Письма в ЖЭТФ, том 85, вып. 9, с. 569 – 575 © 2007 г. 10 мая

Что принципиально нового дает специальная теория относительности для квантовой криптографии в открытом пространстве?

С. Н. Молотков[+*▽], *Д. И. Помозов*[▽□]

[+] *Институт физики твердого тела РАН, 142432 Черноголовка, Московская обл., Россия*

[*] *Академия Криптографии РФ, 121552 Москва, Россия*

[▽] *Факультет вычислительной математики и кибернетики, МГУ им. М.В. Ломоносова, 119899 Москва, Россия*

[□] *Физико-технологический институт РАН, Москва, Россия*

Поступила в редакцию 15 марта 2007 г.

Предложен принципиально новый релятивистский квантовый криптографический протокол распределения ключей через открытое пространство. Протокол гарантирует секретность ключей при любом затухании и не строго однофотонном источнике квантовых состояний.

PACS: 03.65.Bz, 03.67.Db

Проблема распространения секретных ключей является центральной в криптографии. Если существует способ передачи ключей от одного легитимного пользователя к другому с гарантией того, что передаваемые ключи не будут известны третьей стороне, то в этом случае может быть создана абсолютно стойкая криптографическая система, если ключи используются для шифрования в режиме одноразового блокнота [1 – 3].

Информация о ключе – случайной битовой строке – должна быть передана от одного пространственно удаленного легитимного пользователя к другому. Если оставаться в рамках законов классической физики, то информация должна быть передана из одной точки пространства в другую при помощи классических объектов, движение которых в пространстве и времени описывается законами классической физики. В рамках классической ньютоновской картины мира нет запретов на измерение состояния классического объекта с любой степенью точности и без возмущения, поэтому в принципе невозможно гарантировать секретную передачу ключей. То есть невозможно обнаружить пассивное подслушивание передаваемой информации о ключах.

Возможно ли секретное распространение ключей в рамках классической теории поля, точнее говоря, если информация о ключе передается при помощи классических электромагнитных сигналов? В этом случае при описании распространения классических сигналов через пространство необходимо пользоваться уравнениями Максвелла. Группа преобразований пространства-времени становится лоренцовской (или с учетом трансляций, группой Пуанкаре) вместо группы Галилея в классической механике. Возникает также предельная скорость распространения сигналов через пространство-время. Эйнштейновская специальная теория относительности накладывает также релятивистские ограничения на причинно-следственную связь между различными точками в пространстве-времени. Тем не менее, все равно невозможно детектировать попытки подслушивания при передаче информации при помощи классических сигналов электромагнитного поля, поскольку нет запретов на измерение состояния поля без возмущения. Из- за конечности предельной скорости распространения невозможно мгновенно измерить состояния поля, например, форму протяженного электромагнитного сигнала. Но по мере прохождения сигнала через подслушивателя можно без возмущения самого сигнала измерить его состояние. Таким образом, сама по себе специальная теория относительности и релятивистская причинность не дают возможности детектировать попытки подслушивания.

В нерелятивистской квантовой механике группой преобразований пространства и времени остается галиллеева группа. Пространством состояний квантовой системы является гильбертово пространство $\mathcal{H}$. Причем пространство и время являются в определенном смысле внешними по отношению к пространству состояний квантовой системы в том смысле, что для формулировки квантовых криптографических протоколов факт существования пространства и времени явно не используется. Наблюдаемым в квантовой

механике сопоставляются эрмитовы операторы в $\mathcal{H}$. Если информация о ключе передается при помощи квантовых состояний, то оказывается возможным детектировать попытки подслушивания. Это основано на фундаментальных запретах квантовой механики на различимость неортогональных квантовых состояний. Или в более общей форме, на том обстоятельстве, что некоммутирующие операторы, отвечающие наблюдаемым, не могут иметь общей системы собственных векторов. В квантовой криптографии в качестве таких наблюдаемых используются матрицы плотности (положительные эрмитовы операторы со следом единица), как правило, отвечающие чистым состояниям. При этом получение информации о передаваемых состояниях, если они неортогональны, неизбежно приводит к их возмущению [4–6]. Данное обстоятельство позволяет детектировать любые попытки подслушивания. Тот факт, что квантовые объекты распространяются через пространство, явно нигде в квантовых криптографических протоколах не используется. Не важен также физический тип носителя (электрон, фотон и т.д.), важно лишь абстрактное состояние объекта в пространстве состояний $\mathcal{H}$.

Таким образом, в нерелятивистской квантвой криптографии фактически явно не используется ни факт присутствия пространства и времени, ни соображения причинности, ни физический тип квантовой системы. По сути, с этим связаны проблемы с секретностью в квантовой криптографии, связанные с неоднофотонностью источника вместе с затуханием (исчезновением) квантовых состояний в канале связи. Данные обстоятельства приводят к тому, что, начиная с некоторой длины квантового канала связи (соответственно некоторой критической величины затухания), оказывается принципиально невозможно гарантировать секретность передаваемых ключей [7].

На сегодняшний день проводятся интенсивные исследовательские работы по передаче секретных ключей через свободное пространство [8–11]. Целью этих работ является передача ключей через низкоорбитальные спутники на большие расстояния (существенно превышающие предел в 100 км) [11]. Однако все используемые протоколы распределения ключей через открытое пространство основаны на нерелятивистской квантовой криптографии, поэтому все проблемы с секретностью, которые возникают из-за неоднофотонности источника и затуханием, остаются открытыми и для таких систем.

Возникает принципиальный вопрос. Какие еще фундаментальные законы природы и ограничения, диктуемые ими, могут быть использованы для распространения секретных ключей через открытое пространство? Можно ли в принципе сформулировать квантовые криптографические протоколы для открытого пространства, которые избавлены от упомянутых выше проблем? Ответ на этот вопрос оказывается положительным. Ниже будет приведен один из таких протоколов, который гарантирует секретность передаваемых ключей через открытое пространство при любом затухании и оказывается стойким даже в случае не строго однофотонного источника.

В этом протоколе явно используются ограничения на измеримость протяженных в пространстве-времени Минковского квантовых состояний безмассового поля (фотонов). Если для нерелятивистской квантовой криптографии структура пространства и времени фактически не важна, то здесь структура пространства-времени и квантовость неразрывно связаны. Связаны в том смысле, что сам факт существования безмассового поля, распространяющегося с предельно допустимой скоростью, вытекает из групповых свойств пространства-времени. Как известно, такая связь возникает, если рассматривать неприводимые представления группы Пуанкаре в гильбертовом пространстве [12]. Базисные функции одного из неприводимых представлений как раз и описывают состояния фотона с двумя возможными значениями спиральности [12].

В нерелятивистских квантовых криптосистемах обнаружение любых попыток подслушивания гарантируется следующими двумя фундаментальными, тесно связанными между собой, запретами квантовой механики. 1) Невозможностью процесса копирования неизвестного квантового состояния

$$|\varphi_0\rangle \otimes |A\rangle \longmapsto |\varphi_0\rangle \otimes |\varphi_0\rangle \otimes |A_0\rangle, \tag{1}$$

$$|\varphi_1\rangle \otimes |A\rangle \longmapsto |\varphi_1\rangle \otimes |\varphi_1\rangle \otimes |A_1\rangle, \quad \text{если} \quad \langle\varphi_0|\varphi_1\rangle \neq 0.$$

Запрет на копирование неизвестного квантового состояния называется no cloning теоремой [4], и является следствием линейности квантовой теории.

2) Невозможностью получения информации об одном из неортогональных состояний без их возмущения, то есть запрет на процесс

$$|\varphi_0\rangle \otimes |A\rangle \longmapsto U(|\varphi_0\rangle \otimes |A\rangle) = |\varphi_0\rangle \otimes |A_0\rangle, \tag{2}$$

$$|\varphi_1\rangle \otimes |A\rangle \longmapsto U(|\varphi_1\rangle \otimes |A\rangle) = |\varphi_1\rangle \otimes |A_1\rangle,$$
$$\text{если} \quad |A_0\rangle \neq |A_1\rangle,$$

где $|A\rangle$ – состояние прибора наблюдателя, U унитарный оператор, описывающий совместную эволюцию

исследуемого состояния и состояния прибора. Данные запреты, по сути, являются одними из проявлений фундаментального принципа неопределенностей Гейзенберга о невозможности одновременного измерения наблюдаемых, которым отвечают некоммутирующие операторы.

Для ортогональных состояний нет запрета на достоверное и без возмущения различение этих состояний [5], точнее говоря, теорема [5] в этом случае ничего не говорит. Часто произносимые слова при интерпретации данной теоремы о том, что ортогональное состояние "проходит" через вспомогательную систему $|A\rangle$, взаимодействует, по мере прохождения с ней, и изменяет ее состояние, не соответствуют содержанию теоремы. В теореме ничего подобного нет. Теорема носит чисто геометрический характер и утверждает, что вектор состояния вспомогательной системы $|A\rangle$ может быть унитарно повернут в зависимости от входного вектора $|\varphi_{0,1}\rangle$ и переведен в новое состояние $|A_0\rangle$ или $|A_1\rangle$ без изменения входного вектора. При этом неявно предполагается, что входной вектор $|\varphi_{0,1}\rangle$ доступен как целостный объект, то есть для совершения унитарного преобразования U нужно иметь доступ ко всему пространству состояний $\mathcal{H}_{\varphi_{0,1}}$, где отличен от нуля носитель состояния, в противном случае преобразование не будет унитарным. Тот факт, что в доказательстве фигурирует лишь вектор состояния как целостный объект $|\varphi_{0,1}\rangle$ без внутренней координатной "начинки", как раз и подразумевает, что вектор состояния при унитарном преобразовании участвует "сразу целиком".

Для ортогональных состояний безмассового квантованного поля теорема о запрете копирования звучит следующим образом. Ортогональные состояния могут быть с вероятностью сколь угодно близкой к единице скопированы. Но при этом, в результате копирования получаются состояния с той же формой амплитуд, но сдвинутые (транслированные в пространстве-времени). То есть разрешен более слабый процесс по сравнению с нерелятивистским случаем в (1):

$$\begin{aligned} |\varphi_0\rangle &\mapsto (U_L|\varphi_0\rangle) \otimes (U_L|\varphi_0\rangle), \\ |\varphi_1\rangle &\mapsto (U_L|\varphi_1\rangle) \otimes (U_L|\varphi_1\rangle). \end{aligned} \tag{3}$$

Здесь U_L – оператор трансляции в пространстве-времени вдоль ветви светового конуса на величину $L = \Delta(x-t)$ – размер области, где отлична от нуля амплитуда состояний (считаем, для краткости, что оба состояния отличны от нуля в одинаковой пространственно-временной области, но отличаются формой амплитуд $\varphi_{0,1}(x-t)$).

Аналогично модифицируется теорема [5] о различении ортогональных состояний, разрешен лишь более слабый процесс по сравнению с нерелятивистским случаем:

$$\begin{aligned} &|\varphi_0\rangle|A\rangle \mapsto (U_L|\varphi_0\rangle) \otimes |A_0\rangle, \\ &|\varphi_1\rangle \otimes |A\rangle \mapsto (U_L|\varphi_1\rangle) \otimes |A_1\rangle, \quad |A_0\rangle \neq |A_1\rangle. \end{aligned} \tag{4}$$

Сказанное удобно пояснить при помощи следующих диаграмм (рис.1). Поскольку амплитуда состоя-

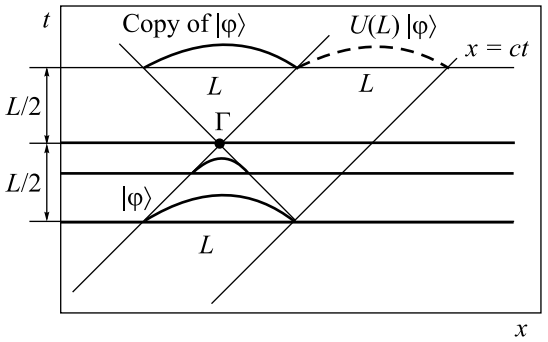

Рис.1

ний безмассового квантованного поля, распространяющихся в одном направлении оси x зависит лишь от разности $x-t$, то можно провести рассуждения, фиксируя время и считая переменной координату, либо наоборот. Этими двумя случаями исчерпываются все ситуации. Пусть задано одно из ортогональных состояний с амплитудой $\varphi(x-t)$, распространяющихся со скоростью света ($c = 1$, индекс состояния 0 или 1 для краткости пока опустим). Пусть состояние сосредоточено в области L, в том смысле, что $\int_L |\varphi(x-t_0)|^2 dx \approx 1$, $\varphi_{0,1}(x-t_0)$ есть амплитуда на временном срезе t_0. Чтобы иметь *сразу все значения амплитуды состояния при всех x, в момент t_0* в той области, где она отлична от нуля, необходимо совершить унитарное преобразование сразу над всем состоянием. Пусть унитарное преобразование над амплитудой состояния – $U\varphi_{0,1}(x-t_0) = \tilde{\varphi}_{0,1}(x'-t)$ $(t > t_0)$, амплитуда нового состояния $\tilde{\varphi}(x'-t)$ может быть отлична от нуля уже в меньшей пространственной области. По существу, минимальный размер области по x' к моменту t диктуется релятивистским принципом причинности. Матричные элементы унитарного оператора отличны от нуля только тогда, когда точки (x, t_0) и (x', t) лежат внутри прошлой части светового конуса, выпущенного из точки Г, и накрывающей область, где отлична от нуля амплитуда состояния в момент t_0. К моменту времени не ранее, чем L амплитуда исходного состояния может быть унитарным образом преобразо-

вана в состояние со сколь угодно сильно локализованной амплитудой в окрестности Г. Принципиально важно, что это будет уже *другое* состояние, чем исходное $\varphi(x-t_0)$. К моменту Г доступны значения амплитуды состояния при всех x сразу (мгновенно). Теперь можно мгновенно получить исход измерения и иметь полную (с вероятностью единица) информацию о состоянии. Если пара исходных состояний была ортогональна, то можно унитарным преобразованием получить также пару ортогональных состояний к моменту Г и, соответственно, достоверно отличить одно от другого (теперь уже можно воспользоваться теоремой [5] о достоверной различимости ортогональных состояний). Подчеркнем еще раз, что это будут уже *другие* ортогональные состояния, отличные от исходных. "Восстановление" или копирование состояния также может быть реализовано обратным унитарным преобразованием, "направленным" вперед во времени. Состояние с той же формой амплитуды, как исходное, может быть получено к моменту не ранее, чем это диктуется релятивистской причинностью. Амплитуда состояния с той же формой, как у исходного, находится в передней части светового конуса, выпущенного из точки Г. Полученное состояние также *другое* по сравнению с исходным в том смысле, что оно запаздывает по времени по отношению к исходному состоянию, которое успело бы распространиться вперед по x к моменту L как раз на величину L, если бы не было попыток копирования или получения информации о нем (рис.1). Пока речь шла о получении информации о состояниях в канале с вероятностью единица. Те же самые рассуждения годятся для получения информации с вероятностью, меньшей единица. Задержка при этом будет меньше L (рис.1).

Фактически, ни один исход измерения над квантовым состоянияем, если доступна лишь часть области, не может иметь большую вероятность, чем доля нормировки, которая набирается в этой простанственно-временной области. Доступ же к конечной пространственно-временной области из-за конечности предельной скорости не может быть получен мгновенно. Ограничения на измеримость квантовых состояний в релятивистской области впервые рассматривались в работах [13, 14].

Сформулируем теперь сам протокол.

1). Алиса в известный ей и случайный момент времени t_A приготавливает сильно локализованное состояние $|\phi\rangle$. Времена с точностью длительности состояния считаются нулевыми и не различаются. Далее состояние поступает на вход разбалансированного интерферометра Маха-Цандера с разностью длин плеч $l = tc$ ($c = 1$). На выходе интерферометра возникает протяженное состояние размером l, состоящее из суперпозиции двух "половинок" (рис.2) вида

$$\frac{1}{\sqrt{2}}\left(|\phi\rangle + |\phi_l\rangle\right), \quad |\phi_l\rangle = U(l)|\phi\rangle, \tag{5}$$

где состояние $|\phi_l\rangle$ получается из $|\phi\rangle$ задержкой на время l, которая описывается оператором трансляции $U(l)$.

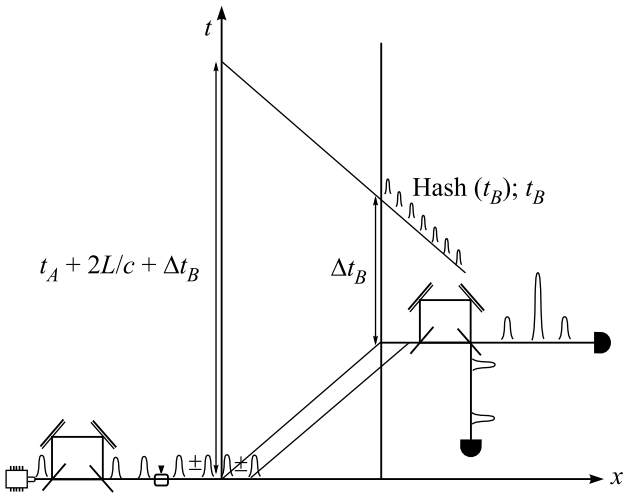

Рис.2

2). Далее состояние поступает на фазовый модулятор (рис.2), на который случайно и равновероятно прикладывается импульс напряжения в момент прохождения задней "половины" состояния. Прикладываемое напряжение изменяет показатель преломления, что приводит в появлению дополнительной относительной разности фаз между "половинками". В результате на выходе в канал связи посылается одно из двух ортогональных состояний, отвечающих 0 и 1, имеем

$$0 \to \frac{1}{\sqrt{2}}\left(|\phi\rangle + |\phi_l\rangle\right), \quad 1 \to \frac{1}{\sqrt{2}}\left(|\phi\rangle - |\phi_l\rangle\right). \tag{6}$$

3). На приемной станции, расстояние до которой известно, имеется интерферометр Маха-Цандера, аналогичный интерферометру на передающей станции. В зависимости от поступающего из канала связи состояния по конструктивному (верхнему) и деструктивному (нижнему) выходам интерферометра возникают состояния вида (рис.2)

$$\frac{1}{\sqrt{8}}\left(|\phi\rangle + 2|\phi_l\rangle + |\phi_{2l}\rangle\right), \quad \frac{1}{\sqrt{8}}\left(|\phi\rangle + |\phi_{2l}\rangle\right) \tag{7}$$

для бита 0, и аналогично для бита 1 (рис.2)

$$\frac{1}{\sqrt{8}}\left(|\phi\rangle + |\phi_{2l}\rangle\right), \quad \frac{1}{\sqrt{8}}\left(|\phi\rangle + 2|\phi_l\rangle + |\phi_{2l}\rangle\right); \qquad (8)$$

здесь $|\phi_{2l}\rangle$ – состояние, сдвинутое относительно $|\phi\rangle$ на время $2l = 2tc$.

4). Детекторы Боба работают в ждущем режиме. После возникновения фотоотсчета либо по верхнему, либо по нижнему выходу Боб фиксирует момент фотоотсчета t_B, запускается электроника для вычисления – хэш-значения от момента регистрации $y = h(t_B)$. Данное вычисление занимает известное число тактов по времени – $\Delta(t_B)$. Затем к Алисе посылается классическое сообщение – хэш-значение y и значение момента регистрации у Боба $h(t_b)$.

Как в нерелятивистской квантовой криптографии, так и в релятивисткой открытый классический канал связи необходим. В обоих случаях на классический канал накладывается требование целостности и аутентичности информации, передаваемой между Алисой и Бобом (так называемый unjumable channel). Принципиальное отличие в релятивистском случае состоит в том, что данный канал также является каналом реального времени – хронометраж отправки и получения классических сообщений принципиален для секретности ключей.

5). Алиса получает классическое сообщение от Боба и фиксирует момент прихода первого бита сигнала. Если не было задержки, как квантового состояния, так и классического сигнала, то момент прихода классического сигнала есть $t_{B\to A} = t_A + 2L/c + \Delta(t_B)$. Возможны три различных значения $t_{B\to A}$ в зависимости от того, в какой момент времени произошел отсчет у Боба. Если значение $t_{B\to A}$ отвечает отсчету в центральном пике, то отсчет принимается. При этом отсчет у Боба по верхнему или нижнему детекторам интерпретируется однозначно как 0 или 1. Обработав сообщение от Боба, Алиса посылает классический сигнал, который она формулирует так же, как и Боб. Сигнал содержит информацию о том, принимается отсчет Боба или отбрасывается (если отсчеты были в крайних временных слотах, (рис.2). Такт передачи одного бита первичного ключа закончен.

6). После передачи необходимого количества состояний раскрывается случайная подпоследовательность и оценивается вероятность ошибки. Далее, если процент ошибок меньше критической величины, происходит их распределенная коррекция и усиление секретности очищенного ключа, аналогично тому, как это происходит в нерелятивиской квантовой криптографии [15].

Анализ секретности протокола существенно проще, чем в нерелятивистском случае. Поскольку информационные состояния ортогональны и все события развиваются в реальном времени, нет необходимости рассматривать коллективные атаки Евы на ключ. Это связано с тем, что ошибки Евы при различении квантовых состояний возникают не за счет их неортогональности, а за счет того, что Ева не может мгновенно получить доступ к протяженным *ортогональным состояниям*.

Для протокола важно, что состояния посылаются в случайные моменты времени, которые неизвестны Еве. Если бы состояния посылались в известные моменты времени, то в этом случае Ева могла заранее приготовить состояние вида (6), которое сразу начнет распространяться в канал связи. При этом Ева одновременно измеряет приходящее состояние Алисы. К моменту, когда задняя "половинка" из суперпозиции достигает Еву, Ева будет точно знать это состояние из-за их ортогональности. В этот же момент Ева может изменить относительную фазу между "половинками" в суперпозиции своего заранее заготовленного состояния. При этом такая атака не детектируется. Строго говоря, такая атака приведет к задержке состояния Евы на время, равное протяженности локализованного состояния, но такие времена в протоколе считаются нулевыми, и задержки на такие времена не детектируются.

Если состояния посылаются в случайные моменты времени, то такая атака не проходит. Ева может измерить состояние в канале, чтобы узнать время прихода передней "половинки" из суперпозиции, однако после такого измерения из-за редукции состояния Ева уже не сможет узнать к какому из двух ортогональных состояний относилась передняя "половинка". Вероятность узнать передаваемый Алисой бит, если доступна только передняя "половинка" в суперпозиции, при условии, что отсчет от нее произошол, равна $1/2$, то есть вероятности простого угадывания. Соответственно информация о передаваемом бите равна нулю. Перепосыл состояний наугад приведет к вероятности ошибки в 50% для тех состояний, которые Ева измеряла и пересылала.

Ева может дождаться момента, когда состояние станет ей доступно целиком, при этом Ева будет с достоверностью знать передаваемый бит. Однако в этом случае Ева внесет задержку равную расстоянию между "половинками". Отсчет о правильном, но задержанном состоянии будет давать отсчеты в центральном временном слоте (рис.2), задней "половинкой" состояния. Такие отсчеты приведут к ошибкам (их вероятность одинакова как по верхнему, так

и нижнему детекторам, в отличие от незадержанного состояния). Это даст 50% ошибок для той доли состояний, с которыми Ева производила манипуляции.

Таким образом, если доля состояний Боба, над которыми Ева производила подслушивание, из общего количества им зарегистрированных, равна $\delta = m/N$ (m – число подслушиваемых состояний, которые дали отсчеты у Боба, N – общее количество состояний, зарегистрированных Бобом), то ошибка от этих состояний равна $1/2$. Общий процент ошибок у Боба есть

$$Q = \frac{1}{2}\frac{m}{N} = \frac{\delta}{2}, \tag{9}$$

соответственно, взаимная информация Евы и Боба о ключе равна

$$\begin{gathered} I_{AE}(Q) = \delta = 2 \cdot Q \quad I_{AB}(Q) = 1 - h(Q), \\ h(Q) = -Q\log Q - (1-Q)\log(1-Q). \end{gathered} \tag{10}$$

Распространение секретного ключа, согласно теореме [16], возможно, если $I_{AB}(Q) > I_{AE}(Q)$. Критическая ошибка определяется из равенства

$$I_{AB}(Q_c) = I_{AE}(Q_c), \quad Q_c \approx 17\%. \tag{11}$$

До сих пор мы считали, что состояния Алисы строго однофотонные. Рассмотрим теперь случай, когда состояния Алисы получаются путем ослабления лазерного излучения. В этом случае состояния описываются когерентными состояниями со средним числом фотонов μ, которое известно всем участникам протокола, включая Еву. В этом случае возможна атака Евы на ключ, которая не приводит к задержкам и ошибкам на приемном конце. Далее считаем, что фотодетектор Боба *не различает число фотонов*. Считаем также, что Боб *не контролирует и не знает априорно затухания в канале связи*.

Атака Евы сводится к следующему. Ева использует светоделитель с коэффициентом деления η, который она может выбрать оптимальным для себя образом, и который зависит от среднего числа фотонов. Часть фотонов отводится к Еве и измеряется Евой. Будут события, которые дадут одновременно фотоотсчеты и у Евы, и у Боба. Для таких событий Ева знает передаемый бит. Для событий, когда регистрация была только у Боба, Ева не знает передаваемого бита. Если фотоотсчет возник только у Евы, и не возник у Боба, то хотя Ева и знает передаваемый бит Алисы, но данная посылка будет далее отброшена Алисой и Бобом как холостая.

Таким образом, задача сводится к подсчету вероятности этих трех событий. Квантовое состояние лазерного излучения, которое поступает в канал связи от Алисы, имеет вид

$$\begin{gathered} |\psi_i(\mu)\rangle_A = e^{-\frac{\mu}{2}} \sum_{n=0}^{\infty} \sqrt{\frac{\mu^n}{n!}} |\psi_i(n)\rangle_A, \\ |\psi_i(n)\rangle_A = \left(\frac{1}{\sqrt{2}}\left(\phi^+ + (-1)^i \phi_l^+\right)\right)^n |0\rangle, \ i = 0,1. \end{gathered} \tag{12}$$

Индекс $i = 0,1$ отвечает информационным состояниям для 0 и 1. ϕ^+, ϕ_l^+ – операторы рождения локализованных состояний, μ – среднее число фотонов в импульсе, $|0\rangle$ – вакуумное состояние, индекс "A" – означает состояние Алисы.

Если Ева использует светоделитель с коэффициентом деления η и отводит часть когерентного состояния себе, то после светоделителя состояния Ева и Боба имеют вид (ниже учтено, что когерентное состояние преобразуется на светоделителе в два когерентных состояния со средним числом фотонов в каждом, пропорциональным коэффициенту деления)

$$\begin{gathered} |\psi_i(\mu)\rangle_{EB} = |\psi_i(\mu_E)\rangle_E| \otimes \psi_i(\mu_B)\rangle_B = \\ = \left(e^{-\frac{\mu_E}{2}} \sum_{n=0}^{\infty} \sqrt{\frac{\mu_E^n}{n!}} |\psi_i(n)\rangle_E\right) \otimes \\ \otimes \left(e^{-\frac{\mu_B}{2}} \sum_{n=0}^{\infty} \sqrt{\frac{\mu_B^n}{n!}} |\psi_i(n)\rangle_B\right); \end{gathered} \tag{13}$$

здесь $\mu_E = \mu \cdot (1-\eta)$, $\mu_B = \mu \cdot \eta$ – среднее число фотонов в квантовом состоянии у Евы и Боба.

Ева может зарегистрировать $n_E = 0,1,2..$ фотонов, Боб может зарегистрировать $n_B = 0,1,2...$ фотонов. Нас интересует вероятность того, что Боб зарегистрировал $n_B \geq 1$ фотонов, а Ева зарегистрировала $n_E = 0$ фотонов. Разность взаимных информаций о ключе Боба I_{AB} и Евы I_{AE} равна

$$\begin{gathered} \Delta I(\mu,\eta) = I_{AB}(\mu,\eta) - I_{AE}(\mu,\eta) = \\ \frac{\Pr\{n_B \geq 1 \wedge n_E = 0\}}{\Pr\{n_B \geq 1\}} = \frac{e^{-(1-\eta)\mu} - e^{-\mu}}{1 - e^{-\eta\mu}}. \end{gathered} \tag{14}$$

При малых η ($\eta\mu \ll 1$), когда Ева отводит себе большую часть когерентного состояния, разность взаимных информаций

$$\Delta I(\mu,\eta) \approx e^{-\mu}, \quad \eta\mu \ll 1. \tag{15}$$

При небольшом среднем числе фотонов в исходном состоянии Алисы, например $\mu = 1 \div 2$, Ева знает $\approx 80\%$ зарегистрированных Бобом бит ключа (соответственно не знает $\approx 20\%$). Зависимость (15) является предельной. Пусть μ фиксировано, даже при

$\eta \to 0$ почти все фотоны отводятся Евой, все равно Еве не будет известна $e^{-\mu}$ доля *зарегистрированных* бит ключа у Боба. Это связано фактически с тем, что в когерентном состоянии с вероятностью $e^{-\mu}$ имеется вакуумная компонента, которая приводит к тому, что всегда будет ненулевая вероятность событий, когда Боб зарегистрировал фотон, а Ева – нет.

В заключение сформулируем выводы.

1. В релятивистской квантовой криптографии для секретности принципиально не требуется строго однофотонный источник. Можно работать при среднем числе фотонов $\mu \approx 1 \div 3$, в отличие от нерелятивистской квантовой криптографии, где обычно приходится ослаблять сигнал до уровня $\mu \approx 0.1 \div 0.3$ фотонов в импульсе.

2. В релятивистской квантовой криптографии секретность ключа гарантируется при любом затухании в канале связи. Действие затухания аналогично действию светоделителя. В светоделите каждый фотон с вероятностью $1-\eta$ попадает к Еве, и с вероятностью η направляется к Бобу. Пусть затухание – вероятность поглощения фотона в канале связи (пространстве между Алисой и Бобом) есть Γ. В случае затухания каждый фотон с вероятностью Γ будет поглощен средой, а с вероятностью $1-\Gamma$ дойдет до Боба. Тогда аналогично ситуации со светоделителем возможны три события. Все фотоны будут поглощены в канале связи. Часть фотонов поглотится в канале, часть дойдет до Боба (данные биты известны как Бобу, так и Еве). Все фотоны дойдут до Боба (данные биты известны только Бобу). Далее подсчет разности взаимных информаций о ключе Боба и Евы (среды) сводится к описанному выше случаю (формулы (14), (15)) с заменой $1-\eta \to \Gamma$. Даже в пределе сильного затухания ключ остается секретным, естественно при этом скорость генерации ключа экспоненциально падает с Γ.

3) Релятивистская квантовая криптография устойчива относительно PNS атаки (Photon Number Splitting). Подслушивателю для того, чтобы определить неразрушающим измерением число фотонов в канале связи требуется доступ к состоянию как целому. Такое измерение описывается разложением единицы по ортогональным проекторам вида $I = \sum_{n=0}^{\infty}(|\psi_0(n)\rangle\langle\psi_0(n)| + |\psi_1(n)\rangle\langle\psi_1(n)|)$, которые нелокальны, если состояние является протяженным в пространстве-времени. То есть чтобы достоверно отличить число фотонов, требуется доступ ко всему состоянию, что приведет к задержкам. Поэтому такая атака в релятивистском случае сводится к описанному выше случаю.

Один из авторов (С.Н.М.) благодарит Академию Криптографии РФ за поддержку. Работа поддержана грантами Российского фонда фундаментальных исследований # 05-02-08306-офи-а, # 05-02-17387.

1. G. S. Vernam, J. Amer. Inst. Elect. Eng. **55**, 109 (1926).
2. В. А. Котельников, Отчет 18 июня 1941 г.
3. C. E. Shannon, Bell Syst. Tech. Jour. **28**, 658 (1949).
4. W. K. Wootters and W. H. Zurek, Nature **299**, 802 (1982).
5. C. H. Bennett, Phys. Rev. Lett. **68**, 3121 (1992); C. H. Bennett, G. Brassard, and N. D. Mermin, Phys. Rev. Lett. **68**, 557 (1992).
6. C. H. Bennett and G. Brassard, Proc.of IEEE Int. Conf. on Comput. Sys. and Sign. Proces., Bangalore, India, December 1984, p. 175.
7. A. Acin, N. Gisin, and V. Scarani, quant-ph/0302037.
8. R. J. Hughes, J. E. Nordholt, D. Derkacs, and C. G. Peterson, New Journal of Physics **4**, 43.1-43.14 (2002).
9. J. G. Rarity, P. R. Tapster, P. M. Gorman, and P. Knight, New J. of Physics **4**, 82.1-82.21 (2002).
10. M. Aspelmeyer, T. Jennewein, M. Pfennigbauer et al., IEEE J. of Selected Topics in Quantum Electronics, spesial issue on Quantum Internet Technologies **9**, 1541 (2003).
11. R. Ursin, F. Tiefenbacher, T. Schmitt-Manderbach et al., quant-ph/0607182.
12. Н. Н. Боголюбов, Д. В. Ширков, *Введение в теорию квантованных полей*, М.: Наука, 1973.
13. Л. Д. Ландау, Р. Пайерлс, Zeits. für Phys. **69**, 56 (1931); *Собрание трудов*, т. 1, М.: Наука, 1969, стр. 56; Zeits. für Phys. **62**, 188 (1930), *Собрание трудов*, т. 1, М.: Наука, 1969, стр. 33.
14. Н. Бор, Л. Розенфельд, Math.-Fys. Medd. **12**, 3 (1933), *Собрание научных трудов*, т. 1, М.: Наука, 1969, стр. 39.
15. C. H. Bennett, G. Brassard, C. Crépeau, and U. Maurer, IEEE Transaction on Information Theory **41**, 1915 (1995).
16. I. Csiszár and J. Körner, IEEE Trns. Inf. Theory **24**, 339 (1978).