Письма в ЖЭТФ, том 94, вып. 6, с. 504 – 512

Релятивистская квантовая криптография для открытого пространства без синхронизации часов на приемной и передающей стороне

С. Н. Молотков

Академия криптографии Российской Федерации, 103025 Москва, Россия

Институт физики твердого тела РАН, 142432 Черноголовка, Россия

Факультет вычислительной математики и кибернетики, МГУ им. М.В. Ломоносова, 119991 Москва, Россия

Поступила в редакцию 4 августа 2011 г.

В квантовой криптографии секретность ключей гарантируется фундаментальными запретами квантовой механики (запреты на клонирование и копирование неортогональных квантовых состояний). Физический тип квантового объекта – носителя информации непринципиален (фотон, электрон, атом и т.д.), важен только его вектор состояния. В релятивистской квантовой криптографии для открытого пространства принципиальны как сам тип носителя информации (фотон, распространяющийся с предельно допустимой скоростью в вакууме), так и его квантовое состояние. Совместные фундаментальные ограничения, диктуемые как специальной теорией относительности, так и квантовой механикой, на различимость неортогональных квантовых состояний позволяют сформулировать принципиально новые протоколы распределения ключей, которые устойчивы относительно любых атак на ключ и гарантируют секретность ключей при не строго однофотонном источнике и любых потерях в канале связи. Несмотря на то что данный протокол является протоколом реального времени в пространстве-времени Минковского, где детектирование вторжений в канал связи происходит по задержкам результатов измерений подслушивателя, *протокол не требует синхронизации часов на передающей и приемной стороне*.

Введение. Квантовая криптография (квантовое распределение ключей) основана на фундаментальных запретах квантовой механики на различимость неортогональных квантовых состояний [1–3]. 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, privacy amplification [4]) очищенного ключа возникает секретный ключ, известный только двум легитимным пользователям.

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 [5]. 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.

Секретность ключей в релятивистской квантовой криптографии основана как на фундаментальных запретах квантовой механики, так и на дополнительных фундаментальных запретах специальной теории относительности на различимость квантовых состояний. Впервые ограничения, накладываемые на изме-

[1)] Величина критической ошибки определяется конкретным протоколом распределения ключей.

римость квантовых состояний в релятивистской области, обсуждались в работе Ландау и Пайерлса еще в 1931 г. [6]. Дальнейшее исследование было предпринято в работе Бора и Розенфельда [7].

В релятивистской квантовой криптографии протоколы распределения ключей принципиально происходят в пространстве-времени Минковского, сам факт существования которого играет первичную роль в том смысле, что векторы состояний фотонов являются базисными векторами унитарного неприводимого представления группы Пуанкаре (сектор с нулевой массой покоя) [8].

Один из таких протоколов релятивистской квантовой криптографии был предложен в работе [9]. Данный протокол гарантирует секретность ключей при любых потерях в канале связи. Общая идея сводится к тому, что для различения пары квантовых состояний в пространстве-времени Минковского требуется доступ к квантовому состоянию как целому. Вероятность результата любого измерения из-за нормировки квантового состояния не может быть больше, чем доля нормировки, которая набирается в доступной области пространства-времени. Поскольку никакие квантовые состояния и классические сигналы не могут распространяться быстрее света, доступ к протяженному квантовому состоянию не может быть получен мгновенно. Поэтому любые измерения с целью получения информации о квантовом состоянии ведут к задержкам, которые детектируются. Поскольку данный протокол является протоколом в реальном времени, для детектирования задержек и секретности ключей необходима синхронизация часов между удаленными пользователями.

В принципе технически такая синхронизация возможна. Однако она является нетривиальной задачей в ситуации, когда подслушиватель может перехватывать классические сигналы, используемые для синхронизации, и сдвигать начало отсчета у одного из пользователей. В дальнейшем этот сдвиг начала отсчета может быть использован для компенсации задержек при измерениях во время подслушивания.

В данной работе предлагается модификация схемы [9], в которой ограничение, связанное с синхронизацией часов на передающей и приемной стороне, снимается. На первый взгляд, существование такой модификации кажется невозможным, поскольку секретность ключей базируется на детектировании задержек, которые вносит подслушиватель.

Изложим сначала неформально общую идею, а затем покажем устойчивость схемы относительно всевозможных атак и любых потерь в канале связи.

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

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

2. Расстояние L между Алисой и Бобом всем известно и является параметром протокола. Алиса и Боб имеют часы, *но не имеют общего начала отсчета времени (часы не синхронизированы).*

3. Происходит передача серии состояний Алисой. Каждая посылка происходит в случайный момент времени внутри интервала ΔT (рис. 1a). Достаточно, чтобы Алиса случайно выбирала один из двух мо-

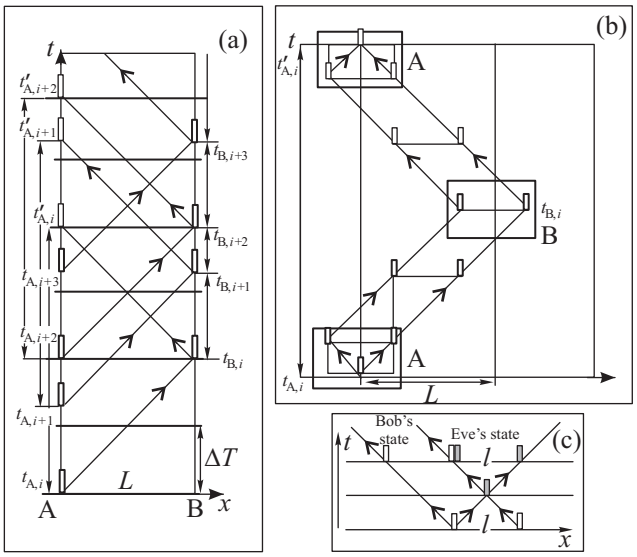

Рис. 1. Пространственно-временные диаграммы работы протокола. (a) – Посылка классических (толстые прямоугольники) и прием квантовых (тонкие) состояний в случайные моменты времени. Показаны только, например, передние половинки состояний. (b) – Приготовление и преобразование протяженных квантовых состояний. (c) – Диаграмма, поясняющая причину задержек по времени протяженных состояний при подслушивании Евой

ментов посылки сигнала внутри интервала ΔT. Алиса готовит *протяженное классическое состояние*, состоящее из пары интенсивных когерентных пакетов, разделенных интервалом $l > l_{\text{pac}}$ (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. 1b); 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.

4. Аппаратура Боба на приемной стороне работает в ждущем режиме. При помощи быстрого классического детектора *Боб фиксирует момент прихода состояния* (технические подробности см. ниже) 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) случайно "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.

5. 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 фотодетекторе, а если $\varphi_A = \varphi_B$, то отсчета не возникает (см. ниже). В результате Алиса знает, какой бит ключа посылал Боб.

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

7. 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 (хеширование) 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 мы увидим ниже, вообще не входят в критерий секретности ключей.

Приготовление и измерение состояний. Алиса активирует лазер (рис. 2) в определенный момент времени и получает на выходе интенсивное когерентное состояние, локализованное в интервале $l_{\text{рас}}$. При прохождении через интерферометр Маха–Цандера[3)] локализованное состояние преобразуется в состояние из двух половинок, $|\alpha_c\rangle_1 \otimes |\alpha_c\rangle_2$, разделенных интервалом l. Затем состояние через линзовую систему направляется в канал связи. Приготовление протяженного состояния из локализованного требует конечного времени (см. рис. 1а и рис. 2).

На приемной стороне Боба классическое состояние вводится в волоконную часть. Через светоделитель состояние поступает на классический детектор, по импульсу тока на котором оцениваются интенсивность и время прилета состояния. 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. Для последовательного преобразования состояний по оптическому тракту имеем

Верхний и нижний входы М–Ц	Верхнее и нижнее плечо М–Ц после РМ	Верхний и нижний выходы М–Ц
$\|\alpha\rangle_1 \otimes \|e^{i\varphi_B}\alpha\rangle_2 \otimes \|vac\rangle_3$	$\|\frac{\alpha}{\sqrt{2}}\rangle_1 \otimes \|\frac{e^{i\varphi_B}\alpha}{\sqrt{2}}\rangle_2 \otimes \|vac\rangle_3$	$\|\frac{\alpha}{2}\rangle_1 \otimes \|\frac{(e^{i\varphi_B} + e^{i\varphi_A})\alpha}{2}\rangle_2 \otimes \|\frac{\alpha}{2}\rangle_3$
$\|vac\rangle_1 \otimes \|vac\rangle_2 \otimes \|vac\rangle_3$	$\|vac\rangle_1 \otimes \|\frac{e^{i\varphi_A}\alpha}{\sqrt{2}}\rangle_2 \otimes \|\frac{\alpha}{\sqrt{2}}\rangle_3$	$\|\frac{\alpha}{2}\rangle_1 \otimes \|\frac{(e^{i\varphi_B} - e^{i\varphi_A})\alpha}{2}\rangle_2 \otimes \|\frac{\alpha}{2}\rangle_3$

(1)

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

[3)] Технически удобнее приготовить состояния, используя волоконный интерферометр.

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 противоположном 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.

Отметим, что данная схема является реализацией двух измерений, которые Алиса выбирает случайно путем выбора фазы ($\varphi_A = \varphi_0$ или $\varphi_A = \varphi_1$). 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 $I - |e^{i\varphi_B}\alpha\rangle_2\ {}_2\langle e^{i\varphi_B}\alpha|$.

Секретность протокола относительно различных атак. 1. Поясним сразу, почему Алиса должна посылать свои состояния в случайные и известные только ей моменты времени. Поскольку часы у Алисы и Боба *не синхронизированы* (*не имеют общего начала отсчета времени*), Боб не знает, когда он получит состояния от Алисы. Если бы Алиса посылала состояния в регулярные и известные всем моменты времени, то подслушиватель Ева могла бы действовать следующим образом.

Ева заранее, до прихода к себе состояния от Алисы, посылает к Бобу состояние, аналогичное состоянию Алисы (напомним, что состояние Алисы 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 (*unambiguous measurements* [5]). Поскольку состояния неортогональны, Ева может с некоторой вероятностью получить как определенный (*conclusive*) исход, так и неопределенный (*inconclusive*). Если получен определенный исход, то Ева однозначно знает передаваемый бит ключа. Тот факт, что на такое измерение требуется конечное время (см. ниже), 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 значение бита в половине этих посылок, где она угадала правильный момент и при этом не произошло сбоя момента прихода состояния к Бобу. Это будет использовано ниже.

2. Теперь 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

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

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

Из (2) 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,

$$\rho(\varphi_B) = \int_0^{2\pi}\frac{d\theta}{2\pi}\left(|\sqrt{\mu}e^{i(\varphi_B+\theta)}\rangle_{11}\langle\sqrt{\mu}e^{-i(\varphi_B+\theta)}|\right)\otimes \otimes\left(|\sqrt{\mu}e^{i\theta}\rangle_{22}\langle\sqrt{\mu}e^{-i\theta}|\right) =$$

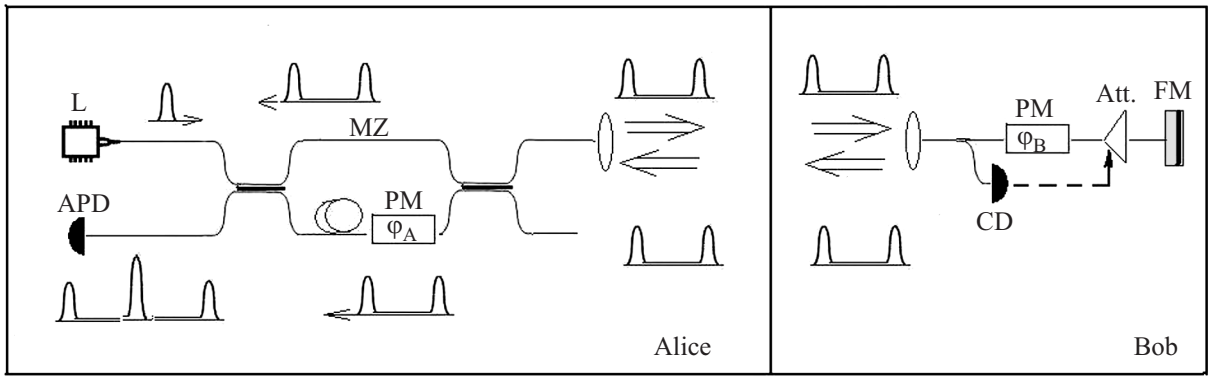

Рис. 2. Двухпроходная оптическая схема приготовления, преобразования и детектирования состояний: MZ – волоконный интерферометр Маха–Цандера с разностью хода по верхнему и нижнему плечу l, L – лазер, PM – фазовый модулятор, Att. – управляемый аттенюатор, FM – фарадеевское зеркало, CD – быстрый классический детектор, APD – лавинный стробируемый однофотонный детектор

$$= e^{-2\mu} \sum_{n,k,n',k'=0}^{\infty} e^{i\varphi_B (n-n')} \frac{\mu^{\frac{n+k-n'-k'}{2}}}{\sqrt{n!k!n'!k'!}} |k\rangle_1 \otimes$$
$$\otimes\, |n\rangle_2\, {}_2\langle n'| \otimes {}_1\langle k'|\ \delta_{n+k,n'+k'}. \qquad (3)$$

Таким образом, для получения информации о ключе необходим доступ к двум половинкам состояния.

В нерелятивистской квантовой криптографии возможны следующие атаки (см., например, [5]). 1. Атака "прием-перепосыл": Ева в каждой посылке измеряет состояния, затем в зависимости от исхода измерения посылает свои состояния. 2. Коллективная атака: Ева готовит в каждой посылке свое состояние (*ancilla*), которое при помощи унитарного преобразования запутывается с информационным состоянием. Ancilla 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 (в более общем виде квантовая операция), сводящее две разделенные в пространстве-времени Минковского половинки состояний, требует конечного времени. (Ситуация поясняется на рис. 1c.) 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. 1c). После сведения половинок вместе Ева может делать либо унитарные преобразования состояния, либо измерения с определенным исходом (unambiquous measurements, далее UM) [10].

Затем ей снова необходимо приготовить растянутое в пространстве-времени состояние. На это также требуется конечное время, равное высоте будущей части светового конуса (рис. 1c). 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. 1b), вторая половинка состояния не будет участвовать в преобразованиях (не успеет прибыть). 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.

3. Ева, конечно, 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 исходы с inconclusive результатом, при которых Ева не знает состояния (она может только гадать, т.е. случайно угадывать фазу). Однако при угадывании на стороне Алисы вероятность ошибки составит 50%. Ева при неопределенном ис-

ходе уже не сможет блокировать свою заранее приготовленную половинку из-за ограничений специальной теории относительности.

Как видно из вышеприведенного анализа, 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 то 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 определенных потерях, поскольку Ева при UM-измерениях не производит ошибок и знает весь ключ, начиная с критической величины потерь [5]. *В данном случае ошибки неизбежны из-за нехватки времени (релятивистское ограничение) и неортогональности квантовых состояний (квантовомеханический запрет на достоверную различимость).*

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 $\rho(\varphi_{\rm B}=\varphi_0)$ и $\rho(\varphi_{\rm B}=\varphi_1)$, минимизирующие ошибку неопределенного (inconclusive – ?) исхода. Поскольку действие любого квантового преобразования (квантовой операции) только уменьшает различимость квантовых состояний, т.к. расстояние между ними уменьшается,

$$\begin{aligned}&||\left(|\alpha\rangle_1\otimes|e^{i\varphi_0}\alpha\rangle_2\right)\left({}_2\langle e^{i\varphi_0}\alpha|\otimes{}_1\langle|\alpha|\right)-\\&-\left(|\alpha\rangle_1\otimes|e^{i\varphi_1}\alpha\rangle_2\right)\left({}_2\langle e^{i\varphi_1}\alpha|\otimes{}_1\langle|\alpha|\right)||_1\geq\\&\geq||\rho(\varphi_{\rm B}=\varphi_0)-\rho(\varphi_{\rm B}=\varphi_1)||_1,\end{aligned}\qquad(4)$$

вероятность неопределенного исхода для чистых состояний меньше, (здесь $||\rho||_1={\rm Tr}\{\sqrt{\rho^+\rho}\}$ – следовая норма). Эта ситуация отвечает тому, что фаза α как бы известна Еве. Таким образом, есть данные оценки оказываются в пользу Евы, т.к. *завышают* ее информацию. Как известно [10], в этом случае минимально возможная вероятность неопределенного исхода при различении пары неортогональных чистых состояний равна

$${\rm Pr}\{?\}={}_2\langle e^{i\varphi_0}\alpha|e^{i\varphi_1}\alpha\rangle_2=e^{-2\mu\sin^2\left(\frac{\varphi}{2}\right)},\quad\varphi=\varphi_0-\varphi_1.\qquad(5)$$

Соответственно, вероятность определенного исхода ${\rm Pr}\{{\rm OK}\}=1-{\rm Pr}\{?\}$. Пусть доля посылок, которые подслушивает Ева, составляет δ. Ошибка на приемной стороне Алисы равна

$$Q\left(\frac{1}{2}\delta{\rm Pr}\{?\}\right)=0\cdot\delta{\rm Pr}\{{\rm OK}\}+\frac{1}{2}\delta{\rm Pr}\{?\}+0\cdot(1-\delta).\qquad(6)$$

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

$$I({\rm A};{\rm B})=1-h\left(\frac{1}{2}\delta{\rm Pr}\{?\}\right),\quad I({\rm A};{\rm E})=\delta(1-{\rm Pr}\{?\}).\qquad(7)$$

Критическая величина ошибки, до которой возможно секретное распределение ключей, и длина секретного ключа R в битах на посылку определяются из условия (см., например, [11])

$$I({\rm A};{\rm B})=I({\rm A};{\rm E}),$$

$$R\left(\frac{1}{2}\delta{\rm Pr}\{?\}\right)=1-h\left(\frac{1}{2}\delta{\rm Pr}\{?\}\right)-\delta(1-{\rm Pr}\{?\}).\qquad(8)$$

4. Обсудим, наконец, 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 (см. выше). Для этих посылок Ева делает коллективные измерения над всей последовательностью в своей квантовой памяти (естественно, 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 [12]. При этом максимум достигается в том случае, когда Ева отводит себе целиком состояния Боба. Таким образом, взаимная информация Алиса–Боб и взаимная информация Алиса(Боб)–Ева при такой атаке равны

$$I({\rm A};{\rm B})=1,\ I({\rm A};{\rm E})\leq\chi(\rho)=S(\rho),\ \rho=\frac{1}{2}(\rho_0+\rho_1),$$

$$\rho_{0,1}=(|\alpha\rangle_1\otimes|e^{i\varphi_{0,1}}\alpha\rangle_2)({}_2\langle^{i\varphi_{0,1}}\alpha|\otimes{}_1\langle|\alpha|),\qquad(9)$$

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

$$R = I(\mathrm{A};\mathrm{B}) - I(\mathrm{A};\mathrm{E}) = 1 - \overline{C}(\varepsilon), \quad \overline{C}(\varepsilon) = \\ = -\left(\frac{1-\varepsilon}{2}\right)\log\left(\frac{1-\varepsilon}{2}\right) - \left(\frac{1+\varepsilon}{2}\right)\log\left(\frac{1+\varepsilon}{2}\right), \tag{10}$$

где $\varepsilon = e^{-2\mu\sin^2[(\varphi_0-\varphi_1)/2]}$, $\overline{C}(\varepsilon)$ – классическая пропускная способность квантового канала связи Боб–Ева, которая в данном случае совпадает с энтропией фон Неймана (напомним, что состояния – чистые; см. также пояснения перед формулой (4)).

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

$$R\left(\frac{1}{2}\delta\mathrm{Pr}\{?\}\right) = 1 - \frac{\eta}{2} - \\ - h\left(\frac{1}{2}\delta\mathrm{Pr}\{?\}\right) - \delta(1-\mathrm{Pr}\{?\}) - \overline{C}(\varepsilon). \tag{11}$$

Поскольку Алиса и Боб не знают доли подслушиваемых посылок δ и Алиса "видит" только ошибку $Q\left(\frac{1}{2}\delta\mathrm{Pr}\{?\}\right)$, удобней привести длину ключа как функцию наблюдаемой ошибки. Зависимости длины секретного ключа R от наблюдаемой ошибки приведены на рис. 3a, а зависимости R от среднего числа фотонов при заданной наблюдаемой ошибке показаны на рис. 3b. Значение параметра η (доли посылок с угадыванием момента времени приготовления состояния Алисы), положено $\eta = 0$ (напомним, что данная доля известна из сравнения сбоев моментов прихода состояний к Алисе). Как видно из рис. 3, протокол обеспечивает достаточно большую критическую ошибку (до 35%, рис. 3a). Кроме того, среднее число фотонов при $Q = 0$ (рис. 3c,d) формально может быть любым. 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.

Учет отличия скорости света c' в атмосфере от скорости света c в вакууме. Этот пункт требует отдельного обсуждения. Скорость света в атмосфере c' слегка отличается от скорости света в вакууме c, что накладывает ограничение на минимальную протяженность состояния l. Для того чтобы Ева не могла скомпенсировать нехватку времени для преобразования состояния, длина состояния должна быть $l > c(T'_L - T_L)$, где $T_L = (L+l)/c$, $T'_L = (L+l)/c'$. Далее, поскольку $c' = c/n$, где n – показатель преломления среды, $\xi = (n - n_{\mathrm{vac}})/n_{\mathrm{vac}}$, находим $l > \xi L$. Типичная величина ξ в атмосфере на расстоянии до ≈ 10 км от поверхности Земли для длин волн $\lambda \approx 0.8$ мкм составляет $\xi \approx 10^{-4}$. На бóльших высотах уже практически $c' = c$. Поэтому Ева может скомпенсировать нехватку времени только на данной высоте, заменяя квантовый канал на идеальный (вакуум). *Минимальная протяженность состояния l лимитируется этим условием и равна $l \geq \xi \cdot 10[\text{км}] = 1$ м. При такой протяженности состояния передача ключей возможна на любые расстояния.*

Таким образом, в протоколе легитимные пользователи закладывают величину c' из оценочных соображений (подчеркнем, что точного априорного знания не требуется). При известном расстоянии L, которое есть параметр протокола, вычисляется время прилета состояния $T_c = L/c$, если последнее распространяется через вакуум со скоростью c. Вычисляется время прилета состояния через среду со скоростью c', $T_{c'} = L/c'$. При этом "запас" времени, которым располагает Ева, есть $\Delta T = T_{c'} - T_c$. Например, Ева может просветлить атмосферу, доведя скорость распространения до предельной (c). Для доступа к состоянию, состоящему из суперпозиции двух локализованных половинок, разделенных интервалом l в вакууме, как целому требуется время $\delta T = l/c$. Временно́е окно, в котором оставляются результаты измерений, выбирается $\gtrsim T_{c'} - T_c$. Протяженность l состояния в вакууме должна быть $l > c(T_{c'} - T_c)$. В этом случае Еве нужно время для доступа к состоянию как целому для измерения и приготовления нового состояния, не меньшее $\delta T = l/c$. Поэтому состояние Евы не успеет прибыть в нужное временно́е окно. Это обстоятельство приведет к ошибкам. Возможны также флуктуации параметров атмосферы, которые в некоторых посылках могут изменить скорость света на величину $\tilde{c}' < c'$. При этом состояние не успеет прибыть в нужное временно́е окно на приемную сторону. Поэтому такая посылка будет отброшена.

Итак, состояние должно быть длиннее, чем $l > T_{c'} - T_c = L(1 - c/c') = \xi L$. В качестве длины L, на которой Ева может скомпенсировать нехватку времени, нужно взять длину той части канала связи, где скорость света c' отличается от скорости света в вакууме c (см. выше).

Таким образом, отличие скорости света в атмосфере от скорости света в вакууме накладывает ограничение лишь на минимально допустимую протяженность квантового состояния.

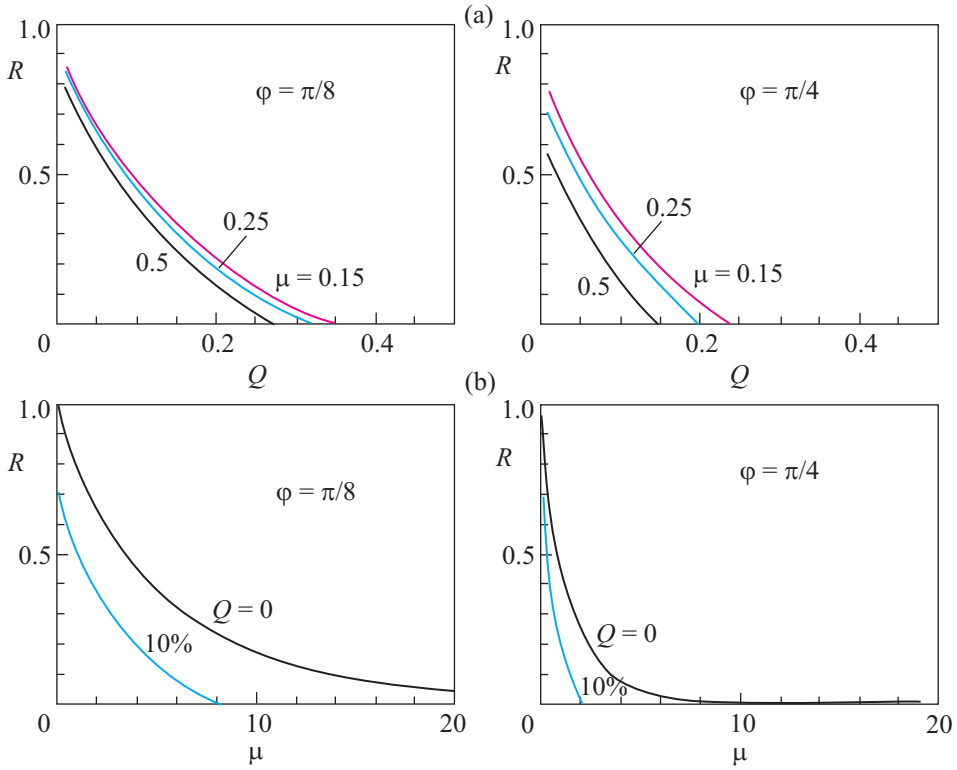

Рис. 3. Зависимости длины секретного ключа R от наблюдаемой ошибки (a) и среднего числа фотонов (b)

Отметим, что в данном протоколе, в отличие от нерелятивистских протоколов квантового распределения ключей, не требуется заранее знать затухание в канале связи. В стандартных протоколах потери в канале связи являются параметром протокола и входят явно в критерий секретности [5].

Разумеется, вещественная и мнимая части показателя преломления связаны между собой соотношением Крамерса–Кронига. Однако в рассуждения, приведенные выше, входит только вещественная часть. Поглощение протяженных состояний в среде аналогично действию Евы. После поглощения Ева может измерить состояние среды, однако это не позволит ей преодолеть нехватку времени. В противном случае возникло бы противоречие со специальной теорией относительности. Извлечение информации о состоянии быстрее, чем за время l/c, позволило бы Еве передавать информацию быстрее скорости света в вакууме.

Отметим, что свести две локализованные "половинки" вместе за время, меньшее, чем l/c, например пропуская их через среду с групповой скоростью, превышающей скорость света в вакууме [13], также нельзя[4)]. Поскольку информация заключена в относительной фазе "половинок" состояния, сведение их вместе за время l/c, позволило бы выйти за пределы причинной части светового конуса. Иначе говоря, при такой процедуре можно было бы узнать информацию, закодированную в протяженное состояние, быстрее скорости света в вакууме.

Заключение. Предложен протокол квантовой криптографии, который максимально использует фундаментальные ограничения, диктуемые законами природы, на измеримость 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, тот факт,

[4)] Можно явно показать, что локализованные состояния распространяются через среду всегда строго со скоростью света в вакууме. Сам по себе тот факт, что групповая скорость света в веществе может превышать скорость света в вакууме, известен с работы Зоммерфельда 1914 г.[14]. Там же было впервые показано, что резкий фронт полубесконечного сигнала движется строго со скоростью света в вакууме. На первый взгляд, возникает кажущееся противоречие со специальной теорией относительности, поскольку частично распространено мнение, что групповая скорость (*это лишь скорость движения вершины огибающей*) и есть скорость распространения информации. Однако при аккуратном рассмотрении [15] скорость распространения информации через такую среду все равно оказывается строго равна скорости света в вакууме.

что с передающей станции Алисы посылаются интенсивные сигналы и детектирование квантовых состояний происходит на той же станции, позволяет упростить оптическую систему на стороне Боба. При этом часть классического сигнала может быть использована для позиционирования.

Выражаю благодарность коллегам по Академии криптографии Российской Федерации за постоянную поддержку. Работа частично поддержана проектом РФФИ # 11-02-00455 и Минобрнауки РФ (госконтракт # 11.519.11.4009).

1. W. K. Wooters and W. H. Zurek, Nature **299**, 802 (1982).
2. C. H. Bennett, Phys. Rev. lett. **68**, 3121 (1992).
3. C. H. Bennett and G. Brassard, *Quantum Cryptography: Public Key Distribution and Coin Tossing*, Proc. of IEEE Int. Conf. on Comput. Sys. and Sign. Proces., Bangalore, India, December 1984, P. 175.
4. C. H. Bennett, G. Brassard, C. Crépeau, and U. Maurer, IEEE Transaction on Information Theory **41**, 1915 (1995).
5. V. Scarani, H. Bechmann-Pasquinucci, N. J. Cerf et al., Rev. Mod. Phys. **81**, 1301 (2009).
6. Л. Д. Ландау, Р. Пайерлс, Zeits. für Phys. **69**, 56 (1931); *Собрание трудов*, Т. 1, М.: Наука, 1969, с. 56; Zeits. für Phys. **62**, 188 (1930); *Собрание трудов*, Т. 1, М.: Наука", 1969, с. 33.
7. Н. Бор, Л. Розенфельд, Math.-Fys. Medd. **12**, 3 (1933); *Собрание научных трудов*, Т. 1, М.: Наука, 1969, с. 39.
8. Н. Н. Боголюбов, Д. В. Ширков, *Введение в теорию квантованных полей*, М.: Наука, 1973.
9. С. Н. Молотков, ЖЭТФ **139**, 429 (2011).
10. I. D. Ivanovic, Phys. Lett. A **123**, 257 (1987); D. Dieks, Phys. Lett. A **126**, 30, (1988); A. Peres, Phys. Lett. A **128**, 19 (1988); G. Jaeger and A. Shimony, Phys. Lett. A **197**, 83 (1995); A. Chefles, Phys. Lett. A **239**, 339 (1998).
11. R. Renner, *Security of Quantum Key Distribution*, arXiv: quant-ph/0512258.
12. A. S. Holevo, *Introduction to Quantum Information Theory*, M.: MTHMO, 2002; Usp. Mat. Nauk **53**, 193 (1998).
13. L. J. Wang, A. Kuzmich, and A. Dogariu, Nature **406**, 277 (2000).
14. A. Sommerfeld in L. Brillouin, *Wave Propagation and Group Velosity*, Academic Press, N.Y.–London, 1960.
15. С. Н. Молотков, Письма в ЖЭТФ **91**, 762 (2010).