ЖЭТФ, 2012, том 141, вып. 5, стр. 812–831

ОБ УЯЗВИМОСТИ БАЗОВЫХ ПРОТОКОЛОВ КВАНТОВОГО РАСПРЕДЕЛЕНИЯ КЛЮЧЕЙ И О ТРЕХ ПРОТОКОЛАХ, УСТОЙЧИВЫХ К АТАКЕ С «ОСЛЕПЛЕНИЕМ» ЛАВИННЫХ ФОТОДЕТЕКТОРОВ

С. Н. Молотков *

Академия криптографии Российской Федерации
121552, Москва, Россия

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

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

Поступила в редакцию 23 июня 2011 г.

Фундаментальные запреты квантовой механики на измеримость квантовых состояний позволяют реализовать секретное распределение ключей между пространственно-удаленными пользователями. Однако экспериментальные и коммерческие реализации систем квантовой криптографии используют компоненты, которые существуют на сегодняшнем технологическом уровне, в частности, однофотонные лавинные фотодетекторы. Данные детекторы подвержены эффекту ослепления. Ранее было показано, что все известные базовые протоколы квантового распределения ключей и системы на их основе уязвимы по отношению к атакам с ослеплением фотодетекторов. При таких атаках подслушиватель знает весь передаваемый ключ, не производит ошибок на приемной стороне и остается необнаруженным. Приведены три протокола квантового распределения ключей, которые устойчивы относительно данных атак. Секретность ключей и детектирование попыток подслушивания гарантируется самой внутренней структурой протоколов, а не дополнительными техническими усовершенствованиями.

1. ВВЕДЕНИЕ

Фундаментальные ограничения и запреты квантовой механики на измеримость квантовых состояний [1–4] позволяют реализовать секретное распределение криптографических ключей между пространственно-удаленными пользователями. При этом секретность ключей гарантируется не ограниченными вычислительными или техническими возможностями подслушивателя, а фундаментальными законами природы — законами квантовой механики. Принято называть секретность ключей в этом случае безусловной (unconditional) [3–5].

Набор действий легитимных пользователей, включающий приготовление, преобразование, передачу[1)], измерение квантовых состояний, интерпретацию результатов измерений, исправление ошибок в первичных ключах и сжатие (усиление секретности — privacy amplification) очищенных ключей, называется протоколом квантового распределения ключей [3–5]. Протокол должен гарантировать детектирование любых попыток подслушивания. Обнаружение любых попыток подслушивания происходит по ошибкам на приемной стороне. Более точно, по изменению статистики измерений — фотоотсчетов. Если существуют атаки на передаваемый ключ, при которых в протоколе не возникает ошибок на приемной стороне, то такой протокол

*E-mail: sergei.molotkov@gmail.com

[1)] Напомним, что квантовый канал связи в квантовой криптографии является открытым и не контролируется легитимными пользователями, т. е. подслушиватель может производить любые модификации квантовых состояний и самого физического канала связи.

считается уязвимым по отношению к данному виду атак и не гарантирует секретность ключей. Критическими атаками являются такие, при которых подслушиватель знает ключ, не производит ошибок на приемной стороне и остается недетектируемым.

На сегодняшний день разработан ряд протоколов квантового распределения ключей и созданы системы квантовой криптографии на их основе, которые даже являются коммерчески доступными (например, ID Quantique и MagiQ Technologies).

В результате длительных и интенсивных исследований была доказана секретность базовых протоколов квантовой криптографии и определены области параметров, при которых протоколы гарантируют секретность распределения ключей [5, 6].

Однако реализации систем квантовой криптографии используют неидеальные компоненты. Источник квантовых состояний (обычно ослабленное лазерное излучение) не является строго однофотонным, однофотонные лавинные фотодетекторы имеют собственные темновые шумы и не единичную квантовую эффективность, квантовый канал связи (оптоволокно или открытое пространство) имеет потери. Данные факторы приводят к возможности атаки с расщеплением по числу фотонов (PNS-атака, Photon Number Splitting attack [7]) и атаке с измерениями с определенным исходом (Unambiguous Measurements [8, 9]). При доказательстве секретности базовых протоколов были учтены данные факторы и выяснены границы параметров, при которых протоколы гарантируют секретное распределение ключей [6].

За последние годы была найдена новая атака на передаваемый ключ, так называемая атака с «ослеплением» лавинных фотодетекторов [10]. Хотя подслушиватель и не имеет прямого доступа к лавинным фотодетекторам на приемной стороне, он может воздействовать на них опосредовано через квантовый канал связи[2)]. Атака с «ослеплением» лавинных фотодетекторов аналогична атаке прием–перепосыл с той лишь разницей, что подслушиватель посылает после интерпретации результатов своих измерений не квантовые состояния, аналогичные тем, которые он получил с приемной стороны, а модифицированные (фальсифицированные — faked) состояния [10, 12]. Данные состояния позволяют контролировать отсчеты или их отсутствие на приемной стороне в зависимости от результата измерений подслушивателя. В итоге подслушиватель может навязывать необходимые ему отсчеты, которые не приводят к ошибкам на приемной стороне. При этом подслушиватель знает весь передаваемый ключ и остается необнаруженным. При такой атаке невозможно гарантировать секретное распределение ключей.

Было продемонстрировано, что все известные базовые протоколы квантового распределения ключей и системы квантовой криптографии на их основе потенциально уязвимы по отношению к данной атаке [10, 12]. Такими базовыми протоколами являются BB84 [3], SARG04 [13], Six-State QKD [14], DPS (Differential Phase Shift) [15], COW (Coherent One Way) [16], E91 [17], Decoy State QKD [18].

Системы квантовой криптографии на основе упомянутых протоколов, в том числе и коммерческие, разрабатывались в разных странах. На основе протокола BB84 созданы система MagiQ Technologies (QPN 5505, США), квантовая сеть в Бостоне (проект по заказу DARPA); SmartQ во Франции; на основе протоколов BB84, SARG04 — система Clavis2 и COW в idQuantique в Швейцарии; на основе протокола DPS — система в Японии, на основе протокола BB84 (поляризационное кодирование) — в Сингапуре, на основе протокола E91 на запутанных состояниях — в Австрии.

Возможность такой атаки, по понятным причинам, вызвала заметную напряженность. Результаты работ [10, 12, 19] докладывались на многих международных конференциях и известны сообществу. Возможны различные варианты реакции на данную атаку. Поскольку пока вразумительного и принципиального ответа на нее нет, можно молчаливо игнорировать ее до поры, пока не будут созданы однофотонные детекторы и схемотехнические решения, не подверженные атаке с ослеплением. Насколько нам известно, единственная опубликованная критика [20] в адрес работ [10, 12, 19] связана с тем, что такая атака, использующая нюансы работы существующих Si и InGaAs:P лавинных однофотонных детекторов, может, тем не менее, оказаться неэффективной. Как бы то ни было, все системы квантовой криптографии, упомянутые выше, в существующем виде потенциально и явно уязвимы по отношению к данной атаке, и игнорировать данный факт нельзя. В принципе, такую атаку можно детектировать, внося различные технические усовершенствования в системы (например, вводя дополнительные сторожевые фотодетекторы и пр.). Однако такие косметические усовершенствования не решают проблему принци-

[2)] Возможны также другие каналы побочной (side information) утечки информации о ключе. Например, подслушиватель может пытаться регистрировать обратное свечение лавинных фотодетекторов [11] или зондировать состояние активных волоконных компонентов — фазовых модуляторов.

пиально и фактически снижают статус квантовой криптографии, поскольку переносят безусловную секретность квантовой криптографии, основанную на фундаментальных запретах квантовой механики, в секретность, базирующуюся на технических ограничениях.

Ответ на вызов атаке [10, 12, 19] должен быть дан не на уровне технических доделок существующих систем квантовой криптографии, а на уровне базовых протоколов квантового распределения ключей. Более точно, должны быть предъявлены протоколы квантового распределения ключей, которые бы гарантировали секретность передаваемых ключей даже при существующих лавинных фотодетекторах, которые могут быть подвергнуты атаке с их «ослеплением».

В данной работе будут описаны три протокола квантового распределения ключей: 1) двухпараметрический протокол с фазово-временны́м кодированием; 2) протокол с эталонным (реперным) «классическим» когерентным состоянием; 3) релятивистский протокол, который использует дополнительные ограничения, диктуемые специальной теорией относительности на измеримость протяженных в пространстве-времени квантовых состояний. Первые два протокола разработаны для оптоволоконных систем квантовой криптографии, третий — для открытого пространства. Данные протоколы устойчивы относительно всех видов атак, в том числе и атаки с «ослеплением» лавинных фотодетекторов даже в идеальных условиях для такой атаки.

Стойкость обеспечивается не дополнительными техническими усовершенствованиями или тонкостями технической реализации управляющей электроники для лавинных фотодетекторов, работающих в режиме счета фотонов, а само́й внутренней структурой протоколов.

Сначала приведем описание существующих атак с ослеплением лавинных детекторов (разд. 2.1, 2.2), а затем приведем анализ причин устойчивости для трех новых протоколов (разд. 3.1, 3.2, 3.3).

2. ОПИСАНИЕ АТАКИ С «ОСЛЕПЛЕНИЕМ» ЛАВИННЫХ ФОТОДЕТЕКТОРОВ

Для самодостаточности изложения приведем краткое и необходимое для дальнейшего описание принципов атаки с «ослеплением» лавинных фотодетекторов, опуская технические подробности, так как последние детально приведены в работах [10, 12, 19].

Возможны два варианта атаки.

I. В первом варианте атаки используется тот факт, что временны́е зависимости чувствительностей лавинных фотодетекторов различны. Поэтому возможно приготовление фальсифицированного состояния, которое «ослепляет» один из фотодетекторов по усмотрению подслушивателя [10, 12, 19].

II. Во втором варианте атаки используются состояния с интенсивностью ниже порога для того, чтобы обеспечить срабатывание только одного из двух фотодетекторов и только при совпадении базиса подслушивателя и базиса легитимных пользователей. Если базисы не совпадают, оба детектора не дают отсчетов [10, 12, 19].

Обе атаки с «ослеплением» лавинных фотодетекторов, работающих в режиме счета фотонов, основаны на двух особенностях работы полупроводниковых InGaAs:P лавинных фотодетекторов[3)]. На лавинный фотодиод приложено запирающее напряжение. В момент прилета фотона накладывается импульс стробирующего напряжения (типичная длительность порядка нескольких наносекунд и амплитуда в несколько вольт), открывающего фотодиод (см., например, подробности в [21]). Поглощение фотона приводит к образованию лавины носителей и импульса напряжения, который регистрируется.

1. Первая атака с ослеплением основана на следующем свойстве. Если увеличить интенсивность излучения несколько выше квазиоднофотонного режима, то это приведет к увеличению тока, протекающего через фотодиод, в момент регистрации. Из-за того, что фотодиод без засветки не активен (заперт), динамический рост тока выше некоторой величины приведет к эффективному уменьшению напряжения смещения в течение действия строба и запиранию диода и, соответственно, уменьшению, вплоть до его отсутствия, тока лавины (режим “no click”). Таким образом фотодиод эффективно ослепляется.

2. Вторая атака связана с переводом фотодиода из счетного режима в линейный классический режим фотодетектирования, когда ток является функцией интенсивности излучения (обычно пропорционален ей). Если далее увеличивать интенсивность излучения, то после ослепления фотодиода (см. пункт 1 выше) и отсутствия тока регистрации, начиная с некоторой пороговой величины интенсивности, снова возникнет сигнал на фотодиоде — через фотодиод будет протекать ток, пропорциональный интенсивности излучения.

[3)] Будем далее иметь ввиду лавинные фотодетекторы, работающие в стробируемом режиме.

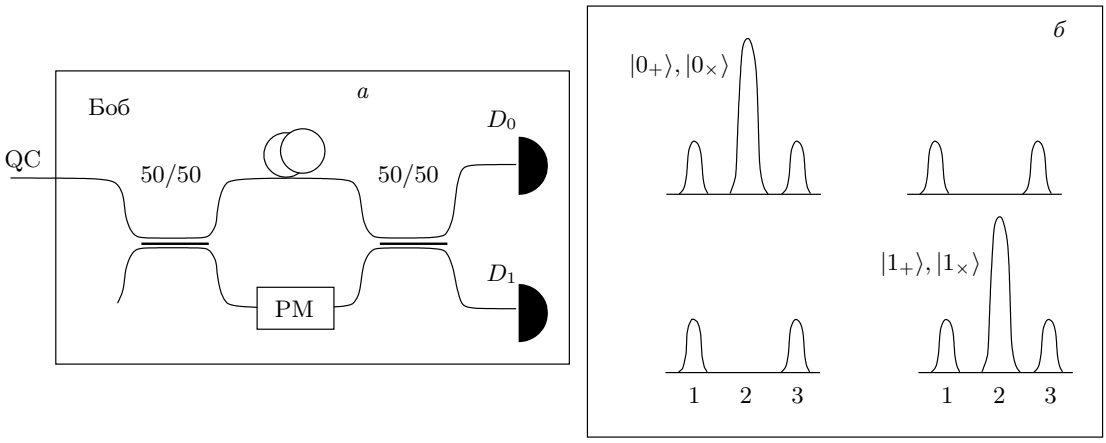

Рис. 1. *а*) Принципиальная схема приемной части оптоволоконной системы квантовой криптографии, реализующей протокол BB84. QC — квантовый канал связи, PM — фазовый модулятор. *б*) Статистика фотоотсчетов в двух детекторах для разных информационных состояний

2.1. Атака с «ослеплением», использующая разные временны́е зависимости чувствительности лавинных фотодетекторов

Для дальнейшего, чтобы понять причину устойчивости предлагаемых протоколов квантового распределения ключей и для сравнения с другими протоколами, которые уязвимы относительно атаки с ослеплением фотодетекторов, приведем описание атаки на примере протокола BB84 [3, 10, 12, 19].

Подробности атаки для других протоколов см. в работах [10, 12, 19]. Стандартная оптоволоконная реализация протокола BB84 на приемной стороне представлена на рис. 1.

Информационные состояния в базисе +, поступающие из квантового канала связи, имеют вид

$$|0_+\rangle = \frac{1}{\sqrt{2}}\left(|1\rangle + |2\rangle\right), \quad |1_+\rangle = \frac{1}{\sqrt{2}}\left(|1\rangle - |2\rangle\right), \quad (1)$$

а в базисе $\times$, соответственно,

$$|0_\times\rangle = \frac{1}{\sqrt{2}}\left(|1\rangle + i|2\rangle\right), \quad |1_\times\rangle = \frac{1}{\sqrt{2}}\left(|1\rangle - i|2\rangle\right), \quad (2)$$

где $|1\rangle$ и $|2\rangle$ — состояния, локализованные во временны́х окнах 1 и 2. Расстояние между локализованными состояниями равно разности хода по верхнему и нижнему плечам разбалансированного интерферометра Маха–Цандера (рис. 1).

Перед входом в фотодетекторы, в зависимости от выбранной фазы с помощью фазового модулятора, информационные квантовые состояния в базисе + (значение $\varphi_B(+) = 0$)[4] имеют вид

$$\begin{aligned} D_0: &\quad |0_+\rangle \to \frac{1}{\sqrt{8}}\left(|1\rangle + (1 + e^{i\varphi_B(+)})|2\rangle + |3\rangle\right), \\ &\quad |1_+\rangle \to \frac{1}{\sqrt{8}}\left(|1\rangle + (-1 + e^{i\varphi_B(+)})|2\rangle + |3\rangle\right), \\ D_1: &\quad |1_+\rangle \to \frac{1}{\sqrt{8}}\left(-|1\rangle + (-1 - e^{i\varphi_B(+)})|2\rangle + |3\rangle\right), \\ &\quad |0_+\rangle \to \frac{1}{\sqrt{8}}\left(-|1\rangle + (1 - e^{i\varphi_B(+)})|2\rangle + |3\rangle\right), \end{aligned} \quad (3)$$

в базисе $\times$ (значение $\varphi_B(\times) = \pi/2$) —

$$\begin{aligned} D_0: &\quad |0_\times\rangle \to \frac{1}{\sqrt{8}}\left(|1\rangle + (i + e^{i\varphi_B(\times)})|2\rangle + |3\rangle\right), \\ &\quad |1_\times\rangle \to \frac{1}{\sqrt{8}}\left(|1\rangle + (-i + e^{i\varphi_B(\times)})|2\rangle + |3\rangle\right), \\ D_1: &\quad |1_\times\rangle \to \frac{1}{\sqrt{8}}\left(-|1\rangle + (-i - e^{i\varphi_B(\times)})|2\rangle + |3\rangle\right), \\ &\quad |0_\times\rangle \to \frac{1}{\sqrt{8}}\left(-|1\rangle + (i - e^{i\varphi_B(\times)})|2\rangle + |3\rangle\right). \end{aligned} \quad (4)$$

При совпадении базисов на приемной и передающей сторонах состояния, отвечающие 0 в обоих базисах, будут давать отсчеты во временно́м окне 2 (рис. 1) только в детекторе D_0. Соответственно, состояния, отвечающие 1 в обоих базисах, дадут отсчеты только в детекторе D_1.

[4] Считаем, что фазовый модулятор активируется только в момент прохождения второй «половины» состояния $|2\rangle$.

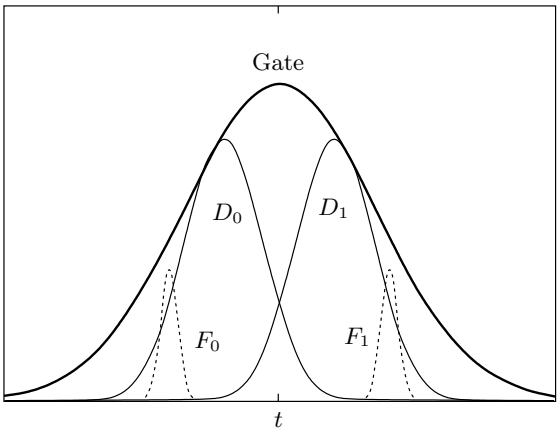

Рис. 2. Пример временны́х зависимостей чувствительностей лавинных фотодетекторов (D_0, D_1), стробирующего импульса (Gate) и фальсифицированных информационных квантовых состояний (F_0 и F_1)

Лавинные детекторы на основе InGaAs:P в оптоволоконных системах квантовой криптографии на телекоммуникационной длине волны 1.55 мкм работают в стробируемом режиме. В момент прилета фотона на них подается импульс напряжения в несколько вольт и длительностью 1–3 нс, накрывающий световой импульс.

Однако лавинные фотодиоды D_0 и D_1 имеют разные временны́е характеристики чувствительности (рис. 2). Атака сводится к следующему. Подслушиватель разрывает квантовый канал связи (оптоволокно) и проводит измерения, аналогичные измерениям на приемной стороне в случайно выбранном базисе.

Возможны два варианта. Сразу отметим, что Ева перепосылает фальсифицированные состояния в базисе, противоположном тому, в котором она проводила свои измерения (см. детали в работах [12, 19]).

1) *Базисы Евы и Алисы–Боба совпадают. Например, пусть это будет базис* +[5]. Ева однозначно получает правильный результат, например, 0 (при этом она, естественно, не знает, что выбранный ею базис и полученный результат являются правильными). Затем Ева готовит фальсифицированное состояние, отвечающее 1 в противоположном базисе ×, но более локализованное (узкое) и слегка сдвинутое по времени так, чтобы оно не попадало в кривую чувствительности фотодетектора D_1 (рис. 2). Таким образом Ева посылает следующее состояние:

$$|1_{F_0\times}\rangle = \frac{1}{\sqrt{2}}\left(|1_{F_0}\rangle - i|2_{F_0}\rangle\right). \tag{5}$$

После прохождения интерферометра и фазового модулятора с фазой в базисе + (напомним, что $\varphi_B(+) = 0$) состояния перед входом в фотодетекторы становятся равными:

$$\begin{aligned} D_0: &\quad \frac{1}{\sqrt{8}}\left(|1_{F_0}\rangle + (i+1)|2_{F_0}\rangle + |3_{F_0}\rangle\right), \\ D_1: &\quad \frac{1}{\sqrt{8}}\left(-|1_{F_0}\rangle + (i-1)|2_{F_0}\rangle + |3_{F_0}\rangle\right). \end{aligned} \tag{6}$$

Тот факт, что перепосланное Евой состояние является неправильным, не важен, поскольку такое фальсифицированное состояние не даст ошибочного отсчета в детекторе D_1 в центральном временно́м окне 2 (рис. 1, 2), так как фальсифицированное состояние не попадает по времени в кривую чувствительности фотодетектора D_1. Отсчет будет только в детекторе D_0, т. е. безошибочным. Уменьшение общего числа отсчетов от фальсифицированных состояний в детекторе D_0 по сравнению с правильными состояниями в базисе + не принципиально. Из-за того, что детекторы имеют квантовую эффективность, не равную единице, и квантовый канал связи имеет потери, полное число отсчетов на приемной стороне, которое должно иметь место в отсутствие Евы, всегда может быть сохранено путем увеличения интенсивности фальсифицированного состояния.

2) *Базисы Евы и Алисы–Боба не совпадают.* Пусть базис Евы +, а Алисы–Боба ×, и Алиса посылала 0. В неправильном базисе + Ева может получить равновероятно как правильный отсчет 0, так и неправильный 1.

2а) *Пусть Ева получила правильный отсчет* 0. Тогда Ева посылает фальсифицированное состояние, отвечающее 1 в противоположном базисе ×, но оно не попадает по времени в кривую чувствительности детектора D_1 (см. выше формулу (6)). Состояние является неправильным в этом базисе, но оно не даст неправильного отсчета в детекторе D_1. Оно также не даст отсчета в детекторе D_0, так как состояние приготовлено в базисе измерений Боба. Ева навязывает в этом случае отсутствие отсчета, но и ошибка отсутствует.

2б) *Пусть Ева получила неправильный отсчет* 1 *в неправильном базисе.* Ева перепосылает фальсифицированное состояние, отвечающее 0 в противоположном своему и совпадающем с Бобом базисе ×, но так сдвинутое по времени, чтобы не давать

[5] Напомним, что посылки, в которых базисы Алисы и Боба не совпадают, отбрасываются путем согласования через открытый классический канал связи.

отсчета в детекторе D_0. Это фальсифицированное состояние имеет вид

$$|0_{F_1\times}\rangle = \frac{1}{\sqrt{2}}\left(|1_{F_1}\rangle + i|2_{F_1}\rangle\right). \qquad (7)$$

Данное состояние, хотя и правильное, но сдвинуто по времени и не попадает в кривую чувствительности детектора D_0, где правильное состояние должно было дать отсчет. Данное модифицированное состояние не даст правильного отсчета в D_0, но важно, что оно не даст и ошибочного отсчета в детекторе D_1, поскольку конструктивная интерференция состояний, распространяющихся по разным плечам интерферометра Маха–Цандера имеет место только на входе фотодетектора D_0, а на входе детектора D_1 имеет место полное гашение (деструктивная интерференция) состояний, прошедших по верхнему и нижнему плечам.

Таким образом, Ева может навязать свои отсчеты и запретить ошибочные. В итоге, Ева знает все зарегистрированные отсчеты у Боба, а также в каком детекторе они произошли. Ева знает весь ключ и не производит ошибок на стороне Боба, т. е. остается необнаруженной. А сам протокол уязвим по отношению к данной атаке и не обеспечивает секретную передачу ключей. Отметим, что данная атака реализуется на сегодняшнем уровне технологий [10, 12, 19].

Разумеется, что это несколько идеализированный вариант атаки в том смысле, что кривые чувствительности не перекрываются и Ева регистрирует все состояния с вероятностью единица, т. е. имеет идеальные фотодетекторы. Однако в криптографии как в классической, так и в квантовой при оценке стойкости любой системы всегда исходят из пессимистических консервативных оценок.

2.2. Атака на ключ посредством перевода лавинных фотодетекторов в классический режим фотодетектирования

При данной атаке, как и при предыдущей, Ева разрывает квантовый канал связи и проводит измерения в своем случайном базисе. Затем перепосылает состояния, которые она получила при измерении, но не однофотонные, а с увеличенной интенсивностью, чтобы ее было достаточно для перевода детектора в линейный классический режим. При этом интенсивность подбирается так, чтобы половины от нее было недостаточно для перевода детектора в линейный режим и чтобы он еще оставался в режиме ослепления (режим "no click") (см. детали в работах [10, 12, 19], а также критику в [20]).

Возможны два случая.

1) *Базисы Евы и Алисы–Боба совпадают.* В этом случае на один из детекторов попадает полная интенсивность, и он дает отсчет в центральном временно́м окне (рис. 1), где имеет место полная конструктивная интерференция.

2) *Базисы Евы и Алисы–Боба не совпадают.* В этом случае на оба детектора попадает половина интенсивности в центральном временно́м окне. Ее недостаточно, чтобы детектор сработал как классический, но она больше интенсивности, которая переводит лавинный детектор в режим ослепления в пике (лежит в зоне "no click").

Пусть интенсивность, начиная с которой детектор выходит из режима ослепления и регистрирует сигнал как линейное устройство, равна I_{th}, а интенсивность, с которой детектор ослепляется (лежит в зоне "no click") равна I_{bl} ($I_{bl} < I_{th}$).

Пусть интенсивность фальсифицированного состояния равна I_{faked}. Интенсивность в боковых временны́х окнах (см. рис. 2) не зависит от выбора базисов Евой и Алисой–Бобом и равна $I_{faked}/8$ (см. рис. 2 и формулы (3)–(7)). При этом возможны две ситуации.

а) Интенсивность I_{faked} такова, что в боковых временны́х окнах, где интенсивность не зависит от конструктивной или деструктивной интерференции, она равна $I_{faked}/8$. При этом $I_{faked}/8$ заведомо меньше пороговой интенсивности I_{th}, при которой детектор работает как линейный, но больше, чем интенсивность I_{bl}, вызывающая эффект ослепления: $I_{bl} < I_{faked}/8 < I_{th}$. Отсчетов в боковых временны́х окнах (рис. 1) в этом случае не будет.

б) Интенсивность I_{faked}, в боковых временны́х окнах равная $I_{faked}/8$, меньше как пороговой интенсивности I_{th}, так и интенсивности I_{bl}, вызывающей эффект ослепления: $I_{faked}/8 < I_{bl}, I_{th}$. В этом случае отсчеты в боковых временны́х окнах (рис. 1) будут иметь место. Детектор не ослепляется и работает как однофотонный в режиме счета.

Отметим, что работа [10] не содержит полного рассмотрения таких ситуаций.

Таким образом, данная атака приводит к тому, что при совпадении базисов Ева знает каждый передаваемый бит. В случае же несовпадения базисов она блокирует отсчеты фотодетекторов и не производит ошибок на приемной стороне Боба.

В стандартной версии базовых протоколов не отслеживается статистика отсчетов в боковых временны́х окнах, а регистрируются только отсчеты в

центральном временно́м окне, поэтому при такой атаке Ева знает весь ключ и не производит ошибок на приемной стороне — протокол не секретен.

3. ПРОТОКОЛЫ КВАНТОВОГО РАСПРЕДЕЛЕНИЯ КЛЮЧЕЙ, УСТОЙЧИВЫЕ К АТАКЕ С «ОСЛЕПЛЕНИЕМ» ФОТОДЕТЕКТОРОВ

3.1. Двухпараметрическое фазово-временно́е квантовое распределение ключей

Для самодостаточности приведем двухпараметрический протокол квантового распределения ключей с фазово-временны́м кодированием.

В протоколе в качестве информационных состояний используется восемь состояний по два состояния в каждом из четырех базисов, которые будем обозначать как $+L$, $\times L$, $+R$, $\times R$. Состояния в базисах $+L$ и $\times L$ имеют вид

$$|0_{+L}\rangle = \frac{1}{\sqrt{2}}(|1\rangle + |2\rangle), \quad |1_{+L}\rangle = \frac{1}{\sqrt{2}}(|1\rangle - |2\rangle), \quad (8)$$

$$|0_{\times L}\rangle = \frac{1}{\sqrt{2}}(|1\rangle + i|2\rangle), \quad |1_{\times L}\rangle = \frac{1}{\sqrt{2}}(|1\rangle - i|2\rangle), \quad (9)$$

в базисах $+R$ и $\times R$, соответственно,

$$|0_{+R}\rangle = \frac{1}{\sqrt{2}}(|2\rangle + |3\rangle), \quad |1_{+R}\rangle = \frac{1}{\sqrt{2}}(|2\rangle - |3\rangle), \quad (10)$$

$$|0_{\times R}\rangle = \frac{1}{\sqrt{2}}(|2\rangle + i|3\rangle), \quad |1_{\times R}\rangle = \frac{1}{\sqrt{2}}(|2\rangle - i|3\rangle). \quad (11)$$

Здесь $|1\rangle$, $|2\rangle$ и $|3\rangle$ — ортонормированные базисные векторы (забегая вперед, отметим, что данные базисные векторы отвечают локализованным во времени однофотонным состояниям, попарно сдвинутым во времени на определенную величину). Формально пространство состояний $\mathcal{H}$ является трехмерным. Состояния внутри одного базиса ортогональны аналогично протоколу BB84 [3], а состояния из разных базисов попарно неортогональны, как в протоколе B92 [4].

Схематически состояния представлены на рис. 3*a*.

Формально протокол выглядит следующим образом (см. детали в [22]).

1) Алиса на передающей станции равновероятно выбирает одно из восьми состояний (8)–(11) и направляет их на приемную станцию Бобу. Технически данные состояния получаются пропусканием через интерферометр Маха–Цандера локализованного состояния, случайно выбранного в один из двух моментов времени (выбор момента времени соответствует выбору одного из базисов L или R), отстоящих на разность хода по двум плечам интерферометра (см. детали в [22]).

2) Боб равновероятно случайно и независимо от Алисы выбирает один из четырех базисов для измерений. Более формально Боб использует случайно одно из четырех измерений, которые описываются следующими разложениями единицы I в $\mathcal{H}$:

$$I = |0_{+L}\rangle\langle 0_{+L}| + |1_{+L}\rangle \times \\ \times \langle 1_{+L}| + |3\rangle\langle 3| \text{ — измерение в базисе } +L, \quad (12)$$

$$I = |0_{\times L}\rangle\langle 0_{\times L}| + |1_{\times L}\rangle \times \\ \times \langle 1_{\times L}| + |3\rangle\langle 3| \text{ — измерение в базисе } \times L, \quad (13)$$

$$I = |1\rangle\langle 1| + |1_{+R}\rangle\langle 1_{+R}| + |2_{+R}\rangle \times \\ \times \langle 2_{+R}| \text{ — измерение в базисе } +R, \quad (14)$$

$$I = |1\rangle\langle 1| + |1_{\times R}\rangle\langle 1_{\times R}| + |2_{\times R}\rangle \times \\ \times \langle 2_{\times R}| \text{ — измерение в базисе } \times R. \quad (15)$$

Технически данные измерения реализуются при помощи интерферометра Маха–Цандера, фазового модулятора и стробирования лавинных фотодетекторов в разных временны́х окнах (рис. 3). Регистрация в «канале» измерений $|3\rangle\langle 3|$ в левом базисе L (аналогично $|1\rangle\langle 1|$ в правом базисе R) отвечает контрольным измерениям в соответствующих контрольных временны́х окнах (рис. 3).

3) Боб сообщает только сам факт получения состояния.

4) После проведения серии посылок Алисой и измерений Бобом Алиса раскрывает базисы, но не раскрывает сами состояния.

5) Боб открыто сообщает номера посылок, где базисы не совпадали, данные посылки отбрасываются. Результаты измерений в тех посылках, в которых базисы совпадали, сохраняются. Если отсчеты были в информационных временны́х слотах (слот 2 в базисе L и слот 3 в базисе R), то результаты измерений Боб интерпретирует следующим образом.

5.1) В базисах $+, \times L$ отсчеты в детекторе D_0 во временно́м окне 2 (рис. 3) интерпретируются как 0, отсчет во временно́м окне 2 в детекторе D_1 — как 1.

5.2) В базисах $+, \times R$ отсчеты в детекторе D_0 во временно́м окне 3 (рис. 3) интерпретируются как 0, отсчет во временно́м окне 3 в детекторе D_1 — как 1.

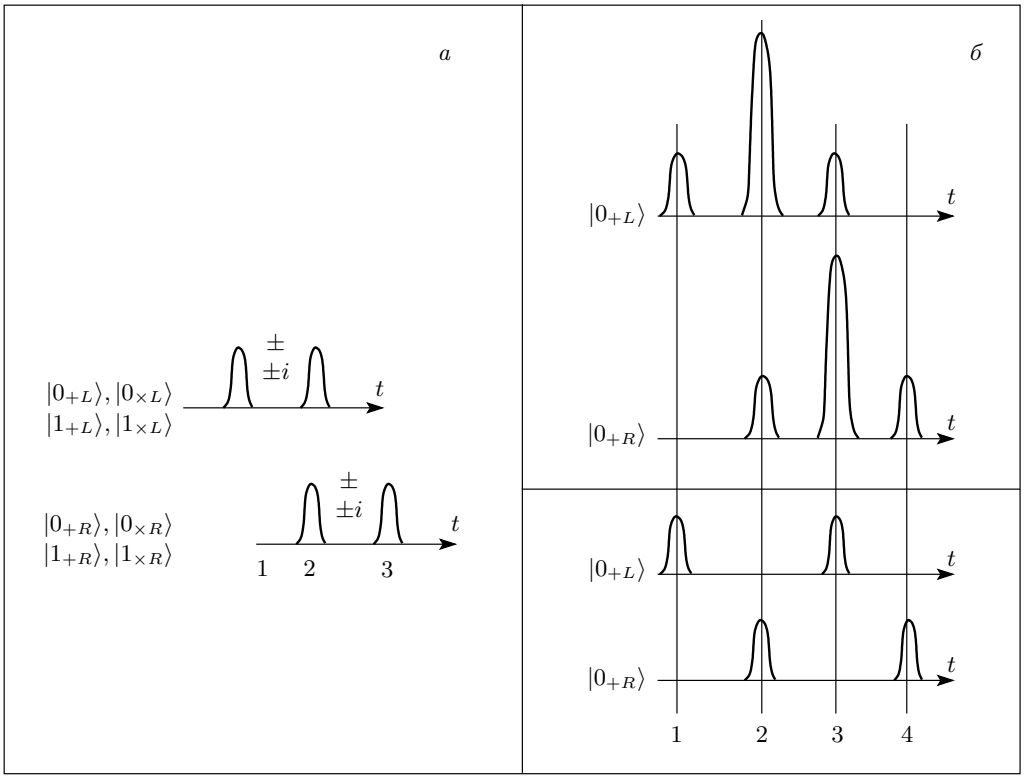

Рис. 3. *а*) Схематическое представление информационных квантовых состояний в двухпараметрическом протоколе с фазово-временны́м кодированием. *б*) Схематическое представление наблюдаемой статистики фотоотсчетов в отсутствие подслушивателя

5.3) Временны́е окна 1 и 3 для состояний в базисе L, а также окна 2 и 4 являются контрольными.

Технически измерения реализуются при помощи интерферометра Маха–Цандера (рис. 1, см. также [23]). После прохождения состояний (8)–(11) через интерферометр Маха–Цандера перед входом в детекторы D_0 и D_1 состояния становятся равными (принята нормировка на единицу в обоих каналах регистрации в детекторах D_0 и D_1):

$$\begin{aligned} D_0: &\quad |0_{+L}\rangle \to \frac{1}{\sqrt{8}}\left(|1\rangle + 2|2\rangle + |3\rangle\right), \\ &\quad |1_{+L}\rangle \to \frac{1}{\sqrt{8}}\left(|1\rangle + |3\rangle\right), \\ D_1: &\quad |1_{+L}\rangle \to \frac{1}{\sqrt{8}}\left(-|1\rangle - 2|2\rangle + |3\rangle\right), \\ &\quad |0_{+L}\rangle \to \frac{1}{\sqrt{8}}\left(-|1\rangle + |3\rangle\right), \end{aligned} \tag{16}$$

$$\begin{aligned} D_0: &\quad |0_{+R}\rangle \to \frac{1}{\sqrt{8}}\left(|2\rangle + 2|3\rangle + |4\rangle\right), \\ &\quad |1_{+R}\rangle \to \frac{1}{\sqrt{8}}\left(|2\rangle + |4\rangle\right), \\ D_1: &\quad |1_{+R}\rangle \to \frac{1}{\sqrt{8}}\left(-|2\rangle - 2|3\rangle + |4\rangle\right), \\ &\quad |0_{+R}\rangle \to \frac{1}{\sqrt{8}}\left(-|2\rangle + |4\rangle\right). \end{aligned} \tag{17}$$

6) Боб сообщает Алисе номера посылок (уже при совпадающих базисах), в которых был отсчет в информационных временны́х окнах, а также в контрольных окнах.

7) Алиса и Боб через открытый канал связи оценивают вероятность ошибки Q, раскрывая часть посылок в информационных временны́х слотах.

8) Для состояний в базисе L Боб подсчитывает процент отсчетов q в контрольных временны́х слотах 4, а для состояний в базисе R — в контрольном слоте 1. Состояния в базисах $+L, \times L$ и $+R, \times R$ неортогональны, поэтому Ева не может достоверно различить состояния из базисов L и R, и ее вторжение

приведет к отсчетам в контрольных слотах. Например, если были посланы состояния из базиса L, то вторжение Евы неизбежно приведет к отсчетам в слоте 4, а там их не должно быть (см. детали анализа стойкости в [22]).

9) Для состояний в базисе L оценивается процент отсчетов δ во временны́х окнах 1 и 3, а для состояний в базисе R — во временны́х окнах 2 и 4. В отсутствие Евы (при совпадении базисов) отношение отсчетов в информационных окнах и контрольных (16), (17) равно

$$\delta = \left(2/\sqrt{8}\right)^2 \left(1/\sqrt{8}\right)^{-2} = 4.$$

Вторжение Евы приведет к изменению данного отношения.

10) Если наблюдаемые параметры Q, q, δ не превышают критические значения, то протокол продолжается. В противном случае протокол прерывается.

Дальнейшие действия аналогичны другим протоколам [5, 6]. Происходит распределенная коррекция ошибок в оставшейся нераскрытой части. Затем проводится сжатие очищенного ключа [23].

В заключение данного раздела отметим, что был рассмотрен случай, когда информационные состояния внутри базисов $+L, \times L$ и $+R, \times R$ ортогональны. В этом случае протокол в однофотонном режиме гарантирует секретное распределение ключей (при идеальных фотодетекторах без темновых шумов) вплоть до ошибки $Q < Q_c = 50\,\%$. Длина секретного ключа r в асимптотическом пределе длинных последовательностей (в пересчете на одну позицию) дается соотношением

$$\begin{gathered} r = 1 - h(Q) - h(q), \\ h(x) = -x\log_2 x - (1-x)\log_2(1-x). \end{gathered} \tag{18}$$

При $q \to 0$ имеем $Q \to Q_c = 50\,\%$ (см. подробности в [22]). Напомним, что для протокола BB84 критическая ошибка и длина секретного ключа определяются из соотношения

$$r = 1 - h(Q) - h(q), \tag{19}$$

что дает знаменитое значение критической ошибки для протокола BB84: $Q_c(\text{BB84}) \approx 11\,\%$.

Рассуждения, приведенные выше, могут быть перенесены на версию протокола с фазово-временны́м кодированием с неортогональными состояниями внутри базисов $+L, \times L$ и $+R, \times R$, которая аналогична конфигурации в протоколе SARG04. Однако, как известно, при не строго однофотонном источнике и квантовом канале с потерями протокол SARG04 становится несекретным, если потери в канале связи позволяют Еве блокировать все посылки, содержащие три и более фотонов. Протокол с фазово-временны́м кодированием устойчив к бо́льшим потерям в канале связи, чем протокол SARG04, поскольку в нем Еве требуется блокировать посылки, содержащие пять и более фотонов. Поэтому критическая длина линии с потерями, до которой гарантируется секретное распределение ключей, оказывается больше [22].

3.1.1. Устойчивость по отношению к атаке I

Для того чтобы показать устойчивость протокола к атакам с ослеплением фотодетекторов, достаточно показать, что такие атаки приводят к ошибкам (изменению статистик) на приемной стороне, т. е. к детектированию вторжения подслушивателя. Для обнаружения атаки, описанной в разд. 2.1, достаточно следить за изменением одной наблюдаемой статистики q, отвечающей за ошибочные отсчеты в контрольных временны́х окнах 4 в базисе L и 1 в базисе R.

Ниже приведем неформальный анализ причин устойчивости данного протокола, опуская математические подробности, которые приведены в работах [22].

Причина устойчивости двухпараметрического протокола с фазово-временны́м кодированием, в отличие от протокола BB84, состоит в том, что в данном протоколе используются два базиса L и R (внутри каждого базиса L или R протокол выглядит как BB84).

Как отмечалось выше, атака с ослеплением аналогична атаке прием–перепосыл, но перепосылаются фальсифицированные состояния, и Ева случайно выбирает базис для измерений L или R, далее внутри этих базисов действует аналогично протоколу BB84. При этом всегда будут ситуации (с вероятностью $1/2$), когда Ева выберет базис, например, L, а базис Алисы–Боба был R. В этом случае независимо от того, какой исход получит Ева в своем базисе — 0 или 1 — и перепошлет фальсифицированные состояния, как и в протоколе BB84, в базисе L, ослепляя любой из двух детекторов, это неизбежно приведет к отсчетам в контрольном временно́м окне 1 (рис. 3). И этот ошибочный отсчет будет иметь место независимо от результата измерения Евы и независимо от фальсифицированного состояния (неважно, отвечает оно 0 или 1), поскольку отсчет в контрольном окне 1 в данной ситуации не зависит от состояния и

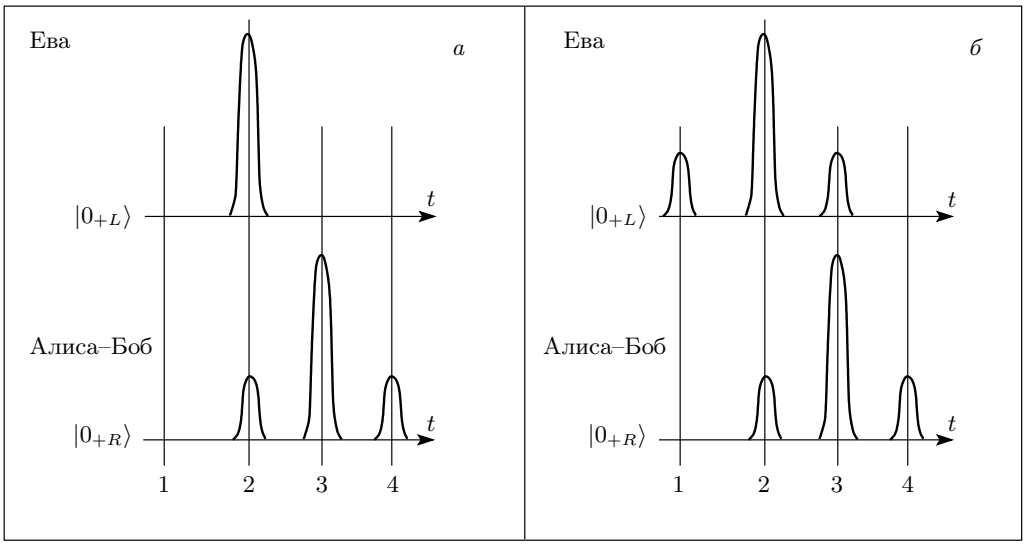

Рис. 4. Схематическое изображение наблюдаемой статистики фотоотсчетов в присутствии Евы и истинной в ее отсутствие. $а$ — $I_{bl} < I_{faked}/8 < I_{th}$, $б$ — $I_{faked}/8 < I_{bl}, I_{th}$

не связан с конструктивной или деструктивной интерференцией.

Принципиально важно, что всегда будет ситуация, когда возникнут ошибочные отсчеты в контрольном временно́м окне 1 или 4.

Итак, возможны две ситуации.

1) Действительно, если базисы Евы и Алисы–Боба совпадают (оба L или оба R), то перепосыл фальсифицированного состояния Евы в ее базисе измерений L (или R) не приведет к ошибочному отсчету в контрольном временно́м окне. Перепосыл же в противоположном базисе приведет к ошибкам, как описано выше.

2) Если базисы измерений Евы и Алисы–Боба не совпадают, например, у Евы L, у Алисы–Боба R, то перепосыл фальсифицированного состояния Евой в ее базисе измерений L приведет к ошибочным отсчетам в контрольном временно́м окне. Перепосыл же в противоположном базисе не приведет к ошибочным отсчетам.

Наличие дополнительных базисов L, R кроме $+, \times$ приводит к тому, что при любой стратегии перепосыла Евой фальсифицированных состояний, Ева может исключить ошибки лишь для одной альтернативы выбора базисов $+, \times$, но не может навязать свои отсчеты для другой дополнительной альтернативы, связанной с выбором базисов L, R.

Таким образом, из-за того, что в отличие от протокола BB84, кроме базисов $+$ и $\times$ имеются еще базисы L и R, неизбежно возникнет ситуация, когда Ева перепошлет фальсифицированные состояния в базисе L, который противоположен базису Алисы–Боба R, и наоборот. Это приведет к ошибочным отсчетам в контрольных временны́х окнах как в одном, так и в другом детекторе. Причем это имеет место независимо от выбора базисов $+$ или $\times$ внутри базисов L или R.

3.1.2. Устойчивость по отношению к атаке II

Нам будет достаточно показать, что существуют ситуации, которые приводят к изменению хотя бы одной из наблюдаемых статистик отсчетов Q, q, δ на приемной стороне.

Согласно разд. 2.2 возможны две ситуации.

1) Пусть базисы Евы и Алисы–Боба не совпадают. Например, пусть Ева делает измерения в базисе $+L$, а Алисой было послано состояние в базисе $0+R$. В этом случае Ева равновероятно и случайно может получить как 0, так и 1. Пусть для определенности Ева получила исход 0.

Согласно стратегии разд. 2.2, Ева посылает состояния, которые она измерила, но с другой интенсивностью I_{faked}. В данном случае Ева перепосылает состояние в базисе $0 + L$.

В зависимости от величины интенсивности I_{faked} также возможны два случая (см. разд. 2.2).

а) Интенсивность I_{faked} такова, что отсчетов в боковых временны́х окнах не возникает. Такая ситуация не интересна с точки зрения Евы, поскольку полное отсутствие отсчетов в боковых временны́х ок-

нах приведет к изменению статистики δ, при этом Ева детектируется по их полному отсутствию (см. рис. 4*а*).

б) Интенсивность I_{faked} такова, что отсчеты в боковых окнах будут иметь место (т. е. $I_{faked} < I_{bl}$). В этом случае при несовпадении базисов (у Евы L, а у Алисы–Боба R) возникнут отсчеты в контрольных временны́х окнах (в данном случае — во временно́м окне 1, см. рис. 4*б*).

Таким образом, ситуация, при которой Ева выбрала базис L (или R), а Алиса–Боб — базис R (соответственно L) будет иметь место с вероятностью $1/2$. Как видно из рассуждений, приведенных выше, при любом значении интенсивности I_{faked} возникают изменения наблюдаемой на приемной стороне статистики фотоотсчетов, по которым вторжение Евы детектируется.

Протокол распределения ключей гарантирует, что никогда не будет ситуации, когда Ева знает весь передаваемый ключ и остается не обнаруженной. Поэтому данный протокол является стойким относительно данной атаки.

Отметим, что анализ статистики фотоотсчетов в боковых временны́х окнах может быть использован для детектирования атаки с ослеплением на протокол BB84 при атаке II. Однако этого недостаточно, чтобы гарантировать детектирование подслушивания относительно атаки I. Для обнаружения атаки I необходимы состояния в базисах L и R, как в двухпараметрическом протоколе с фазово-временны́м кодированием.

3.2. Квантовое распределение ключей с эталонным (реперным) классическим когерентным состоянием

Изначально данный протокол был разработан для того, чтобы обеспечить секретное распределение ключей при не строго однофотонном источнике и квантовом канале связи с произвольными потерями. Кроме того, протокол устойчив относительно PNS-атаки [7] и атаки с измерениями с определенным исходом [8, 9].

Внутренняя структура протокола такова, что он оказывается устойчивым относительно атаки с ослеплением фотодетекторов. Приведем сначала сам протокол, а затем обсудим его устойчивость относительно упомянутой атаки.

Неформальная идея данного протокола состоит в том, чтобы использовать когерентные состояния, полученные из одного источника. Состояния проходят по одному и тому же пути в канале связи, изменение фазы у параметра α одинаково и при измерениях общее изменение не важно. Одно состояние с малым средним числом фотонов ($\mu = |\alpha|^2 \ll 1$) является информационным, а второе когерентное состояние с большим (макроскопически большим) средним числом фотонов — реперным ($\mu_c = |\alpha_c|^2 \gg \gg 1$). Перед измерениями реперное и информационное когерентные состояния расщепляются светоделителем. На линейном светоделителе, как известно, когерентное состояние преобразуется самоподобным образом, т. е. после деления оно остается когерентным на каждом из двух выходов светоделителя. Важно также, что когерентные состояния на двух выходах светоделителя являются незапутанными, и это имеет место только для когерентных состояний.

Перед измерениями проверяется интенсивность части расщепленного когерентного состояния с большим средним числом фотонов калиброванным классическим детектором. Если обнаружено изменение интенсивности по сравнению с той, которая должна быть, то посылка выбрасывается. Если интенсивность имеет правильную величину, то вторая часть состояния после контролируемого ослабления используется для интерференционных измерений вместе со слабым информационным когерентным состоянием.

Оказывается, что такой процедуры достаточно, чтобы ослабленная часть когерентного состояния с большим μ_c играла роль эталонного состояния, с которым проводится сравнение информационного когерентного состояния.

Перейдем к описанию оптической схемы и деталям реализации. Схема приведена на рис. 5.

Длина линии связи и затухание в ней известны заранее и являются параметрами протокола (однако это не означает, что Ева не может их изменять по своему усмотрению во время работы протокола). На передающей стороне в каждой посылке, которые независимы, генерируется пара одинаковых когерентных состояний с большим средним числом фотонов ($\mu_c = |\alpha_c|^2 \gg 1$), сдвинутых по времени и имеющих общую привязку по фазе. Общая привязка фазы позволяет устроить интерференции двух данных состояний при совмещении их по времени.

При прохождении второго состояния через аттенюатор (AT на рис. 5) последний активируется и второе когерентное состояние ослабляется до квазиоднофотонного уровня ($\mu = |\alpha|^2 \ll 1$). При этом состояния остаются когерентными и сфазированными относительно друг друга. Далее, Алиса случайно и равновероятно выбирает 0 или 1 и прикладывает требуемое напряжение на фазовый модулятор (PM

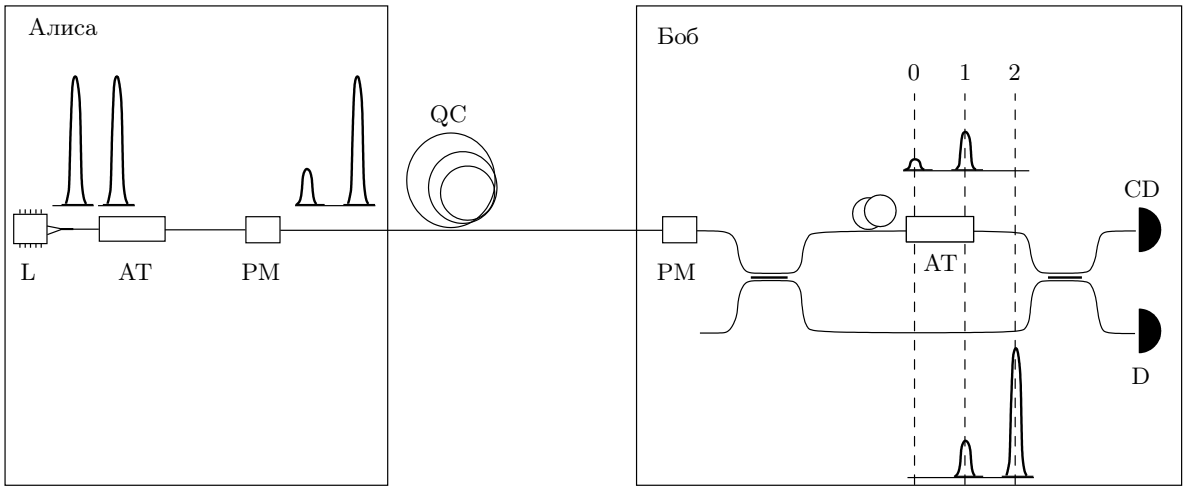

Рис. 5. Принципиальная схема оптоволоконной системы квантовой криптографии с эталонным классическим когерентным состоянием. L — лазер, AT — управляемый аттенюатор, PM — фазовый модулятор, CD — классический фотодетектор, работающий в линейном режиме, D — лавинный однофотонный детектор, работающий в режиме счета фотонов, QC — квантовый канал связи

на рис. 5) в момент прохождения квазиоднофотонного состояния $|\alpha\rangle$. После этого состояние становится равным $|\pm\alpha\rangle$. Далее пара состояний поступает в квантовый канал связи (QC на рис. 5). На приемной стороне Боб случайно и независимо от Алисы прикладывает напряжение на фазовый модулятор в момент прохождения квазиоднофотонного состояния, чтобы скомпенсировать фазу у параметра α, приобретенную на стороне Алисы.

Совмещение состояний по времени достигается при помощи интерферометра Маха–Цандера с разной длиной плеч. Разность оптического пути по верхнему и нижнему плечам интерферометра равна расстоянию между парой состояний. В верхнем плече встроен аттенюатор с фиксированным коэффициентом ослабления, таким чтобы ослабленное когерентное состояние с большим средним числом фотонов сравнялось по интенсивности с квазиоднофотонным. Если фазы Алисы и Боба одинаковы ($\varphi_A = \varphi_B = 0$ или $\varphi_A = \varphi_B = \pi$), то конструктивная интерференция при наложении сдвинутых по времени когерентных состояний из верхнего и нижнего плеч имеет место в нижнем однофотонном детекторе (D на рис. 5).

На первом светоделителе входные состояния на верхнем входе равны $|\sqrt{\mu(L)}\rangle_1 \otimes |\sqrt{\mu_c(L)}\rangle_2$, на нижнем входе — вакуумные. Индексы «1» и «2» обозначают временны́е окна, в которых локализованы когерентные состояния.

После прохождения первого светоделителя когерентные состояния преобразуются следующим образом (см. детали, например, в книге [24]): в верхнем плече с учетом задержки назад во времени

$$\left|\frac{\sqrt{\mu(L)}}{\sqrt{2}}\right\rangle_0 \otimes \left|\frac{\sqrt{\mu_c(L)}}{\sqrt{2}}\right\rangle_1,$$

в нижнем плече

$$\left|-\frac{\sqrt{\mu(L)}}{\sqrt{2}}\right\rangle_1 \otimes \left|-\frac{\sqrt{\mu_c(L)}}{\sqrt{2}}\right\rangle_2.$$

Светоделители можно выбрать симметричными.

Далее в верхнем плече в момент прохождения когерентного состояния с большим средним числом фотонов активируется аттенюатор (AT на рис. 5), который изменяет среднее число фотонов в фиксированное число раз, а именно, в $(\mu(L)/\mu_c(L))^{-1}$ раз. При этом состояния в верхнем плече становятся равными

$$\left|\frac{\sqrt{\mu^2(L)/\mu_c(L)}}{\sqrt{2}}\right\rangle_0 \otimes \left|\frac{\sqrt{\mu(L)}}{\sqrt{2}}\right\rangle_1.$$

Величина ослабления при типичных значениях $\mu \approx 0.1$ и интенсивности классического когерентного состояния в 0.1 мВт приблизительно составляет 170 дБ.

После преобразования на втором светоделителе состояния в нижнем плече имеют вид

$$\left|\frac{\sqrt{\mu^2(L)/\mu_c(L)}}{2}\right\rangle_0 \otimes \left|\sqrt{\mu(L)}\right\rangle_1 \otimes \left|\frac{\sqrt{\mu_c(L)}}{2}\right\rangle_2$$

и соответственно в верхнем плече —

$$\left| -\frac{\sqrt{\mu^2(L)/\mu_c(L)}}{2} \right\rangle_0 \otimes |vac\rangle_1 \otimes \left| \frac{\sqrt{\mu_c(L)}}{2} \right\rangle_2 .$$

Таким образом, в среднем временно́м окне 1 при совпадении фаз Алисы и Боба и в отсутствие внешнего возмущения имеет место конструктивная интерференция информационного состояния и ослабленного когерентного состояния с большим числом фотонов на выходе нижнего плеча интерферометра. По верхнему выходу во временно́м окне 2 классический детектор (CD на рис. 5) регистрирует интенсивность когерентного («классического») состояния $|\sqrt{\mu_c(L)}/2\rangle_2$. Если обнаружено изменение интенсивности когерентного состояния с большим μ_c, то посылка отбрасывается.

Приведем теперь сам протокол.

1) В протоколе используется пара когерентных состояний, отвечающих 0 и 1, которые Алиса выбирает равновероятно. Имеем

$$\begin{array}{l} 0 : |e^{i\varphi_0}\sqrt{\mu}\rangle\ (\varphi_0 = 0) \\ 1 : |e^{i\varphi_1}\sqrt{\mu}\rangle\ (\varphi_1 = \pi) \end{array}, \quad \begin{array}{c} |e^{i\varphi_{0,1}}\sqrt{\mu}\rangle = |\pm\alpha\rangle \\ (|\alpha|^2 = \mu). \end{array} \tag{20}$$

2) Боб проводит измерения, которые формально описываются следующим разложением единицы. Боб выбирает случайно и равновероятно одно из двух измерений, и которые позволяют отличать состояния $|e^{i\varphi_{0,1}}\sqrt{\mu(L)}\rangle$ от любых других состояний. Эти измерения можно записать в виде[6)]

$$I = P\left(e^{i\varphi_{0,1}}\sqrt{\mu(L)}\right) + P_\perp\left(e^{i\varphi_{0,1}}\sqrt{\mu(L)}\right), \tag{21}$$

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

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

Выбор измерения фиксируется выбором $\varphi_{0,1}$. Каждое из двух измерений (21) имеет два исхода. Причем исход $\perp$ никогда не происходит от состояния $|e^{i\varphi_{0,1}}\sqrt{\mu(L)}\rangle$, так как вероятность данного исхода тождественно равна нулю:

$$\begin{aligned} \Pr(\perp, |e^{i\varphi_{0,1}}\sqrt{\mu(L)}\rangle) = \\ = \mathrm{Tr}\left\{P_\perp(e^{i\varphi_{0,1}}\sqrt{\mu(L)})|e^{i\varphi_{0,1}}\sqrt{\mu(L)}\rangle \times \right. \\ \left. \times \langle e^{i\varphi_{0,1}}\sqrt{\mu(L)}|\right\} \equiv 0. \end{aligned} \tag{22}$$

[6)] Возможно использовать одно измерение с тремя исходами (два исхода определенных и один неопределенный [8, 9]), что эквивалентно двум измерениям в смысле различения состояний (20), однако два разных измерения технически проще реализовать.

3) Через открытый канал часть посылок раскрывается. Отдельно сравниваются исходы измерений у Боба для двух множеств посылок:

3.1) когда фазы Алисы и Боба совпадали;

3.2) когда фазы Алисы и Боба были различны.

Оценивается величина наблюдаемой ошибки. Если последняя меньше критической величины, то проводится исправление ошибок через открытый классический канал и усиление секретности очищенного ключа. В противном случае протокол прерывается.

После прохождения через канал связи с затуханием когерентное состояние преобразуется следующим образом (см. подробности, например, в работах [16, 24, 25]):

$$|\pm\alpha\rangle \to |\pm\alpha\sqrt{T(L)}\rangle = |\pm\sqrt{\mu T(L)}\rangle (T(L) = 10^{-\delta L/10},$$

для одномодового оптоволокна SMF-28 величина $\delta \approx 0.2$ дБ/км). Вообще говоря, при прохождении через канал когерентного состояния у комплексного параметра α уменьшается амплитуда ($|\alpha| = |\alpha\sqrt{T(L)}|$) и кроме этого он приобретает дополнительную фазу

$$\alpha \to e^{i\varphi_{channel}}\alpha\sqrt{T(L)}.$$

Однако как увидим ниже, данная дополнительная фаза не играет роли, поэтому ее опускаем.

Основная идея протокола состоит в том, чтобы осуществлять такие измерения, которые бы изначально учитывали изменения когерентного состояния за счет потерь в линии связи, но в отсутствие подслушивателя. Длина канала и потери в нем являются параметрами протокола и калиброваны заранее. В такой ситуации измерения (21) обнаруживают любые изменения исходных состояний.

Напомним еще раз, что классическое когерентное состояние не несет никакой информации о ключе — в каждой посылке это одно и то же состояние. Информация о ключе заключена в относительной фазе информационного и реперного когерентных состояний.

Устойчивость данного протокола относительно PNS-атаки практически очевидна, поскольку данная атака связана с неразрушающим измерением числа фотонов. Измерение дается разложением единицы:

$$I = \sum_{n=0}^{\infty} |n\rangle\langle n|. \tag{23}$$

Ясно, что такое измерение не дает информации о передаваемом бите ключа, поскольку нечувствитель-

но к фазе параметра α, описывающего информационное когерентное состояние. К тому же данное измерение разрушает когерентность самого состояния, что детектируется путем интерференционного измерения данного состояния с реперным когерентным состоянием.

Для самодостаточности изложения покажем причины на неформальном уровне, почему данный протокол устойчив относительно UM-атаки. UM-измерения не позволяют Еве: 1) знать весь ключ, 2) сохранить среднее число регистрируемых посылок на приемной стороне, 3) не произвести ошибок на приемной стороне.

Нам потребуются два факта.

1) Отклик (фототок) классического детектора является некоторой известной (калиброванной) функцией интенсивности сигнала — среднего числа фотонов в когерентном состоянии μ_c.

2) Однофотонный детектор не реагирует на вакуумную компоненту, вероятность регистрации детектора пропорциональна[7] $1 - e^{-\eta\mu(L)}$ (см., например, [16]), где η — квантовая эффективность детектора. Типичное значение на телекоммуникационной длине волны 1.55 мкм равно $\eta \approx 10$–$30\,\%$.

Если в какой-то посылке Ева получила неопределенный исход, то имеется лишь несколько вариантов ее дальнейших действий.

1) Послать наугад произвольное информационное когерентное состояние $|\pm\alpha(L)\rangle$. Очевидно, что это приведет к ошибке на приемной стороне. Будут присутствовать отсчеты во временно́м окне 1, когда их не должно быть. Например, если у Алисы $\varphi_A = 0$, у Боба $\varphi_B = 0$, а Ева выбрала $\varphi_E = \pi$ (см. выше формулы (20)–(22)). Среднее число регистрируемых посылок при этом сохранится.

2) Ничего не посылать. Как было сказано выше, это отвечает перепосылке вакуумного состояния. Это также приведет к ошибкам. Например, если Алиса посылала состояние $|+\alpha(L)\rangle$ ($\varphi_A = 0$), а Боб выбрал значение фазы $\varphi_B = \pi$, то отсчета в однофотонном детекторе не должно быть, поскольку на входе детектора во временно́м окне 1 будет состояние

$$\left|\frac{+\alpha(L) - \alpha(L)}{2}\right\rangle_2 = |vac\rangle_2.$$

Перепосыл наугад неправильного состояния $|-\alpha(L)\rangle$ приведет к тому, что на входе детектора будет состояние

$$\left|\frac{-\alpha(L) - \alpha(L)}{2}\right\rangle_2,$$

что приведет к ошибочному отсчету в тех посылках, где его не должно было бы быть.

3) Блокировать посылку целиком — блокировать как когерентное состояние с большим μ_c, так и квазиоднофотонное когерентное состояние с малым μ. В этом случае детектором CD будет зарегистрировано изменение интенсивности когерентного состояния с большим μ_c. По этой же причине Ева не может увеличить интенсивность контрольного когерентного состояния и оставаться при этом незамеченной.

Таким образом, интенсивность когерентного состояния с большим μ_c контролируется классическим образом, поэтому Ева не может изменить истинное информационное квантовое когерентное состояние ни в одной посылке, поскольку это неизбежно приведет к ошибкам на приемной стороне. Важно отметить, что Ева детектируется при любой длине линии связи, соответственно, при любых потерях. Формально это связано с тем, что среднее число фотонов в когерентном состоянии убывает экспоненциально с длиной $\mu(L) \sim 10^{-\delta L/10}$ и ни при каком L в нуль не обращается. Естественно, скорость генерации ключей при этом экспоненциально уменьшается с уменьшением длины, но секретность ключей гарантируется при любом L. Единственным ограничивающим фактором для данного протокола являются только темновые шумы однофотонного детектора.

3.2.1. Устойчивость по отношению к атакам I и II

Криптографическая стойкость данного протокола квантового распределения ключей по отношению к первой атаке с «ослеплением», связанной с разной временно́й чувствительностью лавинных фотодетекторов, практически самоочевидна. Это следует из внутренней структуры самого протокола. Поскольку в данной схеме используется только один информационный фотодетектор, работающий в счетном режиме, «игра» на разных временны́х чувствительностях разных фотодетекторов невозможна. Фактически для Евы невозможно «ослеплять» один из двух лавинных фотодетекторов по своему выбору, так как в данной схеме такой детектор вообще один. Классический контрольный детектор уже работает в линейном классическом режиме и служит для контроля интенсивности реперного когерентного состояния. Он также может быть использован как стороже-

[7] Конкретный функциональный вид вероятности отсчета однофотонного детектора не важен, он может быть любой функцией от доли компонент с ненулевым числом фотонов в когерентном состоянии.

вой детектор (но таковым по протоколу не является) для дополнительного обнаружения атаки с ослеплением, однако и без этой дополнительной функции можно обойтись, поскольку имеется однофотонный детектор для детектирования нарушения интерференции.

Поскольку Ева не может изменить интенсивность реперного когерентного состояния (этот факт сразу обнаруживается классическим детектором), ослепление однофотонного детектора приведет лишь к отсутствию отсчетов на приемной стороне, что эквивалентно разрыву линии связи. Но при этом никогда не будет ситуации, когда Ева знает ключ и не детектируется.

3.3. Релятивистское квантовое распределение ключей для открытого пространства

Приведем протокол релятивистского квантового распределения ключей для открытого пространства. Кроме фундаментальных ограничений квантовой механики протокол использует дополнительные ограничения, диктуемые специальной теорией относительности. Этот протокол предназначен специально для передачи ключей через открытое пространство. Данный протокол обеспечивает секретность ключей и в случае неоднофотонного источника [26], любых потерь в пространстве и не требует априорного знания величины потерь, в отличие от стандартных протоколов для оптоволоконных систем, где затухание должно быть априорно известно и является параметром протокола. Кроме того, тот факт, что показатель преломления в атмосфере в оптическом диапазоне частот слегка отличается от единицы ($\xi = \delta n/n_{vac} = 10^{-4}$) не принципиален для обеспечения секретности ключей, а лишь диктует нижнюю границу протяженности квантового состояния в пространстве-времени Минковского. Причем не требуется заранее знать величины показателя преломления и затухания, которые могут изменяться в течение передачи ключей.

Релятивистский протокол выглядит следующим образом.

1) Легитимные пользователи Алиса и Боб контролируют области пространства, необходимые для приготовления и детектирования квантовых состояний (рис. 6). Расстояние между точками i_A и f_B известно заранее и равно L (рис. 1). Часы синхронизированы[8)].

[8)] Требование синхронизации часов у Алисы и Боба можно отменить из-за двупроходности схемы.

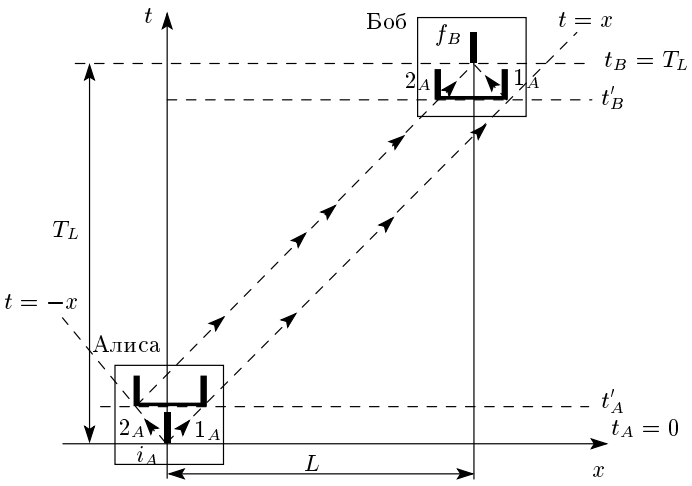

Рис. 6. Схематическая пространственно-временна́я диаграмма работы релятивистского протокола распределения ключей

2) На передающей стороне Алиса готовит в известный момент времени $t_A = 0$ в точке i_A локализованное однофотонное квантовое состояние $|i_A\rangle$. Момент времени $t_A = 0$ считается началом отдельной посылки и всем публично известен, включая подслушивателя.

3) Алиса равновероятно выбирает одно из преобразований (см. рис. 7), переводящее локализованное состояние в момент $t_A = 0$ в одно из протяженных квантовых состояний в момент t'_A. Новое состояние есть суперпозиция пары локализованных состояний

$$|\overline{0}\rangle = \frac{1}{\sqrt{2}}\left(|1_A\rangle + e^{i\varphi}|2_A\rangle\right),$$

$$|\overline{1}\rangle = \frac{1}{\sqrt{2}}\left(|1_A\rangle - e^{-i\varphi}|2_A\rangle\right),$$

отвечающих 0 и 1. Относительная фаза φ является открытым параметром протокола. Состояния $|1_A\rangle$ и $|2_A\rangle$ по форме совпадают с $|i_A\rangle$ и отличаются от него только сдвигом в пространстве-времени по двум ветвям светового конуса, выходящим из точки (i_A, t_A) в точки $(1_A, t'_A)$ и $(2_A, t'_A)$ (см. рис. 6).

4) С момента t'_A протяженные состояния $|\overline{0}\rangle$ либо $|\overline{1}\rangle$ распространяются со скоростью света на приемную сторону Боба. К моменту времени t'_B они оказываются целиком в области пространства, контролируемой Бобом.

5) Боб перед измерением осуществляет унитарное преобразование, преобразующее протяженные квантовые состояния в пространстве-времени в локализованные состояния в точке (f_B, t_B). Исходы с неопределенным результатом отбрасываются. Боб

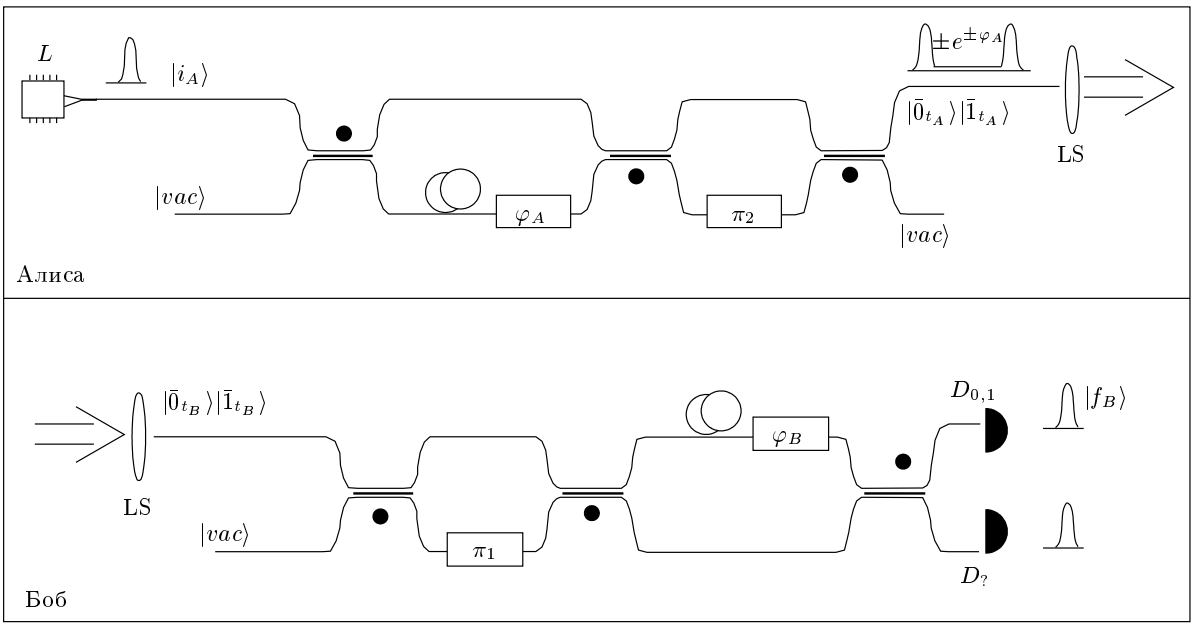

Рис. 7. Принципиальная схема передающей и приемной станций для детерминистического приготовления квантовых состояний для релятивистского протокола распределения ключей. L — лазер, LS — оптические части для вывода и ввода квантовых состояний из открытого пространства в оптоволоконную часть системы, $\varphi_{A,B}$, $\pi_{1,2}$ — фазовые модуляторы (см. [27]), которые активируются в момент прохождения передней и задней «половинок» состояния на соответствующую величину

также отбрасывает все отсчеты, которые задержаны в точке (f_B, t_B) на время, большее $t_B - l/c$ (l — протяженность состояния). Далее часть последовательности раскрывается, оценивается наблюдаемая вероятность ошибки Q_B. Раскрытая часть отбрасывается. Если величина $Q_B < Q_c$ (см. ниже), то ошибки исправляются через открытый канал. Затем для получения финального секретного ключа происходит усиление секретности (privacy amplification) очищенного ключа универсальными хэш-функциями второго порядка.

Выше протокол был приведен для случая однофотонных информационных состояний. Принципиально важно для экспериментальных реализаций, что в качестве информационных состояний могут быть использованы не строго однофотонные когерентные состояния с небольшим средним числом фотонов[9)] (см. детали в [26]).

В случае неоднофотонного источника, когда информационными являются пара неортогональных когерентных состояний, возможно прозрачное подслушивание. При такой атаке Ева отводит часть состояния через асимметричный светоделитель. Ошибок и задержек в этом случае не возникает. Однако из-за неортогональности состояний информация Евы на одну позицию всегда меньше одного бита, в то время как у Боба информация равна одному биту, поскольку исходы с неопределенным результатом отбрасываются (у Евы нет такой возможности). Поэтому длина секретного ключа при такой атаке равна

$$r = \min_{all\ attack} \lim_{N\to\infty} \frac{I(Y^N|X^N) - N_{\chi(\rho_\alpha)}}{N} = 1 - \overline{C}(\rho_\alpha). \quad (24)$$

Здесь

$$\chi(\rho_\alpha) = \overline{C}(\rho_\alpha) = -\frac{1+\varepsilon}{2}\log_2\left(\frac{1+\varepsilon}{2}\right) - \frac{1-\varepsilon}{2}\log_2\left(\frac{1-\varepsilon}{2}\right), \quad (25)$$

$$\varepsilon = |{}_A\langle\overline{0}_\alpha|\overline{1}_\alpha\rangle_A| = \exp\left(-\mu\cos^2\varphi\right),$$

$\overline{C}(\rho_\alpha)$ — классическая пропускная способность квантового канала связи Алиса–Ева, $|\overline{0}_\alpha\rangle$ и $|\overline{1}_\alpha\rangle$ — инфор-

[9)] Формально можно использовать когерентные состояния с любым средним числом фотонов, однако при большом числе фотонов скорость генерации секретного ключа уменьшается как $e^{-\mu}$, но секретность гарантируется при любом среднем числе фотонов.

мационные когерентные состояния, состоящие аналогично однофотонному случаю из двух, разделенных во времени на величину l/c, половинок с относительной фазой φ и средним числом фотонов μ [26].

Отметим, что Боб не должен следить за средним числом долетевших до него посылок.

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 не меньше, чем $l > c(T'_L - T_L)$, где $T_L = (L+l)/c$, $T'_L = (L+l)/c'$. Далее, учитывая, что $c' = c/n$, где n — показатель преломления среды, и $\xi = (n - n_{vac})/n_{vac}$, находим $l > \xi L$. Типичная величина ξ в атмосфере на расстоянии приблизительно до 10 км от поверхности Земли для длин волн $\lambda \approx 0.8$ мкм составляет $\xi \approx 10^{-4}$, выше — уже практически $c' = c$. Ева может скомпенсировать нехватку времени только на данной высоте, заменяя квантовый канал на идеальный (вакуум). Поэтому минимальная протяженность состояния l лимитируется этим условием и равна $l \geq \xi \cdot 10$ 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 точное априорное знание 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, равной 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 не меньшим, чем $T_{c'} - T_c$. Протяженность состояния в вакууме l должна удовлетворять условию $l > c(T_{c'} - T_c)$. В этом случае Еве нужно время, не меньшее, чем $\delta T = l/c$, для доступа к состоянию как целому для измерения и приготовления нового состояния в зависимости от результата измерения. 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 посылка будет отброшена. Состояние должно быть длиннее, чем

$$l > T_{c'} - T_c = L\left(1 - \frac{c}{c'}\right) = \xi L.$$

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). Для атмосферы эта величина составляет десятки километров.

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.

Разумеется, что вещественная и мнимая части показателя преломления связаны между собой соотношением Крамерса–Кронига. Однако в рассуждениях выше учитывалась 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, поскольку 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 вместе две локализованные «половинки», составляющие суперпозицию единого состояния, за время, меньшее, чем l/c, например, пропуская их через среду с групповой скоростью, превышающей скорость света в вакууме [28], также нельзя[10]. Поскольку информация заключена в относительную фазу «половинок» состояния, сведение их вместе за время, меньшее, чем l/c, позволило бы выйти за пределы причинной части светового конуса. Иначе говоря, в противном случае при такой процедуре можно было бы узнать информацию,

[10] 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 еще с 1914 г. из работы Зоммерфельда [29]. На первый взгляд, возникает кажущееся противоречие со специальной теорией относительности, поскольку частично распространено мнение, что групповая скорость и есть скорость распространения информации. Однако при аккуратном рассмотрении [30] скорость распространения информации через такую среду все равно строго равна скорости света в вакууме.

закодированную в протяженное состояние, быстрее скорости света в вакууме.

В заключение данного раздела сделаем небольшое дополнение, важное для понимания протокола. От посылки к посылке фаза параметра α в когерентном состоянии случайна, т. е.

$$\begin{aligned} 0: &\quad |\varphi_0\rangle = |\alpha\rangle_1 \otimes |e^{i\varphi_0}\alpha\rangle_2, \\ 1: &\quad |\varphi_1\rangle = |\alpha\rangle_1 \otimes |e^{i\varphi_1}\alpha\rangle_2, \end{aligned} \tag{26}$$

где, как и выше, $|\alpha\rangle_1$ и $|e^{i\varphi_{0,1}}\alpha\rangle_2$ — локализованные состояния во временных окнах 1 и 2, разделенных временным интервалом l. Фаза θ параметра $\alpha = e^{i\theta}|\alpha|$ случайна, в отличие от относительной фазы, в которую кодируется информация о ключе, $e^{i\varphi_{0,1}}$, поэтому состояния, которые «видит» Ева, равны

$$\begin{aligned} \rho_{0,1} &= \int_0^{2\pi} \frac{d\theta}{2\pi} |\varphi_{0,1}\rangle\langle\varphi_{0,1}| = \\ &= \int_0^{2\pi} \frac{d\theta}{2\pi} \left(|\alpha\rangle_1 \otimes |e^{i\varphi_{0,1}}\alpha\rangle_2\right) \left({}_1\langle\alpha| \otimes {}_2\langle e^{i\varphi_{0,1}}\alpha|\right) = \\ &= \left(e^{-\mu/2} \sum_{n=0}^{\infty} \frac{\mu^n}{n!} |n\rangle_{11}\langle n|\right) \otimes \\ &\quad \otimes \left(e^{-\mu/2} \sum_{n=0}^{\infty} \frac{\mu^n}{n!} |n\rangle_{22}\langle n|\right). \end{aligned} \tag{27}$$

Из формулы (27) следует, что каждое из локализованных когерентных состояний во временны́х окнах не несет никакой информации о ключе. Для получения информации об относительной фазе $\varphi_{0,1}$ необходимо сводить локализованные когерентные состояния вместе (например, как это происходит на приемной стороне Боба), что требует конечного времени и приводит к задержкам.

Факт случайности фазы α в каждой посылке принципиален. Если бы фаза α была неизменна, то Ева могла бы проводить измерения с определенным исходом (unambiguous measurement), в каждой посылке различая состояния, локализованные в окне 2, $|e^{i\varphi_{0,1}}\rangle_2$. В канале с затуханием данные измерения приводили бы к тому, что Ева могла бы знать весь ключ, не создавая задержек и отбрасывая результаты с неопределенным исходом.

3.3.1. Устойчивость по отношению к атакам I и II

Атака с ослеплением фотодетекторов представляет собой атаку прием–перепосыл фальсифицированных состояний. В релятивистской квантовой криптографии, для того чтобы произвести измерения над протяженными в пространстве-времени квантовыми состояниями, необходимо иметь доступ ко всему состоянию как целому. Вероятность результата любого измерения над квантовым состоянием в релятивистской области из-за нормировки квантового состояния не может превышать долю нормировки, набираемую в данной пространственно-временной области. Для получения доступа к конечной пространственно-временной области необходимо конечное время из-за существования предельной скорости распространения сигналов.

Таким образом, атака–прием–перепосыл в релятивистской квантовой криптографии неизбежно приводит к задержкам на приемной стороне независимо от того, какие состояния перепосылаются.

По этой причине атака с ослеплением детекторов неизбежно приведет к ошибкам на приемной стороне, по которым детектируется подслушиватель.

Таким образом, в релятивистском квантовом распределении ключей никогда не будет ситуации, при которой подслушиватель будет знать весь ключ, не произведет ошибок (задержек) и обнаружится.

4. ЗАКЛЮЧЕНИЕ

Как было показано в серии работ [10, 12, 19], все известные базовые протоколы квантового распределения ключей уязвимы по отношению к атакам с ослеплением лавинных фотодетекторов. При такой атаке подслушиватель знает весь ключ и не производит ошибок (не изменяет наблюдаемые статистики фотоотсчетов) на приемной стороне. Уязвимость систем была продемонстрирована на ряде конкретных квантовых криптографических систем, в том числе и коммерческих, которые реализуют различные базовые протоколы [10, 12, 19].

Данная ситуация неприятна тем, что различные технические ухищрения, которые позволяют детектировать вторжения в линию связи, не являются фундаментальными ограничениями для действий подслушивателя. На любые технические усовершенствования подслушиватель может выдвинуть свои технические контрусовершенствования. Такая ситуация неприемлема для квантовой криптографии, которая принципиально должна гарантировать безусловную секретность ключей, основанную на фундаментальных запретах квантовой механики, а не на технических ограничениях подслушивателя.

Приведенные выше три новых протокола кван-

тового распределения ключей являются устойчивыми по отношению к различным модификациям атак с ослеплением фотодетекторов, причем даже в идеальном варианте для подслушивателя, который может изменить схему управления смещением лавинного фотодетектора и величину порога дискриминации. Данные протоколы также гарантируют секретное распределение ключей и при всех других атаках.

Стойкость упомянутых протоколов гарантируется самой внутренней структурой протоколов, а не дополнительными техническими ухищрениями, которые позволили бы детектировать атаки с ослеплением детекторов.

Таким образом, утверждение, высказанное в упомянутых работах [10, 12, 19] о нестойкости квантовой криптографии как таковой, является сильно преувеличенным.

Выражаю благодарность коллегам по Академии криптографии Российской Федерации за постоянную поддержку. Работа выполнена при частичной финансовой поддержке РФФИ (грант № 11-02-00455).

ЛИТЕРАТУРА

1. W. K. Wooters and W. H. Zurek, Nature **299**, 802 (1982).
2. S. Wiesner, SIGACT News **15**, 78 (1983).
3. C. H. Bennett and G. Brassard, Proc. of IEEE Int. Conf. on Comput. Sys. and Sign. Proces., Bangalore, India (1984), p. 175.
4. C. H. Bennett, Phys. Rev. Lett. **68**, 3121 (1992).
5. N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, arXiv:quant-ph/0101098; Rev. Mod. Phys. **74**, 145 (2002).
6. V. Scarani, H. Bechmann-Pasquinucci, N. J. Cerf, M. Dusek, N. Lütkenhaus, and M. Peev, Rev. Mod. Phys. **81**, 1301 (2009).
7. G. Brassard, N. Lütkenhaus, T. Mor, and B. Sanders, Phys. Rev. Lett. **85**, 1330 (2000).
8. D. Dieks, Phys. Lett. A **126**, 303 (1988); I. D. Ivanovic, Phys. Lett. A **123**, 257 (1987); A. Peres, Phys. Lett. A **128**, 19 (1988); G. Jaeger and A. Shimony, Phys. Lett. A **197**, 83 (1995).
9. A. Chefles, Phys. Lett. A **239**, 339 (1998); P. Raynal, arXiv:quant-ph/0611133.
10. L. Lydersen, C. Wiechers, C. Wittmann, D. Elser, J. Skaar, and V. Makarov, Nature Photonics **4**, 686 (2010).
11. А. В. Корольков, К. Г. Катамадзе, С. П. Кулик, С. Н. Молотков, ЖЭТФ **137**, 637 (2010).
12. V. Makarov, A. Anisimov, and S. Sauge, arXiv: quant-ph/0809.3408; V. Makarov and J. Skaar, arXiv: quant-ph/0702262.
13. V. Scarani, A.Acín, G. Ribordy, and N. Gisin, Phys. Rev. Lett. **92**, 057901-1 (2004); A. Acín, N. Gisin, and V. Scarani, arXiv:quant-ph/0302037.
14. D. Bruss, arXiv:quant-ph/9805019; Go Kato and Kiyoshi Tamaki, arXiv:quant-ph/1008.4663; Hoi-Kwong Lo, arXiv:quant-ph/0102.138.
15. K. Inoue, E. Waks, and Y. Yamamoto, Phys. Rev. Lett. **89**, 037902 (2002); E. Waks, H. Takesue, and Y. Yamamoto, arXiv:quant-ph/0508112; Kai Wen, K. Tamaki, and Y. Yamamoto, arXiv: quant-ph/0806.2864; D. Dodson et al., arXiv: quant-ph/0905.4325.
16. N. Gisin, G. Ribordy, H. Zbinden, D. Stucki, N. Brunner, and V. Scarani, arXiv:quant-ph/0411022; D. Stucki, N. Brunner, N. Gisin, V. Scarani, and H. Zbinden, arXiv:quant-ph/0506097.
17. A. Ekert, Phys. Rev. Lett. **67**, 661 (1991).
18. Won-Young Hwang, Phys. Rev. Lett. **95**, 057901-1 (2003).
19. L. Lydersen, C. Wiechers, C. Wittmann, D. Elser, J. Skaar, and V. Makarov, arXiv:quant-ph/1009.2663; S. Sauge, L. Lydersen, A. Anisimov, J. Skaar, and V. Makarov, arXiv:quant-ph/0809.3408; C. Wiechers, L. Lydersen, C. Wittmann, D. Elser, J. Skaar, Ch. Marquardt, V. Makarov, and G. Leuchs, New J. Phys. **13**, 013043 (2011); I. Gerhardt, Qin Liu, A. Lamas-Linares, J. Skaar, C. Kurtsiefer, and V. Makarov, arXiv:quant-ph/1011.0105; L. Lydersen, J. Skaar, and V. Makarov, arXiv:quant-ph/1012.4366; V. Makarov, New J. Phys. **11**, 065003 (2009); V. Makarov, arXiv:quant-ph/0707.3987; V. Makarov, A. Anisimov, and J. Skaar, arXiv:quant-ph/0511032.
20. Z. L. Yuan, J. F. Dynes, and A. J. Shields, Nature Photonics **4**, 800 (2010); L. Lydersen, C. Wiechers, C. Wittmann, D. Elser, J. Skaar, and V. Makarov, Nature Photonics **4**, 801 (2010).
21. С. Н. Молотков, С. П. Кулик, А. И. Климов, *Устройство для регистрации слабых оптических импульсов*, Патент РФ № 2339919, приоритет от 15.06.2007.

22. С. Н. Молотков, С. П. Кулик, *Способ кодирования и передачи ключей*, заявка на Патент РФ № 2010130961 от 23.07.2010; С. Н. Молотков, ЖЭТФ **133**, 5 (2008): Д. А. Кронберг, С. Н. Молотков, ЖЭТФ **136**, 650 (2009).

23. C. H. Bennett, G. Brassard, C. Crépeau, and U. Maurer, IEEE Trans. Inf. Theory **41**, 1915 (1995).

24. 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).]

25. L. J. Wang, X. Y. Zou, and L. Mandel, Phys. Rev. A **44**, 4614 (1991).

26. С. Н. Молотков, С. П. Кулик, *Способ кодирования и передачи ключей*, Патент РФ № 2325039 от 06.06.2006; С. Н. Молотков, ЖЭТФ **139**, 429 (2011).

27. С. Н. Молотков, Письма в ЖЭТФ **91**, 51 (2010).

28. C. G. B. Garrett and D. E. McCumber, Phys. Rev. A **1**, 305 (1970); S. Chu and S. Wong, Phys. Rev. Lett. **48**, 738 (1982); A. M. Akulshin, S. Barreiro, and A. Lezama, Phys. Rev. Lett. **83**, 4277 (1999); D. L. Fisher and T. Tajima, Phys. Rev. Lett. **71** 4338 (1993); R. Y. Chiao, Phys. Rev. A **48**, R34 (1993); E. L. Bolda, R. Y. Chiao, and J. C. Garrison, Phys. Rev. A **48**, 3890 (1993); A. M. Steinberg and R. Y. Chiao, Phys. Rev. A **49** 2970 (1994); V. W. Mitchell and R. Y. Chiao, Amer. J. Phys. **66**, 14 (1998); L. J. Wang, A. Kuzmich, and A. Dogariu, Nature **406**, 277 (2000); M. D. Stenner, D. J. Gauthier, and M. A. Neifeld, Nature **425**, 695 (2003); K. Kim, H. S. Moon, Ch. Lee, S. K. Kim, and J. B. Kim, Phys. Rev. A **68**, 013810 (2003).

29. A. Sommerfeld, *in* L. Brillouin, *Wave Propagation and Group Velocity*, Acad. Press, New York, London (1960).

30. С. Н. Молотков, Письма в ЖЭТФ **91**, 762 (2010).