ЖЭТФ, 2014, том 145, вып. 1, стр. 5–16

ОБ АТАКЕ СО СВЕТОДЕЛИТЕЛЕМ И МЯГКОЙ ФИЛЬТРАЦИИ КОГЕРЕНТНЫХ СОСТОЯНИЙ В ДИФФЕРЕНЦИАЛЬНО-ФАЗОВОЙ КВАНТОВОЙ КРИПТОГРАФИИ

Д. А. Кронберг [a], ***С. Н. Молотков*** [a,b*]

[a] *Московский государственный университет им. М. В. Ломоносова*
119991, Москва, Россия

[b] *Институт физики твердого тела Российской академии наук*
142432, Черноголовка, Московская обл., Россия

Поступила в редакцию 10 июня 2013 г.

Предложена комбинированная атака на протокол квантового распределения ключей с дифференциально-фазовым кодированием. Получены оценки для длины линии связи, до которой гарантируется секретное распределение ключей.

DOI: 10.7868/S0044451014010015

1. ВВЕДЕНИЕ

Центральной задачей криптографии является проблема распределения ключей. В рамках законов классической физики не существует гарантии секретности ключей при их распределении, основанной на фундаментальных законах природы. Поэтому протоколы и системы распределения ключей в классической криптографии основаны либо на предположениях о технических ограничениях подслушивателя, либо на недоказанной вычислительной сложности алгоритмов. При этом физическая природа носителя информации, с которым ассоциированы биты ключа, несущественна.

В квантовой криптографии — квантовом распределении ключей — носителем ключевой информации является состояние квантовой системы. Детектирование попыток подслушивания и гарантии секретности ключей в квантовой криптографии гарантируются фундаментальными законами квантовой механики. Поэтому секретность ключей в квантовой криптографии называют безусловной. Отметим, что секретность ключей в любой системе квантовой криптографии гарантируется, если наблюдаемая ошибка не превышает некоторой критической величины, являющейся фундаментальной константой протокола.

Основная задача теории состоит в вычислении длины секретного ключа, который может быть получен при заданных параметрах системы и наблюдаемой вероятности величины ошибки на приемной стороне. Поскольку в квантовой криптографии считается, что квантовый канал не контролируется легитимными пользователями, свои выводы о присутствии подслушивателя в канале связи они делают исходя из наблюдаемой ошибки на приемной стороне. Для этого часть последовательности (значения битов, отвечающие переданным квантовым состояниям) раскрывается через открытый и доступный для прослушивания классический канал связи[1)]. Затем раскрытая часть последовательности отбрасывается. Для раскрытой части вычисляется доля несовпадений, что дает оценку вероятности ошибки, которая в асимптотическом пределе бесконечно длинных последовательностей совпадает с вероятностью ошибки.

В асимптотическом пределе длинных последовательностей вероятности ошибки в нераскрытой и раскрытой частях последовательности совпадают. Чем больше наблюдаемая ошибка, тем больше

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

[1)] Напомним, что классический канал является открытым, но требует аутентичности передаваемых сообщений.

информации может получить подслушиватель при вторжении в квантовый канал связи. Собственно, ошибки и возникают в результате возмущения передаваемых состояний подслушивателем.

Ошибки могут возникнуть как от подслушивателя, так и от собственных шумов аппаратуры. Поскольку принципиально нельзя отличить собственные ошибки аппаратуры от ошибок, привносимых подслушивателем, все ошибки приходится списывать на действия подслушивателя.

Подслушиватель, вторгаясь в канал связи, получает частичную информацию о передаваемой последовательности и при этом производит ошибки на приемной стороне. Для исправления ошибок легитимные пользователи должны передать через открытый классический канал связи в пересчете на посылку не менее $h(Q)$ (Q — вероятность ошибки, $h(Q)$ — бинарная энтропийная функция Шеннона, см. ниже) битов информации, которая доступна подслушивателю. Передавая такое количество информации, в асимптотическом пределе длинных последовательностей легитимные пользователи исправляют ошибки с вероятностью единица, т. е. с достоверностью.

Кроме этой информации подслушиватель имеет информацию о ключе, полученную из квантового канала связи — χ_{QC}. Данная величина зависит от протокола квантового распределения ключей, среднего числа фотонов в ослабленном лазерном излучении, потерь в канале связи. Величина χ_{QC} является фундаментальной верхней границей этой информации, которую может извлечь подслушиватель из передаваемых квантовых состояний, производя при этом ошибку Q. Длина секретного ключа в пересчете на одну посылку есть

$$l_{secr} \leq 1 - h(Q) - \chi_{QC}.$$

При некотором критическом значении ошибки Q_c длина секретного ключа обращается в нуль, $l_{secr} = 0$, и соответственно, $1-h(Q_c) = \chi_{QC}$. Если ошибка превышает критическое значение, то гарантировать секретность передаваемых ключей невозможно.

Несовершенство существующей элементной базы приводит к тому, что секретность ключей в оптоволоконных системах квантовой криптографии и системах, работающих через открытое пространство, можно гарантировать только в том случае, если длина канала связи не превышает некоторой критической величины. Главным техническим ограничением являются следующие факторы: темновые шумы лавинных однофотонных фотодетекторов, потери в канале связи и квазиоднофотонность источника информационных квантовых состояний. Сильно ослабленное излучение лазера (когерентное состояние) даже в пределе малого среднего числа фотонов является квазиоднофотонным и имеет пуассоновскую статистику по числу заполнения фотонов, поэтому всегда существует вероятность появления в канале двух, трех и более фотонов. Квазиоднофотонность когерентного состояния совместно с потерями в линии связи, если они превышают некоторую величину, приводят к возможности так называемых измерений с определенным исходом (unambiguous), которые позволяют подслушивателю, начиная с некоторой критической величины потерь, знать весь ключ, не производить ошибок на приемной стороне и остаться недетектируемым (см. обзор [1] и ссылки в нем).

При достаточно большой длине линии связи все бóльшая часть состояний не достигает приемной стороны, поэтому в основном происходит регистрация темновых шумов, что приводит к превышению наблюдаемой ошибки над критической. Однако даже при идеальных фотодетекторах без темновых шумов остаются ограничения на длину линии связи для секретной передачи ключей при неоднофотонном источнике и потерях в канале связи.

Для решения упомянутых проблем был предложен ряд протоколов квантовой криптографии [2]. Для открытого пространства проблема неоднофотонного источника и произвольных потерь в канале решается использованием дополнительных ограничений, диктуемых специальной теорией относительности [3]. Однако для волоконно-оптических систем из-за существенного отличия скорости распространения в волокне (примерно в полтора раза) от предельной скорости света в вакууме это оказывается неприемлемым.

В работе [2] был предложен протокол, который, возможно, обеспечивает секретность передачи ключей при больших длинах линии связи (при идеальных фотодетекторах). Этот протокол был назван дифференциально-фазовым. Главное отличие данного протокола от всех нерелятивистских протоколов квантового распределения ключей состоит в том, что кодирование в нем является распределенным. Если в обычных протоколах каждая посылка независима от других, то и каждый бит ключа привязан к отдельной посылке. Поэтому достаточно провести подслушивание в каждой посылке и сделать затем коллективные измерения. Такая стратегия действий перехватчика получила название коллективной атаки.

В протоколе DPS (Differential Phase Shift) ин-

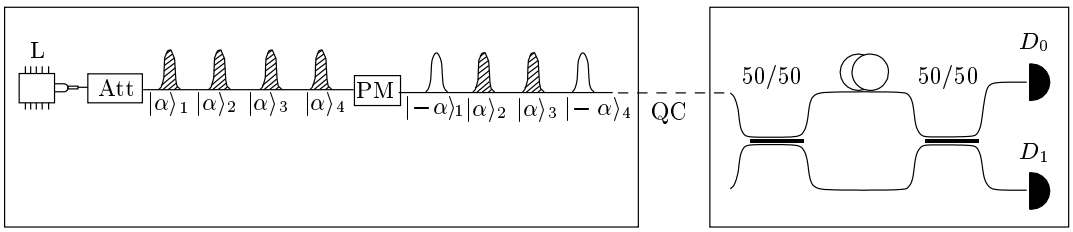

Рис. 1. Принципиальная схема оптоволоконной системы когерентной квантовой криптографии. L — лазер, работающий в режиме синхронизации мод (mode-locked), Att — управляемый аттенюатор, PM — фазовый модулятор, $D_{0,1}$ — информационные детекторы, QC — оптоволоконный квантовый канал связи

формация о ключе кодируется в относительную разность фаз когерентных состояний в каждой соседней посылке. Поэтому наиболее общая атака не может быть устроена в виде атаки на отдельные посылки.

В отличие от других протоколов, где получены доказательства секретности, для данного протокола существуют лишь частичные результаты. Например, даже неизвестны результаты по прозрачной атаке, которая дает границу для ошибки даже в случае идеального канала связи.

Потери в канале связи, которые неизбежны, открывают возможности для новых атак. Основная мотивация данной работы состоит в получении оценок критической длины линии связи, до которой гарантируется секретное распределение ключей, с учетом конкретных требований к величине критической ошибки. Рассмотрен ряд атак, которые ранее не исследовались.

2. ДИФФЕРЕНЦИАЛЬНО-ФАЗОВЫЙ ПРОТОКОЛ РАСПРЕДЕЛЕНИЯ КЛЮЧЕЙ (DPS)

Дифференциально-фазовая система квантовой криптографии (рис. 1) внешне достаточно проста и во многом близка к классическим оптоволоконным системам передачи данных. Для самодостаточности приведем краткое описание протокола, необходимое для дальнейшего. На передающей стороне используется лазер, работающий в режиме синхронизации мод (mode-locked) и выдающий серии сфазированных импульсов. Быстрый аттенюатор формирует последовательность ослабленных импульсов (когерентных состояний $|\alpha\rangle$) одинаковой интенсивности, разделенных одинаковым временным интервалом. Все импульсы в разных посылках когерентны между собой, т. е. частотная «набивка» имеет одинаковую фазу. После аттенюатора световые импульсы поступают на фазовый модулятор, который либо изменяет фазу $|\alpha\rangle \to |-\alpha\rangle$, либо оставляет ее неизменной в зависимости от того, какое состояние передается — 0 или 1.

При малом среднем числе фотонов $\mu = |\alpha|^2 \leq 1$ когерентные состояния существенно неортогональны, что гарантирует их достоверную неразличимость. Принципиально важно для протокола, что не существует измерений, которые с вероятностью единица позволяют различать данные квантовые состояния.

На приемной стороне состояния через симметричный светоделитель поступают на интерферометр Маха–Цандера. Из-за когерентности непустых импульсов в разных посылках при прохождении двух соседних импульсов через интерферометр Маха–Цандера с разностью длин плеч, равной расстоянию между импульсами, на одном из детекторов D_0 в соответствующем временном окне наблюдается конструктивная интерференция (отсчет в детекторе D_0), а во втором D_1 — деструктивная интерференция (отсчеты отсутствуют). Вероятности отсчетов в двух детекторах соответственно равны $|\alpha_i \pm \alpha_{i+1}|^2/4$ и зависят от разности фаз состояний в соседних посылках. В отсутствие подслушивателя должна наблюдаться идеальная видность V интерференционной картины, $V = 100\,\%$.

Детектирование подслушивателя происходит по изменению видности интерференционной картины V — вероятности ($q = (1 - V)/2$) ошибки в информационной последовательности. У подслушивателя нет возможности достоверно отличить информационные состояния, поэтому любое вторжение в канал связи приведет к возникновению ошибки на приемной стороне.

3. СТОЙКОСТЬ ПРОТОКОЛА ПРИ АТАКЕ ПРИЕМ–ПЕРЕПОСЫЛ

Прием–перепосыл является концептуально самым простым методом атаки на протоколы квантового распределения ключей. В данном разделе будет получена зависимость значения критической ошибки протокола DPS от интенсивности используемых состояний при такой стратегии подслушивания. Результаты понадобятся в дальнейшем при рассмотрении новых атак на протокол.

При стратегии прием–перепосыл Ева в каждой посылке производит попытку различения состояний $|+\alpha\rangle$ и $|-\alpha\rangle$. Ошибка, возникающая при различении пары неортогональных состояний, равна [4]

$$q = \frac{1-\sqrt{1-\varepsilon^2}}{2}, \quad \varepsilon = |\langle +\alpha| - \alpha\rangle|. \tag{1}$$

Необходимо связать информацию подслушивателя с возмущением квантовых состояний. Для описания искажения состояний удобно воспользоваться представлением Стайнспринга [4]. Любая модификация квантовых состояний может быть представлена как совместная унитарная эволюция исходного квантового и вспомогательного состояний [1]. Применительно к случаю измерения одного состояния имеем

$$\begin{aligned} |\alpha\rangle &\to \sqrt{1-q}|\alpha\rangle|e_0\rangle + \sqrt{q}|-\alpha\rangle|e_1\rangle = \widetilde{|\alpha\rangle}, \\ |-\alpha\rangle &\to \sqrt{q}|\alpha\rangle|e_0\rangle + \sqrt{1-q}|-\alpha\rangle|e_1\rangle = \widetilde{|-\alpha\rangle}, \end{aligned} \tag{2}$$

где $|e_0\rangle$ и $|e_1\rangle$ — вспомогательные взаимно ортогональные состояния подслушивателя, которые соответствуют двум возможным исходам при измерении (различении) одного из двух исходных состояний. Из формулы (2) видно, что условия унитарности эволюции $\widetilde{\langle -\alpha|}\widetilde{|\alpha\rangle} = \langle -\alpha|\alpha\rangle = \varepsilon$ выполняются при

$$q = \frac{1-\sqrt{1-\varepsilon^2}}{2},$$

что совпадает с вероятностью правильного различения состояний (1).

Учтем теперь тот факт, что в более общем случае атаки прием–перепосыл подслушиватель атакует лишь долю посылок p из их полного числа. Далее удобно использовать дополнительные вспомогательные взаимно ортогональные квантовые состояния $|e_i\rangle$ и $|f\rangle$. В результате эволюция исходных состояний может быть представлена в виде

$$\begin{aligned} |\alpha\rangle &\to \sqrt{p(1-q)}|\alpha\rangle|e_0\rangle + \sqrt{pq}|-\alpha\rangle|e_1\rangle + \\ &\quad + \sqrt{1-p}|\alpha\rangle|f\rangle = \widetilde{|\alpha\rangle}, \\ |-\alpha\rangle &\to \sqrt{pq}|\alpha\rangle|e_0\rangle + \sqrt{p(1-q)}|-\alpha\rangle|e_1\rangle + \\ &\quad + \sqrt{1-p}|-\alpha\rangle|f\rangle = \widetilde{|-\alpha\rangle}. \end{aligned} \tag{3}$$

Данная атака вносит ошибку величиной pq в исходную последовательность, и состояния Алисы и Боба описываются операторами плотности

$$\begin{aligned} \rho_+^{AB} &= (1-pq)|\alpha\rangle\langle\alpha| + pq|-\alpha\rangle\langle -\alpha|, \\ \rho_-^{AB} &= pq|\alpha\rangle\langle\alpha| + (1-pq)|-\alpha\rangle\langle -\alpha|. \end{aligned} \tag{4}$$

При атаке методом приема–перепосыла Ева совершает измерения в ортонормированном базисе $\{|e_0\rangle, |e_1\rangle, |f\rangle\}$, поэтому после измерения ее состояния описываются диагональными в этом базисе операторами плотности

$$\rho_+^E = p(1-q)|e_0\rangle\langle e_0| + pq|e_1\rangle\langle e_1| + (1-p)|f\rangle\langle f|,$$

$$\rho_-^E = pq|e_0\rangle\langle e_0| + p(1-q)|e_1\rangle\langle e_1| + (1-p)|f\rangle\langle f|.$$

Состояния, которые используются легитимными пользователями для передачи ключа, представляют собой кортежи состояний ρ_+ и ρ_- длиной N, причем измерения на приемной стороне устроены таким образом, что учитывают только разность фаз состояний в соседних посылках. Из N состояний возникает битовая строка длиной $N-1$. Например, битовой строке, состоящей из нулей, соответствует состояние

$$\rho_{00\ldots0} = \frac{1}{2}\left((\rho_+^E)^{\otimes N} + (\rho_-^E)^{\otimes N}\right).$$

Взаимная информация между Алисой и Евой ограничена сверху величиной Холево [4], которая, по сути, равна классической пропускной способности квантового канала между Алисой и Евой, и дается выражением [4]

$$\chi_{AE} = H\left(\frac{1}{2^N}\sum_i \rho_i\right) - H\left(\frac{1}{2}\left((\rho_+^E)^{\otimes N} + (\rho_-^E)^{\otimes N}\right)\right).$$

Первое слагаемое согласно правилу аддитивности равно

$$NH\left(\frac{1}{2}(\rho_+^E + \rho_-^E)\right),$$

второе можно оценить, исходя из того, что классическая пропускная способность квантового канала с двумя выходными информационными состояниями не может превосходить одного бита на посылку. Имеем

$$\begin{aligned} &\chi\left(\left\{\frac{1}{2}, \frac{1}{2}\right\}, (\rho_+^E)^{\otimes N}, (\rho_-^E)^{\otimes N}\right) = \\ &= H\left(\frac{1}{2}\left((\rho_+^E)^{\otimes N} + (\rho_-^E)^{\otimes N}\right)\right) - H\left((\rho_+^E)^{\otimes N}\right) \le 1, \end{aligned}$$

откуда следует

$$H\left(\frac{1}{2}\left((\rho_+^E)^{\otimes N} + (\rho_-^E)^{\otimes N}\right)\right) \le 1 + NH(\rho_+^E),$$

что дает оценку для пропускной способности канала между Алисой и Евой в пересчете на одну посылку:

$$I_{AE} \geq \frac{1}{N-1}\left[NH\left(\frac{1}{2}(\rho_+^E+\rho_-^E)\right) - 1 - NH(\rho_+^E)\right], \quad (5)$$

которая окончательно принимает вид

$$I_{AE} \geq \frac{Np(1-h(q))-1}{N-1}. \quad (6)$$

Величина q выражается по формуле (1) через скалярное произведение между состояниями, а параметр p однозначно связан с наблюдаемой на приемной стороне ошибкой Q,

$$Q = 2pq(1-pq).$$

Таким образом, выражение (6) и условие

$$I_{AE} \geq I_{AB} = 1 - h(Q)$$

определяют величину критической ошибки протокола при использовании приема–перепосыла, до которой возможно секретное распределение ключей.

4. КРИТИЧЕСКАЯ ОШИБКА ПРОТОКОЛА DPS ПРИ АТАКЕ С ИСПОЛЬЗОВАНИЕМ СВЕТОДЕЛИТЕЛЯ

Данная атака (Beam Splitting Attack) возможна в канале с потерями и сводится к следующему. Когерентные состояния на светоделителе преобразуются самоподобно, поэтому подслушиватель, используя асимметричный светоделитель, может отвести часть когерентного состояния для себя, а оставшуюся направить через канал с меньшими потерями (в пределе вообще без потерь) на приемную сторону. При такой атаке никаких ошибок на приемной стороне не возникает, и подслушиватель не детектируется. Цель данного раздела — определить критическую ошибку на приемной стороне, которая возникает не из-за подслушивателя, а из-за неидеальностей аппаратуры (темновых шумов, неточности балансировки интерферометра и т. д.), и до которой при данных исходных потерях в линии связи и среднего числа фотонов в когерентном состоянии возможно секретное распределение ключей.

Пусть каждое из передаваемых состояний в кортеже имеет среднее число фотонов μ. После прохождения через оптоволоконную линию связи длиной L эта интенсивность уменьшается до величины $\mu 10^{-\delta L/10}$, где типичные потери на единицу длины для одномодового волокна SMF-28 равны $\delta = 0.2$ Дб/км. Подслушиватель имеет возможность заменить линию связи на идеальный канал без потерь и использовать асимметричный светоделитель, делящий исходное состояние на состояния со средним числом фотонов $\mu 10^{-\alpha L/10}$, которое направляется на приемную сторону, при этом состояние с числом фотонов

$$\mu' = \mu(1 - 10^{-\alpha L/10})$$

остается в распоряжении подслушивателя.

Вычислим классическую информацию, которую подслушиватель может получить из передаваемого кортежа. Пусть длина битовой строки равна $N-1$, для ее передачи необходимо использовать кортеж когерентных состояний длиной N. Информационный бит на приемной стороне зависит только от разности фаз состояния в двух соседних посылках, поэтому кортежи, получаемые друг из друга сменой знака фазы в каждой посылке, отвечают одной и той же конечной битовой строке. Таким образом, подслушивателю надо различать не отдельные кортежи, а пары кортежей, отличающиеся сменой знака фазы. Например, для битовой строки, целиком состоящей из нулей, подслушиватель должен отличать матрицу плотности

$$\rho_{\tilde{0}} = \frac{1}{2}\left(|\sqrt{\mu'}\rangle\langle\sqrt{\mu'}|^{\otimes N} + |-\sqrt{\mu'}\rangle\langle-\sqrt{\mu'}|^{\otimes N}\right) \quad (7)$$

от других.

Классическая информация, которую можно получить из ансамбля квантовых состояний, ограничена сверху величиной Холево. Полное число состояний в ансамбле всевозможных состояний равно $2^{(N-1)}$ и соответствующая матрица плотности записывается как

$$\frac{1}{2^N}\sum_i \rho_{\tilde{i}}. \quad (8)$$

Матрица плотности есть смесь всех чистых состояний, составленных из кортежей длиной N, со всевозможными комбинациями $|\sqrt{\mu'}\rangle$ и $|-\sqrt{\mu'}\rangle$ внутри. Оператор (8) является N-й тензорной степенью

$$\frac{1}{2}\left(|\sqrt{\mu'}\rangle\langle\sqrt{\mu'}| + |-\sqrt{\mu'}\rangle\langle-\sqrt{\mu'}|\right), \quad (9)$$

а значит, его энтропия фон Неймана равна $Nh((1-\varepsilon)/2)$, где $h(x)$ — бинарная энтропийная функция Шеннона, и

$$\varepsilon = \langle\sqrt{\mu'}|-\sqrt{\mu'}\rangle = e^{-2\mu'}.$$

Далее, с учетом того, что средние значения энтропий фон Неймана всех возможных состояний вида (7) совпадают, вместо усредненной суммы можно записать энтропию одного из элементов, которая

равна $h((1-\varepsilon^N)/2)$. Окончательно информация подслушивателя в пересчете на одну позицию становится равной

$$I_{AE}^{BS} = \frac{N}{N-1} h\left(\frac{1-e^{-2\mu'}}{2}\right) - \\ - \frac{1}{N-1} h\left(\frac{1-e^{-2N\mu'}}{2}\right). \quad (10)$$

Несложно видеть, что при $N \to \infty$ информация подслушивателя стремится к энтропии обычного кортежа когерентных состояний. В этом состоит причина того, что рассматриваемая атака более эффективна при больших длинах используемых кортежей, в то время как, например, атака с использованием измерений с определенным исходом, напротив, более эффективна при относительно коротких кортежах.

При длине линии связи, равной L, подслушиватель имеет дело с состояниями интенсивности

$$\mu' = (1 - 10^{-\alpha L/10})\mu.$$

Информация, извлекаемая из этих состояний, всегда меньше единицы в пересчете на посылку. Информация на приемной стороне в отсутствие ошибок и после отбрасывания пустых исходов равна единице. Подслушиватель может скомпенсировать этот дефицит информации, внося ошибку Q в канал связи. Схема внесения ошибки проста. Внесение одной ошибки в итоговую битовую строку соответствует одной смене режима работы фазового модулятора (всего режима два — либо состояние остается без изменения, либо его фаза меняется на противоположную). В самом деле, одна смена фазы означает, что все последующие позиции передаваемого кортежа изменят свой знак. Смена знака двух следующих друг за другом состояний не дает ошибки, поэтому единственная ошибка произойдет в позиции, соответствующей непосредственной смене фаз. Таким образом, для внесения нужной величины ошибки подслушивателю следует с вероятностью Q сменить фазу при прохождении каждого из состояний кортежа. Вероятность ошибки, при которой информации подслушивателя и легитимных пользователей сравниваются, определяется уравнением

$$I_{AB} = 1 - h(Q) = I_{AE}^{BS}. \quad (11)$$

Обнаружив ошибки, легитимные пользователи вынуждены исправлять их через открытый классический канал связи, при этом необходимо обменяться $Nh(Q)$ битами — это как раз то количество информации, которого не хватало подслушивателю до полного знания ключа. Формула (11) понадобится ниже при конструировании более эффективной комбинированной атаки.

5. ОБЪЕДИНЕНИЕ АТАКИ ПРИЕМ–ПЕРЕПОСЫЛ С ОТВОДОМ ЧАСТИ СОСТОЯНИЙ

Описанную атаку можно модифицировать. С точки зрения подслушивателя выгоднее не просто искусственно добавлять помехи в канал, не получая при этом непосредственно информации о ключе, а попытаться получить информацию из отведенного состояния, применяя атаку прием–перепосыл и подбирая параметр p таким образом, чтобы внесенная ошибка давала нужное значение.

Рассмотрим комбинацию атак в тех же обозначениях, которые использовались при анализе стойкости против атаки прием–перепосыл. Пусть потери в канале связи позволяют подслушивателю отвести от каждой посылки состояние со средним числом фотонов μ_E, на приемную сторону направляются состояния со средним числом фотонов $\mu_B = \mu - \mu_E$. Далее Ева выбирает параметр m между нулем и единицей, затем отводит состояния с числом фотонов $m\mu_E$, после чего применяет атаку прием–перепосыл и, наконец, отводит оставшиеся состояния интенсивности $(1-m)\mu_E$.

Представление Стайнспринга для описанных действий подслушивателя выглядит следующим образом. Первый отвод части состояний преобразует их по правилу

$$|\sqrt{\mu}\rangle \to |\sqrt{\mu_B + (1-m)\mu_E}\rangle|\sqrt{m\mu_E}\rangle,$$

$$|-\sqrt{\mu}\rangle \to |-\sqrt{\mu_B + (1-m)\mu_E}\rangle|-\sqrt{m\mu_E}\rangle.$$

Последующая атака прием–перепосыл с параметром p дает

$$\begin{aligned} |\sqrt{\mu}\rangle \to (&\sqrt{p(1-q)}|\sqrt{\mu_B + (1-m)\mu_E}\rangle|e_0\rangle + \\ &+ \sqrt{pq}|-\sqrt{\mu_B + (1-m)\mu_E}\rangle|e_1\rangle + \\ &+ \sqrt{1-p}|\sqrt{\mu_B + (1-m)\mu_E}\rangle|f\rangle) \otimes |\sqrt{m\mu_E}\rangle, \\ |-\sqrt{\mu}\rangle \to (&\sqrt{pq}|\sqrt{\mu_B + (1-m)\mu_E}\rangle|e_0\rangle + \\ &+ \sqrt{p(1-q)}|-\sqrt{\mu_B + (1-m)\mu_E}\rangle|e_1\rangle + \\ &+ \sqrt{1-p}|-\sqrt{\mu_B + (1-m)\mu_E}\rangle|f\rangle) \otimes \\ &\otimes |-\sqrt{m\mu_E}\rangle, \end{aligned} \quad (12)$$

где q — величина вносимой ошибки, равная

$$q = \frac{1}{2}\left(1 - \sqrt{1 - \exp\{-4(\mu_B + (1-m)\mu_E)\}}\right). \quad (13)$$

После второго применения светоделителя получаем

$$|\sqrt{\mu}\rangle \to (\sqrt{p(1-q)}|\sqrt{\mu_B}\rangle|\sqrt{(1-m)\mu_E}\rangle|e_0\rangle + \\ + \sqrt{pq}|-\sqrt{\mu_B}\rangle|-\sqrt{(1-m)\mu_E}\rangle|e_1\rangle + \\ + \sqrt{1-p}|\sqrt{\mu_B}\rangle|\sqrt{(1-m)\mu_E}\rangle|f\rangle) \otimes |\sqrt{m\mu_E}\rangle, \quad (14)$$

$$|-\sqrt{\mu}\rangle \to (\sqrt{pq}|\sqrt{\mu_B}\rangle|\sqrt{(1-m)\mu_E}\rangle|e_0\rangle + \\ + \sqrt{p(1-q)}|-\sqrt{\mu_B}\rangle|-\sqrt{(1-m)\mu_E}\rangle|e_1\rangle + \\ + \sqrt{1-p}|-\sqrt{\mu_B}\rangle|-\sqrt{(1-m)\mu_E}\rangle|f\rangle) \otimes \\ \otimes |-\sqrt{m\mu_E}\rangle. \quad (15)$$

Частичные состояния Алисы и Боба в этом случае совпадают с (4) с точностью до изменения интенсивности, а состояния Евы теперь описываются операторами плотности

$$\rho_+^E = \\ = \Big[p(1-q)|\sqrt{(1-m)\mu_E}\rangle\langle\sqrt{(1-m)\mu_E}| \otimes |e_0\rangle\langle e_0| + \\ + pq|-\sqrt{(1-m)\mu_E}\rangle\langle-\sqrt{(1-m)\mu_E}| \otimes |e_1\rangle\langle e_1| + \\ + (1-p)|\sqrt{(1-m)\mu_E}\rangle\langle\sqrt{(1-m)\mu_E}| \otimes |f\rangle\langle f|\Big] \otimes \\ \otimes |\sqrt{m\mu_E}\rangle\langle\sqrt{m\mu_E}|,$$

$$\rho_+^E = \Big[pq|\sqrt{(1-m)\mu_E}\rangle\langle\sqrt{(1-m)\mu_E}| \otimes |e_0\rangle\langle e_0| + \\ + p(1-q)|-\sqrt{(1-m)\mu_E}\rangle\langle-\sqrt{(1-m)\mu_E}| \otimes |e_1\rangle\langle e_1| + \\ + (1-p)|\sqrt{(1-m)\mu_E}\rangle\langle\sqrt{(1-m)\mu_E}| \otimes |f\rangle\langle f|\Big] \otimes \\ \otimes |-\sqrt{m\mu_E}\rangle\langle-\sqrt{m\mu_E}|.$$

Несложно выписать матрицы таких операторов в ортонормированном базисе (базис будет содержать 8 векторов), вычислить величину информации подслушивателя по формуле (5) и определить критическую ошибку для данного вида атак. Существует некоторое оптимальное значение m при заданной длине линии связи, которое минимизирует критическую ошибку протокола.

На рис. 2 показаны графики зависимости критической ошибки (при оптимальном выборе параметра m) от длины линии связи для разных значений исходной интенсивности μ и длины кортежа $N = 10$ для комбинированной атаки прием–перепосыл и атаки с отводом части состояния. Из рис. 2 видно, что для типичных значений среднего числа фотонов $\mu \approx 0.5$, используемых в данном протоколе, критическая ошибка, до которой гарантируется секретное распределение ключей, составляет менее 5 %, что является достаточно малой величиной.

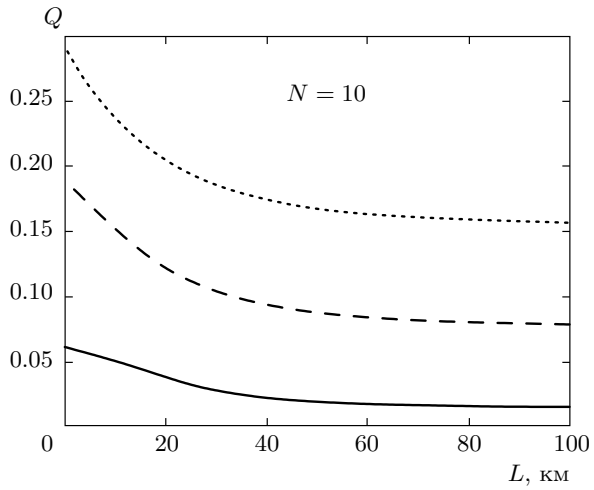

Рис. 2. Графики зависимости критической ошибки от длины линии связи для кортежей длиной 10 для комбинированной атаки прием–перепосыл и атаки с отводом части состояния. Пунктирная линия соответствует интенсивности 0.1, штриховая — интенсивности 0.2, сплошная — интенсивности 0.5

6. МЯГКАЯ ФИЛЬТРАЦИЯ КОРТЕЖЕЙ КОГЕРЕНТНЫХ СОСТОЯНИЙ

Важным классом атак на протоколы квантовой криптографии на когерентных состояниях является атака с определенным исходом при измерениях (UM, Unambiguous Measurements). Информационные когерентные состояния во многих протоколах квантовой криптографии линейно независимы, что является необходимым и достаточным условием для измерений с определенным исходом [1]. Такие измерения позволяют точно различать передаваемые состояния, но с некоторой вероятностью определенного исхода. Вероятность неопределенного исхода (inconclusive) зависит от структуры состояний, и проведение атаки возможно в канале с потерями, если последние превышают вероятность неопределенного исхода. Атака строится следующим образом: если подслушиватель получил определенный исход, то на приемную сторону посылается исходное состояние, если необходимо — с увеличенной интенсивностью, что гарантирует достижение состоянием при-

емной стороны. При неопределенном исходе посылка блокируется. Начиная с некоторой длины канала, удается компенсировать потери, вызванные блокировкой части импульсов. В этой ситуации подслушиватель знает весь ключ и не производит ошибок на приемной стороне, оставаясь тем самым недетектируемым.

Протокол DPS использует в качестве сигнальных состояний кортежи когерентных состояний, что делает вероятность определенного исхода достаточно малой при большой длине кортежа. Поэтому эффективное использование данной атаки возможно только при больших потерях в линии связи.

В этом разделе будет рассмотрено обобщение атаки с однозначным измерением для протокола DPS, при котором подслушиватель не ставит цели получения полной информации о передаваемых состояниях, а ставит задачу увеличения с некоторой вероятностью интенсивности всех передаваемых состояний, чтобы создать тем самым более благоприятные условия для проведения других атак, таких как прием–перепосыл или атака с отводом части состояния.

Рассмотрим кортеж из N состояний, каждое из которых имеет вид $|\pm\alpha\rangle$, $\mu = a^2$. Будем обозначать такой кортеж как $\overline{|\alpha\rangle}_i$, где i принимает значения от 0 до 2^N-1, а на k-й позиции кортежа стоит $|(-1)^{p_k(i)}\alpha\rangle$, где $p_k(i)$ — число на k-й позиции двоичной записи i. Например, для длины кортежа $N=3$ имеем

$$\overline{|\alpha\rangle}_0 = |\alpha\rangle|\alpha\rangle|\alpha\rangle,$$
$$\overline{|\alpha\rangle}_5 = |-\alpha\rangle|\alpha\rangle|-\alpha\rangle,$$
$$\overline{|\alpha\rangle}_7 = |-\alpha\rangle|-\alpha\rangle|-\alpha\rangle.$$

Определим преобразование, действующее на каждый из возможных кортежей состояний, по следующему правилу:

$$\overline{|\alpha\rangle}_i \to \sqrt{p}\,\overline{|\beta\rangle}_i|e_i\rangle + \sqrt{1-p}|0\rangle|f_i\rangle, \qquad (16)$$

где $\overline{|\beta\rangle}_i$ — аналогичным образом определенный кортеж из когерентных состояний интенсивности $\mu' = b^2$, $|0\rangle$ — вакуумное состояние, а $\{|e_i\rangle\}$ и $\{|f_i\rangle\}$ — наборы из вспомогательных состояний, для которых выполняется условие

$$\langle e_i|f_j\rangle = 0 \quad \forall i,j \in \{0,1,2,\ldots,2^N-1\}.$$

Преобразование (16) либо с вероятностью p увеличивает интенсивность каждого из состояний исходного кортежа до величины b^2, либо с вероятностью $1-p$ переводит состояние в вакуумное. Назначение наборов $\{|e_i\rangle\}$ и $\{|f_i\rangle\}$ в том, чтобы после преобразования становилось понятно, удачно ли прошла фильтрация, или состояние перешло в вакуум (неудача). Удачный исход от неудачного из-за ортогональности наборов вспомогательных состояний всегда можно достоверно отличить, проведя измерения над вспомогательными состояниями.

Назовем такое преобразование мягкой фильтрацией по аналогии со сходным преобразованием фильтрации (Filtering), введенным в работе [5]. Обычно под преобразованием фильтрации понимается такое преобразование, которое с некоторой вероятностью делает все состояния из набора взаимно ортогональными (различимыми), либо дает несовместный — неопределенный — исход. В нашем случае полная ортогональность полученных в случае успеха состояний не требуется, достаточно лишь улучшить их различимость за счет увеличения интенсивности — увеличить угол между состояниями $|\alpha\rangle$ и $|-\alpha\rangle$.

Для того чтобы преобразование было физически реализуемым, от него требуется унитарность, что дает $N+1$ условий сохранения скалярных произведений между входными и выходными состояниями:

$$_i\overline{\langle\alpha||\alpha\rangle}_j = \exp\left(-2a^2d(i,j)\right) =$$
$$= p\exp\left(-2b^2d(i,j)\right)E_{d(i,j)} + (1-p)F_{d(i,j)}, \qquad (17)$$

где $d(i,j)$ — расстояние Хемминга между двоичными записями i и j, а $E_{d(i,j)} = \langle e_i|e_j\rangle$ и $F_{d(i,j)} = \langle f_i|f_j\rangle$ — скалярные произведения, которые для нашего преобразования зависят только от расстояния Хемминга между кортежами.

В дальнейшем будем рассматривать преобразование, в котором все $E_d = 1$. Это соответствует тому, что на этапе мягкой фильтрации нет попытки получить информацию о входных состояниях, а стоит лишь задача повышения их интенсивности. Такой выбор параметров позволяет провести фильтрацию с наибольшей вероятностью успеха.

Отметим, что другой частный случай преобразования, при котором $E_d = 0$ при $d > 0$, а $E_0 = 1$, соответствует как раз «полной» фильтрации, при которой становится известна вся информация о передаваемых состояниях (она получается простым измерением вспомогательного состояния $|e_i\rangle$ в случае успеха), что эквивалентно проведению измерения с определенным исходом.

В случае, когда все $E_d = 1$, атака задается лишь параметрами p и b, а все F_d выражаются как

$$F_d = \frac{\exp(-2a^2d) - p\exp(-2b^2d)}{1-p}. \qquad (18)$$

Из условий унитарности следует также требование того, чтобы существовала система векто-

ров $\{|f_i\rangle\}$ со скалярными произведениями, заданными (18). Как известно, можно построить систему векторов по заданным взаимным скалярным произведениям в том случае, когда соответствующая матрица Грама неотрицательно определена.

Поскольку цель мягкой фильтрации состоит в повышении интенсивности до нужной величины b^2 с максимальной вероятностью успеха p, возникает вопрос о том, при каком минимальном p это возможно. Кортежи когерентных состояний линейно независимы, над ними можно провести измерение с определенным исходом, откуда следует, что существует ненулевая вероятность фильтрации. С другой стороны, эта вероятность не может быть равна единице, так как это означало бы возможность достоверного различения неортогональных квантовых состояний. Следовательно, стоит задача нахождения максимальной вероятности фильтрации до нужной величины.

Самый простой способ найти максимальную вероятность фильтрации до величины b — выбрать методом «вилки» на отрезке $(0,1)$ максимальное значение p, при котором матрица Грама будет положительной. Однако такую задачу решить численно при больших длинах кортежа N достаточно сложно, потому что размер матрицы Грама составляет $2^N \times 2^N$ и подсчет ее собственных значений превращается в экспоненциально сложную задачу. Тем не менее, из-за специфичного вида матрицы Грама для данной системы векторов эту задачу можно существенно упростить.

Матрица Грама G для данной системы векторов имеет вид $g_{ij} = F_{d(i,j)}$, где $d(i,j)$ — расстояние Хемминга между двоичными записями i и j. Рассмотрим вспомогательную матрицу

$$B = \begin{pmatrix} 1 & 2 \\ 2 & 1 \end{pmatrix}$$

и ее тензорную степень $B^{\otimes N}$. Непосредственно из свойств кронекеровского произведения для B следует, что

— $b_{ij} = 2^{d(i,j)}$;

— собственные векторы $B^{\otimes N}$ имеют вид

$$|\psi_i\rangle = \bigotimes_{l=1}^{N} |\xi_{i(l)}\rangle,$$

где $i(l)$ — l-й элемент в двоичной записи числа i, а

$$|\xi_0\rangle = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ 1 \end{pmatrix}, \quad |\xi_1\rangle = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ -1 \end{pmatrix};$$

— соответствующие им собственные значения записываются как

$$b_i = \sum_{j=0}^{2^N-1} (-1)^{\sum_{l=1}^{N} j(l)\, i(l)} 2^{d(j,0)}. \tag{19}$$

Несложно видеть, что элементы матриц G и B связаны соотношением $g_{ij} = F_{\log_2 b_{ij}}$. Докажем по индукции, что собственные векторы этих матриц совпадают. Утверждение очевидно для матриц размером 2×2. Далее, пусть собственные векторы совпадают для матриц размером $2^N \times 2^N$. Тогда из соответствия между G и B матрица Грама размером $N+1$ имеет структуру вида

$$G_{N+1}(\{F_0, \ldots, F_N\}) = \\ = \left(\begin{array}{c|c} G_N(\{F_0, \ldots, F_{N-1}\}) & G_N(\{F_1, \ldots, F_N\}) \\ \hline G_N(\{F_1, \ldots, F_N\}) & G_N(\{F_0, \ldots, F_{N-1}\}) \end{array} \right),$$

где как $G_N(\{F_i, \ldots, F_j\})$ обозначается матрица Грама размером $2^N \times 2^N$ для набора скалярных произведений $\{F_i, \ldots, F_j\}$. Собственные векторы $G_N(\{F_0, \ldots, F_{N-1}\})$ и $G_N(\{F_1, \ldots, F_N\})$ совпадают и равны $\{|\psi_i\rangle\}$, а их собственные значения обозначим соответственно как $\{g_i^0\}$ и $\{g_i^1\}$. Тогда, очевидно, собственные векторы $G_{N+1}(\{F_0, \ldots, F_N\})$ равны $|\xi_0\rangle \otimes |\psi_i\rangle$ и $|\xi_1\rangle \otimes |\psi_i\rangle$, а соответствующие собственные значения — $\{g_i^0 + g_i^1\}$ и $\{g_i^0 - g_i^1\}$. Таким образом, собственные векторы матриц G и B совпадают. Поэтому, пользуясь (19), несложно написать выражения для собственных значений G:

$$g_i = \sum_{j=0}^{2^N-1} (-1)^{\sum_{l=1}^{N} j(l)\, i(l)} F_{d(j,0)}. \tag{20}$$

Сгруппируем элементы этого выражения, относящиеся к F_m, их число равно C_N^m. Знак перед каждым из этих членов зависит от того, сколько из m единичных элементов в двоичной записи j оказались на тех же позициях, что и единицы в двоичной записи кортежа i: если это число нечетное, элемент входит со знаком минус, если четное, то со знаком плюс. Поскольку перебор происходит по всем кортежам с m единицами, из симметрии задачи следует, что коэффициент перед каждым F_m для собственного значения g_i зависит только от количества единиц в двоичной записи i и не зависит от их расположения. Это значит, что существует лишь $N+1$ разных собственных значений матрицы G, и несложно получить, что они равны (символом g_k будем обозначать

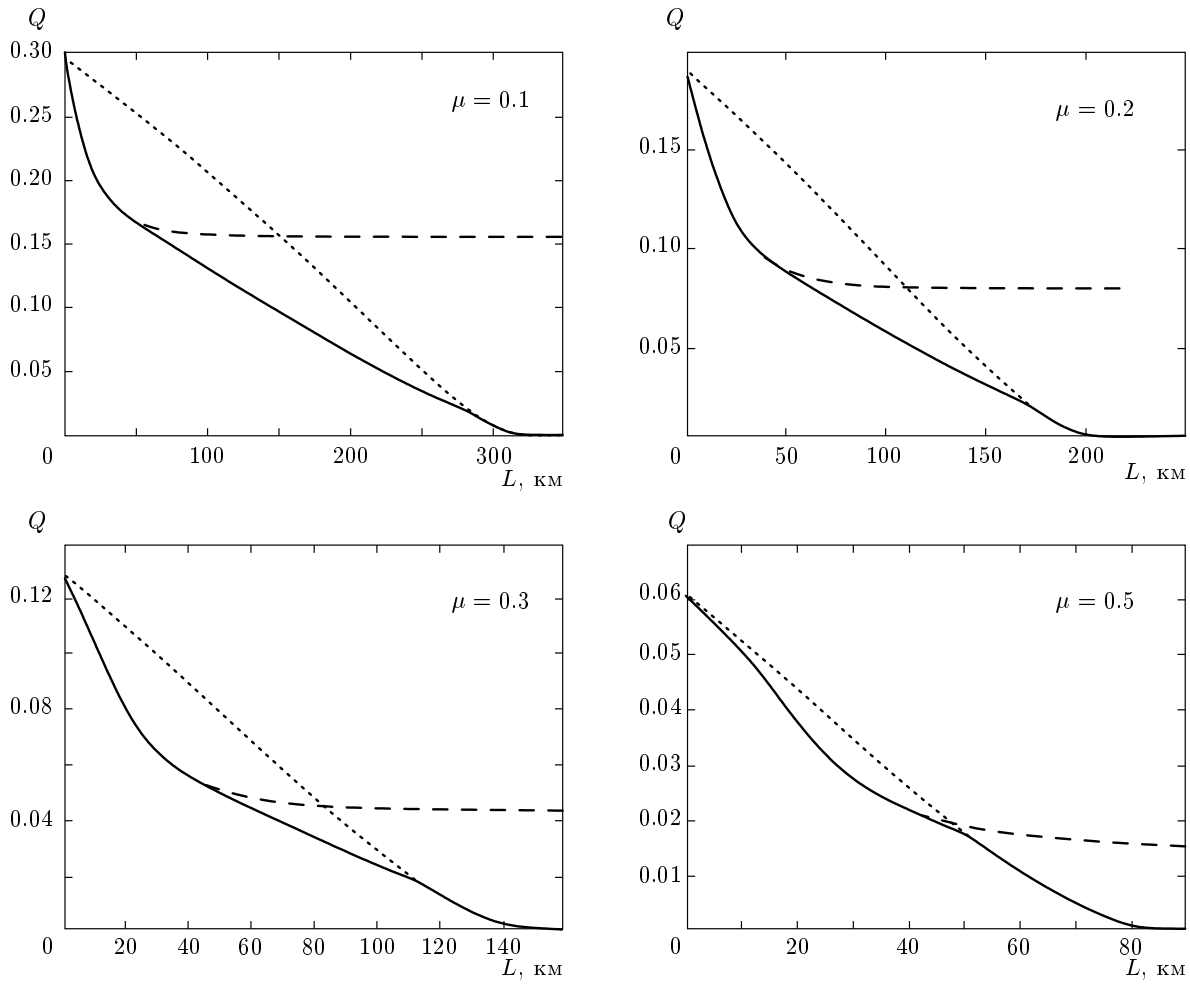

Рис. 3. Графики зависимости критической ошибки от длины линии связи для кортежей длиной 10 при различных значениях исходной интенсивности μ. Пунктирные линии отвечают атаке с отведением части состояния, штриховые — мягкой фильтрации с последующим получением информации о ключе с помощью атаки прием–перепосыл, сплошные — комбинированной атаке

собственное значение, для которого двоичная запись кортежа i содержит k единиц)

$$g_k = \sum_{d=0}^{N} \sum_{p=0}^{d} (-1)^p C_k^p C_{N-k}^{d-p} F_d. \qquad (21)$$

Перебор $N+1$ разных собственных значений G, вычисляемых по формуле (21), представляет собой существенно более простую задачу, чем подсчет собственных значений матрицы G размера $2^N \times 2^N$. Таким образом, существует относительно простой способ проверки, можно ли провести мягкую фильтрацию до нужной интенсивности с заданной вероятностью успеха p.

Рассмотрим предельный случай атаки, когда интенсивность новых состояний b^2 стремится к бесконечности, что соответствует полному различению передаваемых состояний. Тогда можно считать, что $E_0 = 1$, а $E_i = 0$ при $i > 0$, и F_i вычисляются по формулам

$$F_i = \frac{1}{1-p} e^{-2a^2 i} = \frac{A^i}{1-p}.$$

Отметим, что аналогичные соотношения получаются, если в преобразовании (16) потребовать ортогональности $|e_i\rangle$. Матрица Грама системы векторов $\{|f_i\rangle\}$ тогда представляется в простом виде:

$$G = \frac{1}{1-p} \left[\begin{pmatrix} 1 & A \\ A & 1 \end{pmatrix}^{\otimes N} - \mathrm{diag}(p) \right],$$

и, очевидно, она будет неотрицательно определена

Таблица

Длина кортежа для $\mu = 0.1$	$Q = 5\,\%$	$Q = 2\,\%$	$Q = 1\,\%$	UM-атака
6	139.3	155.9	162.7	172.5
8	184.5	220.0	230.2	246.7
10	223.9	281.5	297.6	320.8
12	262.9	335.7	365.0	395.0
Длина кортежа для $\mu = 0.2$	$Q = 5\,\%$	$Q = 2\,\%$	$Q = 1\,\%$	UM-атака
6	76.3	92.9	99.8	109.6
8	95.5	131.2	141.3	157.8
10	109.1	166.7	182.7	206.0
12	121.4	194.9	224.2	254.2
Длина кортежа для $\mu = 0.3$	$Q = 5\,\%$	$Q = 2\,\%$	$Q = 1\,\%$	UM-атака
6	43.9	60.7	67.6	77.5
8	49.4	85.4	95.6	112.1
10	49.4	107.3	123.4	146.7
12	48.0	121.9	151.2	181.2
Длина кортежа для $\mu = 0.5$	$Q = 5\,\%$	$Q = 2\,\%$	$Q = 1\,\%$	UM-атака
6	7.8	26.5	33.8	44.0
8	10.4	37.0	47.5	64.3
10	10.5	44.5	61.0	84.4
12	9.8	44.3	74.3	104.4

в том случае, когда p не больше минимального собственного значения

$$\begin{pmatrix} 1 & A \\ A & 1 \end{pmatrix}^{\otimes N},$$

которое равно

$$(1 - A)^N = (1 - e^{-2a^2})^N,$$

что как раз соответствует вероятности однозначного различения кортежей когерентных состояний длины N (т. е. последовательного получения совместных исходов при измерении каждого из состояний кортежа). Таким образом, измерение с определенным исходом является частным случаем мягкой фильтрации.

7. МЯГКАЯ ФИЛЬТРАЦИЯ ПРИ АТАКЕ НА ПРОТОКОЛ DPS И ОБСУЖДЕНИЕ РЕЗУЛЬТАТОВ

Применим теперь мягкую фильтрацию для прослушивания протокола DPS. Сама по себе процедура не дает подслушивателю полной информации о ключе, но в то же время повышается интенсивность передаваемых состояний, что облегчает подслушивание с помощью атаки прием–перепосыл или отвода части состояния. Сначала проводится мягкая фильтрация передаваемого кортежа до величины, не превышающей максимально допустимую для данной длины линии связи. Далее применяется описанная выше комбинация атаки прием–перепосыл и атаки с отводом части состояния, где в качестве интенсивности μ_E выступает величина, которую подслушиватель может отвести. Величина μ_E определяет-

ся из условия, чтобы ожидаемое число отсчетов на приемной стороне после вторжения подслушивателя оставалось таким же, как после прохождения состояний через канал связи заданной длины. Такая схема действий соответствует комбинированной атаке с использованием мягкой фильтрации, отвода части состояний и атаки прием–перепосыл, поэтому она будет эффективнее каждой из этих атак по отдельности.

На рис. 3 показаны зависимости критической ошибки от длины линии связи для длины кортежа, равной 10, и разных значений исходной интенсивности. Для сравнения приведены графики для атаки с отведением части состояния, мягкой фильтрации с последующим получением информации о ключе с помощью приема–перепосыла и для комбинированного случая, который оказывается эффективнее каждого из них.

В таблице даны критические длины линии связи для разных значений исходной интенсивности и при разных допустимых ошибках. Случай ошибки в 5 % соответствует низкой практической скорости передачи ключей, этой ошибке соответствует длина линии связи, при которой протокол демонстрирует малую эффективность. Критическую ошибку, равную 2 %, можно считать минимальным значением, при котором вообще возможно практическое распространение ключей. Наконец, при критической ошибке, равной 1 %, практическую передачу ключей можно считать невозможной.

Из приведенных в таблице данных видно, что при значениях длины кортежа, равных 10, и больших длинах линий связи необходимо использовать малые значения входной интенсивности, не превышающие 0.2 фотона на импульс, что соответствует достаточно низкой скорости передачи ключа из-за большого количества несовместных исходов. Так, для значения интенсивности в 0.2 фотона на импульс и длине канала в 100 км доля совместных исходов будет равна $p_{conc} \approx 0.002$. В сочетании с эффективностью детекторов, типичные значения которой $\eta = 10\,\%$, и вероятностью темновых шумов $p_d = 10^{-5}$ это дает ошибку

$$Q = \frac{1}{2}\,\frac{p_d}{p_d + \eta p_{conc}} \approx 2.38\,\%$$

при критической ошибке, равной 5.53 % для данных значений дистанции и интенсивности. При такой разнице между критической и наблюдаемой ошибками скорость генерации ключа чрезвычайно мала. Уменьшение входной интенсивности до 0.1 дает схожие результаты (наблюдаемая ошибка 4.55 %, критическая ошибка 13.1 % при вероятности совместных исходов без учета эффективности детекторов, равной $p_{conc} \approx 0.001$), это означает, что практическое использование протокола для распространения ключей на дистанции в 100 км при использовании кортежей состояний длиной 10 проблематично.

Работа выполнена при частичной финансовой поддержке РФФИ (гранты №№ 12-02-31200, 11-02-00455).

ЛИТЕРАТУРА

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

2. K. Inoue, E. Waks, and Y. Yamamoto, Proc. SPIE **4917**, 32 (2002).

3. С. Н. Молотков, ЖЭТФ **139**, 429 (2011); Письма в ЖЭТФ **94**, 504 (2011); **96**, 374 (2012).

4. А. С. Холево, *Квантовые системы, каналы, информация*, МЦМО, Москва (2010).

5. A. Acin, N. Gisin, and V. Scarani, Phys. Rev. A **69**, 012309 (2004).