Письма в ЖЭТФ, том 87, вып. 10, с. 674 – 679 © 2008 г. 25 мая

О предельных возможностях квантового распределения ключей с контролем статистики неоднофотонного источника

С. Н. Молотков

Институт физики твердого тела РАН, 142432 Черноголовка, Московская обл., Россия

Академия криптографии РФ

Факультет вычислительной математики и кибернетики МГУ им. М.В. Ломоносова, 119992 Москва, Россия

Поступила в редакцию 11 марта 2008 г.

После переработки 8 апреля 2008 г.

Найдена верхняя граница длины квантового канала связи, на которую можно рассчитывать при передаче ключей в методе с имитирующими квантовыми состояниями (decoy states).

PACS: 03.65.Hk, 03.67.Dd

Квантовая криптография позволяет передавать ключи и гарантировать их секретность на уровне законов природы, если ошибка на приемной стороне не превышает некоторой критической величины. Протокол распределения ключей BB84 [1] является базовым способом передачи ключей и используется как основа для построения различных систем квантовой криптографии. Для данного протокола различными способами доказана секретность в случае строго однофотонного источника квантовых состояний, идеальных фотодетекторов и канала связи без потерь [2–6]. В реальных условиях квантовые состояния не являются строго однофотонными, а источник представляет собой сильно ослабленное лазерное излучение (когерентное состояние со средним числом фотонов $\mu = 0.1{-}0.5$ в импульсе). Лавинные фотодетекторы, обычно используемые в системах квантовой криптографии, также являются неидеальными. Квантовая эффективность фотодетекторов заметно меньше 100% (характерная величина 10%–40%) и, что более критично, они имеют собственные темновые шумы, которые составляют $10^{-5} - 10^{-7}$ отсч./строб. Квантовый канал связи – оптоволокно имеет потери ($\alpha \approx 0.2$ дБ/км), что приводит к исчезновению квантовых состояний при передаче. Перечисленные неидеальности являются крайне критичными для обеспечения секретности передаваемых ключей. В квантовой криптографии всегда исходят из консервативных посылок. Считается, что легитимные пользователи ограничены существующим технологическим уровнем, а действия подслушивателя, кроме законов природы, ничем не лимитируются. Одна из проблем квантовой криптографии с реальными, а не идеальными устройствами, связана с тем, что возникает ограничение на длину канала связи. Одной из основных задач теории является разработка способов передачи ключей и доказательство их секретности, которые обеспечивают максимально возможную дальность передачи.

При перечисленных выше неидеальностях системы длина канала связи ограничивается так называемой PNS-атакой подслушивателя (Photon Number Splitting) [7–9]. Данная атака при наличии потерь в канале связи сводится к следующему. Сильно ослабленное лазерное излучение представляет собой когерентное состояние $|\alpha\rangle$ со средним числом фотонов $\mu = |\alpha|^2$ (α – комплексное число, параметризующее когерентное состояние). Комплексный параметр может быть представлен в виде $\alpha = \sqrt{\mu}e^{i\varphi}$, где φ – фаза в каждой посылке, которая Алисой[1)] никак не фиксируется и является случайной величиной. Поэтому в канале подслушиватель "видит" статистическую смесь состояний, которая получается усреднением по случайной фазе φ когерентного состояния:

$$\rho_\mu = \int_0^{2\pi} \frac{d\varphi}{2\pi} |\sqrt{\mu}e^{i\varphi}\rangle\langle\sqrt{\mu}e^{i\varphi}| = e^{-\mu} \bigoplus_{n=1}^{\infty} \frac{\mu^n}{n!} |n\rangle\langle n|. \quad (1)$$

Подслушиватель может неразрушающим измерением определить число фотонов в канале связи, но не их состояние, в каждой посылке. Такие измерения не запрещаются законами квантовой механики. Если обнаружено однофотонное состояние, то такая посылка блокируется. Если обнаружено многофотонное состояние $|n\rangle$ ($n > 1$), то часть фотонов Ева отводит себе и сохраняет в квантовой памяти, а остальной

[1)] Обычно передающую сторону называют Алисой, приемную – Бобом, а подслушивателя – Евой.

ные направляет к Бобу на приемную сторону. После передачи всей серии состояний происходит раскрытие базисов Алисой и Бобом. После этой стадии Ева измеряет свои состояния в квантовой памяти в уже известном базисе и узнает каждый бит ключа. Очевидно, что если затухание таково, что Ева может блокировать все однофотонные посылки, то с этой критической величины потерь в канале связи Ева будет знать весь переданный ключ, не производя ошибок на приемной стороне. Ясно, что критическая длина, до которой можно передавать ключи при данном среднем числе фотонов μ, не может превышать $L_c = -\frac{10}{\alpha}\log_{10}\left(1 - \frac{\mu e^{-\mu}}{1-e^{-\mu}}\right)$ (при $\mu = 0.1$, $L_c \approx 60$ км). Критическая длина определяется фактически условием, когда доля однофотонной компоненты в состоянии (1) становится равной потерям в канале связи. С учетом квантовой эффективности и темновых шумов фотодетекторов она оказывается меньше [10].

Такое ограничение на длину канала связи фактически связано с тем, что существующие лавинные фотодетекторы не различают число фотонов, а атака Евы не изменяет общего числа посылок, достигающих приемной стороны. Стратегия изменяет относительную долю однофотонных и многофотонных посылок. Даже если бы фотодетекторы на приемной станции различали число фотонов, то все равно подслушиватель мог бы остаться недетектируемым. Поскольку Ева может сохранить относительные доли однофотонной и многофотонных посылок такими же, как в исходном состоянии, набирая однофотонную, двух, трех и т.д. компоненты из многофотонных с $n > 1$ таким образом, чтобы относительная доля на приемной стороне была такая же, как и в исходном невозмущенном состоянии.

Для преодоления данной трудности и увеличения критической длины квантового канала связи был предложен метод имитирующих состояний (decoy state) [11]. Алиса, кроме исходного состояния, посылает случайным образом имитирующее когерентное состояние, которое отличается от исходного только средним числом фотонов. В этом случае матрица плотности, которую "видит" Ева в канале связи, выглядит как

$$\rho = G\rho_\mu + (1-G)\rho_{\mu'} = \\ = \bigoplus_{n=1}^{\infty}\left(\frac{Ge^{-\mu}\mu^n + (1-G)e^{-\mu'}\mu'^n}{n!}\right)|n\rangle\langle n|, \qquad (2)$$

где G и $1-G$ – относительные доли посылок информационного и имитирующего состояний. Поскольку матрицы плотности ρ_μ и $\rho_{\mu'}$ некоммутируют, то *в принципе* не существует измерений, которые бы позволили достоверно отличить одно состояние от другого. Любое измерение, которое различает, пусть даже недостоверно с некоторой вероятностью ошибки, эти состояния, приводит к их возмущению [12]. Это означает, что описанные выше атаки будут неизбежно приводить к возмущению распределения вероятностей по числам заполнения. Возмущение состояний гарантируется фундаментальными ограничениями квантовой механики на различимость некоммутирующих наблюдаемых ρ_μ и $\rho_{\mu'}$. После передачи всей серии Алиса раскрывает те посылки, в которых посылалось контрольное имитирующее состояние $\rho_{\mu'}$. Боб проверяет отклонение распределений по числу фотонов от эталонного. Таким образом, детектирование попыток подслушивания происходит не только по вероятности ошибки Q в первичных ключах, но и по отклонению распределений по числу фотонов. Дальнейшая задача легитимных пользователей состоит в том, чтобы найти верхнюю границу количества информации у Евы при наблюдаемых на приемной стороне совокупности параметров $\{\tilde{p}_n(\mu'), Q\}$ ($\tilde{p}_n(\mu')$ – вероятности распределения по числу фотонов).

В полном объеме данная задача до сих пор не решена, имеются лишь частичные результаты. Неизвестна даже максимальная длина канала связи, на которую можно рассчитывать при передаче ключей с использованием данного метода. Ниже будет получена верхняя граница длины линии связи, на которую можно передавать ключи и гарантировать их секретность.

Общая идея получения предельной длины линии связи в методе имитирующих состояний для протокола BB84 состоит в следующем. Ясно, что если "запретить" Еве атаки, которые приводят к изменению статистики распределения по числу фотонов по сравнению с исходным, то полученная при этом длина линии связи будет заведомо больше, чем для случая, когда атаки с изменением распределения по числу фотонов будут разрешены. Иначе говоря, это означает, что если обнаружено отклонение распределений $\{\tilde{p}_n(\mu')\}$ от эталонных, то протокол прерывается легитимными пользователями. По существу, это запрещает Еве производить какие бы ни было манипуляции с числом фотонов. В этом случае Еве остаются только стратегии, которые сводятся к тому, чтобы извлечь максимум информации при наблюдаемой ошибке Q на приемной стороне и неизменных числах заполнения фотонных состояний по сравнению с исходными.

Обсудим кратко, как можно регистрировать изменение статистики по числу фотонов с использованием стандартных лавинных фотодетекторов[2)].

На рис.1 приведена схема, поясняющая идею. Вместо обычно используемой пары фотодетекторов

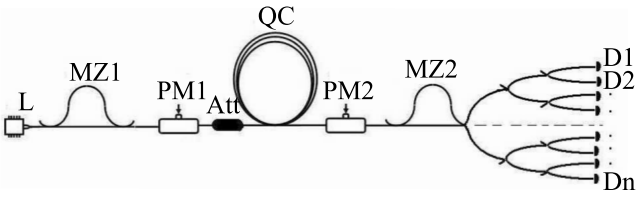

Рис.1. Схема для определения изменения статистики по числу фотонов: L – лазер; MZ1, MZ2 – инферферометры Маха-Цандера на передающей и приемной станциях; PM1, PM2 – фазовые модуляторы, Att – аттенюатор; QC – квантовый канал связи; D1, D2,...Dn – лавинные фотодетекторы

при оптоволоконной реализации протокола BB84, применяется n фотодетекторов. Увеличение числа каналов регистрации производится при помощи симметричных светоделителей (рис.1). Такая схема позволяет "разбить" m-фотонное состояние на суперпозицию n-состояний перед их детектированием:

$$|m\rangle \to \left(\frac{1}{2^{\frac{n}{2}}}\right)(|x_1\rangle + |x_2\rangle + \ldots + |x_n\rangle)^{\otimes m}, \qquad (3)$$

где $|x_i\rangle$ – состояние в i-м канале регистрации. Вероятности срабатывания одного, двух, трех, ..., n фотодетекторов равны

$$\sum_{i=j}^{n} \tilde{q}_i(\mu') C_n^{i,j} = \tilde{p}_j(\mu'), \quad i,j = 1,2... \qquad (4)$$

Здесь $\tilde{q}_i(\mu')$ и $\tilde{p}_j(\mu')$ – наблюдаемые распределения.

Вероятность срабатывания k фотодетекторов из полного числа n $(1 \le k \le n)$ от m-фотонной компоненты равна

$$C_n^{m,k} = \sum_{\substack{l_1+l_2+\ldots+l_n=m \\ \chi(l_1)+\chi(l_2)+\ldots+\chi(l_n)=k}} \begin{pmatrix} m \\ l_1 l_2 \ldots l_n \end{pmatrix},$$

$$\begin{pmatrix} m \\ l_1 l_2 \ldots l_n \end{pmatrix} = \frac{m!}{l_1! \cdot l_2! \ldots l_n!}, \qquad (5)$$

здесь $\chi(l_i)$ – характеристическая функция ($\chi(l) = 0$, если $l = 0$, и $\chi(l) = 1$, если $l \ge 1$). Далее, эталонные распределения

$$p_j(\mu') = \sum_{i=j}^{n} q_i(\mu') C_n^{i,j},$$

$$q_i(\mu') = e^{-\mu'} \sum_{m=i}^{\infty} \frac{\mu'^m}{m!} \begin{pmatrix} m \\ i \end{pmatrix} \Gamma^i, \quad \Gamma = 10^{-\alpha L/10}. \qquad (6)$$

Второе выражение в (6) представляет собой вероятность (эталонную) присутствия i-фотонной компоненты от когерентного состояния на приемной стороне после прохождения через канал связи с линейным затуханием α. Сравнение наблюдаемых распределений (4) с эталонными (6) позволяет обнаружить вторжения в канал связи. Формально в когерентном состоянии присутствуют многофотонные компоненты с любыми n, однако из-за того, что их вес экспоненциально убывает как $\mu^n/n!$, можно обойтись конечным числом фотодетекторов. При $\mu = 0.1$ вероятность срабатывания фотодетектора от многофотонной компоненты при $n = 4$ уже сравнивается с вероятностью срабатывания за счет темновых отсчетов. Поэтому в реальной ситуации достаточно 4–6 фотодетекторов.

Информационные состояния для 0 и 1 в базисах $+$ и $\times$ имеют обычный вид:

$$|+,0\rangle = \frac{1}{\sqrt{2}}(|1\rangle + |2\rangle), \quad |+,1\rangle = \frac{1}{\sqrt{2}}(|1\rangle - |2\rangle), \qquad (7)$$

$$|\times,0\rangle = \frac{1}{\sqrt{2}}(|1\rangle + i|2\rangle), \quad |\times,1\rangle = \frac{1}{\sqrt{2}}(|1\rangle - i|2\rangle). \qquad (8)$$

Здесь $|1\rangle$ и $|2\rangle$ – базисные локализованные во времени однофотонные состояния. Для соответствующих когерентных состояний Алисы получаем ($b = +, \times$, $i = 0, 1$)

$$\rho_A(b,i) = e^{-\mu} \bigoplus_{n=1}^{\infty} \frac{\mu^n}{n!} \rho_n(b,i),$$
$$\rho_n(b,i) = \left(|b,i\rangle^{\otimes n}\right)\left({}^{\otimes n}\langle b,i|\right). \qquad (9)$$

Невозмущенные состояния на приемной стороне Боба с учетом потерь в канале связи имеют аналогичный (9) вид:

$$\rho_B(b,i) = \bigoplus_{n=1}^{\infty} q_n(\mu) \rho_n(b,i). \qquad (10)$$

Наиболее общая атака Евы, допустимая квантовой механикой, сводится к использованию вспомогательного состояния (ancilla). Взаимодействие вспомогательной системы Евы $|A\rangle$ и передаваемого состояния

[2)] Возможно измерение распределения по числам заполнения фоковских состояний при помощи гомодинного детектирования, однако такой метод требует существенного изменения всей стандартной оптоволоконной системы квантовой криптографии.

описывается унитарным оператором U, который Ева задает по своему усмотрению. После взаимодействия состояние Алисы и ancilla оказываются, вообще говоря, в запутанном (не факторизованном) состоянии. Возмущенное состояние Алисы направляется к Бобу, а ancilla остается у Евы. Симметрия 0 и 1 внутри каждого базиса, и симметрия между базисами $+$ и $\times$ позволяют однозначно параметризовать унитарный оператор для однофотонного состояния одним параметром Q[3)]. Поскольку n-фотонная компонента состояния представляет собой тензорное произведение n идентичных копий однофотонного состояния, для которого унитарный оператор Евы для оптимальной атаки известен, то унитарный оператор для тензорного произведения идентичных однофотонных состояний естественным образом представляется в виде тензорного произведения n копий однофотонных унитарных операторов. Действие унитарного U состояния в базисе $+$ можно представить в виде (см. детали в [6, 13])

$$U(|+,0\rangle \otimes |A\rangle)^{\otimes n} = (|+,0\rangle \otimes |\Phi_0^+\rangle + |+,1\rangle \otimes |\Theta_0^+\rangle)^{\otimes n}, \tag{11}$$

$$U(|+,1\rangle \otimes |A\rangle)^{\otimes n} = (|+,1\rangle \otimes |\Phi_1^+\rangle + |+,0\rangle \otimes |\Theta_1^+\rangle)^{\otimes n}, \tag{12}$$

Параметр Q определяется из следующих соотношений:

$$\begin{gathered} 1-Q = \langle\Phi_0^+|\Phi_0^+\rangle = \langle\Phi_1^+|\Phi_1^+\rangle, \\ Q = \langle\Theta_0^+|\Theta_0^+\rangle = \langle\Theta_1^+|\Theta_1^+\rangle. \end{gathered} \tag{13}$$

Аналогично для состояний в базисе $\times$.

Боб производит измерения и оставляет только те события, которые отвечают фотоотсчетам либо только верхней половине фотодетекторов ("канал" регистрации 0 в базисе $+$, или "канал" регистрации 1 в базисе $\times$), либо только нижней половине фотодетекторов ("канал" регистрации 1 в базисе $+$, или "канал" регистрации 0 в базисе $\times$). События, когда отсчеты имели место как в "верхних", так и в "нижних" фотодетекторах, отбрасываются (см. рис.1). Матрица плотности Боба, с учетом этого, имеет вид

$$\begin{aligned} \rho_B(+,0) = \bigoplus_{n=1}^{\infty} \big(&\overline{q}_n(1-Q,\mu,L)|+,0\rangle^{\otimes n\otimes n}\langle+,0| + \\ &+ \overline{q}_n(Q,\mu,L)|+,1\rangle^{\otimes n\otimes n}\langle+,1|\big), \end{aligned} \tag{14}$$

$$\begin{aligned} \rho_B(+,1) = \bigoplus_{n=1}^{\infty} \big(&\overline{q}_n(1-Q,\mu,L)|+,1\rangle^{\otimes n\otimes n}\langle+,1| + \\ &+ \overline{q}_n(Q,\mu,L)|+,0\rangle^{\otimes n\otimes n}\langle+,0|\big), \end{aligned} \tag{15}$$

где введены обозначения

$$\begin{gathered} q_n(Q,\mu,L) = \sum_{k=n}^{\infty} Q^k e^{-\mu}\frac{\mu^k}{k!}\Gamma^n \begin{pmatrix} n \\ k \end{pmatrix}, \\ q_n(1-Q,\mu,L) = \sum_{k=n}^{\infty} (1-Q)^k e^{-\mu}\frac{\mu^k}{k!}\Gamma^n \begin{pmatrix} n \\ k \end{pmatrix}, \end{gathered} \tag{16}$$

$$\begin{gathered} \Sigma(Q,\mu,L) = \sum_{n=1}^{\infty} \Sigma_n(Q,\mu,L), \\ \Sigma_n(Q,\mu,L) = (q_n(Q,\mu,L) + q_n(1-Q,\mu,L)), \end{gathered} \tag{17}$$

$$\begin{gathered} \overline{q}_n(Q,\mu,L) = \frac{q_n(Q,\mu,L)}{\Sigma(Q,\mu,L)}, \\ \overline{q}_n(1-Q,\mu,L) = \frac{q_n(1-Q,\mu,L)}{\Sigma(Q,\mu,L)}. \end{gathered} \tag{18}$$

Аналогично в базисе $\times$.

Поскольку Ева не может изменять распределение по числам фотонов (иначе протокол будет прерван), то Еве остается единственная возможность атаковать только те состояния, которые достигают приемной стороны Боба. С учетом этого обстоятельства матрица плотности Евы, после измерений Боба, имеет вид

$$\begin{aligned} \rho_E(+,0) = \bigoplus_{n=1}^{\infty} \big(&\overline{q}_n(1-Q,\mu,L)|\Phi_0^+\rangle^{\otimes n\otimes n}\langle\Phi_0^+| + \\ &+ \overline{q}_n(Q,\mu,L)|\Theta_0^+\rangle^{\otimes n\otimes n}\langle\Theta_0^+|\big), \end{aligned} \tag{19}$$

$$\begin{aligned} \rho_E(+,1) = \bigoplus_{n=1}^{\infty} \big(&\overline{q}_n(1-Q,\mu,L)|\Phi_1^+\rangle^{\otimes n\otimes n}\langle\Phi_1^+| + \\ &+ \overline{q}_n(Q,\mu,L)|\Theta_1^+\rangle^{\otimes n\otimes n}\langle\Theta_1^+|\big). \end{aligned} \tag{20}$$

Взаимная информация о ключе между Бобом и Алисой равна

$$\begin{gathered} I_{AB}(\tilde{Q},\mu,L) = 1 - H\left(\tilde{Q}(Q)\right), \\ \tilde{Q}(Q) = \sum_{n=1}^{\infty} \overline{q}_n(Q,\mu,L), \\ H(x) = -x\log x - (1-x)\log(1-x). \end{gathered} \tag{21}$$

Взаимная информация зависит от наблюдаемой ошибки $\tilde{Q}(Q)$, среднего числа фотонов μ и длины канала связи L.

[3)] Атака, приводящая к теоретическому пределу критической ошибки $Q \approx 11\%$ в идеальном случае, может быть построена явно [6].

Взаимная информация Евы о ключе определяется классической пропускной способностью квантового канала связи $\overline{C}$ [14, 15]. Для достижения этой величины Еве требуется квантовая память. С учетом симметрии по базисам получаем

$$\overline{C}(\tilde{Q},\mu,L) = S\left(\frac{\rho_E(+,0)+\rho_E(+,1)}{2}\right) - \\ - \frac{1}{2}(S(\rho_E(+,0)) + S(\rho_E(+,1))), \qquad (22)$$

здесь $S(\rho) = -\mathrm{Tr}\{\rho\log\rho\}$ – энтропия фон Неймана.

Окончательно имеем

$$I_{BE}(\tilde{Q},\mu,L) = \overline{C}(\tilde{Q},\mu,L) = \\ = \sum_{n=1}^{\infty}\Sigma_n(Q,\mu,L)\cdot H\left(\frac{1+(1-2Q)^n}{2}\right). \qquad (23)$$

Отсюда видно, что эффективная ошибка Евы при различении n-фотонной компоненты падает с ростом n как Q^n.

Критическая длина линии связи определяется из уравнения[4)]

$$I_{AB}(\tilde{Q},\mu,L) = I_{BE}(\tilde{Q},\mu,L). \qquad (24)$$

Зависимости взаимных информаций, максимальной длины ключа и наблюдаемой ошибки ($\tilde{Q}$) как функции параметра Q приведены на рис.2.

Пока не учитывались темновые шумы и тот факт, что квантовая эффективность фотодетекторов меньше единицы. Приведем выражения, определяющие критическую ошибку и длину канала связи, до которой возможна передача ключей. Задача может быть решена для n фотодетекторов, но ниже приведем выражения для случая двух фотодетекторов, как это имеет место в стандартной оптоволоконной реализации протокола BB84. В этом случае выражение для ошибки на приемной стороне принимает вид[5)]

$$\tilde{Q}(Q) = \frac{\eta\cdot\left(\sum_{n=1}^{\infty}\overline{q}_n(Q,\mu,L)\right) + p_{\mathrm{dark}}}{\eta\cdot\Sigma(Q,\mu,L) + 2p_{\mathrm{dark}}}, \qquad (25)$$

где η, p_{dark} – квантовая эффективность фотодетекторов и вероятность темновых отсчетов во временном окне стробирования, которые считаем одинаковыми для двух фотодетекторов.

[4)] В случае строго однофотонного источника ($q_1 = 1$, $q_n = 0$ при $n > 1$) получается известное уравнение $(1 - 2H(Q) = 0)$, которое определяет критическую ошибку Q_c для протокола BB84, $Q_c \approx 11\%$. Отметим также, что уравнение (24) подразумевает, что Алиса и Боб исправляют ошибки в первичных ключах при помощи случайных кодов.

[5)] Здесь мы пренебрегаем квадратичными слагаемыми вида $\eta\cdot p_{\mathrm{dark}}$, имеющими второй порядок малости.

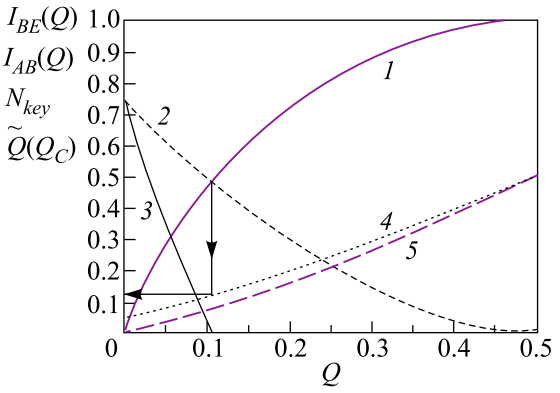

Рис.2. Взаимные информации в пересчете на одну позицию $I_{BE}(\tilde{Q},\mu,L)$ (кривая *1*), $I_{AB}(\tilde{Q},\mu,L)$ (кривая *2*), максимальная длина ключа $N_{\mathrm{key}}(\tilde{Q},\mu,L) = I_{AB}(\tilde{Q},\mu,L) - I_{BE}(\tilde{Q},\mu,L)$ (кривая *3*) и наблюдаемая ошибка на приемной стороне $\tilde{Q}(Q)$ как функции параметра Q (кривые *4* – $p_{\mathrm{dark}} = 1\cdot10^{-5}$ и *5* – $p_{\mathrm{dark}} = 0$). Длина линии связи $L = 150$ км, $\mu = 0.5$, $\eta = 0.4$. Критическая ошибка находится путем определения точки Q, где $I_{AB}(\tilde{Q},\mu,L) = I_{BE}(\tilde{Q},\mu,L)$, а затем по этому значению вычисляется реально наблюдаемая ошибка $\tilde{Q}(Q_c)$. Такое графическое вычисление показано линиями со стрелками

Взаимная информация $I_{AB}(\tilde{Q},\mu,L)$ имеет такое же выражение, как и (21), только в аргумент входит выражение для наблюдаемой ошибки (25).

Информация Евы о ключе принимает вид

$$I_{BE}(\tilde{Q},\mu,L) = \\ = \sum_{n=1}^{\infty}\left(\frac{\eta\cdot\Sigma_n(Q,\mu,L) + 2p_{\mathrm{dark}}\frac{\Sigma_n(Q,\mu,L)}{\Sigma(Q,\mu,L)}}{\eta\cdot\Sigma(Q,\mu,L) + 2p_{\mathrm{dark}}}\right)\times \\ \times H\left(\frac{1+(1-2Q)^n}{2}\right). \qquad (26)$$

На рис.3 приведены зависимости максимально возможной длины ключа и наблюдаемой ошибки $\tilde{Q}$ на приемной стороне как функции длины квантового канала связи L. Допустимая длина линии связи при вероятности темновых отсчетов $p_{\mathrm{dark}} = 1\cdot10^{-5}$ отсч./строб находится в пределах 150–210 км (рис.3a). Данная величина вероятности темновых отсчетов является типичной для лавинных фотодетекторов при их охлаждении до $-40\,^{\circ}\mathrm{C}$ – $-60\,^{\circ}\mathrm{C}$. При вероятности темновых отсчетов $p_{\mathrm{dark}} = 1\cdot10^{-7}$ отсч./строб критическая длина линии связи может уже достигать 250–300 км (рис.3b). Такие вероятности темновых отсчетов достигаются при охлаждении лавинных фотодетекторов до азотных температур. И, наконец, вероятности темновых отсчетов (в пересчете на время длительности строба) $p_{\mathrm{dark}} = 1\cdot10^{-13}$ отсч./строб достигаются на сегодняшний день для сверхпроводящих фотодетекторов (см. подроб-

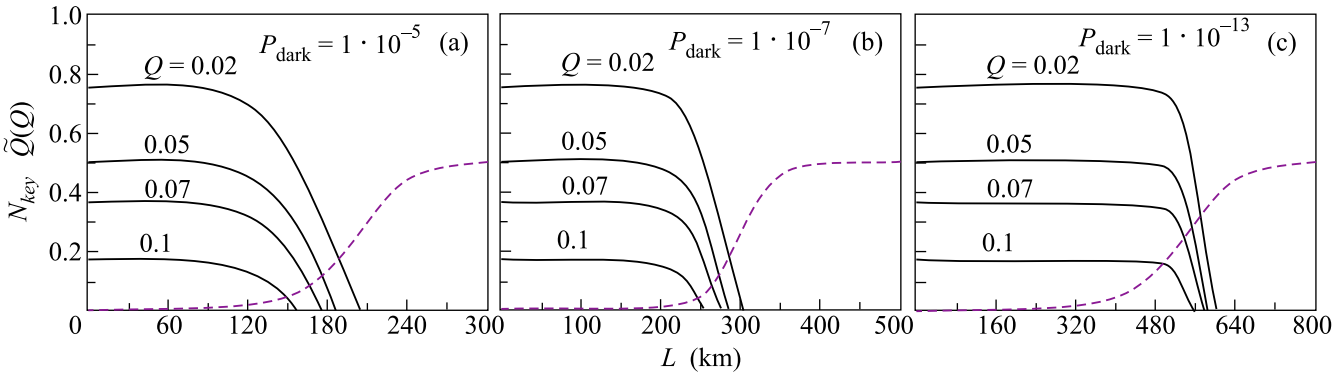

Рис.3. Максимальная длина ключа в пересчете на одну позицию $N_{\text{key}}(\tilde{Q}, \mu, L) = I_{AB}(\tilde{Q}, \mu, L) - I_{BE}(\tilde{Q}, \mu, L)$ как функция длины L при разных значениях параметра Q. Среднее число фотонов $\mu = 0.5$ и одинаково для всех графиков. Пунктирная кривая соответствует наблюдаемой величине ошибки $\tilde{Q}(Q)$, вычисленной по формуле (25)

ности в [16]). В этом случае достижимая критическая длина канала связи может превышать 500 км (рис.3c).

Таким образом, контроль изменений статистики неоднофотонного источника позволяет увеличить длину линии связи, до которой можно передавать ключи и гарантировать их секретность, в несколько раз по сравнению со случаем, когда такой контроль не используется. Полное доказательство стойкости данного метода не может быть получено в отрыве от экспериментальной процедуры, которая используется для контроля изменения статистики по числу фотонов. Трудность таких доказательств состоит в том, что в любой экспериментальной процедуре измеряются отклонения не непосредственно от самих распределений по числу фотонов, а некоторые их интегральные характеристики. Здесь была получена верхняя граница длины, на которую вообще можно рассчитывать в методе с имитирующими состояниями. Отметим, что данная граница принципиально достижима, если контролировать на приемной стороне не только сохранение общего числа регистрируемых посылок, но и изменение распределения вероятностей по числу фотонов. Верхняя граница достигается, если "запрещать" атаки Евы, которые приводят к изменению распределения вероятностей по числу фотонов. "Запрещать" – означает, что протокол прерывается легитимными пользователями, если такое отклонение обнаружено. Такой "запрет" на атаки Евы, связанные с изменением распределения вероятностей по числу фотонов, сильно ограничивает ее действия, оставляя возможность только унитарной атаки на передаваемые состояния, аналогично однофотонному случаю.

Выражаю благодарность Академии Криптографии РФ за поддержку. Работа частично поддержана проектом Российского фонда фундаментальных исследований. Выражаю также благодарность С.П. Кулику за обсуждения, а также неизвестному рецензенту, замечания которого позволили устранить недостатки и неточности в исходном варианте работы.

1. C. H. Bennett and G. Brassard, *Proc.of IEEE Int. Conf. on Comput. Sys. and Sign. Proces.*, Bangalore, India, December 1984, p. 175.
2. D. Mayers, arXiv:quant-ph/9802025.
3. E. Biham, M. Boyer, P. O. Boykin et al., arXiv:quant-ph/9912053.
4. P. W. Shor and J. Preskill, arXiv:quant-ph/0003004.
5. S. Watanabe, R. Matsumoto, and T. Uyematsu, arXiv:quant-ph/0412070.
6. С. Н. Молотков, А. В. Тимофеев, Письма в ЖЭТФ **85**, 632 (2007).
7. G. Brassard, N. Lütkenhaus, T. Mor, and B. Sanders, Phys. Rev. Lett., **85**, 1330 (2000).
8. N. Lütkenhaus, Phys. Rev. A **61**, 052304 (2000).
9. H. Inamori, N. Lütkenhaus, and D. Mayers, arXiv:quant-ph/0107017.
10. С. Н. Молотков, ЖЭТФ (2008, в печати).
11. W.-Y. Hwang, Phys. Rev. Lett. **91**, 057901-1 (2003).
12. C. H. Bennett, Phys. Rev. Lett. **68**, 3121 (1992).
13. C. A. Fuchs, N. Gisin, R. Griffiths et al., Phys. Rev. A **56**, 1163 (1997).
14. А. С. Холево, *Введение в квантовую теорию информации*, серия *Современная математическая физика*, вып.5, М.: МЦНМО, 2002; Успехи математических наук **53**, 193 (1998).
15. B. Schumacher and M. D. Westmoreland, Phys. Rev. A **56**, 131 (1997).
16. Book of Abstracts, *Single-Photon Workshop 2007, Source, Detectors, Applications and Measurements Methods*, 25–28 September 2007, INRIM, Torino, Italy.