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 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), 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, 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 [1] [2-6] 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. 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 наличия 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 являетс 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 случайны выбирала один из двух моментов посылки сигнала внутри интервала ΔT. 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); 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 мужде сосендними посылками, 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 классчисеский канал связи. Затем происходит сжатие

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

очищенного ключа. В результате возникает секретный ключ, известный только Алисе и Бобу.

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.

3 Технические подробности приготовления и измерения состояний

Алиса активирует лазер в определенныый 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.

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 **??** отражает последовательное преобразование состояний по оптическому тракту.

На входе лавинного фотодетектора в центральном временно 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 $|e^{i\varphi_B}\alpha\rangle_{22}\langle e^{i\varphi_B}\alpha|$ и на его ортогональное дополнение $I - |e^{i\varphi_B}\alpha\rangle_{22}\langle e^{i\varphi_B}\alpha|$.

Список литературы

1. Автор. Название книги / под ред. Редактор. Издательство, 2012.