ЖЭТФ, 2011, том 140, вып. 5 (11), стр. 857–870

КВАНТОВОЕ РАСПРЕДЕЛЕНИЕ КЛЮЧЕЙ С ЭТАЛОННЫМ КВАНТОВЫМ СОСТОЯНИЕМ

С. Н. Молотков*

Институт физики твердого тела Российской академии наук
142432, Черноголовка, Московская обл., Россия

Академия криптографии Российской Федерации
121552, Москва, Россия

Московский государственный университет им. М. В. Ломоносова
119899, Москва, Россия

Поступила в редакцию 25 марта 2011 г.

Предлагается новый протокол квантового распределения ключей, устойчивый к произвольным потерям в квантовом канале связи. Принципиально важно для стойкости протокола, что изменения состояний, связанные с потерями в канале связи (в отсутствие подслушивателя), уже включены в измерения.

1. ВВЕДЕНИЕ

Одной из проблем при реализации систем квантовой криптографии является проблема неидеальности аппаратуры. Основными причинами, ограничивающими дальность передачи ключей, являются потери в квантовом канале связи и не строгая однофотонность источника информационных квантовых состояний [1]. Темновые шумы лавинных детекторов также ограничивают дальность передачи ключей. Однако даже при идеальных фотодетекторах неизвестно ни одного протокола квантового распределения ключей, который бы гарантировал секретность ключей при любых потерях, соответственно, при любой сколь угодно большой длине квантового канала связи и неоднофотонном источнике. Более точно, при неоднофотонном источнике существует критическая длина линии связи (и величина потерь в ней), при превышении которой невозможно гарантировать передачу секретных ключей.

При анализе криптографической стойкости протоколов квантового распределения ключей величина потерь в линии связи считается заранее известной и является параметром протокола. Поскольку в квантовой криптографии квантовый канал связи[1)] не контролируется легитимными пользователями, подслушиватель может проводить любые модификации квантовой линии связи в своих интересах. Например, подслушиватель может заменить исходную линию связи с потерями своей линией связи, но с меньшими потерями (в предельном случае вообще без потерь). Поскольку в канале с потерями часть квантовых состояний поглощается в линии связи, этот факт может использоваться подслушивателем для извлечения информации о передаваемом ключе и дальнейшей перепосылки модифицированных состояний через канал с меньшими потерями, чтобы сохранить общее число состояний, которые должны достигать приемной стороны (см., например, [1, 2]).

Вопрос о возможности существования протоколов квантового распределения ключей, которые при не строго однофотонном источнике и при любой длине квантового канала (любых потерях в нем) гарантировали бы секретность передаваемых ключей, носит принципиальный характер для квантовой криптографии. Естественно, скорость передачи ключей с ростом длины уменьшается (как правило, экспоненциально), но секретность ключей при этом все равно гарантируется фундаментальными запретами квантовой механики на различимость квантовых состояний[2)].

Если кроме фундаментальных ограничений квантовой механики на различимость квантовых состо-

*E-mail: molotkov@issp.ac.ru

1) В данной работе будем иметь в виду только оптоволоконные системы квантовой криптографии.

2) Имеется в виду без темновых шумов фотодетекторов.

яний использовать дополнительные фундаментальные ограничения, диктуемые специальной теорией относительности — релятивистской причинностью, то можно сформулировать релятивистские квантовые протоколы распределения ключей через открытое пространство, которые гарантируют секретность ключей при любом затухании (и идеальных детекторах) и передачу их на любое расстояние даже при не строго однофотонном источнике квантовых состояний [3].

Принципиальным отличием релятивистской квантовой криптографии для открытого пространства от систем квантовой криптографии, которые основаны только на запретах квантовой механики, является тот факт, что заранее не требуется знать потери в канале связи. Величина потерь может быть любой и может изменяться в процессе передачи ключей [3]. Это обстоятельство оказывается принципиально важным для передачи ключей через открытое пространство, поскольку, в отличие от волоконных линий связи, потери в открытом пространстве заранее неизвестны.

Протоколы квантового распределения ключей должны быть стойкими — гарантировать секретность ключей при всевозможных атаках. Неоднофотонность источника квантовых состояний и потери в линии связи открывают возможность для ряда новых атак, которые были бы невозможны при однофотонном источнике и линии связи без потерь [1, 2].

Рассмотрим виды атак.

1) Атака с неразрушающими измерениями числа фотонов (Photon Number Splitting, PNS-атака) [2]. В квантовой механике нет запретов на неразрушающие (без возмущения) измерения числа фотонов в линии. При такой атаке подслушиватель измеряет число фотонов, но не их состояние. Если обнаружен один фотон, то посылка блокируется. Если обнаружено более одного фотона в линии, то один из них посылается на приемную станцию через канал с меньшими потерями (в пределе без потерь), а остальные сохраняются у подслушивателя в квантовой памяти до раскрытия базисов. Затем после стадии раскрытия базисов легитимными пользователями подслушиватель проводит измерения в известном базисе и получает достоверную информацию о передаваемом состоянии, не производя ошибок на приемной стороне. Для протоколов с ортогональными состояниями внутри базиса, как, например, протокола BB84 [4], начиная с некоторой длины линии связи, секретная передача ключей становится невозможной. Для протокола BB84 для типичных величин потерь в одномодовом оптоволокне и среднего числа фотонов в когерентном состоянии протокол не секретен, начиная с длины линии в несколько десятков километров. Данная атака не приводит к ошибкам на приемной стороне. При превышении критической длины линии подслушиватель знает весь ключ и не детектируется легитимными пользователями.

2) Подслушиватель отводит часть состояния для своих измерений, а оставшиеся состояния посылает через свой идеальный без потерь канал связи на приемную сторону. Отводится такая доля состояний, чтобы сохранить число посылок, которые должны достичь приемной стороны через исходный канал с потерями и без подслушивателя. Для такой атаки подслушивателю нужен идеальный (или с меньшими потерями) канал связи и, возможно, квантовая память. Такая атака не приводит к ошибкам на приемной стороне.

3) Подслушиватель разрывает квантовый канал связи вблизи приемной и передающей сторон и проводит измерения с определенным результатом (unambiguous measurements, см., например, [5–7]). Такие измерения позволяют однозначно, но с определенной вероятностью такого исхода, различать неортогональные информационные квантовые состояния. Если получен определенный (conclusive) исход, то подслушиватель наверняка знает передаваемое квантовое состояние. Вблизи приемной стороны можно приготовить правильное невозмущенное квантовое состояние и послать его на приемную сторону. Если получен неопределенный (inconclusive) исход, то подслушиватель не знает передаваемое состояние, и в канале с потерями, начиная с некоторой критической величины потерь (длины), может блокировать данную посылку, сохраняя среднее число посылок, достигающих приемной стороны. Если вероятность неопределенных (inconclusive) исходов равна вероятности потерь в канале связи, то среднее число посылок при этом сохранится. Например, протокол B92 [8], в котором используется пара неортогональных состояний, становится несекретным даже при строго однофотонном источнике, когда вероятность потерь в линии связи становится равной вероятности неопределенных исходов[3)].

[3)] Ниже покажем, что использование неоднофотонных когерентных состояний и измерений, которые учитывают потери в канале связи, приводит к тому, что протокол B92 становится секретным при любой длине линии (в отсутствие темновых шумов детекторов). Поэтому оказывается, что неоднофотонное состояние для данного протокола лучше, чем строго однофотонное. Формальная причина этого кроется в том, что когерентное состояние в отличие от строго однофотонного пакета содержит вакуумную компоненту.

Данная атака может быть использована в комбинации с предыдущей PNS-атакой. Например, если состояния внутри базиса неортогональны, как это имеет место в протоколе SARG04 [9] и в протоколе с фазово-временным кодированием [10], то после неразрушающих измерений и определения числа фотонов в линии подслушиватель проводит измерения с определенным исходом над частью фотонов. Если получен положительный исход, то часть фотонов посылается на приемную сторону. Если получен неопределенный исход, то посылка блокируется. Оказывается, что с определенной величины потерь в линии (соответственно, длины) подслушиватель может блокировать все посылки, которые содержат менее трех фотонов. Из остальных посылок, с числом фотонов более трех, подслушиватель знает достоверно все передаваемые состояния и не производит ошибок на приемной стороне, т. е. остается недетектируемым. В протоколе с фазово-временным кодированием подслушиватель, чтобы знать весь ключ и остаться незамеченным, должен блокировать все посылки, содержащие менее пяти фотонов. Поэтому данный протокол обеспечивает передачу секретных ключей на бóльшие расстояния по сравнению с протоколом SARG04.

4) Подслушиватель (Ева) применяет атаку с «прозрачным» подслушиванием. Используется вспомогательное квантовое состояние, которое приводится во взаимодействие с передаваемым состоянием, вследствие чего происходит их запутывание. Искаженное состояние с передающей стороны (Алисы) направляется на приемную сторону (Бобу), а над своим подслушиватель проводит измерения. Такая атака является универсальной и не зависит от неоднофотонности источника и потерь в канале. Однако она приводит к ошибкам на приемной стороне, т. е. к детектированию подслушивателя.

За последние годы были предложены новые протоколы квантового распределения ключей, которые, по-видимому, обеспечивают секретность по отношению к атаке с измерениями с определенным исходом, PNS-атаке и потерям в канале связи (см. работы [11–16]). В этом семействе протоколов используется серия когерентных состояний. Для детектирования подслушивателя измеряется интерференция состояний из различных посылок внутри серии. Анализ данных протоколов до конца не сделан. Трудность состоит в том, что состояния из разных посылок, в отличие от всех предыдущих протоколов, не являются независимыми — они являются когерентными во всей передаваемой серии состояний. По этой причине подслушиватель не может блокировать отдельные посылки, если получен неопределенный исход, поскольку такое отсутствие посылки будет детектироваться. Однако в реальности серия состояний, имеющих общую фазовую когерентность, не является бесконечной (содержит порядка десяти когерентных между собой импульсов). Поэтому подслушиватель может проводить измерения с определенным исходом для различения состояний не в отдельной посылке, а в целой серии (нескольких посылках), рассматривая серию как единое квантовое состояние. При этом, если получен неопределенный исход, то Ева блокирует целую серию посылок. Ясно, что с некоторой критической величины потерь в линии связи такое блокирование возможно с сохранением общего среднего числа серий посылок и не будет детектироваться, поскольку не приводит к появлению ошибок на приемной стороне. Также ясно, что критическая длина линии при этом будет больше, чем в протоколах, где можно блокировать лишь отдельные посылки. Однако при этом все равно нельзя передавать ключи на произвольно большие расстояния.

Ниже приведен пример протокола квантового распределения ключей, который обеспечивает секретность ключей при любых потерях (длине линии связи) и неоднофотонном источнике. Дальность ограничивается только шумами фотодетекторов. Основная идея состоит в том, чтобы осуществлять такие измерения, которые бы изначально учитывали изменения когерентного состояния за счет потерь в линии связи, но без подслушивателя. В отличие от протоколов [11–16], в которых нарушение когерентности состояний проводится путем сравнения состояний из разных посылок, которые все прошли через канал связи и были подвержены возмущению подслушивателем, в данном протоколе детектирование нарушения когерентности состояния в канале связи происходит путем сравнения этого состояния с эталонным состоянием. Эталонное квантовое состояние «хранится» на приемно-передающей стороне и недоступно подслушивателю. Это обстоятельство позволяет рассматривать каждую посылку индивидуально, что делает анализ криптографической стойкости достаточно простым.

Чтобы отделить саму идею протокола от конкретной технической реализации, отметим, что приводимая ниже схема на основе волоконного интерферометра Майкельсона не является единственной, существуют и другие более технологические реализации.

2. ОСНОВНАЯ ИДЕЯ КВАНТОВОГО РАСПРЕДЕЛЕНИЯ КЛЮЧЕЙ С ЭТАЛОННЫМ СОСТОЯНИЕМ

Любой протокол квантовой криптографии должен быть устроен и реализован таким образом, чтобы детектировать любые возмущения информационных квантовых состояний на приемной стороне при любых атаках и любых потерях в канале связи. В канале без потерь все состояния достигают приемной стороны. В канале с потерями некоторые состояния поглощаются средой и не достигают приемной стороны либо достигают приемной стороны искаженными с меньшим числом фотонов, если используется неоднофотонный источник.

В реальных системах используется ослабленное лазерное излучение, которое описывается когерентным состоянием $|\alpha\rangle$ (среднее число фотонов в когерентном состоянии $\mu = |\alpha|^2$). Потери приводят к тому, что приемной стороны достигает когерентное состояние с меньшим средним числом фотонов $\mu(L) = \mu T(L)$. При распространении по одномодовому оптоволокну с линейными потерями когерентное состояние преобразуется как $|\alpha\sqrt{T(L)}\rangle$, где $T(L) = 10^{-\gamma L/10}$ — пропускание канала длиной L, γ — коэффициент линейного поглощения (для одномодового оптоволокна SMF-28 $\gamma \approx 0.2$ дБ/км). Здесь мы пренебрегаем другими механизмами декогерентности кроме потерь. Потери наиболее критичны для секретности ключей. Другие механизмы — сбой фазы, поляризации — приводят к ошибкам на приемной стороне, поэтому детектируются.

Пусть длина линии связи фиксирована и величина потерь в ней может быть прокалибрована заранее. Тогда при заданных потерях заранее известно, какое когерентное состояние должно поступить на приемную сторону из канала связи в отсутствие подслушивателя. Это состояние имеет вид $|e^{i\varphi}\sqrt{\mu(L)}\rangle$, где φ — фаза комплексного параметра α, описывающего когерентное состояние.

Основная идея состоит в том, чтобы построить измерения на приемной стороне таким образом, чтобы заранее учесть ослабление когерентного состояния за счет потерь в канале связи, но без подслушивателя.

Измерение, которое позволяет отличить состояние $|e^{i\varphi}\sqrt{\mu(L)}\rangle$ от любых других состояний, может быть записано в виде следующего разложения единицы:

$$I = P\left(e^{i\varphi}\sqrt{\mu(L)}\right) + P_\perp\left(e^{i\varphi}\sqrt{\mu(L)}\right), \qquad (1)$$

$$P\left(e^{i\varphi}\sqrt{\mu(L)}\right) = |e^{i\varphi}\sqrt{\mu(L)}\rangle\langle e^{i\varphi}\sqrt{\mu(L)}|,$$

$$P_\perp\left(e^{i\varphi}\sqrt{\mu(L)}\right) = I - P\left(e^{i\varphi}\sqrt{\mu(L)}\right).$$

Данное измерение имеет два исхода, каждому из которых сопоставлен проектор. При этом исход $\perp$ никогда не происходит от состояния $|e^{i\varphi}\sqrt{\mu(L)}\rangle$. Вероятность данного исхода тождественно равна нулю:

$$\Pr\left(\perp, |e^{i\varphi}\sqrt{\mu(L)}\rangle\right) = \mathrm{Tr}\left\{P_\perp\left(e^{i\varphi}\sqrt{\mu(L)}\right) \times \right.$$
$$\left. \times\ |e^{i\varphi}\sqrt{\mu(L)}\rangle\langle e^{i\varphi}\sqrt{\mu(L)}|\right\} \equiv 0. \qquad (2)$$

С формальной точки зрения данный протокол аналогичен протоколу B92 [8], однако в отличие от исходного протокола данный протокол устойчив к потерям в квантовом канале связи за счет специальных измерений на приемной стороне. Как будет показано ниже, в отсутствие темновых шумов фотодетекторов длина линии связи с потерями не ограничена, т. е. секретность передаваемых ключей гарантируется при любых потерях (длине линии связи). Разумеется, скорость генерации ключей при этом уменьшается, но секретность сохраняется.

В протоколе используется пара неортогональных состояний, отвечающих 0 и 1:

$$\begin{array}{ccll} 0 & — & |e^{i\varphi_0}\sqrt{\mu}\rangle, & \varphi_0 = 0, \\ 1 & — & |e^{i\varphi_1}\sqrt{\mu}\rangle, & \varphi_1 = \pi, \end{array} \qquad (3)$$

которые посылаются в канал связи равновероятно.

На приемной стороне случайно и независимо от передающей стороны используется одно из двух разных измерений, каждое из которых имеет два исхода. Измерения имеют вид[4)]

$$I = P\left(e^{i\varphi_{0,1}}\sqrt{\mu(L)}\right) + P_\perp\left(e^{i\varphi_{0,1}}\sqrt{\mu(L)}\right), \qquad (4)$$

$$P\left(e^{i\varphi_{0,1}}\sqrt{\mu(L)}\right) = |e^{i\varphi_{0,1}}\sqrt{\mu(L)}\rangle\langle e^{i\varphi_{0,1}}\sqrt{\mu(L)}|,$$

$$P_\perp\left(e^{i\varphi_{0,1}}\sqrt{\mu(L)}\right) = I - P\left(e^{i\varphi_{0,1}}\sqrt{\mu(L)}\right).$$

Индексы «0» и «1» обозначают номер измерения.

Пара таких измерений позволяет детектировать любые изменения входных состояний (3) после прохождения через канал с затуханием.

Принципиально важным для стойкости протокола является то, что изменения состояний, связанные с потерями в канале связи (в отсутствие подслушивателя) уже включены в измерения. По этой же причине PNS-атака для данного протокола, в отличие от

[4)] Вместо двух измерений (4) можно использовать измерение с тремя исходами (два определенных исхода и один неопределенный, см., например, [6, 7]). Однако измерения (4) проще технически реализовать при помощи одного светоделителя.

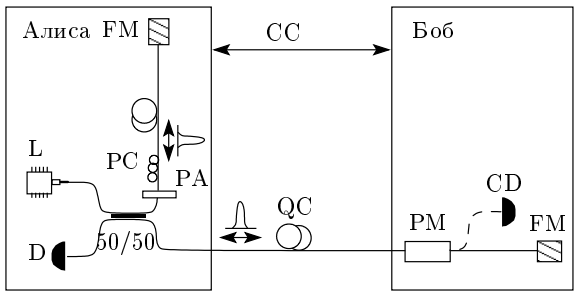

Рис. 1. Принципиальная схема оптоволоконной системы квантовой криптографии на базе интерферометра Майкельсона с эталонным квантовым состоянием в одном из плеч. L — лазер, QC — квантовый канал связи, CC — классический канал связи, PM — фазовые модуляторы, FM — фарадеевское зеркало, D — лавинный детектор, PC — поляризационный контроллер, PA — тонкая фазовая подстройка, CD — контрольный детектор. Поляризационный контроллер обеспечивает выравнивание поляризаций состояний из разных плеч, а тонкая фазовая подстройка используется для точной, с точностью до долей длины волны (долей микрона), балансировки плеч интерферометра

упомянутых выше протоколов, является неэффективной, поскольку приводит к ошибкам на приемной стороне и детектируется.

Принципиальная оптоволоконная схема, реализующая данный протокол, приведена на рис. 1. Схема, по сути, представляет собой сбалансированный оптоволоконный интерферометр Майкельсона. Одно плечо является каналом связи, а второе находится под контролем Алисы на передающей–приемной стороне.

Когерентное состояние с выхода лазера поступает на симметричный светоделитель. Замечательным свойством когерентного состояния (см., например, [17]) является то, что на светоделителе оно преобразуется самоподобным образом. Если на один из входов подано когерентное состояние $|\alpha\rangle$, а на второй — вакуумное состояние, то на двух выходах будет пара когерентных состояний: $|-\alpha/\sqrt{2}\rangle$ по верхнему выходу (рис. 1) и $|\alpha/\sqrt{2}\rangle$ по нижнему выходу.

Далее одно состояние поступает в канал связи, а второе — в плечо интерферометра, находящееся у Алисы (термостабилизированную катушку оптоволокна). На стороне Боба когерентное состояние подвергается преобразованию при помощи фазового модулятора, на который подается напряжение в момент прохождения состояния. Подача напряжения на фазовый модулятор приводит к изменению оптического показателя преломления и появлению дополнительной фазы у комплексного параметра α. Интенсивность излучения лазера на стороне Алисы подобрана таким образом, чтобы после прохождения канала связи от Алисы к Бобу на выходе со станции Боба интенсивность — среднее число фотонов μ — составляла типичное значение для систем квантовой криптографии $\mu \approx 0.1 \ll 1$. Для контроля интенсивности состояния, поступающего от Алисы к Бобу, может быть предусмотрен контрольный детектор (рис. 1) и при необходимости аттенюатор. Состояние на выходе станции Боба обозначим $|e^{i\varphi_B}\sqrt{\mu}\rangle$.

Информацию о ключе кодирует Боб, выбирая значение фазы у параметра α. Если бит ключа 0, то $\varphi_B = 0$, если бит ключа 1, то $\varphi_B = \pi$. После отражения на фарадеевском зеркале состояние возвращается к Алисе на приемно-передающую станцию.

Алиса случайно, равновероятно и независимо от Боба выбирает два значения фазы у α — $\varphi_A = \pi$ и $\varphi_A = 0$. Выбор фазы Алисой фактически означает выбор одного из измерений в формуле (4). Далее состояния возвращаются на светоделитель, где происходит их интерференция.

Таким образом, состояние, контролируемое Алисой, выполняет роль эталонного (контрольного) квантового состояния, которое сравнивается при измерениях с состоянием, полученным от Боба.

Состояния Алисы и Боба перед входом в интерферометр на обратном проходе таковы:

$$|e^{i\varphi_A}\sqrt{\mu T(L)}\rangle_A, \quad |e^{i\varphi_B}\sqrt{\mu T(L)}\rangle_B. \tag{5}$$

После интерференции состояние на выходе светоделителя с детектором равно

$$\left|\frac{e^{i\varphi_A}+e^{i\varphi_B}}{\sqrt{2}}\sqrt{\mu T(L)}\right\rangle_D. \tag{6}$$

Конструктивная интерференция на выходе светоделителя с детектором имеет место, если $\varphi_A = \varphi_B$. На втором выходе с лазером в этом случае имеет место полностью деструктивная интерференция — гашение состояний Алисы и Боба. Если $\varphi_A \neq \varphi_B$, то конструктивная интерференция имеет место на втором выходе с лазером, который в данном случае является холостым на обратном проходе. На выходе с детектором при таком значении фаз имеет место полностью деструктивная интерференция. Для тех посылок, в которых $\varphi_A \neq \varphi_B$, никогда не должно быть фотоотсчетов, если состояние от Боба пришло невозмущенным.

В отсутствие подслушивателя отсчет в детекторе однозначно указывает Алисе на значение бита, который выбрал Боб, так как Алиса знает значение своей фазы, а отсчет имеет место только при совпадении фазы у Алисы и Боба.

По открытому каналу Алиса сообщает номера посылок, где были зарегистрированы отсчеты в фотодетекторе. Если не было подслушивателя, то в посылках, где $\varphi_A \neq \varphi_B$, никогда не должно быть отсчетов. Для обнаружения подслушивателя, как обычно, часть посылок раскрывается. Алиса и Боб через открытый канал открывают выбранные ими значения фаз. Оценивается вероятность ошибки — доля посылок, где было выбрано $\varphi_A \neq \varphi_B$, но имели место фотоотсчеты в детекторе.

Далее происходят исправление ошибок через открытый канал связи и сжатие очищенного ключа при помощи однородных хэш-функций второго порядка [18]. В итоге Алиса и Боб имеют общий секретный ключ.

3. СТОЙКОСТЬ СИСТЕМЫ ОТНОСИТЕЛЬНО РАЗЛИЧНЫХ АТАК

Исследование стойкости системы сводится фактически к вычислению длины финального секретного ключа как функции от наблюдаемой ошибки на приемной стороне. Вычислим длину финального ключа в асимптотическом пределе длинных последовательностей, когда число зарегистрированных посылок $N \to \infty$. К Бобу от Алисы в каждой посылке поступают одинаковые состояния (заготовки), у которых Боб изменяет фазу α (проводит кодирование), поэтому подслушиватель Ева должна фактически различать пару неортогональных когерентных состояний на выходе со станции Боба, отвечающих 0 и 1, соответственно, $|\sqrt{\mu}\rangle$ и $|-\sqrt{\mu}\rangle$.

После достаточно большого числа посылок N ситуация для всех участников протокола описывается совместной матрицей плотности Боба и Евы — $\rho_{B^N E^N}$. Напомним, что эталонное состояние Алисы недоступно подслушивателю. Далее через открытый классический канал связи Алиса и Боб осуществляют согласованные случайные перестановки состояний своих подсистем в разных посылках. Это приводит к тому, что частичная матрица плотности $\rho_{B^N E^N}$ становится инвариантной относительно перестановок и, согласно квантовому аналогу классической теоремы де Финетти (см. детали в работе [19]), может быть сколь угодно точно представлена в виде тензорного произведения матриц плотности, относящихся к отдельным посылкам,[5)] — $\rho_{B^N E^N} \approx \sigma_{BE}^{\otimes N}$.

Неформально это означает, что Ева модифицирует только состояния в каждой отдельной посылке. При этом Ева может сохранять свою подсистему в квантовой памяти до стадии согласования результатов измерений Алисы и Боба по открытому классическому каналу связи. Затем Ева проводит коллективные измерения над всей последовательностью состояний в квантовой памяти. Именно при таких коллективных измерениях достигается максимум классической информации Евы о ключе, диктуемый фундаментальной границей Холево [20].

После проведения измерений и оценки вероятности ошибки Боб и Алиса имеют бинарные последовательности, соответственно, $X = \{0,1\}^N$ и $Y = \{0,1\}^N$. При этом последовательность Алисы Y, вообще говоря, содержит ошибки. В распоряжении Евы в каждой посылке остается матрица плотности

$$\sigma_E = \mathrm{Tr}_B\{\sigma_{BE}\} = \sum_{x=0,1} p_X(x)\sigma_E^x,$$

где σ_E^x — частичные матрицы плотности, отвечающие каждому посылаемому биту. Биты ключа из алфавита $\{0,1\}$ выбираются в соответствии с распределением вероятности $p_X(x)$ (как правило, равновероятно).

Длина секретного ключа в битах в пересчете на одну позицию определяется как (см. детали в работе [19])

$$R = \min_{\sigma_X \in \Gamma(Q)} (I(X;Y) - \chi(\sigma_E)), \tag{7}$$

где минимизация проводится по всевозможным атакам Евы $\Gamma(Q)$, которые приводят к наблюдаемой вероятности ошибки Q в последовательности Y Алисы. Здесь, как обычно,

$$I(X;Y) = H(X) + H(Y) - H(X,Y),$$

$$\chi(\sigma_E) = S\left(\sum_x p_X(x)\sigma_E^x\right) - \sum_x p_X(x) S(\sigma_E^x),$$

$I(X;Y)$ — взаимная информация Алиса–Боб,

$$I(X;Y) = -\sum_{x,y=0,1} p_{XY}(x,y)\log_2(p_{XY}(x,y)), \tag{8}$$

$$\begin{aligned} H(X) &= -\sum_{x=0,1} p_X(x)\log_2(p_X(x)),\\ H(Y) &= -\sum_{y=0,1} p_Y(y)\log_2(p_Y(y)), \end{aligned} \tag{9}$$

$p_{XY}(x,y)$ — совместное распределение вероятностей (x,y), $p_X(x)$ и $p_Y(y)$ — соответствующие маргинальные распределения вероятностей. Далее, $\chi(\sigma_E)$ —

[5)] Из этого факта следует, что когерентная (coherent) атака Евы не является более эффективной, чем коллективная атака. Таким образом, достаточно ограничиться только коллективной атакой.

величина Холево [20], которая определяет фундаментальную верхнюю достижимую границу классической информации, которая может быть получена Евой из квантового ансамбля $\{p_X(x), \sigma_E^x\}$. Последняя выражается через энтропию фон Неймана $S(\sigma) = -\mathrm{Tr}(\sigma \log_2 \sigma)$.

Рассмотрим всевозможные атаки Евы, причем некоторые из них оказываются возможными только в квантовом канале с потерями. Ниже будет видно, что при идеальных фотодетекторах распространение секретных ключей принципиально возможно при любых потерях в канале связи (скорость передачи при этом, разумеется, уменьшается, но секретность ключей гарантируется при любых потерях).

3.1. Атака со светоделителем

Схема атаки приведена на рис. 2. При данной атаке Ева не производит ошибок на приемной стороне, но не знает целиком передаваемого ключа.

Подслушиватель вблизи станции Боба разрывает линию связи и отводит часть состояния для своих измерений, остальная часть через канал с меньшими потерями (в идеале без потерь) направляется на приемную станцию к Алисе, чтобы скомпенсировать потерю отведенной части состояния. Поскольку на светоделителе когерентное состояние преобразуется самоподобным образом, Ева, имея одно из состояний $|\pm\sqrt{\mu}\rangle$ на выходе станции Боба, может отвести часть состояния, чтобы к Алисе поступило состояние $|\pm\sqrt{\mu T(L)}\rangle$, которое должно было бы достичь станцию Алисы в отсутствие Евы, но при учете затухания в исходном канале связи. Таким образом, коэффициент светоделителя должен быть выбран равным $\sqrt{1-T(L)}$. Поэтому в распоряжении Евы остается одно из состояний $|\pm\sqrt{\mu(1-T(L))}\rangle$. К Алисе через идеальный канал направляется состояние $|\pm\sqrt{\mu T(L)}\rangle$.

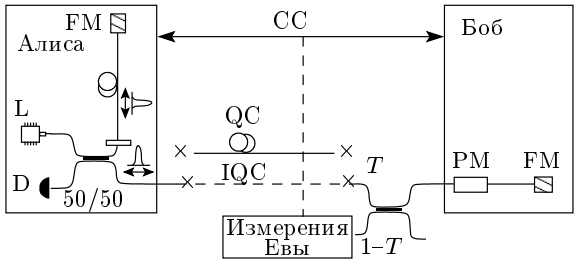

Рис. 2. Принципиальная схема атаки Евы со светоделителем. Новыми элементами по сравнению со схемой на рис. 1 являются IQC — идеальный квантовый канал Евы — и асимметричный светоделитель с коэффициентом деления $\sqrt{1-T(L)}/\sqrt{T(L)}$

Очевидно, что при такой атаке, хотя Ева и не производит ошибок на стороне Алисы, но не знает ключ целиком. Поэтому после измерений на стороне Алисы и отбрасывания посылок, где выбранные фазы Алисы и Боба не совпадали, взаимная информация равна

$$I(X;Y) = 1. \tag{10}$$

Верхняя граница классической информации, которую может извлечь Ева из квантового ансамбля

$$\sigma^E = \sum_{x=-,+} p_X(x)\sigma_E^x, \quad \sigma_E^x = |x\sqrt{\mu_E}\rangle\langle x\sqrt{\mu_E}|, \quad \mu_E = \sqrt{\mu(1-T(L))}, \quad x = +,-, \tag{11}$$

дается величиной Холево [20]:

$$\chi(\sigma^E) = \overline{C}(\varepsilon) = -\frac{1-\varepsilon}{2}\log_2\left(\frac{1-\varepsilon}{2}\right) - \frac{1+\varepsilon}{2}\log_2\left(\frac{1+\varepsilon}{2}\right), \tag{12}$$

$$\varepsilon = \langle -\sqrt{\mu_E}| + \sqrt{\mu_E}\rangle,$$

где знаки «+», «−» отвечают значениям бита 0, 1. Отметим, что $\overline{C}(\varepsilon)$ является классической пропускной способностью идеального квантового канала связи с источником, который описывается квантовым ансамблем (11).

Длина финального секретного ключа есть

$$R = 1 - \overline{C}(\varepsilon). \tag{13}$$

Поскольку реально используемые лавинные фотодетекторы имеют квантовую эффективность η, меньшую единицы, (типичные значения $\eta \approx 10$–$30\,\%$ на телекоммуникационной длине волны 1.55 мкм) и не реагируют на вакуумную компоненту когерентного состояния, вероятность детектирования когерентного состояния со средним числом фотонов $\mu T(L)$ равна $1 - e^{-\eta\mu T(L)}$. Окончательно для скорости генерации секретного ключа получаем

$$R' = (1 - e^{-\eta\mu T(L)})(1 - \overline{C}(\varepsilon)). \tag{14}$$

Длина секретного ключа при различных значениях параметров приведена на рис. 3. Как следует из формулы (14), длина секретного ключа отлична от нуля при любой длине квантового канала связи и любых значениях квантовой эффективности и среднего числа фотонов в состоянии. Последние параметры влияют на скорость генерации ключа. При этом,

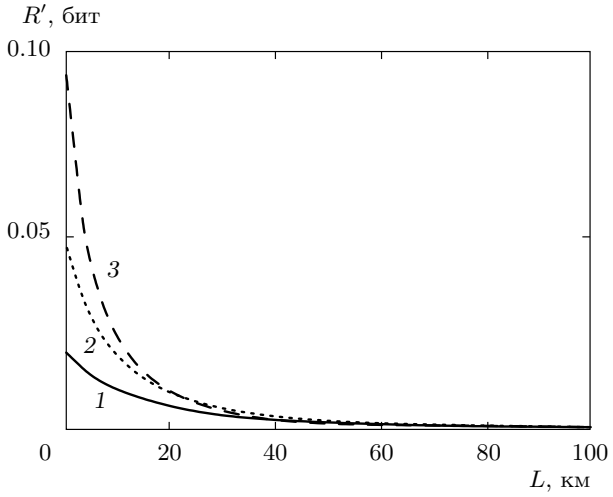

Рис. 3. Длина секретного ключа в пересчете на одну позицию при различных значениях среднего числа фотонов и квантовой эффективности лавинных фотодетекторов как функция длины линии связи. Значения параметра $\mu = 0.1$ (*1*), 0.25 (*2*), 0.5 (*3*), значение квантовой эффективности одинаково для всех трех кривых $\eta = 0.2$

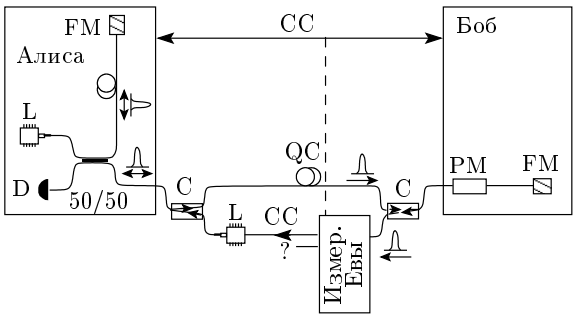

Рис. 4. Принципиальная схема атаки с использованием измерений с определенным исходом. Обозначения и элементы аналогичны обозначениям на рис. 1. CC — дополнительный классический канал связи подслушивателя, C — два оптоволоконных коммутатора, которые перенаправляют квантовые состояния при прямом и обратном проходах, L — дополнительный лазер подслушивателя для генерации квантовых состояний, который должен быть синхронизирован с лазером на передающей стороне

чем больше среднее число фотонов, тем меньше длина секретного ключа, поскольку различимость квантовых состояний тем лучше, чем больше среднее число фотонов.

При больших длинах линии связи длина секретного ключа имеет вид

$$R' \approx \mu\eta T(L) = \mu\eta 10^{-\gamma L/10}, \qquad (15)$$

т. е. представляет линейную зависимость по коэффициенту прохождения канала связи $T(L)$ и, соответственно, экспоненциальную по длине линии связи $10^{-\gamma L/10}$, не обращаясь в нуль ни при какой длине.

Подчеркнем в заключение, что при данной атаке, хотя Ева и не производит ошибок на приемной стороне, тем не менее она не знает ключа целиком. Формулы (13), (14) для длины секретного ключа учитывают сжатие исходного ключа без ошибок длины N при помощи универсальных хэш-функций второго порядка [18] до длины NR'. Таким образом, гарантируется, что при длине ключа NR' Ева с вероятностью единица не знает данную ключевую битовую последовательность.

3.2. Атака с использованием измерений с определенным исходом

Для данной атаки Еве не требуются ни квантовая память, ни идеальный (без потерь) квантовый канал связи. Еве необходимы лишь дополнительный классический канал связи и источник квантовых состояний. Принципиальная схема атаки приведена на рис. 4.

Атака сводится к следующему. Ева разрывает квантовый канал связи и проводит измерения с определенным исходом (unambiguous measurements [5–7]), которые описываются следующим разложением единицы:

$$I = M_0 + M_1 + M_?, \qquad (16)$$

$$M_{0,1} = \frac{I - |\mp\sqrt{\mu}\rangle\langle\mp\sqrt{\mu}|}{1 + \langle\sqrt{\mu}|-\sqrt{\mu}\rangle}, \quad M_? = I - M_0 - M_1,$$

где знаки «+» и «−» отвечают соответственно 0 и 1. Данные измерения являются оптимальными в смысле минимизации вероятности неопределенных исходов.

Данные измерения позволяют достоверно отличать информационные квантовые состояния Боба, поступающие в линию, хотя принципиально лишь с некоторой вероятностью определенного исхода из-за неортогональности состояний.

Исход в канале M_0 никогда не может произойти от состояния $|-\sqrt{\mu}\rangle$, отвечающего 0. Поэтому, если исход имел место, то он мог быть только от состояния либо $|\sqrt{\mu}\rangle$, либо другого, но не $|-\sqrt{\mu}\rangle$. Аналогично для канала измерений M_1. Для исходов

в каналах измерений $M_{0,1}$ Ева однозначно знает передаваемое состояние — это исходы с определенным результатом. Вероятность исходов с определенным результатом есть

$$\Pr(0|0) = \Pr(1|1) = \mathrm{Tr}\{|\mp\sqrt{\mu}\rangle\langle\mp\sqrt{\mu}|M_{0,1}\} = \\ = 1 - \langle\sqrt{\mu}| - \sqrt{\mu}\rangle. \quad (17)$$

Соответственно вероятность исходов с неопределенным результатом (канал измерений $M_?$), которые неизбежны из-за неортогональности — достоверной неразличимости состояний, равна

$$\Pr(?|0) = \Pr(?|1) = \mathrm{Tr}\{|\mp\sqrt{\mu}\rangle\langle\mp\sqrt{\mu}|M_?\} = \\ = \langle\sqrt{\mu}| - \sqrt{\mu}\rangle = e^{-2\mu}. \quad (18)$$

Таким образом, если получен исход с определенным результатом, то Ева достоверно знает передаваемое Бобом состояние. В таких посылках Ева по своему открытому классическому каналу посылает сигнал на приемную сторону, где готовится состояние, которое посылается Алисе[6)]. Для таких посылок вероятность определенного исхода дается формулой (17).

Однако неизбежно будут иметь место исходы с неопределенным результатом. Доля таких исходов дается формулой (18). При таких исходах Ева не знает передаваемое состояние Боба.

Принципиально важно для секретности протокола, что Ева не может блокировать данные посылки. Блокирование посылки означает, что Ева ничего не посылает. Точнее это означает, что в данной посылке Алиса получит вакуумное состояние, которое после прохождения светоделителя и интерференции с эталонным когерентным состоянием Алисы приведет к ошибкам на приемной стороне в половине таких посылок. Лучшее, что может делать Ева, — это угадывать, какое состояние, $|+\alpha\rangle$ или $|-\alpha\rangle$, дало исход с неопределенным результатом. Это наихудший случай, поскольку вероятность простого угадывания дает ошибку на приемной стороне Алисы $1/2$, независимо от перепосланного Евой состояния. Это принципиально для данного протокола, в отличие от других протоколов, где измерения с неопределенным исходом позволяют Еве блокировать эти посылки. При этом отсутствие отсчетов на приемной стороне списывается на потери в канале связи. Среднее число посылок при этом можно сохранить, используя канал с меньшими потерями. В данном протоколе Ева принципиально не может блокировать ни одну из посылок или посылать какое-либо другое состояние, поскольку в каждой посылке происходит сравнение с эталонным состоянием. Из-за структуры когерентного состояния ни при каком затухании (длине линии связи) Еве невозможно блокировать или ошибаться ни в одной из посылок, поскольку это всегда будет приводить к ошибкам и детектированию Евы.

Таким образом, никогда и ни при какой сколь угодно большой длине линии связи с потерями не будет ситуации, когда Ева знает весь передаваемый ключ и не производит ошибок на приемной стороне.

Пусть Ева подслушивает лишь часть посылок из полного числа N. Обозначим долю этих посылок δ. С учетом сказанного и формул (17), (18) вероятность наблюдаемой ошибки на приемной стороне Алисы равна

$$Q(\delta) = \frac{1}{2}\delta\Pr(?|0,1) = \frac{1}{2}\delta e^{-2\mu}. \quad (19)$$

Взаимная информация Алисы и Боба, с учетом исправления ошибок через открытый классический канал связи, равна

$$I(A;B) = 1 + h(Q(\delta)), \quad (20)$$

где

$$h(x) = -x\log_2(x) - (1-x)\log_2(1-x)$$

— бинарная энтропийная функция Шеннона. Соответственно, взаимная информация Боб–Ева равна

$$I(B;E) = \delta(1 - e^{-2\mu}). \quad (21)$$

Формула (21) следует из того факта, что в δN посылках Ева знает состояния достоверно, поэтому информация равна 1. Ошибка Евы в остальных посылках равна $1/2$, соответственно, взаимная информация при такой ошибке равна 0.

В итоге длина финального секретного ключа равна (см. детали в работе [19])

$$R = I(A;B) - I(B;E) = \\ = 1 + h(Q(\delta)) - \delta(1 - e^{-2\mu}). \quad (22)$$

С учетом того, что детектор Алисы не реагирует на вакуумную компоненту когерентного состояния, имеем

$$R' = (1-e^{-\eta\mu T(L)})(1+h(Q(\delta))-\delta(1-e^{-2\mu})). \quad (23)$$

[6)] Несмотря на внешнюю простоту, техническая реализация такой атаки является крайне сложной, поскольку требует приготовления когерентного квантового состояния при помощи лазера L (рис. 4) с той же фазой, что и состояние Алисы и Боба, что само по себе требует точной синхронизации лазеров.

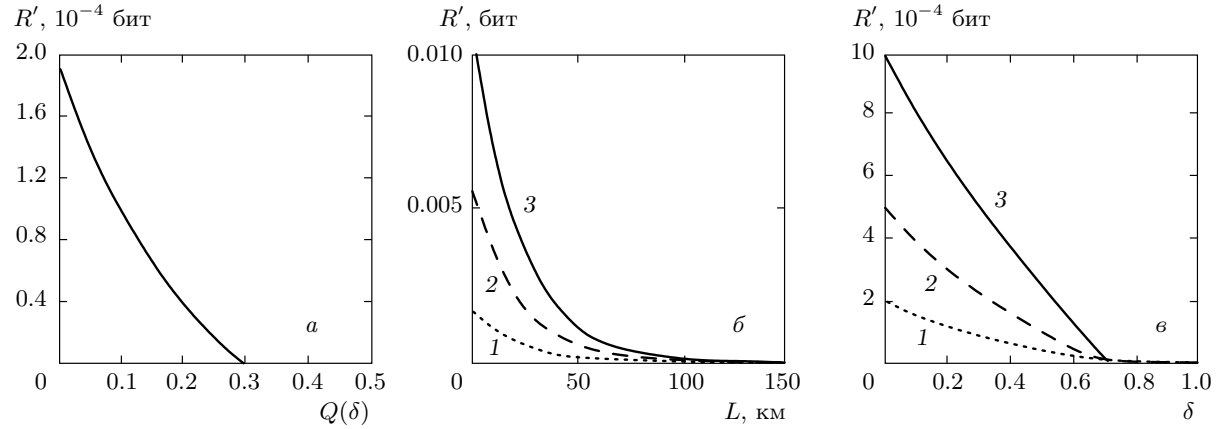

Рис. 5. *а*) Зависимость длины ключа R' как функции наблюдаемой ошибки $Q(\delta)$ на приемной стороне при длине канала связи $L = 100$ км; величина квантовой эффективности фотодетекторов $\eta = 0.2$, среднее число фотонов $\mu = 0.1$. *б*) Зависимости длины ключа от длины линии связи при разных значениях доли подслушиваемых посылок $\delta = 0.2$ (*1*), 0.4 (*2*), 0.6 (*3*). Квантовая эффективность и среднее число фотонов такие же, как на рис. 3. *в*) Зависимости длины ключа при длине линии связи $L = 100$ км как функции среднего числа фотонов; $\mu = 0.1$ (*1*), 0.25 (*2*), 0.5 (*3*)

Типичные зависимости длины ключа при различных значениях параметров приведены на рис. 5. Отметим, что при ошибке, меньшей критической, длина ключа не обращается в нуль ни при какой длине линии связи. Асимптотическое поведение длины ключа как функции длины линии связи аналогично предыдущему случаю (15). Длина ключа ведет себя линейно как функция пропускания канала связи.

3.3. «Прозрачная» атака

Данная атака является универсальной и возможна, в отличие от двух предыдущих, даже в канале без потерь. Действия Евы сводятся к следующему. В каждой посылке Ева готовит свое вспомогательное квантовое состояние $|E\rangle_E$, которое взаимодействует с передаваемым состоянием. Совместная эволюция описывается унитарным преобразованием (см. рис. 6)

$$|\alpha\rangle_B \otimes |E\rangle_E \to U_{BE}(|\alpha\rangle_B \otimes |E\rangle_E) = A|\alpha\rangle_B \otimes \otimes |E_\alpha\rangle_E + B|-\alpha\rangle_B \otimes |E_{-\alpha}\rangle_E = |\Phi_\alpha\rangle_{BE}, \quad (24)$$

$$|-\alpha\rangle_B \otimes |E\rangle_E \to U_{BE}(|-\alpha\rangle_B \otimes |E\rangle_E) = B|\alpha\rangle_B \otimes \otimes |E_\alpha\rangle_E + A|-\alpha\rangle_B \otimes |E_{-\alpha}\rangle_E = |\Phi_{-\alpha}\rangle_{BE}. \quad (25)$$

Здесь $|E_\alpha\rangle_E$, $|E_{-\alpha}\rangle_E$ — состояния в пространстве, натянутом на $|\alpha\rangle_B$ и $|-\alpha\rangle_B$, A и B — вещественные коэффициенты, которые выбираются подслушивателем. Квантовая схема, реализующая совместную унитарную эволюцию, может быть построена явно (см., например, оптоволоконную квантовую схему для квантового распределения ключей с фазово-временным кодированием [10]).

Требование унитарности оператора эволюции U_{BE} в формулах (24), (25) приводит к следующим условиям:

$$\begin{gathered}\cos\alpha = 2AB + (A^2+B^2)\cos\alpha\cos\gamma, \\ A^2 + B^2 + 2AB\cos\alpha\cos\gamma = 1.\end{gathered} \quad (26)$$

Первое уравнение фактически является условием нормировки состояний. С учетом формул (24)–(26) находим явное выражение для $\cos\gamma$:

$$\cos\gamma = \frac{\sqrt{1-(1-2Q)^2} - \cos\alpha}{\cos\alpha\left[\sqrt{1-(1-2Q)^2}\cos\alpha - 1\right]}, \quad (27)$$

где наблюдаемая ошибка на приемной стороне имеет вид

$$Q = \frac{B^2}{A^2+B^2} \quad (28)$$

и

$$\cos\alpha = {}_B\langle\alpha|-\alpha\rangle_B, \quad \cos\gamma = {}_E\langle E_\alpha|E_{-\alpha}\rangle_E, \quad (29)$$

$$A^2 = \frac{1+z(Q)^2-2z(Q)\cos\alpha}{(1-z(Q)^2)^2}, \quad z(Q) = \sqrt{\frac{Q}{1-Q}}. \quad (30)$$

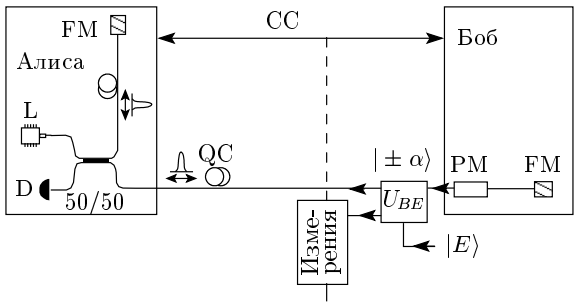

Рис. 6. Принципиальная схема «прозрачной» атаки на передаваемый ключ

Частичные матрицы плотности Евы после измерений Алисы равны

$$\sigma_E^{\alpha} = (1-Q)|\alpha\rangle_{BB}\langle\alpha| + Q|-\alpha\rangle_{BB}\langle-\alpha|, \qquad (31)$$

когда Боб посылал состояние $|\alpha\rangle_B$, и

$$\sigma_E^{-\alpha} = (1-Q)|-\alpha\rangle_{BB}\langle-\alpha| + Q|\alpha\rangle_{BB}\langle\alpha|, \qquad (32)$$

когда Боб посылал состояние $|-\alpha\rangle_B$. Полная матрица плотности равна

$$\sigma_E = \frac{1}{2}\left(\sigma_E^{\alpha} + \sigma_E^{-\alpha}\right). \qquad (33)$$

С учетом (28) взаимная информация Алиса–Боб равна

$$I(A;B) = 1 + h(Q). \qquad (34)$$

Верхняя граница классической информации Евы с учетом (27)–(33) дается выражением

$$\chi(\sigma_E) = -\frac{1-\cos(\gamma)}{2}\log_2\left(\frac{1-\cos\gamma}{2}\right) - \\ - \frac{1+\cos(\gamma)}{2}\log_2\left(\frac{1+\cos\gamma}{2}\right) + \\ + \lambda_1\log_2\lambda_1 + \lambda_2\log_2\lambda_2, \qquad (35)$$

где собственные значения частичных матриц плотности (31), (32) равны

$$\lambda_{1,2} = \frac{1}{2}\left(F \pm \sqrt{F^2 - 4D}\right). \qquad (36)$$

Здесь введены следующие обозначения:

$$f = \frac{1-Q+Q\cos^2\gamma}{2}, \quad d = \frac{(1-Q)\cos^2\gamma+Q}{2}, \qquad (37)$$

$$F = \frac{f+d-\cos\gamma}{1-\cos^2\gamma}, \quad D = \frac{fd-1/4}{1-\cos^2\gamma}. \qquad (38)$$

С учетом формул (34), (35) получаем окончательное выражение для длины финального ключа:

$$R' = (1-e^{-\eta\mu T(L)})(1+h(Q)-\chi(\sigma_E)). \qquad (39)$$

Зависимости длины секретного ключа от длины линии связи приведены на рис. 7. Критическая ошибка при «прозрачной» атаке, до которой гарантируется распространение секретных ключей, оказывается меньше, чем при атаке с измерениями с определенным исходом. Это обстоятельство связано с тем, что прозрачная атака является оптимальной в том смысле, что дает максимум информации Евы о ключе при заданной наблюдаемой ошибке Q.

Как видно из формулы (39), при больших длинах линии связи величина ключа, так же как и в предыдущем случае, зависит линейно от пропускания канала: $R' \approx \eta\mu T$.

4. УЧЕТ ТЕМНОВЫХ ШУМОВ ФОТОДЕТЕКТОРОВ

Анализ различных критических атак на передаваемый ключ показывает, что в отсутствие темновых отсчетов распределение секретных ключей принципиально возможно при любой длине линии связи и, соответственно, любых потерях в ней. Учтем теперь темновые шумы фотодетекторов. Для данного протокола, как будет видно ниже, расстояние, на которое можно передавать ключи, лимитируется только темновыми шумами. Напомним, что в квантовой криптографии принципиально невозможно отделить ошибки на приемной стороне из-за действий подслушивателя от ошибок из-за неидеальностей аппаратуры (в том числе и темновых шумов), поэтому все наблюдаемые ошибки легитимные пользователи относят на счет действий подслушивателя.

Атака со светоделителем. Поскольку такая атака Евы не приводит к ошибкам на приемной стороне Алисы, ошибки в битовой последовательности Y возникают только за счет темновых отсчетов. Обозначим вероятность темновых отсчетов как p_d (count/gate). Темновые отсчеты происходят независимо от регистрации состояний, которая имеет место с вероятностью $1-e^{-\eta\mu T(L)}$, поэтому ошибка принимает вид

$$Q_d = \frac{1}{2}\,\frac{p_d}{(1-e^{-\eta\mu T(L)})+p_d}. \qquad (40)$$

С учетом формул (13), (40) длина финального секретного ключа становится равной

$$R' = (1-e^{-\eta\mu T(L)})R, \quad R = (1+h(Q_d)-\overline{C}(\varepsilon)), \qquad (41)$$

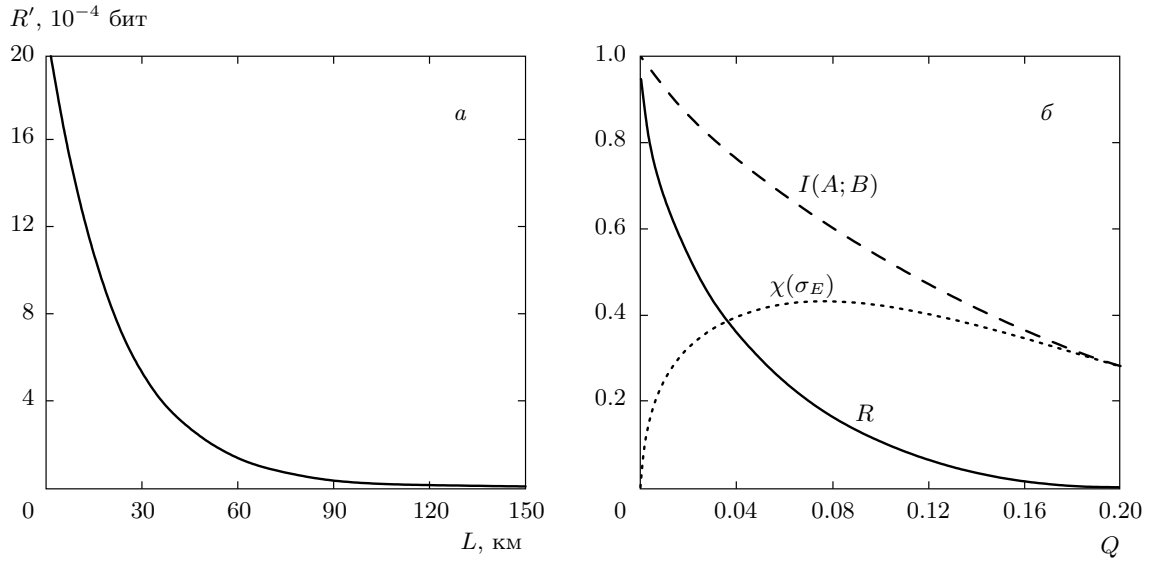

Рис. 7. *а*) Длина финального ключа как функция длины линии связи; $\eta = 0.2$, $\mu = 0.1$. *б*) Зависимости взаимной информации $I(A;B)$, $\chi(\sigma_E)$ и длины ключа R как функции наблюдаемой ошибки на приемной стороне Алисы; $\eta = 0.2$, $\mu = 0.1$

где $\overline{C}(\varepsilon)$ дается выражением (12).

Атака с использованием измерений с определенным исходом. В этом случае ошибка на приемной стороне Алисы становится равной

$$Q(\delta, p_d) = \frac{1}{2}\delta e^{-2\mu} + \frac{1}{2}\,\frac{p_d}{(1 - e^{-\eta\mu T(L)}) + p_d}. \qquad (42)$$

Для длины финального ключа имеем

$$R' = (1-e^{-\eta\mu T(L)})(1+h(Q(\delta, p_d))-\delta(1-e^{-2\mu})). \quad (43)$$

Прозрачная атака. Учет темновых шумов приводит к следующему выражению для длины ключа:

$$R' = (1 - e^{-\eta\mu T(L)})(1 + h(Q_d) - \chi(\sigma_E)), \qquad (44)$$

где Q_d — наблюдаемая ошибка на приемной стороне, которая с учетом ошибки Q (см. формулу (28)), вносимой подслушивателем, равна

$$Q_d = Q + \frac{1}{2}\,\frac{p_d}{(1 - e^{-\eta\mu T(L)}) + p_d}. \qquad (45)$$

Зависимости длины ключа R с учетом темновых шумов лавинных фотодетекторов для различных атак приведены на рис. 8 как функции длины линии связи для различной вероятности темновых отсчетов p_d. Как видно из рис. 8, темновые шумы приводят к тому, что появляется критическая длина линии связи, до которой гарантируется распределение секретных ключей.

5. ОБСУЖДЕНИЕ РЕЗУЛЬТАТОВ

Как было сказано во Введении, ряд схем квантовой криптографии при неоднофотонном источнике и потерях в канале связи становится несекретным. Протоколы квантовой криптографии с базисами и ортогональными состояниями внутри базиса, как BB84 [2], становятся несекретными относительно PNS-атаки. Начиная с некоторой длины, подслушиватель знает весь передаваемый ключ и не производит ошибок на приемной стороне. Протоколы квантового распределения ключей с неортогональными состояниями, например, SARG04 [9] или протокол с фазово-временным кодированием [10], также становятся несекретными при определенной длине канала связи. Данное семейство протоколов уязвимо относительно атаки с измерениями с определенным исходом.

Предлагаемый протокол обеспечивает секретность как при PNS-атаке, так и при более критической атаке с измерениями с определенным исходом. Данное свойство достигается из-за измерений специального вида на приемной стороне. Формально говоря, эти измерения сводятся к проектированию состояний из линии связи на эталонное состояние, которое «хранится» недоступным для подслушивателя на приемной стороне. Такое измерение обеспечивает детектирование подслушивателя в каждой посылке, где подслушивателем получен

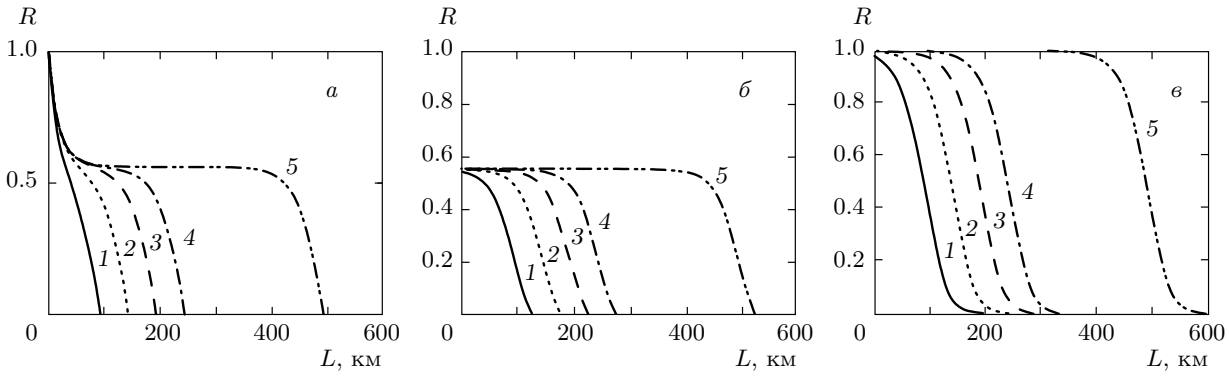

Рис. 8. Зависимости длины секретного ключа R от длины линии связи при $p_d = 10^{-4}$ (*1*), 10^{-5} (*2*), 10^{-6} (*3*), 10^{-7} (*4*), 10^{-12} (*5*), $\mu = 0.1$, $\eta = 0.2$. *а* — атака со светоделителем; *б* — атака с измерениями с определенным исходом, $\delta = 0.2$ (см. (19), (21)); *в* — «прозрачная» атака, $Q = 0$. Уровень темновых шумов $p_d = 10^{-12}$ (кривые *5*) отвечает сверхпроводящим фотодетекторам в пересчете на временное окно 1 нс (напомним, что такие детекторы, в отличие от лавинных, работают без стробирования)

неопределенный исход. Подслушиватель принципиально не может блокировать данные посылки и остаться незамеченным. Важно подчеркнуть, что это будет иметь место даже при неидеальной квантовой эффективности детекторов.

Формальная причина состоит в том, что блокирование посылки эквивалентно тому, что подслушиватель перепосылает вакуумное состояние, которое сравнивается с неискаженным эталонным когерентным состоянием у Алисы. Перепосылка любого другого состояния вместо истинного также приведет к ошибкам. Поэтому атака подслушивателя с измерениями с определенным исходом всегда будет приводить к ошибкам на приемной стороне независимо от величины потерь в линии связи.

Техническая реализация данной схемы является достаточно сложной, поскольку для обеспечения интерференции на светоделителе требуется обеспечить фазовую когерентность двух состояний, распространяющихся по разным путям — волоконным линиям.

Для обеспечения интерференции необходимо, чтобы длины линий были сбалансированы с точностью до долей длины волны, т. е. долей микрона, что достижимо с помощью тонкой юстировки (рис. 1). За время распространения состояний туда и обратно изменения длин линий, связанные с изменением температуры, не играют роли и не приводят к сбою интерференции, поскольку не успевают произойти. Уход поляризации также является медленным за время прохождения туда и обратно.

Основным механизмом, приводящим к разрушению интерференции и ошибкам на приемной стороне, является сбой фазы. Как показывают эксперименты для оптоволокна, проложенного в городских условиях, основной вклад в сбой фазы вносят случайные механические деформации оптоволокна [21]. При этом ночью такие изменения в несколько раз меньше, чем в дневное время.

Характерная величина ухода фазы за время распространения на расстояние порядка 30 км составляет $\Delta\varphi \approx 0.1$ рад [21]. Для устойчивой работы схемы требуются активная стабилизация и компенсация случайных сбоев фазы. На сегодняшний день достигнуты рекордные значения, которые позволяют синхронизовать независимые источники с временным джиттером (jitter) 10^{-19} с$^{-1}$ в течение времени 100 с и на расстоянии 250 км (см. [22, 23] и ссылки в этих работах).

Фактически, для того чтобы обеспечить секретность ключей при любых потерях, необходимо реализовать измерение, которое по сути сводится к проектированию на когерентное состояние с учетом потерь в канале связи без подслушивателя. Схема на базе интерферометра Майкельсона, предлагаемая в данной работе, по сути является одним из способов реализации такого измерения, но не единственным.

Автор выражает благодарность коллегам по Академии криптографии Российской Федерации за постоянную поддержку.

Работа выполнена при частичной поддержке РФФИ (гранты №№ 11-02-00455, 10-02-90036-Бел).

ЛИТЕРАТУРА

1. V. Scarani, H. Bechmann-Pasquinucci, N. J. Cerf, M. Dusek, N. Lütkenhaus, and M. Peev, Rev. Mod. Phys. **81**, 1301 (2009).

2. G. Brassard, N. Lütkenhaus, T. Mor, and B. Sanders, Phys. Rev. Lett. **85**, 1330 (2000).

3. С. Н. Молотков, ЖЭТФ **139**, 429 (2011).

4. C. H. Bennett and G. Brassard, Proc. IEEE Int. Conf. on Comput. Syst. and Sign. Proces., Bangalore, India (1984), p. 175.

5. D. Dieks, Phys. Lett. A **126**, 303 (1988).

6. I. D. Ivanovic, Phys. Lett. A **123**, 257 (1987).

7. A. Peres, Phys. Lett. A **128**, 19 (1988).

8. C. H. Bennett, Phys. Rev. Lett. **68**, 3121 (1992).

9. V. Scarani, A. Acin, G. Ribordy, and N. Gisin, Phys. Rev. Lett. **95**, 057901-1 (2004); A. Acin, N. Gisin, and V. Scarani, arXiv:quant-ph/0302037.

10. Д. А. Кронберг, С. Н. Молотков, ЖЭТФ **136**, 650 (2009); **138**, 33 (2010).

11. N. Gisin, G. Ribordy, H. Zbinden, D. Stucki, N. Brunner, and V. Scarani, arXiv:quant-ph/0411022.

12. D. Stucki, N. Brunner, N. Gisin, V. Scarani, and H. Zbinden, arXiv:quant-ph/0506097.

13. C. Branciard, N. Gisin, N. Lütkenhaus, and V. Scarani, arXiv:quant-ph/0609090.

14. C. Branciard, N. Gisin, and V. Scarani, arXiv: quant-ph/0710.4884.v2.

15. M. Curty, L.-L. Zhang, H.-K. Lo, and N. Lütkenhaus, arXiv:quant-ph/0609094.

16. K. Inoue, E. Waks, and Y. Yamamoto, Phys. Rev. Lett. **89**, 037902 (2002); K. Inoue, E. Waks, and Y. Yamamoto, Phys. Rev. A **68**, 022317 (2003).

17. Л. Мандель, Э. Вольф, *Оптическая когерентность и квантовая оптика*, Физматлит, Москва (2000); L. Mandel and E. Wolf, *Optical Coherence and Quantum Optics*, Cambridge Univ. Press, Cambridge (1995).

18. J. L. Carter and M. N. Wegman, J. Comp. Syst. Sci. **18**, 143 (1979).

19. R. Renner, arXiv: quant-ph/0512258.

20. А. С. Холево, *Введение в квантовую теорию информации*, сер. *Современная математическая физика, вып.5*, МЦНМО, Москва (2002); УМН **53**, 193 (1998).

21. J. Minar, H. de Riedmatten, C. Simon, H. Zbinden, and N. Gisin, arXiv:quant-ph/0712.0740.

22. N. R. Newbury, P. A. Williams, and W. C. Swann, Opt. Lett. **32**, 3056 (2007).

23. S. M. Foreman, K. W. Holman, D. D. Hudson, D. J. Jones, and Jun Ye, Rev. Sci. Instr. **78**, 021101 (2007).