ЖЭТФ, 2019, том 155, вып. 4, стр. 636–644

ДОСТАТОЧНО ЛИ СОСТОЯНИЙ ЛОВУШЕК (DECOY STATE-МЕТОДА) ДЛЯ ГАРАНТИИ СЕКРЕТНОСТИ КЛЮЧЕЙ В КВАНТОВОЙ КРИПТОГРАФИИ?

С. Н. Молотков [a,b,c*], ***К. С. Кравцов*** [d,e], ***М. И. Рыжкин*** [a]

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

[b] *Академия криптографии Российской Федерации*
121552, Москва, Россия

[c] *Факультет вычислительной математики и кибернетики,*
Московский государственный университет им. М. В. Ломоносова
119899, Москва, Россия

[d] *Физический факультет, Московский государственный университет им. М. В. Ломоносова*
119899, Москва, Россия

[e] *Институт общей физики им. А. М. Прохорова Российской академии наук*
119991, Москва, Россия

Поступила в редакцию 17 октября 2018 г.,
после переработки 17 октября 2018 г.
Принята к публикации 29 октября 2018 г.

Метод с состояниями ловушками (Decoy state-метод) был предложен для детектирования атаки с расщеплением по числу фотонов — PNS-атаки (Photon Number Splitting attack). На сегодняшний день Decoy state-метод считается чуть ли не универсальным методом при доказательстве секретности протоколов квантовой криптографии и вычислении длины секретного ключа. В работе показано, что существуют атаки, например атака со светоделителем, к которым Decoy state-метод оказывается не чувствительным. Decoy state-метод ориентирован на обнаружение изменений статистики фотоотсчетов информационных состояний и состояний ловушек при PNS-атаке. При атаке со светоделителем статистика фотоотсчетов не меняется. В результате Decoy state-метод существенно завышает длину ключа. Таким образом, Decoy state-метод не является универсальным методом, который позволяет детектировать различные атаки. По-видимому, из-за большого числа работ по Decoy state-методу возникло широко распространенное мнение, что данный метод является универсальным. Это привело к попыткам принять метод в качестве международного стандарта в квантовой криптографии, что явно преждевременно.

DOI: 10.1134/S0044451019040060

1. ВВЕДЕНИЕ

Квантовая криптография решает одну из главных проблем симметричной криптографии — проблему распределения секретных ключей по доступным для вторжения квантовому и вспомогательному классическому аутентичному каналам связи. На формальном уровне легитимные пользователи (Алиса, Боб), не имея общего секрета, при помощи квантовой криптографии из слабого криптографического примитива — аутентичного обмена классической информацией и пересылки квантовых состояний — могут получить общий секретный ключ. Общий секретный ключ является самым сильным криптографическим примитивом, из которого могут быть получены все остальные криптографические функции. Секретность ключей в квантовой криптографии гарантируется фундаментальными запретами квантовой механики на различимость квантовых состояний.

Секретность ключей в квантовой криптографии на уровне фундаментальных принципов строго доказана только в однофотонном случае для прото-

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

кола BB84 [1]. Доказательство основано на фундаментальных энтропийных соотношениях неопределенностей [2]. Данные соотношения позволяют не перебирать всевозможные атаки на передаваемые квантовые состояния, а получить верхнюю границу утечки информации к подслушивателю (Еве), когда известна только наблюдаемая ошибка на приемной стороне.

Однако в реальных системах ситуация отличается от идеализированного случая однофотонных информационных состояний. В реальных системах используются квазиоднофотонные состояния сильно ослабленного лазерного излучения — сильно ослабленные когерентные состояния. Когерентное состояние имеет пуассоновскую статистику по числу фотонов, что при наличии потерь в квантовом канале связи приводит к новым атакам, которые невозможны в строго однофотонном случае.

Одной из таких атак является PNS-атака (Photon Number Splitting attack) — атака с расщеплением по числу фотонов [3]. Данная атака имеет место, поскольку в квантовой механике возможны неразрушающие измерения числа фотонов. Причем такая атака возможна в системах квантовой криптографии как с поляризационным, так и фазовым кодированием, хотя при фазовом кодировании неразрушающие измерения числа фотонов более тонкие, чем при поляризационном кодировании [4]. Далее, чтобы избежать излишних выкладок, будем рассматривать системы с поляризационным кодированием, при этом все утверждения переносятся и на системы с фазовым кодированием.

PNS-атака сводится к следующему. Подслушиватель разрывает квантовый канал связи и неразрушающим способом проводит измерение числа фотонов в линии. Если обнаружен один фотон, то подслушиватель либо блокирует часть однофотонных посылок, либо проводит унитарную атаку, которая возмущает однофотонную компоненту когерентного состояния. Если обнаружено в канале два фотона и более, то часть из них подслушиватель оставляет себе в квантовой памяти, а остальные через канал с меньшими потерями (в идеале без потерь) доставляет на приемную сторону без возмущений. Дождавшись стадии раскрытия базисов, подслушиватель делает измерения в известном базисе и достоверно знает передаваемый бит ключа в тех посылках, где были многофотонные компоненты. Начиная с некоторого уровня потерь в линии связи подслушиватель может блокировать все однофотонные посылки, не меняя общего числа зарегистрированных посылок на приемной стороне, и знает весь ключ. Начиная с некоторых потерь, соответственно длины линии связи, система не обеспечивает секретность ключей.

При PNS-атаке, поскольку часть посылок с однофотонными состояниями блокируется, изменяется статистика фотоотсчетов на приемной стороне. Такое изменение в принципе можно обнаружить, если бы были детекторы, которые различают число фотонов, что на сегодняшний день находится за пределами технологического уровня. Существующие стандартные однофотонные лавинные детекторы не различают число фотонов, поэтому PNS-атаку нельзя детектировать. Для детектирования PNS-атаки был предложен Decoy state-метод, который состоит в посылке случайным образом когерентных состояний с разным средним числом фотонов (decoy state). Измерение полного числа отсчетов в посылках с разным средним числом фотонов позволяет оценить изменение статистики фотоотсчетов, в том числе долю однофотонной компоненты, и связать данные изменения с утечкой информации к подслушивателю.

Существует очень большое число работ, посвященных исследованию секретности ключей для Decoy state-метода [5–16], хотя практически все работы в значительной степени базируются на результатах [7, 8].

Известно также попытки принять Decoy state-протокол в качестве международного стандарта в квантовой криптографии[1)]. По-видимому, большое число работ привело к широко распространенному мнению, что данный метод оценки длины секретного ключа является универсальным. Универсальным в том смысле, что дает наименьшую длину секретного ключа для всевозможных атак. Однако принципиально важно понимать, что Decoy state-метод предназначен для детектирования PNS-атаки и логически ниоткуда не следует, что для других атак метод будет гарантировать получение секретного ключа. Логически нельзя исключить существование других атак, учет которых приведет к тому, что «секретный» ключ, полученный по Decoy state-методу, не будет секретным относительно других атак. Например, могла бы существовать атака, при которой секретным будет ключ меньшей длины, чем

[1)] Kai Chen, Jiajun Ma, and Hongsong Shi, Talk, ISO/IEC JTC1 SC27 WG3 SP Proposal, *Security Requirements, Test and Evaluation Methods for the Decoy State BB84 Quantum Key Distribution* (*QKD*), Berlin, Germany, 10/31/2017; ISO/IEC JTC 1/SC 27/WG 3 N 1537, 30th ISO/IEC JTC1/SC27 Working Group Meeting, Hongsong Shi, Jiajun Ma, and Gaetan Pradel Wuhan, China, April 2018 30th *Security Requirements, Test and Evaluation Methods for Quantum Key Distribution*.

получается по Decoy state-методу. То есть, неформально говоря, например, по Decoy state-методу получен «секретный» ключ длиной 256 бит, а при другой атаке секретный ключ должен быть 218 бит, т. е. из ключа в 256 бит известно 38 бит. Использование такого ключа как секретного приведет к катастрофическим последствиям. Ниже будет показано, что Decoy state-метод не гарантирует секретность ключа относительно других атак.

В данной работе построен явный пример простой атаки со светоделителем, при которой длина секретного ключа получается принципиально меньше, чем по Decoy state-методу. Удивительно, что такая простая атака, несмотря на сотни работ по Decoy state-методу, была пропущена.

2. ИНФОРМАЦИОННЫЕ КОГЕРЕНТНЫЕ СОСТОЯНИЯ ПРИ ПОЛЯРИЗАЦИОННОМ КОДИРОВАНИИ

В качестве информационных состояний используются сильно ослабленные когерентные состояния лазерного излучения. Ослабление происходит до уровня в несколько десятых среднего числа фотонов в когерентном квантовом состоянии. Когерентное состояние, как известно, имеет вид

$$|\alpha,\sigma\rangle = e^{-\mu/2}\sum_{n=0}^{\infty}\frac{\alpha^n}{n!}|n,\sigma\rangle = e^{-\mu/2}e^{\alpha a^{\dagger}(\sigma)}|\mathrm{vac}\rangle, \quad \mu = |\alpha|^2, \tag{1}$$

где μ — среднее число фотонов в когерентном состоянии, $|n,\sigma\rangle$ — фоковское состояние с n фотонами с поляризацией σ, $a^{\dagger}(\sigma)$ — оператор рождения фотона с поляризацией σ, $|\mathrm{vac}\rangle$ — вакуумное состояние.

Поскольку фаза когерентного состояния (фаза θ, $\alpha\sqrt{\mu}e^{i\theta}$ в (1)) меняется случайно от посылки к посылке, подслушиватель в канале связи «видит» не чистое квантовое когерентное состояние, а статистическую смесь — матрицу плотности

$$\rho(\mu,\sigma) = \int_0^{2\pi}\frac{d\theta}{2\pi}|e^{i\theta}|\alpha|,\sigma\rangle\langle e^{i\theta}|\alpha|,\sigma| = e^{-\mu}\sum_{n=0}^{\infty}\frac{\mu^n}{n!}|n,\sigma\rangle\langle n,\sigma|. \tag{2}$$

Состояние (2) имеет пуассоновскую статистику по числу фотонов. Квантовая механика допускает неразрушающие измерения числа фотонов (Nondemolishing Measurements). Данные измерения позволяют определить число фотонов, при этом не возмущая состояние поляризации фотона. После определения числа фотонов состояние поляризации остается неизвестным.

3. ФОРМАЛЬНОЕ ОПИСАНИЕ PNS-АТАКИ, ПРОТОКОЛ BB84

Для самодостаточности дальнейшего изложения нам потребуется формальное описание PNS-атаки. Проиллюстрируем PNS-атаку на примере протокола квантовой криптографии BB84, хотя она применима и для ряда других протоколов. В протоколе BB84 с поляризационным кодированием используется два базиса: + и ×. В каждом базисе состояниям 0 и 1 сопоставляются ортогональные внутри данного базиса состояния поляризации: σ_0^+ и σ_1^+. Фоковские состояния с ненулевым числом фотонов $n \geq 1$ при известном базисе достоверно различимы и имеют вид

$$0 \to |n,\sigma_0^+\rangle, \quad 1 \to |n,\sigma_1^+\rangle, \quad \langle n,\sigma_0^+|n,\sigma_1^+\rangle = 0. \tag{3}$$

Аналогично в сопряженном базисе:

$$0 \to |n,\sigma_0^{\times}\rangle, \quad 1 \to |n,\sigma_1^{\times}\rangle, \quad \langle n,\sigma_0^{\times}|n,\sigma_1^{\times}\rangle = 0. \tag{4}$$

Рассмотрим неразрушающие измерения на более формальном уровне. Любое измерение в квантовой механике дается разложением единичного оператора I. Неразрушающее измерение по числу фотонов дается проекционным (ортогональным) разложением единицы:

$$I = \sum_{n=0}^{\infty}\mathcal{P}_n, \quad \mathcal{P}_n = \sum_{\sigma=0,1}|n,\sigma\rangle\langle\sigma,n|. \tag{5}$$

Такое измерение не позволяет определить состояние поляризации фотонов, но позволяет определить число фотонов и при этом оставляет значение поляризации невозмущенным:

$$\mathcal{P}_{n'}|n,\sigma_{0,1}^+\rangle = \delta_{n,n'}|n,\sigma_{0,1}^+\rangle, \quad \mathcal{P}_{n'}|n,\sigma_{0,1}^{\times}\rangle = \delta_{n,n'}|n,\sigma_{0,1}^{\times}\rangle. \tag{6}$$

Если обнаружен один фотон в линии ($n = 1$), то подслушиватель блокирует канал связи либо осуществляет унитарную атаку, которая возмущает однофотонное состояние. Если обнаружены два или более фотонов ($n \geq 2$ — состояние $|n,\sigma_{0,1}^{\times}\rangle$ или $|n,\sigma_{0,1}^+\rangle$, состояние поляризации пока неизвестно), то подслушиватель оставляет часть фотонов в своей квантовой памяти, а остальные посылает на приемную сторону через канал с меньшими потерями, в идеале без потерь.

4. DECOY STATE-МЕТОД ДЛЯ ДЕТЕКТИРОВАНИЯ PNS-АТАКИ

Блокирование посылок с разным числом фотонов изменяет исходную пуассоновскую статистику (формула (2)). Для детектирования изменения статистики используются случайным образом посылки когерентных состояний с разным средним числом фотонов. Основное наблюдение, которое используется в Decoy state-методе, состоит в следующем. Обнаружив состояние с данным числом фотонов, подслушиватель не знает, из какого когерентного состояния и с каким средним числом фотонов происходит данная посылка. Поэтому решение подслушивателя блокировать или нет данную посылку приведет к изменению пуассоновской статистики. Пусть Y_k — условная вероятность того, что подслушиватель оставит данное среднее число фотонов k в посылке, которое будет доставлено на приемную сторону для детектирования, возможно через идеальный без потерь канал связи. Иначе говоря, величина Y_k не зависит от среднего числа фотонов. Ниже рассмотрим Decoy state-метод с двумя состояниями ловушками со средним числом фотонов $\nu_1 > \nu_2$ и информационными состояниями со средним числом фотонов $\mu > \nu_1 + \nu_2$. Возможны и другие варианты Decoy state-метода, но это не принципиально, поэтому воспользуемся общеупотребительным вариантом. Ниже ограничимся асимптотическим пределом длинных последовательностей. В этом случае частота наблюдаемых отсчетов и ошибок на приемной стороне совпадает с соответствующими вероятностями. При конечных длинах последовательностей соотношение между длиной ключа при PNS-атаке и при атаке со светоделителем не изменяется.

Полная вероятность компонент состояний с разным средним числом фотонов, собранная по всем посылкам с одинаковым средним числом фотонов, имеет вид (см. детали в [8])

$$\begin{gathered} Q(\mu) = e^{-\mu}\sum_{k=0}^{\infty} Y_k \frac{\mu^k}{k!} = e^{-\mu}\sum_{k=0}^{\infty} Q_k(\mu), \\ Q(\nu_i) = e^{-\nu_i}\sum_{k=0}^{\infty} Y_k \frac{\nu_i^k}{k!} = e^{-\nu_i}\sum_{k=0}^{\infty} Q_k(\nu_i), \\ i = 1, 2. \end{gathered} \tag{7}$$

Средняя ошибка детектирования на приемной стороне для посылок с информационными состояниями есть сумма ошибок с соответствующими вероятностями, имеем

$$\mathrm{Err}(\mu) = e^{-\mu}\sum_{k=0}^{\infty} e_k Y_k \frac{\mu^k}{k!}. \tag{8}$$

Аналогичное выражение имеет место для средней ошибки по серии decoy state со средним числом фотонов ν_1 и ν_2.

Поскольку подслушиватель для посылок с числом фотонов $n \geq 2$ имеет в квантовой памяти «копию» исходного состояния, после разглашения базисов он точно знает состояние в данной посылке, и секретный ключ получается только из части посылок с однофотонной компонентой. Для длины секретного ключа имеем (см. детали в [8, 17])

$$\begin{gathered} R_{PNS} = \left\{ \frac{Q_1(\mu)}{Q(\mu)} \left(1 - h(e_1)\right) - \mathrm{leak} \right\}, \\ \mathrm{leak} = h\left(\frac{\mathrm{Err}(\mu)}{Q(\mu)}\right). \end{gathered} \tag{9}$$

Посылки с состояниями ловушками (decoy states) служат для оценки параметров, фигурирующих в формуле для длины секретного ключа (9). Для метода с двумя состояниями ловушками известны следующие общеупотребительные оценки [8]. Вероятность регистрации однофотонной компоненты состояния равна

$$\begin{aligned} Q_1(\mu) = \frac{\mu^2 e^{-\mu}}{\mu(\nu_1 - \nu_2) - (\nu_1^2 - \nu_2^2)} \Big[& Q(\nu_1) e^{\nu_1} - \\ & - Q(\nu_2) e^{\nu_2} - \frac{\nu_1^2 - \nu_2^2}{\mu^2} \left(Q(\mu) e^{\mu} - Y_0 \right) \Big], \end{aligned} \tag{10}$$

$$Y_0 = \max\left\{ \frac{\nu_1 Q(\nu_2) E^{\nu_2} - \nu_2 Q(\nu_1) e^{\nu_1}}{\nu_1 - \nu_2}, 0 \right\}. \tag{11}$$

Ошибка в однофотонной компоненте информационных состояний имеет вид

$$e_1 \leq \frac{\mathrm{Err}(\nu_1) e^{\nu_1} - \mathrm{Err}(\nu_2) e^{\nu_2}}{(\nu_1 - \nu_2) Y_1}, \tag{12}$$

где

$$\begin{aligned} Y_1 \geq \frac{\mu}{\mu(\nu_1 - \nu_2) - (\nu_1^2 - \nu_2^2)} \Big[& Q(\nu_1) e^{\nu_1} - \\ & - Q(\nu_2) e^{\nu_2} - \frac{\nu_1^2 - \nu_2^2}{\mu^2} \left(Q(\mu) e^{\mu} - Y_0 \right) \Big]. \end{aligned} \tag{13}$$

Если лавинный детектор на приемной стороне имеет не единичную квантовую эффективность, то в этом случае в формулах (7), (8), (10)–(13) нужно провести замену $\mu \to \eta\mu$. Типичные значения квантовой эффективности лавинных детекторов в телекоммуникационном диапазоне длин волн имеют значения $\eta = 0.1 \div 0.25$.

5. АТАКА СО СВЕТОДЕЛИТЕЛЕМ

Рассмотрим теперь атаку со светоделителем (BS, beam split). Схема атаки приведена на рис. 1. Пусть длина квантового канала связи L. Без подслушивателя на приемную сторону поступают неискаженные квантовые состояния со средним числом фотонов $\mu(L) = \mu 10^{-\delta L/10}$, где δ — удельные потери в канале связи. Типичные значения для одномодового волокна $\delta = 0.2$ дБ/км. При атаке подслушиватель разрывает линию связи, отводит через асимметричный поляризационно нечувствительный светоделитель долю состояния $1 - T(L)$ в квантовую память, а остальную долю когерентного состояния $T(L)$ через канал с меньшими потерями (в идеале без потерь) доставляет на приемную сторону без искажений. Свое квантовое состояние подслушиватель сохраняет в квантовой памяти до раскрытия базисов. После раскрытия базисов производит измерения в известном базисе.

Фундаментальным и хорошо известным свойством когерентного состояния является его самоподобное преобразование на линейных оптических элементах, в нашем случае на светоделителе. Важно, что на двух выходах светоделителя возникают независимые когерентные состояния, но с меньшим средним числом фотонов по сравнению с входным когерентным состоянием. Независимость состояний означает, что измерения когерентного состояния на выходах светоделителя не влияют друг на друга.

Самоподобное преобразование когерентного состояния на асимметричном поляризационно нечувствительном светоделителе удобно представить через преобразование операторов, имеем

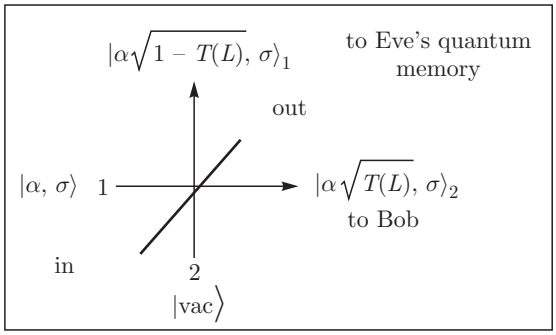

Рис. 1. Атака со светоделителем

$$\begin{pmatrix} a_1^\dagger(\sigma) \\ a_2^\dagger(\sigma) \end{pmatrix}_{out} = \begin{pmatrix} \sqrt{1-T(L)} & \sqrt{T(L)} \\ -\sqrt{T(L)} & \sqrt{1-T(L)} \end{pmatrix} \times \times \begin{pmatrix} a^\dagger(\sigma) \\ 0 \end{pmatrix}_{in}. \quad (14)$$

На выходе светоделителя два независимых когерентных состояния имеют вид

$$|\alpha\sqrt{1-T(L)},\sigma\rangle_1 \otimes |\alpha\sqrt{T(L)},\sigma\rangle_2 = = \left(e^{-\mu(1-T(L))/2}\, e^{\alpha\sqrt{1-T(L)}\, a_1^\dagger(\sigma)}|\mathrm{vac}\rangle_1\right) \otimes \otimes \left(e^{-\mu(T(L))/2}\, e^{\alpha\sqrt{T(L)}\, a_2^\dagger(\sigma)}|\mathrm{vac}\rangle_2\right). \quad (15)$$

Подчеркнем, что на выходе светоделителя возникает чистое когерентное состояние, а не статистическая смесь — матрица плотности.

При измерении подслушивателем состояния в квантовой памяти фаза когерентного состояния (фаза θ параметра α) подслушивателю в каждой посылке неизвестна, поэтому подслушиватель «видит» статистическую смесь состояний — матрицу плотности, аналогично ситуации с неразрушающим измерением числа фотонов. Матрица плотности имеет вид

$$\rho_1(\mu,\sigma) = e^{-\mu(1-T(L))} \sum_{k=0}^{\infty} \frac{\mu^k (1-T(L))^k}{k!} \times \times |k,\sigma\rangle_{11}\langle\sigma,k|. \quad (16)$$

После раскрытия базисов подслушиватель знает базис, поэтому далее индекс базиса опускаем. Длина секретного ключа выражается через условную энтропию фон Неймана для совместной матрицы плотности Алиса–Ева [18]. Совместная матрица плотности Алиса–Ева имеет вид

$$\rho_{XE}(\mu) = \frac{1}{2}|0\rangle_{X\,X}\langle 0| \otimes \rho_1(\mu,\sigma_0) + + \frac{1}{2}|1\rangle_{X\,X}\langle 1| \otimes \rho_1(\mu,\sigma_1), \quad (17)$$

где $|0\rangle_X$ и $|1\rangle_X$ — копии информационных состояний, которые Алиса оставляет у себя и которые доступны только ей. Длина секретного ключа в асимптотическом пределе длинных последовательностей в пересчете на зарегистрированную посылку дается формулой

$$R_{BS} = H(\rho_{XE}|\rho_E) - \mathrm{leak} = 1 - \overline{C}(\mu) - \mathrm{leak}, \quad (18)$$

где условная энтропия

$$H(\rho_{XE}|\rho_E) = H(\rho_{XE}) - H(\rho_E). \quad (19)$$

По определению

$$H(\rho) = -\mathrm{Tr}\{\rho \log(\rho)\} = -\sum_k \lambda_k \log(\lambda_k),$$

λ_k — собственные числа матрицы плотности ρ, $\log \equiv \equiv \log_2$. Собственные числа матрицы плотности Алиса–Ева ρ_{XE} равны

$$\left\{\frac{1}{2}e^{-\mu(1-T(L))}\frac{\mu^k(1-T(L))^k}{k!}, \right. \\ \left. \frac{1}{2}e^{-\mu(1-T(L))}\frac{\mu^k(1-T(L))^k}{k!}\right\}_{k=0}^{\infty}. \quad (20)$$

Соответственно собственные числа матрицы плотности Евы $\rho_E = \mathrm{Tr}\{\rho_{XE}\}$ равны

$$\{e^{-\mu(1-T(L))}\}_{k=0}, \ \left\{\frac{1}{2}e^{-\mu(1-T(L))}\frac{\mu^k(1-T(L))^k}{k!}, \right. \\ \left. \frac{1}{2}e^{-\mu(1-T(L))}\frac{\mu^k(1-T(L))^k}{k!}\right\}_{k=1}^{\infty}. \quad (21)$$

С учетом (20), (21) получаем для условной энтропии фон Неймана

$$H(\rho_{XE}|\rho_E) = 1 - \overline{C}(\mu), \quad (22)$$

где величина Холево [19–22]

$$\overline{C}(\mu) = e^{-\mu(1-T(L))}\sum_{k=1}^{\infty}\frac{\mu^k(1-T(L))^k}{k!} = \\ = 1 - e^{-\mu(1-T(L))}. \quad (23)$$

Важно отметить, что величина (23) достигается на коллективных измерениях над всей квантовой памятью. Величина Холево, по сути, является пропускной способностью квантово-классического канала между Алисой и Евой, она равна максимальному количеству классических битов на посылку, которое Ева может извлечь из ансамбля квантовых состояний. Как видно из формулы (23), величина Холево возрастает с ростом $\mu(1-T(L))$. Неопределенность информации Евы о передаваемом бите ключа связана только с вакуумной компонентой состояния, которая возникает с вероятностью $e^{-\mu(1-T(L))}$. Из компонент состояния с ненулевым числом фотонов ($k \geq 1$), имеющих вероятность

$$e^{-\mu(1-T(L))}\frac{\mu^k(1-T(L))^k}{k!},$$

Ева получает достоверную информацию о передаваемом бите ключа. При такой атаке ошибочные отсчеты на приемной стороне возникают только за счет темновых шумов лавинного детектора с вероятностью p_d. Полная вероятность детектирования детектором с квантовой эффективностью η как правильных, так и ошибочных отсчетов равна

$$Q_{BS}(\mu) = p_d + e^{-\eta\mu T(L)}\sum_{k=1}^{\infty}\frac{(\eta\mu T(L))^k}{k!} = \\ = p_d + 1 - e^{-\eta\mu T(L)}, \quad (24)$$

соответственно вероятность ошибочных отсчетов

$$\mathrm{Err}_{BS}(\mu) = \frac{p_d}{2}, \\ \frac{Err_{BS}(\mu)}{Q_{BS}(\mu)} = \frac{1}{2}\frac{p_d}{p_d + 1 - e^{-\eta\mu T(L)}}. \quad (25)$$

В итоге для информации leak, требуемой для коррекции ошибок в асимптотическом пределе длинных последовательностей, имеем

$$\mathrm{leak} = h\left(\frac{\mathrm{Err}_{BS}(\mu)}{Q_{BS}(\mu)}\right). \quad (26)$$

Отметим, что утечка информации к подслушивателю при коррекции ошибок в (9) и (26) записана в шенноновском пределе, т. е. при коррекции ошибок случайными шенноновскими кодами, что на практике в полной мере недостижимо. При использовании конструктивных кодов величину leak в (9) и (26) нужно заменить на $f \cdot \mathrm{leak}$, где f — величина эффективности кода, обычно $f = 1.1 \div 125$.

6. СРАВНЕНИЕ ДЛИНЫ СЕКРЕТНОГО КЛЮЧА ПРИ АТАКЕ СО СВЕТОДЕЛИТЕЛЕМ И АТАКЕ С РАСЩЕПЛЕНИЕМ ПО ЧИСЛУ ФОТОНОВ

В этом разделе проведем сравнение эффективностей атак. Оценим длину секретного ключа и длину квантового канала связи, до которой гарантируется распределение секретных ключей. В асимптотическом пределе длинных последовательностей частоты отсчетов (10), (24) равны вероятностям отсчетов для информационных состояний со средним числом фотонов μ, для decoy state со средним числом фотонов ν_1 и ν_2, а также наблюдаемой вероятности ошибки для информационных состояний и состояний ловушек (decoy states). Легитимные пользователи не могут в принципе различить, есть в канале подслушиватель или нет. Оценка длины секретного ключа должна быть применима как при наличии подслушивателя, так и в его отсутствие.

Пусть подслушиватель в линии связи отсутствует, тогда величины (7), (24) определяются только потерями в линии связи, а ошибки (8), (25) возникают только за счет темновых шумов лавинных детекторов. Считаем, что оптическая приемная часть системы не вносит ошибок, т. е. идеально настроена. В этом случае по Decoy state-методу длина секретного ключа получается по формулам (9)–(13), где нужно заменить $\mu, \nu_{1,2} \to \mu T(L), \nu_{1,2} T(L)$, где $T(L)$ — прохождение в канале связи. Предельная длина линии связи определяется из условия обращения в нуль длины секретного ключа.

Длина секретного ключа при атаке со светоделителем определяется по формулам (18)–(26). При такой атаке подслушиватель действует «прозрачно» — не изменяет число отсчетов, не производит ошибок, не изменяет статистику отсчетов и соотношение между вероятностями для состояний с разными средними значениями числа фотонов.

Поскольку не существует универсальной оценки длины секретного ключа для всех возможных атак (исключение составляет однофотонный случай, см. Введение), необходимо вычислять длину ключа для каждой отдельной атаки, а затем выбирать наименьшую длину по всем атакам. Ниже покажем, что оценка длины секретного ключа при прозрачной атаке со светоделителем дает существенно меньшую длину секретного ключа, чем оценки по Decoy state-методу при PNS-атаке.

Вопрос фактически формулируется следующим образом. Имеется набор наблюдаемых величин в асимптотическом пределе длинных последовательностей — вероятностей (10)–(13), (24), (25). Ключ какой длины после коррекции ошибок и сжатия (усиления секретности очищенного ключа) нужно оставить, чтобы быть уверенным, что он является секретным? Decoy state-метод оставляет бóльшую длину ключа, чем это допустимо, т. е. ключ фактически является не секретным.

Прежде чем представить численные расчеты, для большей наглядности и убедительности сделаем аналитические вычисления. Асимптотические значения параметров для Decoy state-метода можно получить из формул (9)–(13), если устремить величину среднего числа фотонов в decoy state $\nu_1, \nu_2 \to 0$. В этом пределе получаем следующие значения для вероятностей:

$$Q(\mu) = p_d + 1 - e^{-\eta\mu T(L)}. \tag{27}$$

Полная ошибка есть

$$\mathrm{Err}(\mu) = e_0 p_d, \quad e_0 = \frac{1}{2}. \tag{28}$$

При малых $\eta_{1,2} \to 0$ получаем

$$Y_1 = p_d + \eta, \quad e_1 = \frac{1}{2}\,\frac{p_d}{\eta}. \tag{29}$$

Разность длин ключей в Decoy state-методе и BS-атаке равна

$$R_{PNS} - R_{BS} \approx 1 - h\left(\frac{p_d}{2\eta}\right) - e^{-\mu(1-T(L))} \approx$$
$$\approx \mu(1 - T(L)) - \frac{p_d}{2\eta} \approx \mu(1 - T(L)) > 0. \tag{30}$$

Из формулы (30) видно, что Decoy state-метод всегда завышает длину секретного ключа, так как среднее число фотонов в информационном состоянии $\mu > 0$.

Типичные значения квантовой эффективности лавинных детекторов $\eta = 0.1 \div 0.25$, характерные значения вероятности темновых шумов на строб $p_d = 10^{-6} \div 10^{-7}$. Поэтому слагаемое $p_d/2\eta \approx \approx 10^{-5} \div 10^{-6}$. Типичные значения среднего числа фотонов в информационных состояниях $\mu = = 0.1 \div 0.5$. Коэффициент прохождения канала связи $T(L) = 10^{-L\delta/10}$ длиной L для одномодового волокна с коэффициентом потерь $\delta = 0.2$ дБ/км, например, при длине 10 км равен $T(L = 20) = 0.398$, поэтому разница в длине ключей составляет при $\mu = = 0.25$

$$\frac{R_{PNS} - R_{BS}}{R_{PNS}} = 85\,\%,$$

что на 15 % превышает длину секретного ключа при атаке со светоделителем.

Причина завышения длины ключа и принципиальной нечувствительности Decoy state-метода к атаке со светоделителем состоит в том, что «квантовая часть» нехватки информации Евы о ключе (см. первое слагаемое в формуле (30)) в Decoy state-методе оценивается через наблюдаемую ошибку в однофотонной компоненте состояния (формулы (12), (28)). Фактически, чем больше ошибка в однофотонной компоненте, тем больше «квантовая часть» утечки информации к Еве.

При прозрачной атаке со светоделителем Ева, начиная уже с небольших длин линии связи, может отвести себе почти все квантовые состояния, не производя ошибки на приемной стороне и не меняя числа отсчетов по сравнению с тем, которое должно быть в отсутствие подслушивателя. Отводя состояния почти целиком, Ева получает всю информацию, содержащуюся в квантовом ансамбле, и эта информация никоим образом не зависит от ошибки в однофотонной компоненте состояния на приемной

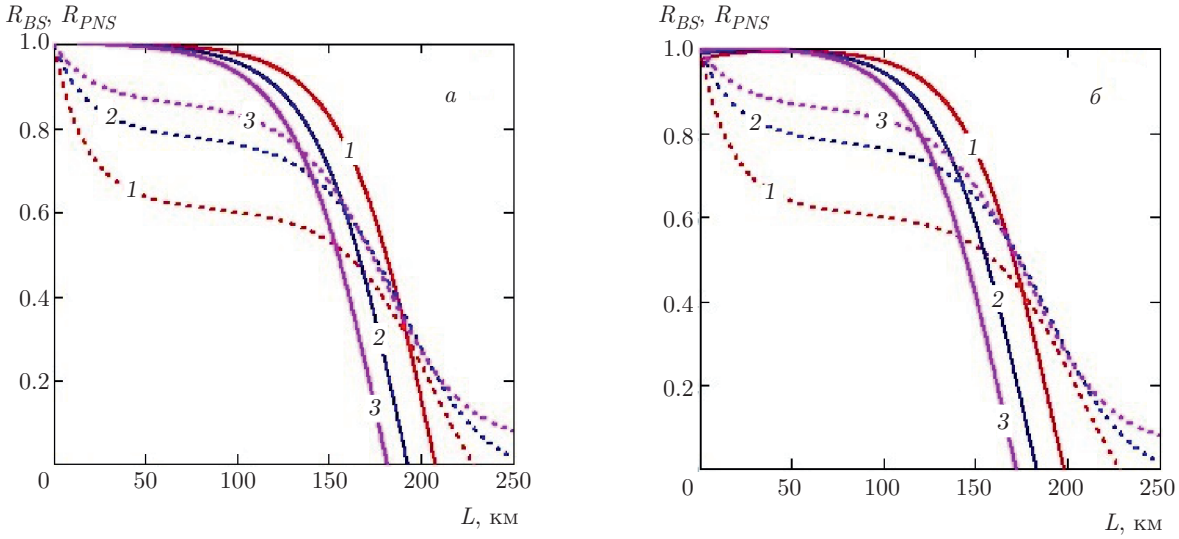

Рис. 2. *а*) Зависимости длины секретного ключа в пересчете на зарегистрированную посылку от длины линии связи, рассчитанные по асимптотическим формулам для Decoy state-метода (PNS) — сплошные линии, для атаки со светоделителем (BS) — пунктирные линии. *б*) Зависимости длины секретного ключа в пересчете на зарегистрированную посылку от длины линии связи, рассчитанные для Decoy state-метода (PNS) — сплошные линии, для атаки со светоделителем (BS) — пунктирные линии. Общие значения параметров кривых *1–3*: $\mu = 0.5$ (*1*), 0.25 (*2*), 0.15 (*3*). Среднее число фотонов в decoy state для всех кривых на рис. *б*: $\nu_1 = 0.01$, $\nu_2 = 0.001$. Общие параметры для всех кривых: вероятность темновых шумов на строб $p_d = 10^{-6}$, квантовая эффективность однофотонного детектора $\eta = 0.1$, удельные потери в линии связи $\delta = 0.2$ дБ/км

стороне. Точнее говоря, информация Евы вообще не зависит от ошибок на приемной стороне, а ограничена лишь структурой квантовых состояний в ансамбле, а именно, только фундаментальной величиной Холево [19–22].

Рассмотрим пример. Пусть получена длина секретного ключа по Decoy state-методу 256 бит, при этом длина ключа, который должен получиться по BS-атаке на 15 % меньше. Иначе говоря, из 256 бит подслушивателю известно 38 бит секретного ключа, что, очевидно, неприемлемо.

Результаты численных расчетов длины секретного ключа для Decoy state-метода и PNS-атаки, а также для атаки со светоделителем, приведены на рис. 2 для различных параметров. Как видно из рис. 2, для типичных значений среднего числа фотонов в состоянии ловушки (decoy state) результаты практически не отличаются от результатов расчетов по формулам (9), (10)–(13).

7. ЗАКЛЮЧЕНИЕ

Таким образом, показано, что Decoy state-метод не чувствителен к детектированию прозрачной атаки со светоделителем. Такая атака не изменяет статистики отсчетов и соотношение между статистиками фотоотсчетов для состояний с разным средним числом фотонов. При оценке длины секретного ключа получается заметно бóльшая длина ключа, чем при оценках по правильным формулам, учитывающим возможность атаки со светоделителем. Для типичных значений среднего числа фотонов в информационном состоянии и при длине линии связи от 5 до 150 км Decoy state-метод существенно завышает длину «секретного ключа», поэтому использование таких ключей, например, в банковской сфере [23], может привести к непредсказуемым последствиям.

Поэтому при вычислении длины секретного ключа крайне необходимо делать оценки для всех возможных атак Евы на передаваемые состояния, а не ограничиваться только одной PNS-атакой и Decoy state-методом.

Благодарности. Авторы выражают благодарность коллегам по Академии криптографии Российской Федерации за постоянную поддержку и обсуждения. Авторы благодарят И. М. Арбекова, К. А. Балыгина, А. Н. Климова и С. П. Кулика за многочисленные и интенсивные обсуждения.

Финансирование работы. Работа поддержана Российским научным фондом (П-(П-2019)).

ЛИТЕРАТУРА

1. M. Tomamichel, Ch. Ci Wen Lim, N. Gisin, and R. Renner, Nature Commun. **3**, 1 (2012); arXiv:1103.4130 v2 (2011).

2. M. Tomamichel and R. Renner, Phys. Rev. Lett. **106**, 110506 (2011).

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

4. S. P. Kulik and S. N. Molotkov, Laser Phys. Lett. **14**, 125205 (2017).

5. Won-Young Hwang, arXiv[quant-ph]:0211153.

6. Xiang-Bin Wang, Phys. Rev. Lett. **94**, 230503 (2005).

7. Hoi-Kwong Lo, Xiongfeng Ma, and Kai Chen, Phys. Rev. Lett. **94**, 230504 (2005).

8. Xiongfeng Ma, Bing Qi, Yi Zhao, and Hoi-Kwong Lo, arXiv[quant-ph]:0503005.

9. Yi Zhao, Bing Qi, Xiongfeng Ma, Hoi-Kwong Lo, and Li Qian, arXiv[quant-ph]:0503192.

10. D. Rosenberg, J. W. Harrington, P. R. Rice, P. A. Hiskett, C. G. Peterson, R. J. Hughes, A. E. Lita, Sae Woo Nam, and J. E. Nordholt, Phys. Rev. Lett. **98**, 010503 (2007).

11. B. Fröhlich, J. F. Dynes, M. Lucamarini, A. W. Sharpe, Zh. Yuan, and A. J. Shields, Nature **501**, 69 (2013).

12. M. Lucamarini, K. A. Patel, J. F. Dynes, B. Fröhlich, A. W. Sharpe, A. R. Dixon, Z. L. Yuan, R. V. Penty, and A. J. Shields, Opt. Express **21**, 24550 (2013).

13. Sellami Ali, Shuhairi Saharudin, and M. R. B. Wahiddin, Amer. J. Engin. Appl. Sci. **2**, 694 (2009).

14. Ch. Ci Wen Lim, M. Curty, N. Walenta, Feihu Xu, and H. Zbinden, Phys. Rev. A **89**, 022307 (2014); arXiv[quant-ph]:1311.7129.

15. Feihu Xu, Shihan Sajeed, Sarah Kaiser, Zhiyuan Tang, V. Makarov, and Hoi-Kwong Lo, Phys. Rev. A **92**, 032305 (2014).

16. Zhen Zhang, Qi Zhao, Mohsen Razavi, and Xiongfeng Ma, Phys. Rev. A **95**, 012333 (2017).

17. D. Gottesman, H.-K. Lo, N. Lütkenhaus, and J. Preskill, Quant. Inf. Comp. **4**, 325 (2004).

18. R. Renner, PhD thesis, ETH Zürich, arXiv:0512258 (2005).

19. A. S. Holevo, Probl. Inf. Transm. **9**, 177 (1973).

20. А. С. Холево, УМН **53**, 193 (1998).

21. *Введение в квантовую теорию информации*, сер. *Современная математическая физика*, вып. 5, МЦНМО, Москва (2002).

22. А. С. Холево, *Квантовые системы, каналы, информация*, МЦНМО, Москва (2010).

23. A. V. Duplinskiy, E. O. Kiktenko, N. O. Pozhar, M. N. Anufriev, R. P. Ermakov, A. I. Kotov, A. V. Brodskiy, R. R. Yunusov, V. L. Kurochkin, A. K. Fedorov, and Y. V. Kurochkin, arXiv: [quant-ph]:1712.09831 (2017).