа фотонов (b)

Заключение

Рассмотрен протокол квантовой криптографии, который максимально использует фундаментальные ограничения, диктуемые законами природы, на различимость квантовых состояний. Данная схема может быть использована для передачи ключей через открытое пространство как между наземными объектами, так и через низкоорбитальные спутники. Двухпроходность схемы обеспечивает большую стабильность ее работы по сравнению с однопроходными схемами.

Кроме того, разработана программа, визуализирующая процесс распределения ключей по описанному протоколу, с имитацией атак Евы и последующим детектированием возникающих из-за этого задержек. ПО требует для своей работы установленного .NET Framework 4.5, исходные коды доступны по адресу: http://github.com/rombolshak/Requc

Список литературы

1. 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.

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

3. Quantum cryptography / N. Gisin, G. Ribordy, W. Tittel [и др.] // Rev. Mod. Phys. 2002. March. Т. 74, № 1. С. 145–195.

4. 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.

5. Hughes Richard, Nordholt Jane. Refining quantum cryptography // Science. 2011. Т. 333, № 6049. С. 1584–1586.

6. Lam PK, Ralph TC. Quantum cryptography: Continuous improvement // Nature Photonics. 2013. Т. 7, № 5. С. 350–352.

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

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

9. Dieks DGBJ. Communication by EPR devices // Physics Letters A. 1982. Т. 92, № 6. С. 271–272.

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

11. Lounis Brahim, Moerner WE. Single photons on demand from a single molecule at room temperature // Nature. 2000. Т. 407, № 6803. С. 491–493.

12. Benjamin Simon. Single photons"on demand-// Science. 2000. Т. 290, № 5500. С. 2273–2274.

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

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