

МЕТОДИЧЕСКИЕ ЗАМЕТКИ

Релятивистское квантовое распределение ключей между стационарными объектами на когерентных состояниях

С.П. Кулик, С.Н. Молотков

Совместные ограничения квантовой механики и специальной теории относительности открывают новые возможности для квантовых коммуникаций. В данном сообщении обсуждается протокол релятивистского квантового распределения ключей (КРК) через открытое пространство. Протокол не требует однофотонных состояний, достаточно ослабленных когерентных состояний лазерного излучения. При небольшом среднем числе фотонов в когерентных состояниях состояния с разными значениями относительной фазы не могут быть достоверно различимы. Не нужно использовать состояния "ловушки", как в decoy state-методе, которые являются обязательными для нерелятивистских протоколов КРК, что упрощает оптическую часть на приёмной стороне, и позволяет обойтись без активных элементов — фазового модулятора. На передающей стороне не требуется модулятор интенсивности, который необходим для реализации decoy state-метода в нерелятивистских системах. Протокол обеспечивает распределение ключей при больших потерях в линии связи ≈ 60 дБ. В протоколе используются только два информационных состояния, поэтому не нужно согласование базисов, все зарегистрированные послышки используются в ключе, что увеличивает скорость распределения ключей. Наиболее подходящим применением релятивистских систем КРК является распределение ключей между стационарными неподвижными объектами, например, станциями сотовой связи или другими объектами, прокладка волоконной линии между которыми является дорогостоящей или практически невозможной. В отличие от анализа криптостойкости нерелятивистских систем КРК, в котором используется довольно изощрённый математический аппарат, анализ стойкости релятивистского КРК проводится на интуитивно понятном для физической аудитории уровне, не требует предварительных специальных знаний и доступен аспирантам и студентам старших курсов университетов, знакомым с основами квантовой оптики, квантовой информатики и квантовой криптографии в объёме стандартных университетских курсов.

Ключевые слова: специальная теория относительности, квантовая криптография в свободном пространстве, когерентные состояния

PACS numbers: 03.30.+p, 03.67.Dd, 89.70.-a

DOI: <https://doi.org/10.3367/UFN.2026.08.040188>

Содержание

1. Введение (1086).
2. Информационные состояния (1088).
3. Релятивистские ограничения на различимость протяжённых квантовых состояний (1089).
4. Измерение состояний на приёмной стороне (1089).

5. Анализ различных атак (1091).
5.1. Унитарная атака. 5.2. Унитарная атака с предварительной посылкой передней части состояния. 5.3. Прозрачная атака со светоделителем. 5.4. Атака с измерениями с определённым исходом и предварительной посылкой передней части состояния.
 6. Некоторые численные примеры (1094).
 7. Заключение (1095).
- Список литературы (1096).

С.П. Кулик^(1,*), С.Н. Молотков^(2,3)

⁽¹⁾ Центр квантовых технологий,
Московский государственный университет им. М.В. Ломоносова,
Ленинские горы 1, стр. 35, 119991 Москва,
Российская Федерация

⁽²⁾ Академия криптографии Российской Федерации,
а/я 100, 119331 Москва, Российская Федерация

⁽³⁾ Институт физики твёрдого тела им. Ю.А. Осипьяна РАН,
ул. Академика Осипьяна 2, 142432 Черноголовка,
Московская обл., Российская Федерация

E-mail: * kuliksp@my.msu.ru

Статья поступила 16 октября 2024 г.,
после доработки 13 апреля 2026 г.

1. Введение

Квантовая криптография направлена на решение главной проблемы симметричной криптографии — проблемы распределения ключей [1].

Квантовое распределение ключей (КРК) основано на фундаментальных ограничениях квантовой теории на различимость квантовых состояний.

1) Одно из таких ограничений формализуется в виде известной теоремы о запрете копирования (клонирования) неизвестного квантового состояния — *no cloning theorem* [2].

2) Второе ограничение квантовой механики — невозможно извлечь информацию о *неортогональных состояниях* без их возмущения [3]. *Ортогональные состояния* могут быть достоверно различимы без возмущения.

Данные ограничения фактически следуют из линейности квантовой теории, и более формально из того факта, что пара *наблюдаемых*, которым в квантовой механике отвечают *эрмитовы операторы*, не может иметь общей системы собственных векторов, если операторы не коммутируют.

3) Третье ограничение относится к составным квантовым системам, что имеет место в квантовом распределении ключей — передатчик (Алиса), приёмник (Боб), нарушитель (Ева), и связано с явлением *квантовой запутанности*, которая приводит к *энтропийным соотношениям неопределённости для составных квантовых систем* [4, 5]. Данные соотношения связывают верхнюю границу для утечки информации к третьей квантовой подсистеме — нарушителю, со степенью запутанности двух подсистем из составной системы [4, 5].

Квантовое распределение ключей, по сути, представляет собой согласование двух независимых случайных последовательностей на передающей и приёмной сторонах посредством посылки квантовых состояний.

Первое ограничение запрещает, без знания передаваемого квантового состояния, сделать из него копию, а значит и множество копий, измерение которых позволит достоверно узнать передаваемое состояние и, соответственно, передаваемый бит ключа.

Второе ограничение гарантирует, что любая попытка получить информацию о передаваемом состоянии, неизбежно приведёт к его возмущению, и обнаружению вторжения в квантовый канал связи. По этой причине в протоколах квантовой криптографии всегда используется набор состояний, который обязательно содержит внутри себя неортогональные состояния.

Третье ограничение позволяет количественно связать степень возмущения передаваемого квантового состояния с верхней границей утечки информации к нарушителю. Степень возмущения состояний проявляется через ошибки, возникающие на приёмной стороне.

Все, упомянутые выше, ограничения, по сути, связаны с геометрическими свойствами пространства состояний квантовых систем, и в них никак не фигурирует тот факт, что квантовые состояния приготавливаются и распространяются в пространстве-времени Минковского. Измерения и их исходы над квантовыми состояниями также имеют место в пространстве-времени Минковского.

В нерелятивистских системах КРК используются квазидвухфотонные состояния — ослабленные когерентные состояния лазерного излучения, которые представляют собой *суперпозицию фоковских состояний с разным числом фотонов*. Существующие стандартные лавинные телекоммуникационные фотодетекторы не способны различать компоненты состояний с разным числом фотонов. Поскольку в нерелятивистских системах КРК секретные ключи формируются только из однофотонной компоненты когерентных состояний, то для оценки доли однофотонной компоненты в когерентных состояниях, достигающей приёмной стороны, был разработан decoy state method [6–9].

В реальных условиях квантовыми носителями информации являются фотоны, которые в вакууме распространяются с предельно допустимой скоростью — скоростью света.

Кроме фундаментальных ограничений на различимость квантовых состояний, связанных с неортогональностью, существуют ограничения, связанные с принципом релятивистской причинности — фактически с конечной скоростью света. Ни классические сигналы, ни квантовые состояния не могут распространяться быстрее света.

В волоконных системах КРК передача квантовых состояний происходит в волокне, где скорость распространения света примерно в полтора раза меньше, чем в открытом пространстве (вакууме). По этой причине ограничения на различимость квантовых состояний, связанные с предельной скоростью света, применительно к волоконным системам КРК, не работают (см. ниже).

В системах КРК, работающих через открытое пространство, релятивистские ограничения открывают принципиально новые возможности для квантового распределения ключей. Тот факт, что скорость света в атмосфере несколько меньше скорости света в вакууме, не играет принципиальной роли, поскольку показатель преломления воздуха отличается от единицы в четвёртом знаке после запятой (см. ниже).

Общая идея использования релятивистских ограничений для КРК связана с приготовлением и измерением протяжённых в пространстве–времени квантовых состояний. Далее для краткости будем называть такие состояния просто протяжёнными (см. детали ниже).

Измерение протяжённых квантовых состояний с целью их различения, из-за нормировки квантовых состояний, требует доступа ко всей области пространства–времени, где состояния присутствуют (локализованы). Доступ к конечной области пространства, где локализовано квантовое состояние, требует конечного времени, связанного с размером данной области, что будет приводить к задержкам при измерениях, которые детектируются на приёмной стороне.

Первый протокол релятивистского КРК был предложен в [10]. В этом протоколе использовались однофотонные фоковские состояния, которые посылались в канал связи в случайные моменты времени. В данном протоколе квантовые состояния "растягивались" на всю длину канала связи, что практически невозможно реализовать на практике. В протоколе [10] квантовые состояния при передаче целиком не присутствовали в канале связи. В этом смысле, данный релятивистский протокол отчасти близок к нерелятивистскому протоколу, когда квантовое состояние никогда целиком не присутствует в канале связи [11].

Впоследствии было предложено несколько вариантов релятивистских протоколов КРК [12–21]. Были также реализованы экспериментальные демонстраторы релятивистских систем КРК [17, 18].

Важно отметить, что, поскольку релятивистское КРК происходит в реальном пространстве–времени Минковского, то расстояние L между приёмной и передающей станциями является параметром протокола. Требуется также синхронизация часов. В двупроходном варианте систем КРК синхронизация часов не требуется [15, 18].

В предыдущих релятивистских протоколах КРК [12–21], анализ стойкости проводился в основном для однофотонных состояний.

Зачем нужен поиск новых протоколов КРК, и что принципиально нового предлагается в данном сообщении? Новые протоколы КРК нужны для того, чтобы увеличить критическую ошибку, соответственно, дальность и допустимые потери в квантовом канале, до которых можно гарантированно распределять секретные ключи. Кроме того, протокол КРК должен быть реализуем наиболее простыми техническими средствами, насколько это допустимо. Предлагаемый релятивистский протокол КРК как раз и решает данную задачу.

Принцип релятивистский причинности вместе с ограничениями квантовой механики позволяет использовать не строго однофотонные состояния, а когерентные состояния ослабленного лазерного излучения без состояний "ловушек", как это необходимо в decoy state методе в нерелятивистских системах КРК [6–9]. Будет показано, что достаточно только двух информационных ослабленных когерентных состояний, что значительно упрощает реализацию системы КРК. Приёмная часть системы КРК не содержит никаких активных оптических компонентов, таких как контроллеры поляризации и фазовые модуляторы. На передающей стороне, не требуется модулятор интенсивности для приготовления состояний "ловушек", как это необходимо в нерелятивистских системах КРК [6–9].

Далее, поскольку релятивистский протокол КРК происходит в реальном пространстве–времени, то анализ криптостойкости протокола по сравнению с нерелятивистскими протоколами КРК радикально упрощается и становится более понятным на уровне физической интуиции.

Отметим следующее обстоятельство. Поскольку системы КРК представляют собой криптографический продукт, то использованием систем КРК как криптографического продукта требует лицензирования. Процесс лицензирования, это достаточно длительный итерационный процесс, который включает в себя уточнение имеющихся исследований по секретности ключей, соответствие математической схемы технической, программной реализации системы и т.д.

Цель данной заметки состоит в том, чтобы донести до аудитории физические идеи, на которых базируется секретное распределение ключей, при этом не перегружая изложение излишним математическим аппаратом и подробностями технической реализации, а также нюансами процесса лицензирования.

2. Информационные состояния

Возможны два способа кодирования логических 0 и 1 в информационные состояния.

Первый способ использует поляризационное кодирование. В атмосфере, в отличие от волокна, состояние поляризации сохраняется. Однако, даже для неподвижных объектов ориентация осей в плоскости нормальной направлению распространения, соединяющего приёмник и передатчик, может изменять относительное положение, поэтому, для правильной регистрации состояний поляризации, требуется совпадение координатных осей в нормальной плоскости у передатчика и приёмника.

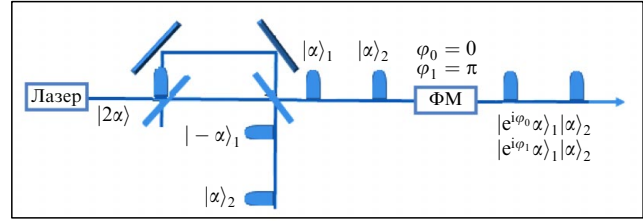


Рис. 1. Реализация передающей части. В каждом такте, включением Лазера, готовится локализованное когерентное состояние $|2\alpha\rangle = |\exp(i\theta)|\alpha\rangle$, со средним число фотонов $|2\alpha|^2$, фаза θ когерентного состояния случайна в каждой посылке, $\theta \in [0, 2\pi]$, что обычно достигается включением/выключением лазера. После прохождения интерферометра Маха–Цандера, на выходе возникает пара идентичных когерентных состояний $(|\alpha\rangle_1|\alpha\rangle_2)$, сдвинутых по времени на разность хода в плечах интерферометра. При прохождении состояния $|\alpha\rangle_1$ через фазовый модулятор (ФМ), относительная фаза (ϕ_0 или ϕ_1) состояния изменяется в зависимости от того, какой логический бит ключа передаётся. Для идеальных светоделителей 50/50 в интерферометре состояния $|\alpha\rangle_1$ и $|\alpha\rangle_2$ по сути одинаковы, но сдвинуты относительно друг друга на разность хода по верхнему и нижнему пути в интерферометре. На практике из-за неидеальности светоделителей фазы α в первом и втором состоянии могут отличаться. Стандартно данная неидеальность устраняется соответствующей калибровкой напряжения на фазовом модуляторе, таким образом, чтобы в канал выходили состояния $|\exp(i\phi_{0,1})\alpha\rangle_1|\alpha\rangle_2$ с правильным значением относительной фазы $\phi_0 = 0, \phi_1 = \pi$.

Второй способ — фазовое кодирование. Биты ключа кодируются в относительную фазу пары независимых когерентных состояний (см. рис. 1, 2). В этом случае не требуется согласование оптических осей в плоскости, нормальной направлению распространения от передатчика к приёмнику.

Ниже используем фазовый способ кодирования. Оптическая схема передающей станции имеет стандартный вид рис. 1.

В протоколе используются два когерентных состояния:

$$\begin{cases} 0 \rightarrow |0\rangle = |\exp(i\phi_0)\alpha\rangle_1 \otimes |\alpha\rangle_2 \\ 1 \rightarrow |1\rangle = |\exp(i\phi_1)\alpha\rangle_1 \otimes |\alpha\rangle_2 \end{cases} \quad \phi_0 = 0, \quad \phi_1 = \pi. \quad (1)$$

Индексы 1 и 2 отвечают состояниям локализованным во временных окнах 1 и 2 (см. рис. 1, 2).

Важно отметить, что состояние $|\pm\alpha\rangle_1$, несущее информацию о логическом бите в относительной фазе, поступает в квантовый канал связи с задержкой по времени. Первым в канал поступает состояние $|\alpha\rangle_2$, которое не несёт информацию о логическом бите и служит для "привязки" общей фазы.

"Протяжённость" когерентных состояний в (1) $\tau \ll T$, где T — раздвижка состояний по времени, L — расстояние между передающей и приёмной станциями, которое фиксировано и является параметром протокола. Часы на приёмной и передающей станциях синхронизированы. Система без синхронизации часов рассмотрена в [15], в [18] приведён экспериментальный демонстратор такой системы. Фаза $\theta \in [0, 2\pi]$ ($\alpha = \exp(i\theta)|\alpha\rangle$) когерентного состояния в каждой посылке случайна (рандомизирована), что технически достигается стандартным образом, включением/выключением лазера в каждой посылке.

Отметим, что в каждой посылке в канале присутствует чистое когерентное состояние (1) со случайной фазой,

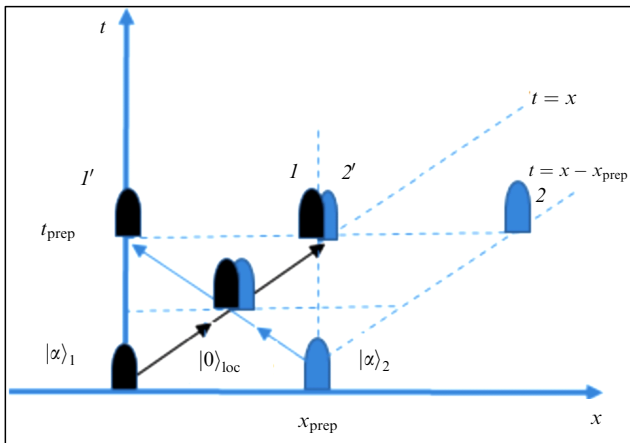


Рис. 2. Распространение половинок состояний в открытом пространстве происходит по ветвям светового конуса (скорость света $c = 1$). Пример преобразования протяжённого квантового состояния $|\exp(i\varphi_0)\alpha\rangle_1 \otimes |\alpha\rangle_2$ в одну точку пространства–времени — накрытие прошлой частью светового конуса двух половинок, и сведение их в локализованное состояние $|0\rangle_{\text{loc}}$ для измерений. В зависимости от исхода измерений приготавливается новое протяжённое состояние — локализованное состояние "выпускается" в переднюю часть светового конуса. Новое протяжённое состояние состоит из двух половинок в моменты $1'$ и $2'$. Приготовление нового протяжённого состояния, состоящего из локализованных в моменты $1'$ и $2'$ половинок, диктуется процедурой измерения на приёмной стороне. Такое состояние, по сравнению с исходным состоянием 1 и 2 , сдвинуто по времени на расстояние между половинками. При предварительном приготвлении состояния, нарушитель вместо оригинальной половинки второго состояния, готовит свое состояние, а исходные состояния 1 и 2 сводит вместе. В зависимости от результата измерений в "точке пространства–времени" $(t_{\text{преп}}, x_{\text{преп}})$, нарушитель готовит заднюю половинку когерентного состояния с фазой относительно передней половинки, которая зависит от исхода измерений в точке $(t_{\text{преп}}, x_{\text{преп}})$. При предварительном приготвлении передней половинки состояния, ошибок на приёмной стороне, из-за задержки состояний нарушителем, не происходит. Ошибки с определённой вероятностью (см. ниже) возникают только из-за неправильного приготвления задней половинки, что связано с неортогональностью когерентных состояний, и соответственно, с принципиальной невозможностью достоверного различения состояний, отвечающих логическому 0 и 1.

которое является суперпозицией фоковских состояний с разным числом фотонов, а отнюдь не статистическая смесь фоковских состояний с определённым числом фотонов с пуассоновским распределением по числу фотонов. Подробное обсуждение данного факта см. в [22]. Когерентные состояния имеют поляризацию. Процедура приготовления информационных состояний такова, что состояние поляризации одинаково для состояний локализованных во временном окне 1 и окне 2 (см. рис. 2). Направление поляризации не существенно, и может быть любым.

После прохождения через атмосферный канал связи поляризация состояний может изменяться, но остаётся одинаковой для состояний, локализованных в окнах 1 и 2 , поскольку типичная раздвижка по времени T составляет несколько наносекунд, поэтому за такие времена относительное состояние поляризации во временных окнах 1 и 2 при распространении через канал связи не успевает измениться, поэтому состояние поляризации половинок на выходе из передающей станции не влияет на исходы измерений на приёмной стороне — не приводит к ошибкам, поэтому опускаем из рассмот-

рения поляризационные степени свободы для состояний.

Посылки состояний осуществляются в каждый такт времени. Поскольку расстояние между передающей и приёмной станциями известно, и часы синхронизированы, то известно штатное время прибытия состояния на приёмную станцию — время срабатывания детекторов.

3. Релятивистские ограничения на различимость протяжённых квантовых состояний

Обсудим подробно релятивистские ограничения на различение протяжённых квантовых состояний — различение требует конечного времени, которое зависит от протяжённости состояний в пространстве–времени Минковского.

Когерентные состояния (далее для краткости будем говорить "половинки") во временных окнах 1 и 2 *независимы*. Если фаза состояний θ ($\alpha = \exp(i\theta)|\alpha|$) в каждой посылке случайна, то для измерения *относительной фазы* двух "половинок" требуется сведение обеих половинок в одну точку пространства–времени (см. рис. 2).

Ограничения релятивистской причинности, при сведении двух состояний в одну точку пространства–времени, требуют "накрытия" всего состояния — двух половинок, прошлой частью светового конуса (см. рис. 2), что требует конечного времени T . После сведения вместе, состояния готовы для измерений с целью их различения. *Доступ отдельно только к половинкам состояний из-за случайной фазы θ не даёт информацию об относительной фазе.*

Поскольку на приёмной стороне перед детектированием состояний происходит сведение половинок вместе при помощи интерферометра (рис. 2, 3), то подслушиватель после различения состояний, должен приготовить исходные состояния из двух половинок.

Приготовление протяжённого состояния (1) также требует конечного времени T (см. рис. 2) — необходимо "выпустить" состояния в будущую (переднюю) часть светового конуса. Однако, данные состояния, из-за конечной скорости света, будут сдвинуты по времени по отношению к исходным состояниям, которые свободно распространялись бы в пространстве–времени (см. рис. 2).

Таким образом, процедура различения протяжённых состояний неизбежно приводит к сдвигу состояний в пространстве–времени по отношению к оригинальным состояниям, что неизбежно приводит, либо к задержкам, либо к ошибкам на приёмной стороне.

4. Измерение состояний на приёмной стороне

Прежде, чем рассмотреть измерения, подчеркнём, что при среднем числе фотонов в когерентных состояниях менее нескольких единиц, вероятность точного (достоверного) различения состояний всегда меньше единицы. Данный факт является базовым и широко известным результатом из квантовой оптики. Отличие от единицы вероятности успешного различения при малом числе фотонов связана с тем, что в этом случае, независимо от фазы когерентного состояния, в нём велика доля вакуумной компоненты. По этой причине, в квантовых протоколах (релятивистских и нерелятивистских) всегда используются *сильно ослабленные когерентные состояния*.

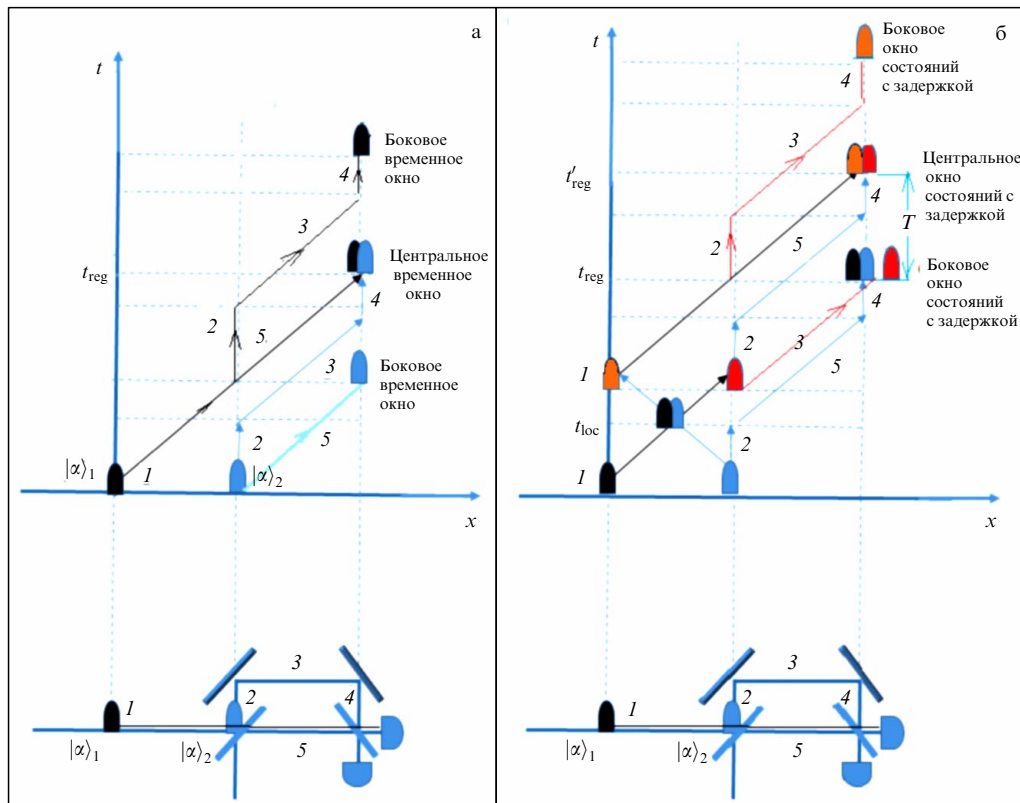


Рис. 3. Преобразование состояния 0 в приёмном интерферометре — (а) в штатном режиме без нарушителя и задержки состояний, (б) регистрация задержанных состояний из-за атаки нарушителя. (а) Чёрная линия отвечает прохождению задней половинки (1) (обозначена чёрным цветом) по верхнему длинному пути в интерферометре (1–4), по короткому нижнему пути (1–5). Красная линия отвечает прохождению передней половинки состояния (2) (обозначена голубым цветом) по короткому нижнему пути (2–5), и по длинному верхнему пути (2–4). В штатном режиме интерференция происходит в центральном временном окне в момент времени t_{reg} для состояний 1 и 2, прошедших соответственно, по нижнему пути и верхнему пути. В зависимости от входного состояния 0 или 1 конструктивная интерференция (фотоотсчёт) имеет место в верхнем или в нижнем детекторе. Состояние (1) прошедшее по верхнему длинному пути, и состояние (2), прошедшее по нижнему короткому пути не испытывают интерференции (обозначены как боковые — side состояния). (б) Прохождение через интерферометр задержанных состояний. Показаны красным цветом (2 — передняя половинка) и оранжевым цветом (1 — задняя половинка). Накрытие прошлой частью светового конуса оригинальных состояний — сведение их в одну точку пространства–времени происходит к моменту времени t_{loc} . По результатам измерений в момент времени t_{loc} , нарушитель готовит протяжённые состояния из двух половинок — "выпускает" состояния в будущую часть светового конуса — данные состояния оказываются задержанными на время T . Распространение через интерферометр задержанных состояний аналогично рис. 3а. Из-за задержки, по отношению к штатному распространению, передняя половинка состояния оказывается в центральном временном окне, в котором происходит детектирование. Поскольку данная половинка не испытывает интерференции, то отсчёты равновероятно будут как в верхнем, так и нижнем детекторах, в отличие от штатного состояния, которое даёт отсчёты только в одном из детекторов. Равновероятные отсчёты в обоих детекторах приводят к ошибке равной 1/2. Задержанные состояния интерферируют в более поздний момент t'_{reg} .

Для секретности распределяемых ключей важны как квантовость состояний, гарантирующая невозможность достоверного различения состояний, так и релятивистские ограничения — невозможность распространения состояний быстрее скорости света.

Разберём процедуру измерения на приёмной стороне и покажем, что задержка состояний неизбежно приводит к ошибкам, независимо от исхода измерения.

Наиболее удобным способом измерения на приёмной стороне, реализующим сведения пары половинок вместе, является использование интерферометра Маха–Цандера (см. рис. 3).

Пусть на интерферометр поступает одно из протяжённых состояний, например, отвечающее логическому 0 (см. рис. 3). Распространение состояний по плечам интерферометра показано на пространственно–временной диаграмме (см. рис. 3).

В отсутствии нарушителя для состояния логического 0 конструктивная интерференция имеет место в цент-

ральном временном окне на верхнем детекторе (см. рис. 3) — отсчёт на нижнем детекторе отсутствует, а для состояния логической 1 конструктивная интерференция имеет место на нижнем детекторе — отсчёт на верхнем детекторе отсутствует.

Если отсутствуют задержки в линии связи, то детектирование имеет место в момент времени $L + T$ (см. рис. 3). Если было вторжение в линию связи, то состояния 1 или 2 придут на приёмную станцию с задержкой на время T (см. рис. 3). Поэтому в штатный момент времени на приёмной станции будет регистрироваться не интерференционная составляющая состояний, а боковые состояния, которые не испытывают интерференции и одинаковы перед обоими детекторами, и не зависят от состояний для 0 и 1. Регистрация состояний с задержкой показана на рис. 3. Регистрация задержанных состояний в штатном временном окне приводит к ошибкам (см. детали описания в подписи к рис. 3).

5. Анализ различных атак

Обсудим различные атаки. Принципиальное отличие релятивистского протокола КРК, который является протоколом в реальном пространстве–времени, по сравнению с нерелятивистскими протоколами состоит в том, что Ева в каждой посылке должна действовать "на ходу" по мере возникновения доступа к состояниям.

5.1. Унитарная атака

Атака в тех посылках, в которых Ева проводит данную атаку приводит к вероятности ошибки Q на приёмной стороне равной $Q = 1/2$. Унитарная атака требует доступа ко всему пространству состояний — доступа одновременно к обеим половинкам, что требует сведение половинок вместе в одну точку пространства–времени.

После совместного унитарного преобразования над локализованными половинками и вспомогательным состоянием Евы (*ancilla*), необходимо растянуть локализованное и искажённое информационное состояние на две половинки — этого требует структура измерения на приёмной стороне.

Однако, из-за того, что время T (см. рис. 3) будет потеряно, то на приёмной стороне в центральном временном окне будет состояние, которое не испытывает интерференцию (см. рис. 3) — *side* состояние, которое будет давать отсчёт равновероятно в обоих детекторах, причём независимо от структуры унитарного преобразования. Равновероятные отсчёты в обоих детекторах, причём независимо от искажённого информационного состояния, приводят к вероятности ошибки $Q = 1/2$.

Оценим длину секретного ключа в пересчёте на одну зарегистрированную позицию на приёмной стороне. Пусть Ева атакует долю посылок p , остальная доля не атакуемых посылок есть $1 - p$. Чтобы не загромождать выкладки техническими деталями проведём рассмотрение в асимптотическом пределе длины передаваемых последовательностей.

Свяжем долю атакуемых посылок с вероятностью ошибки на приёмной стороне. Каждая атакуемая посылка из-за задержки состояний приводит к вероятности ошибки в $1/2$, имеем

$$\frac{1}{2} p = Q, \quad (2)$$

где Q — вероятность ошибки у Боба, откуда находим $p = 2Q$.

В пользу Евы, считаем, что в атакуемых посылках, в доле p , Ева достоверно знает передаваемые состояния¹, а в остальной доле $1 - p$ не атакуемых, Ева не знает передаваемые состояния. Для длины секретного ключа ℓ в пересчёте на одну посылку получаем

$$\ell = (1 - p) - h(Q) = (1 - 2Q) - h(Q), \quad (3)$$

где $h(Q) = -Q \log(Q) - (1 - Q) \log(1 - Q)$ — бинарная энтропийная функция Шеннона, все логарифмы по основанию 2.

¹ Хотя это не так из-за неортогональности когерентных состояний.

Формула (3) имеет интуитивно понятную интерпретацию. Первое слагаемое есть *дефицит информации Евы* относительно бита Алисы, второе слагаемое *нехватка информации Боба*, из-за ошибок, относительно бита Алисы. Разница нехватки информации Евы и Боба относительно бита Алисы является общим секретом Алисы и Боба.

Минимальное количество информации в битах — в шенноновском пределе, которое Алиса должна передать Бобу через открытый классический аутентичный канал связи для того, чтобы Боб мог, в асимптотическом пределе длинных последовательностей с вероятностью единица исправить все ошибки — свести свой дефицит информации к нулю, есть $h(Q)$.

5.2. Унитарная атака с предварительной посылкой передней части состояния

Предыдущая атака приводит к задержкам состояний, что неизбежно приводит к вероятности ошибок $Q = 1/2$ в посылках, которые атаковала Ева.

Атака Евы может быть улучшена. Ева может предварительно приготовить и послать к Бобу переднюю половинку своего когерентного состояния. Далее, Ева собирает обе половинки состояний от Алисы в одну точку пространства–времени (см. рис. 2). После этого Ева имеет доступ ко всему протяжённому состоянию и может проводить унитарную атаку. В результате атаки возникает искажённое информационное локализованное состояние — искажённая вторая половинка состояния Евы.

Из-за предварительной посылки передней половинки состояния Евой, задержек по времени регистрации состояний на приёмной стороне не возникает. Однако, из-за неортогональности информационных состояний, отвечающих 0 и 1, Ева гарантировано будет готовить заднюю половину состояния с ошибкой.

Найдём вероятность ошибки при регистрации состояний на приёмной стороне для данной атаки.

Поскольку фаза α в каждой посылке случайна, то Ева в среднем по посылкам "видит" не чистые состояния, а статистическую смесь. Среднее по случайной фазе θ $\alpha = |\alpha| \exp(i\theta)$, с учётом (1), даёт

$$\begin{aligned} \rho_{0,1} &= \int_0^{2\pi} \frac{d\theta}{2\pi} (|\exp(i\varphi_{0,1})|\alpha| \exp(i\theta)\rangle_1 \otimes ||\alpha| \exp(i\theta)\rangle_2) \times \\ &\times ({}_2\langle \exp(i\varphi_{0,1})|\alpha| \exp(i\theta)| \otimes {}_1\langle |\alpha| \exp(i\theta)|) = \\ &= \exp(-2\mu) \sum_{k=0}^{\infty} \frac{(2\mu)^k}{k!} |\Psi_k^{0,1}\rangle_{\text{loc loc}} \langle \Psi_k^{0,1}| = \\ &= \sum_{k=0}^{\infty} P_k(\mu) |\Psi_k^{0,1}\rangle_{\text{loc loc}} \langle \Psi_k^{0,1}|, \quad (4) \\ P_k(\mu) &= \exp(-2\mu) \frac{(2\mu)^k}{k!}, \\ |\Psi_k^{0,1}\rangle_{\text{loc}} &= \sqrt{\frac{k!}{2^k}} \sum_{m=0}^k \exp(i\varphi_{0,1}m) \frac{|m\rangle_{\text{loc}_1} \otimes |k-m\rangle_{\text{loc}_2}}{\sqrt{m!(k-m)!}}, \end{aligned}$$

где индексы loc_1 и loc_2 символизируют состояния, сведённые в одну точку пространства–времени, и происходящие из разнесённых двух половинок когерентных состояний (см. (1)).

Неформально говоря, измерения над квантовой системой, находящейся в одном из двух состояний, отве-

чающих 0 и 1, с целью определения в каком из двух состояний находится система, сводятся к проектированию на измерительный набор квантовых состояний (в более общем виде на набор операторно-значных мер). При этом подразумевается, что сам набор квантовых состояний, подлежащих различению, известен.

Из-за случайной фазы когерентного состояния, $\theta \in [0, 2\pi]$, невозможно построить измерения для различения пары состояний 0 или 1, из бесконечного набора чистых состояний из-за "размазанной фазы на отрезке $[0, 2\pi]$ ".

Поясним ситуацию.

В нашем случае имеем источник чистых когерентных состояний со случайной фазой. В каждой i -й посылке в канал поступает пара чистых когерентных состояний со случайной фазой θ_i ,

$$\begin{aligned} &(|\exp(i\varphi_{0,1})\alpha\rangle|\exp(i\theta_1)\rangle_1 \otimes |\alpha\rangle|\exp(i\theta_1)\rangle_2) \otimes \\ &(|\exp(i\varphi_{0,1})\alpha\rangle|\exp(i\theta_2)\rangle_1 \otimes |\alpha\rangle|\exp(i\theta_2)\rangle_2) \otimes \dots \\ &(|\exp(i\varphi_{0,1})\alpha\rangle|\exp(i\theta_n)\rangle_1 \otimes |\alpha\rangle|\exp(i\theta_n)\rangle_2). \end{aligned}$$

Данный источник отличается от источника фоковских состояний — статистической смеси чистых состояний, которая описывается матрицей плотности. В каждой i -й посылке в канал поступает чистое фоковское состояние, с вероятностью $P_k(\mu) = \exp(-2\mu)((2\mu)^k/k!)$, зависящей от числа фотонов k ,

$$|\Psi_k^{0,1}\rangle_{\text{loc}_1} \otimes |\Psi_k^{0,1}\rangle_{\text{loc}_2} \otimes \dots \otimes |\Psi_k^{0,1}\rangle_{\text{loc}_n}.$$

Минимальная ошибка при различении состояний (4) есть (см., например, [23])

$$\begin{aligned} Q_E &= \frac{1}{2} \{1 - \|\rho_0 - \rho_1\|_1\} = \frac{1}{2} \{1 - (1 - \exp(-2\mu))\} = \\ &= \frac{1}{2} \exp(-2\mu), \end{aligned} \quad (5)$$

здесь $\|\rho_0 - \rho_1\|_1 = \text{Tr}\{\rho_0 - \rho_1\}$ — следовое расстояние.

Фактически неортогональность двух информационных состояний возникает из-за присутствия одинаковой вакуумной компоненты в когерентных состояниях для 0 и 1. При $\mu \rightarrow 0$, ошибка при различении состояний Евой стремится к вероятности простого угадывания, $Q_E \rightarrow 1/2$, а при $\mu \rightarrow \infty$ — классический случай, доля вакуумной компоненты стремится к 0, соответственно, ошибка различения $Q_E \rightarrow 0$ — состояния становятся достоверно различимыми.

Интерпретация формулы (5) физически достаточно прозрачна, и основывается на статистической интерпретации матриц плотности. В каждой посылке нарушитель предварительно проводит неразрушающее измерение по числу фотонов, которое дается разложением единицы

$$I = \sum_{k=0}^{\infty} P_k, \quad P_k = \sum_{m=0}^k (|m\rangle_1 \otimes |k-m\rangle_2) ({}_1\langle m| \otimes {}_2\langle k-m|).$$

В результате измерений у нарушителя возникает исход k с вероятностью $P_k(\mu)$. Если возник исход, отвечающий конкретному значению k , то измеряемое состояние переходит в новое состояние $|\Psi_k^{0,1}\rangle_{\text{loc}}$, в зависимости от входного состояния 0 или 1.

$$|\Psi_k^{0,1}\rangle_{\text{loc}} = \frac{1}{\sqrt{P_k(\mu)}} P_k(|\exp(i\varphi_{0,1})\alpha\rangle_1 \otimes |\alpha\rangle_2).$$

При $k \geq 1$ состояния $|\Psi_k^0\rangle_{\text{loc}}$ и $|\Psi_k^1\rangle_{\text{loc}}$ ортогональны, и поэтому достоверно различимы. При $k = 0$ состояния одинаковы, $|\Psi_k^0\rangle_{\text{loc}} = |\Psi_k^1\rangle_{\text{loc}}$, и соответствуют вакуумной компоненте состояний. Именно, из-за вакуумной компоненты состояний возникает ошибка различения. Вакуумная компонента состояний возникает при измерениях с вероятностью $P_{k=0}(\mu) = \exp(-2\mu)$. Если при измерениях возникает вакуумная компонента, которая одинакова в обоих состояниях для 0 и 1, нарушитель может только угадывать из какого состояния для 0 или 1 произошла данная компонента. Ошибка угадывания равна $1/2$. В доле посылок $P_{k=0}(\mu) = \exp(-2\mu)$ нарушитель производит ошибку в $1/2$, в остальных посылках, где возникают компоненты с $k \geq 1$, состояния достоверно различимы, и ошибки не возникает. Таким образом, приходим к формуле (5).

Пусть Ева подслушивает долю состояний p , пусть вероятность ошибки на приёмной стороне Боба, по всем посылкам есть Q . Данная вероятность ошибки включает в себя все ошибки, как от действий Евы, так и от неидеальностей аппаратуры и канала связи.

Доля посылок из p в асимптотическом пределе длинных последовательностей, в которых Ева знает — достоверно различает состояния и перепосылает правильную вторую половину состояния в доле посылок $(1-Q_E)p$, доля ошибочных перепосылок равна pQ_E . Данные перепосылки приведут к ошибкам на стороне Боба.

Поскольку ошибки от действий Евы и ошибки от неидеальностей аппаратуры неотличимы, то все ошибки на приёмной стороне списываются на действия Евы.

С учётом сказанного, можно через вероятность ошибки на стороне Боба найти долю атакуемых посылок p , $p = Q/Q_E$.

Дефицит информации Евы в битах из p посылок, есть $ph(Q_E)$. Соответственно суммарный дефицит информации Евы о бите Алисы $(1 - p - ph(Q_E))$. Для длины ключа получаем

$$\ell = \left(1 - \frac{Q}{Q_E} + \frac{Q}{Q_E} h(Q_E)\right) - h(Q). \quad (6)$$

Интерпретация формулы (6) аналогична (3).

Выделение фоковских компонент с разным числом фотонов из чистого когерентного состояния на практике требует неразрушающих измерений по числу фотонов, по этой причине данная атака на сегодняшний день является лишь умозрительной. Кроме того, как будет видно ниже, данная атака является не самой эффективной для Евы.

5.3. Прозрачная атака со светоделителем

Рассмотрим атаку со светоделителем. Данная атака является прозрачной, при данной атаке Ева не производит ошибок на приёмной стороне — нет задержек, и нет возмущения состояний Алисы. Ошибки возникают только из-за неидеальностей аппаратуры и естественных возмущений в канале связи.

Атака основана на том факте, что на светоделителе когерентные состояния преобразуются самоподобно. Используя светоделитель, Ева отводит часть состояния к себе, затем производит измерения.

После преобразований состояний Алисы на светоделителе, состояния оказываются следующими

$$|\alpha\rangle_1 \otimes |\pm\alpha\rangle_2 \rightarrow \begin{cases} |\sqrt{\eta}\alpha\rangle_{1E} \otimes |\pm\sqrt{\eta}\alpha\rangle_{2E} \\ |\sqrt{1-\eta}\alpha\rangle_{1B} \otimes |\pm\sqrt{1-\eta}\alpha\rangle_{2B} \end{cases}, \quad (7)$$

индексы E и B относятся к состояниям Евы и Боба, η — коэффициент светоделителя.

Еве важны только те посылки, в которых произошла регистрация состояния у неё и у Боба.

Ева может отвести почти всё когерентное состояние, $\eta \rightarrow 1$. В этом случае вероятность регистрации у Евы есть $1 - \exp(-\eta\mu)$. Остальная доля когерентного состояния $1 - \eta \rightarrow 0$ направляется к Бобу. В пользу Евы считаем, что Ева может "донести" данное состояние через идеальный канал без потерь.

Вероятность регистрации на приёмной стороне будет

$$P(B) = 1 - \exp(-(1-\eta)\mu), \quad (8)$$

напомним, среднее число фотонов в каждой половинке когерентных состояний равно μ .

Ева получает достоверную информацию о передаваемом состоянии только в доле посылок $(1 - \exp(-\eta\mu)) \times (1 - \exp(-(1-\eta)\mu))$, где была регистрация состояний у неё и у Боба. Поскольку детекторы не реагируют на вакуумную компоненту состояний, то в пользу Евы считаем, что Еве достаточно факта регистрации только одного когерентного состояния, отведённого к себе, а не двух, вероятность такого события $(1 - \exp(-\eta\mu))(1 - \exp(-(1-\eta)\mu))$. Для двух состояний, чтобы иметь доступ к относительной фазе, вероятность меньше $(1 - \exp(-\eta\mu))^2(1 - \exp(-(1-\eta)\mu))$.

В итоге, на каждую зарегистрированную Бобом посылку, Ева будет знать передаваемые состояния только с вероятностью $(1 - \exp(-\eta\mu))(1 - \exp(-(1-\eta)\mu))$. Информация Евы в этих посылках в битах равна 1. Соответственно, с вероятностью $(1 - \exp(-(1-\eta)\mu)) - (1 - \exp(-\eta\mu))(1 - \exp(-(1-\eta)\mu))$ Ева не будет знать передаваемые состояния. В такой доле посылок её информация в битах равна 0, именно, эти посылки дают вклад в секретный ключ.

В итоге, длина секретного ключа в пересчёте на зарегистрированную Бобом посылку, есть

$$\ell = \exp(-\eta\mu) - h(Q) \geq \exp(-\mu) - h(Q), \quad \eta \rightarrow 1. \quad (9)$$

Интерпретация формулы (9) аналогична (3), (6). Первое слагаемое — дефицит информации Евы о бите Алисы, второе — дефицит информации Боба о бите Алисы.

Отметим, что Ева не обязана доставлять на приёмную сторону точную долю $(1 - \exp(-(1-\eta)\mu))$ когерентного состояния, например, заменив реальный канал на канал без потерь. Формально такое не запрещается Еве, хотя на практике вряд ли реализуемо. Пусть приёмной стороны достигает из-за потерь в канале связи только часть отведённого для Боба состояния, пусть эта доля $\zeta(1 - \exp(-(1-\eta)\mu))$ ($0 < \zeta \leq 1$). Повторя рассуждения выше, приходим к (9).

При больших потерях все меньшая доля состояний достигает приёмной стороны, поэтому скорость распределения ключей падает. Но при этом, для состояний, достигших приёмной стороны, должны выполняться опре-

делённые требования, чтобы обеспечить секретность ключей. И это справедливо для любого протокола квантового распределения ключей.

5.4. Атака с измерениями с определённым исходом и предварительной посылкой передней части состояния

В данной атаке Ева предварительно посылает свою переднюю половину когерентного состояния. Сводит обе половинки состояния Алисы в одну точку пространства–времени и производит измерения с определённым исходом. По результатам измерений готовит вторую половину состояния и направляет к Бобу. Задержек состояния при этом не происходит, но возникают ошибки у Боба из-за ошибок при различении состояний Евой.

Измерения с определённым исходом (UM — Unambiguous Measurements) возможны для набора любых N линейно независимых состояний [24]. Такие измерения имеют $N+1$ исходов. Если произошёл один из определённых исходов, например, i -й исход ($i = 1, 2, \dots, N$), то точно известно, что этот исход мог произойти только от i -го состояния. Вероятность определённых исходов меньше единицы. $N+1$ -й исход является неопределённым исходом и может происходить от любого состояния. В этом случае нарушитель может только угадывать от какого состояния был данный исход.

Нижняя граница вероятности неопределённого исхода, применительно к нашему случаю при различении пары состояний может быть оценена как (см., например, [25])

$$Q^{\text{opt}} \geq \mathcal{F}(\rho_0, \rho_1), \quad (10)$$

где *фиделити* между матрицами плотности (4)

$$\mathcal{F}(\rho_0, \rho_1) = \text{Tr} \left\{ \sqrt{\sqrt{\rho_0} \rho_1 \sqrt{\rho_0}} \right\} = \exp(-2\mu),$$

т.е. чем больше перекрытие между состояниями, тем состояния менее различимы, тем больше вероятность неопределённого исхода. Данная оценка является оценкой с запасом в пользу нарушителя.

Пусть Ева атакует долю посылок p . В доле посылок $p(1 - Q^{\text{opt}})$ с определённым исходом Ева точно знает передаваемое состояние и не производит ни задержек, ни ошибок на приёмной стороне Боба, поскольку может приготовить правильную заднюю половину состояния с правильной относительной фазой.

В доле посылок pQ^{opt} с неопределённым исходом Ева не знает передаваемое состояние и *вынуждена наугад посылать вторую половину*. В этой доле посылок Ева производит ошибку равную $1/2$ на приёмной стороне.

При большом среднем числе фотонов в когерентном состоянии, $\mu \rightarrow \infty$, состояния, отвечающие 0 и 1 становятся достоверно различимыми — реализуется классический предел состояний.

Пусть вероятность ошибки на приёмной стороне есть Q , отсюда можно оценить долю p посылок атакуемых Евой. Имеем, $1/2pQ^{\text{opt}} = Q$. В доле посылок $p(1 - Q^{\text{opt}})$, где у Евы был определённый исход, Ева знает передаваемые информационные состояния. В итоге, для

длины ключа получаем

$$\begin{aligned}\ell &= (1 - p - p(1 - Q^{\text{opt}})) - h(Q) = \\ &= \left(1 - 2\frac{Q}{Q^{\text{opt}}} - 2Q\right) - h(Q).\end{aligned}\quad (11)$$

Интерпретация слагаемых в формуле (11) аналогична (3), (6), (9). Первое слагаемое есть дефицит информации Евы о передаваемом бите Алисы, второе слагаемое представляет собой дефицит информации Боба о бите Алисы.

Имеет смысл обсудить данную атаку более подробно. При предварительной посылке передней половины состояния задержек не возникает. После получения обеих половинок состояния Ева проводит измерения. Из-за недостоверной различимости состояний Ева получает определённый исход, при котором она знает передаваемое состояние, с вероятностью меньше единицы, это определённый исход (conclusive) (см. формулу (10)), и тогда у Боба также должен быть получен хоть какой отсчёт в данной посылке. Только такие совместные события интересны для Евы. Для получения гарантированного отсчёта у Боба, Ева может заранее послать интенсивную переднюю половинку, а затем такую же интенсивную вторую при получении определённого исхода у неё. В таких посылках все отсчёты у Боба будут правильными, и Ева в этих посылках будет знать передаваемый бит.

Но что делать Еве, если у неё получен неопределённый исход? Такие исходы всегда будут из-за недостоверной различимости состояний.

Еве остаётся только гадать, какое состояние было послано Алисой. Вероятность угадать вторую половинку состояния, а значит и полное состояние, есть $1/2$, что приведёт к ошибке в 50 % в таких посылках.

Блокировать (вернуть назад) предварительно посланную первую половинку уже невозможно из-за релятивистских ограничений. Неформально говоря, первую половинку догнать уже нельзя. Посланная наугад вторая половина, соответственно полное состояние, как уже сказано приведёт к ошибке $1/2$.

Если не посылать вторую половинку, то одна первая половинка приведёт также к ошибке в $1/2$, поскольку отсчёты будут иметь место в двух детекторах вместо одного отсчёта в нужном детекторе.

По этим причинам, Ева никогда не будет иметь точную копию состояния Алисы.

Здесь важны как квантовость состояния, гарантирующая не достоверную различимость, так и релятивистские ограничения. Фактически невозможность догнать или блокировать, заранее посланную переднюю половину состояния. Ева "зажата" двумя фундаментальными ограничениями — ограничениями квантовой механики и релятивистской причинностью. Если заранее не посылать переднюю половину, а собирать в одну пространственно-временную точку обе половины состояния, то это (см. рис. 1 и пояснения к нему) приведёт к неизбежной задержке при регистрации на приёмной стороне, и неизбежным ошибкам с вероятностью $1/2$ (см. рис. 3 и пояснения к нему).

Имеет смысл отметить принципиальное отличие атаки с УМ измерениями (измерениями с определённым исходом) в релятивистском и нерелятивистском квантовом распределении ключей.

В нерелятивистском случае, Ева при неопределённом исходе может ничего не посылать на приёмную сторону Боба. В этой посылке не будет срабатывания детекторов, что списывается на потери в квантовом канале связи.

В релятивистском случае, без предварительного посылки состояния, в случае неопределённого исхода Ева может ничего не перепосылать. В случае определённого исхода, Ева знает передаваемое состояние, но перепосыл правильного состояния Евы, приведёт к задержке состояния в этих посылках, и к вероятности ошибки $1/2$.

В атаке УМ измерениями и предварительной посылкой передней части состояния Евой, при неопределённом исходе, чтобы не произвести ошибок на приёмной стороне, Ева уже не сможет (не успеет) заблокировать предварительно посланную переднюю половинку, так как невозможно "догнать" переднюю половинку, движущуюся с предельной скоростью света.

Аналогичные рассуждения справедливы и для других, рассмотренных выше, атак.

6. Некоторые численные примеры

Интересно оценить длину ключа при различных потерях в линии связи. Поскольку квантовый канал связи не контролируется Алисой и Бобом, то все ошибки на приёмной стороне списываются на действия нарушителя.

Потери в линии даже в отсутствии нарушителя будут приводить к ошибкам на приёмной стороне из-за темновых шумов детекторов. Чем больше потери, тем меньше состояний достигает приёмной стороны, тем больше доля темновых отсчётов. Сами по себе темновые отсчёты приводят к ошибке $1/2$ — оба детектора срабатывают случайно. Даже, если нет нарушителя, то на приёмной стороне вероятность темновых отсчётов будет приводить к вероятности ошибки

$$Q = \frac{1}{2} \frac{p_d}{p_d + (1 - \exp(-\eta_d \mu T))}, \quad (12)$$

где η_d — квантовая эффективность детекторов, типичные значения кремниевых однофотонных лавинных фотодетекторов есть $\eta_d = 0,5-0,8$, нами принято значение $\eta_d = 0,5$, T — коэффициент прохождения линии связи, $T^{-1} = \text{Loss}$ — потери в линии связи, $(1 - \exp(-\eta_d \mu T))$ — вероятность регистрации когерентного состояния в центральном временном окне (см. рис. 3). Как видно из формулы (12), при $T \rightarrow 0$ вероятность ошибки $Q \rightarrow 1/2$, фактически детекторы регистрируют только собственные темновые шумы.

Зависимости длины секретного ключа для различных атак в зависимости от потерь в квантовом канале связи приведены на рис. 4а–г. Зависимости длины ключа как функции среднего числа фотонов в когерентных состояниях показаны на рис. 4д, е.

Как следует из рис. 4 до некоторого уровня потерь, который зависит от среднего числа фотонов и вероятности темновых отсчётов, наиболее эффективной атакой для нарушителя является атака со светоделителем. До уровня потерь ($\approx 50-60$ дБ) данная атака наиболее эффективна для нарушителя — даёт меньшую длину ключа по сравнению с другими атаками. При более высоких

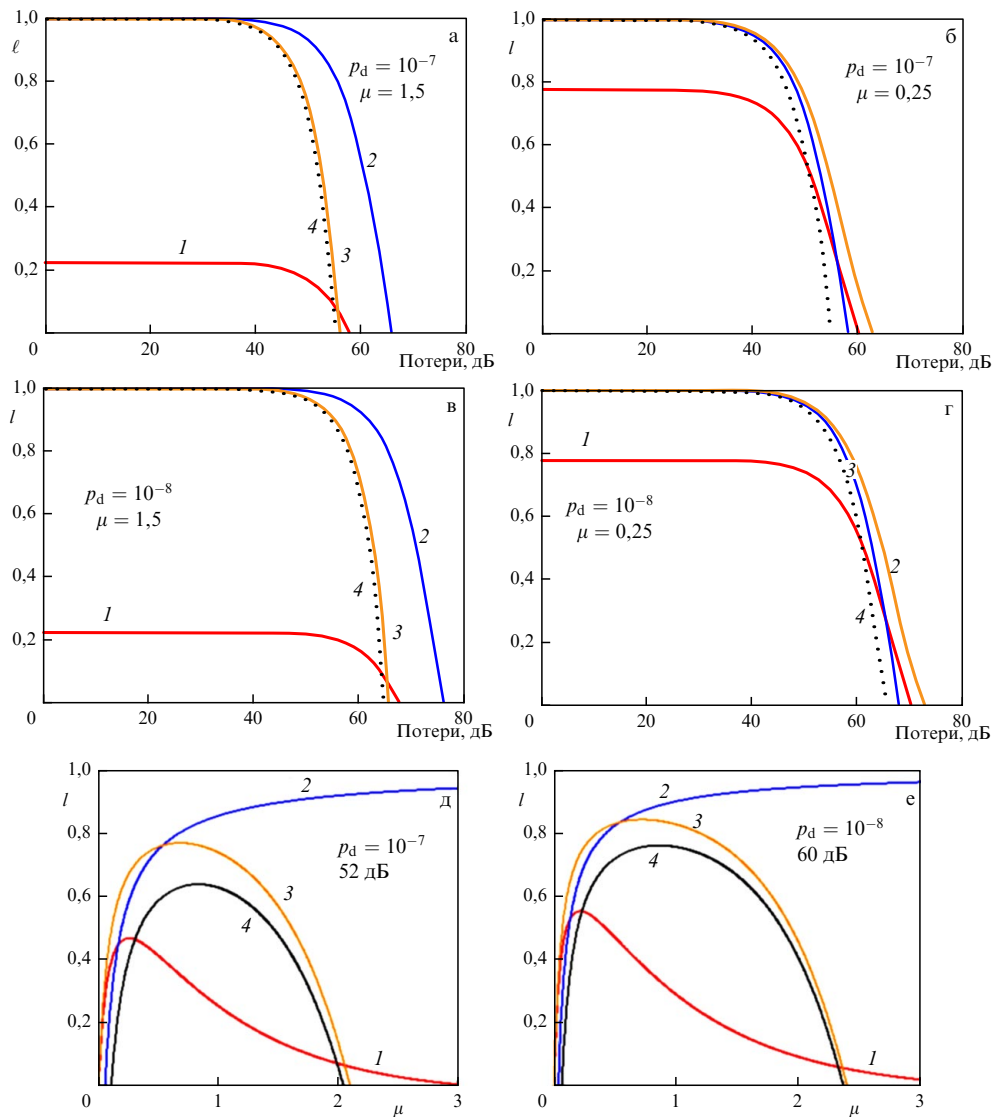


Рис. 4. На всех рис. 4 кривые отвечают следующим атакам: 1 — атака со светоделителем; 2 — унитарная атака без предварительной посылки состояния; 3 — унитарная атака с предварительной посылкой состояния; 4 — атака с измерениями с определённым исходом и предварительной посылкой состояния. Рисунки (а–г) зависимости длины ключа как функция потерь в квантовом канале связи. Рисунки д, е зависимости длины ключа при фиксированных потерях как функции среднего числа фотонов в когерентных состояниях. Квантовая эффективность детекторов $\eta_d = 0,5$. Остальные параметры указаны на рисунках.

потерях эффективными оказываются другие атаки (см. рис. 4).

Далее, из рис. 4д, е следует, что оптимальным средним числом фотонов для состояний Алисы, которое даёт наибольшую длину ключа для атаки со светоделителем, является величина $\mu \approx 0,25-0,5$.

Из рисунка 4 также следует, что протокол обеспечивает распределение секретных ключей ≈ 60 дБ, что соответствует длине волоконной линии связи из стандартного одномодового волокна 300 км.

Примечательной, и на первый взгляд, контринтуитивной, является зависимость от среднего числа фотонов для унитарной атаки без предварительной посылки состояния Евой. Длина ключа выходит при больших μ на единицу.

При больших средних числах фотонов $\eta_d \mu T \gg 1$ — классический предел, и $\eta_d \mu T \gg p_d$, вероятность ошибки стремится к нулю. В этом случае для длины ключа из (3)

получаем

$$\ell \approx 1 - h(Q) \rightarrow 1,$$

поскольку $h(Q) \propto Q$ при малых Q , поэтому стремление $\ell \rightarrow 1$ при больших μ перестаёт быть удивительным. Фактически, это связано ещё и с тем, что без предварительной посылки состояния и любом исходе измерений Евы возникает ошибка равная $1/2$ из-за задержек перепосылаемого Евой состояния (см. обсуждение выше). Данная атака наименее эффективна для Евы.

7. Заключение

Предложенный протокол релятивистского КРК позволяет распределять ключи через открытое пространство, протокол не требует однофотонных состояний, достаточно ослабленного лазерного излучения — когерентных состояний. По этой же причине не нужно исполь-

зовать состояния "ловушки" как в decoy state методе [6–9], которые являются обязательными для *нерелятивистских КРК* из-за атаки с расщеплением по числу фотонов (PNS — Photon Number Splitting Attack) [6–9], работающих, как в волоконных линиях связи, так и через открытое пространство. Для PNS атаки с измерением фоковского числа фотонов в протяжённом состоянии (см. формулу (1)) необходим доступ ко всему состоянию — сведение протяжённого состояния (1) в локальное, аналогично унитарной атаке, что неизбежно приводит к задержкам и к ошибкам на приёмной стороне.

В заключение отметим, что скорость света в атмосфере отличается от скорости света в вакууме в четвёртом знаке. Показатель преломления в атмосфере $n = 1,00029 = 1 + \delta$. Для того, чтобы подслушиватель не смог компенсировать задержки из-за разности скоростей света в вакууме и атмосфере, раздвижка состояний не должна быть меньше определённой величины, которая зависит от расстояния между передающей и приёмной станциями. Типичные расстояния между вышками сотовой связи $L = 10$ км (в основном меньше, только в удалённых районах достигают 20 км). Отсюда можно определить расстояние между половинками когерентных состояний

$$\Delta \ell = \Delta t c_{\text{atm}} = \frac{L \delta}{1 + \delta} \approx 300 \text{ см} , \quad (13)$$

где Δt — сдвиг по времени при прохождении расстояния L со скоростью света в вакууме и атмосфере, $c_{\text{atm}} = c/(1 + \delta)$ — скорость света в атмосфере.

Таким образом, разность хода длинного и короткого плечей интерферометра должна отличаться не менее, чем на данную величину.

Однако, надо понимать, что для того, чтобы нарушитель мог использовать факт отличия скоростей света в вакууме и атмосфере, нарушитель должен заменить атмосферный канал связи между передающей и приёмной станциями на вакуумный канал. Неформально говоря, выкачать весь воздух между станциями. По этой причине, на практике такой атакой воспользоваться нельзя, и можно использовать существенно меньшую разность хода между плечами интерферометра, хотя, разность хода (13) не есть техническая проблема, поскольку приёмный интерферометр выполняется в волоконном варианте.

Ещё одним замечательным свойством протокола является то, что в нём нет процедуры согласования базисов, как в других протоколах. При согласовании базисов примерно половина зарегистрированных посылок, в которых базисы Алисы и Боба не совпадают, отбрасывается. В данном протоколе имеются только два информационных состояния, поэтому все зарегистрированные посылки "идут в дело — в ключ", что обеспечивает более высокую скорость распределения ключей.

Интересно отметить в заключение, что фундаментальные ограничения на различимость квантовых состояний, диктуемые принципом релятивистской причинности, оказываются полезными и для нерелятивистской квантовой криптографии, в которой различимость квантовых состояний и секретность ключей основаны, фактически только на геометрических свойствах квантовых состояний — на неортогональности состояний.

В недавно появившейся публикации [26], авторам, после многих безуспешных попыток в течении почти 25 лет исследований различных групп удалось доказать секретность нерелятивистского протокола квантового распределения ключей DPS (Differential Phase Shift), относительно самых общих атак, используя, как отмечено самими авторами, релятивистские ограничения, ранее использованные в работах [14, 16–18, 28] для релятивистского квантового распределения ключей. Это означает, что дополнительные фундаментальные релятивистские ограничения на различимость квантовых состояний открывают новые возможности при разработке систем защищённой передачи информации и для нерелятивистских систем [29].

Благодарности. Выражаем благодарность И.М. Арбекову, коллегам по Академии криптографии Российской Федерации, ИнфоТекс и СФБ Лаборатории за интерес к работе и обсуждения.

Список литературы

1. Bennett C H, Brassard G *Proc. of IEEE Int. Conf. on Comput. Sys. and Sign. Proces.* (India, Bangalore (1984) стр. 175
2. Wootters W K, Zurek W H *Nature* **299** 802 (1982)
3. Bennett C H *Phys. Rev. Lett.* **68** 3121 (1992)
4. Tomamichel M et al. *Nature Commun.* **3** 634 (2011)
5. Renes J M, Boileau J-C *Phys. Rev. Lett.* **103** 020402-1 (2009)
6. Won-Young Hwang *Phys. Rev. Lett.* **91** 057901 (2003); arXiv[quant-ph]: 0211153
7. Xiang-Bin Wang *Phys. Rev. Lett.* **94** 230503 (2005)
8. Hoi-Kwong Lo, Xiong-feng Ma, Kai Chen *Phys. Rev. Lett.* **94** 230504 (2005)
9. Xiong-feng Ma et al. *Phys. Rev.* **A72** 012326 (2005); arXiv[quant-ph]: 0503005
10. Goldenberg L, Vaidman L *Phys. Rev. Lett.* **75** 1239 (1995)
11. Молотков С Н *Письма в ЖЭТФ* **93** 389 (2011)
12. Molotkov S N, Pomozov D I *Relativistic No-Cloning Theorem, NATO Series for Peace and Security, Information and Communication Security* **11** 31 (ed. M. Zhukowski, S. Kilin, J. Kowalik)(Amsterdam, Berlin, Oxford, Washington: IOS Press, 2007)
13. Молотков С Н, Помозов Д И *Письма в ЖЭТФ* **85** 569 (2007)
14. Молотков С Н *ЖЭТФ* **139** 429 (2011)
15. Молотков С Н *Письма в ЖЭТФ* **94** 504 (2011)
16. Молотков С Н *Письма в ЖЭТФ* **96** 374 (2012)
17. Kravtsov K S et al., Radchenko I V, Kulik S P, Molotkov S N *Sci. Rep.* **8**:6102 1 (2018)
18. Kravtsov K S, Radchenko I V, Kulik S P, Molotkov S N *Laser Phys. Lett.* **11** 065203 (2014)
19. Cotler J S, Shor P W J. *Quantum Information and Computation* **14** 1081 (2014); arXiv: 1401.5493
20. Bebrov G *Sci. Rep.* **11**:23543 1 (2021)
21. Bebrov G *Sci. Rep.* **12**:15377 1 (2022)
22. Kulik S P, Kravtsov K S, Molotkov S N *Laser Phys. Lett.* **19** 025203 (2022)
23. Wilde M M *From Classical to Quantum Shannon Theory*, arXiv:1106.1445v6 [quant-ph] 2 Dec 2015
24. Barnett S M, Croke S *Adv. Optics and Photonics* **1** 238 (2009)
25. Raynal P *Unambiguous State Discrimination of two density matrices in Quantum Information Theory* Den Naturwissenschaftlichen Fakultäten der Friedrich-Alexander-Universität Erlangen-Nürnberg zur Erlangung des Doktorgrades (2006), arXiv:quant-ph/0611133
26. Martin Sandfuchs et al. *Quantum* **9** 1611 (2025)
27. Kyo Inoue, Edo Waks, Yoshihisa Yamamoto *Phys. Rev. Lett.* **89** 037902-1 (2002)

28. Молотков С Н *УФН* **176** 777 (2006); Molotkov S N *Phys. Usp.* **49** 750 (2006) 29. Арбеков И М, Молотков С Н *УФН* **195** 1021 (2025); Arbekov I M, Molotkov S N *Phys. Usp.* **68** 963 (2025)

Relativistic quantum key distribution between stationary objects based on coherent states

S.P. Kulik^{(1,*), S.N. Molotkov^(2,3)}

⁽¹⁾ *Quantum Technology Center of Lomonosov Moscow State University, Leninskie Gory 1, str. 35, 119991 Moscow, Russian Federation*

⁽²⁾ *Academy of Cryptography of the Russian Federation, PO Box 100, 119331 Moscow, Russian Federation*

⁽³⁾ *Osipyan Institute of Solid State Physics, Russian Academy of Sciences,
ul. Akademika Osipyana 2, 142432 Chernogolovka, Moscow region, Russian Federation*

E-mail: * kuliksp@my.msu.ru

The combined constraints of quantum mechanics and special relativity open new possibilities for quantum communications. This paper discusses a relativistic quantum key distribution (QKD) protocol over open space. The protocol does not require single-photon states, but rather attenuated coherent states of laser radiation. With a small average number of photons in coherent states, states with different relative phase values cannot be reliably distinguished. There is no need to use deceptive states, as in the decoy state method, which are mandatory for non-relativistic QKD protocols. This simplifies the optical design at the receiving end and eliminates the need for active elements — a phase modulator. An intensity modulator is not required at the transmitting end, which is necessary for implementing the decoy state method in non-relativistic systems. The protocol enables key distribution with high line losses of approximately ≈ 60 dB. The protocol uses only two information states, eliminating the need for base agreement. All registered packets are used in the key, increasing the speed of key distribution. The most suitable application for relativistic QKD systems is key distribution between stationary objects, such as cellular base stations or other objects between which laying fiber optic cables is expensive or practically impossible. Unlike the analysis of the cryptographic strength of non-relativistic QKD systems, which uses rather sophisticated mathematical apparatus, the analysis of the strength of relativistic QKD is presented at a level that is intuitively understandable for a physics audience. It does not require prior specialized knowledge and is accessible to graduate students and senior university undergraduates familiar with the fundamentals of quantum optics, quantum information science, and quantum cryptography, as taught in standard university courses.

Keywords: special relativity, quantum cryptography in free space, coherent states

PACS numbers: **03.30.+p**, 03.67.Dd, **89.70.-a**

Bibliography — 29 references

Received 16 October 2024, revised 13 April 2026

Uspekhi Fizicheskikh Nauk **196** (10) 1086–1097 (2026)

Physics – Uspekhi **69** (10) (2026)

DOI: <https://doi.org/10.3367/UFNr.2026.08.040188>

DOI: <https://doi.org/10.3367/UFNe.2026.08.040188>