Письма в ЖЭТФ, том 88, вып. 4, с. 315 – 320 © 2008 г. 25 августа

О стойкости квантового распределения ключей с фазово-временным кодированием при больших длинах линии связи

С. Н. Молотков

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

Академия Криптографии РФ, 119899 Москва, Россия

Факультет вычислительной математики и кибернетики, МГУ им. М.В. Ломоносова, 119899 Москва, Россия

Поступила в редакцию 15 мая 2008 г.

После переработки 7 июля 2008 г.

Проанализирована криптографическая стойкость квантового протокола распределения ключей с фазово-временным кодированием для случая не строго однофотонного источника и канала связи с потерями. Показано, что при больших длинах линии связи информация подслушивателя о ключе определяется лишь энтропией фон Неймана источника на передающей стороне, а критическая длина линии связи определяется в основном темновыми отсчетами фотодетекторов.

PACS: 03.65.Hk, 03.67.Dd

Неидеальность систем квантовой криптографии (неоднофотонность источника, затухание в канале связи, собственные шумы и не 100%-ная квантовая эффективность фотодетекторов) приводит к тому, что невозможно передавать ключи и гарантировать их безусловную секретность[1)], если длина линии превышает некоторую критическую величину. Критическая длина зависит от используемого протокола распределения ключей.

Ограничение на длину линии связи связано с так называемой PNS-атакой (Photon Number Splitting) [1]. Применительно к одному из основных протоколов распределения ключей BB84 [2] PNS-атака сводится к следующему [1]. Подслушиватель (Ева) определяет неразрушающим образом число фотонов в каждой посылке, но не их состояние. На такие измерения не существует принципиальных запретов в квантовой механике. Если обнаружен один фотон, то посылка блокируется. Если обнаружено два и более фотонов, то один из фотонов Ева направляет через свой канал с меньшим затуханием (в идеале без затухания) на приемную сторону к Бобу, а остальные сохраняет в квантовой памяти и ждет стадии раскрытия базисов. При длине линии выше критической, соответственно потерях в линии, Ева может блокировать все однофотонные посылки, из-за которых она производит ошибки на приемной стороне, и остаться незамеченной. После раскрытия базисов Ева измеряет состояния в своей квантовой памяти уже в известном базисе. Поскольку в каждом базисе в протоколе BB84 состояния ортогональны, то при известном базисе Ева достоверно узнает каждый передаваемый бит и не производит ошибок на приемной стороне. Таким образом, для достоверного знания каждого бита ключа Еве достаточно двухфотонной компоненты. Критическая длина линии связи, до которой можно передавать ключи, фактически определяется из того условия, что вероятность потери фотона в линии равна вероятности (доле) однофотонной компоненты в передаваемых квантовых состояниях.

PNS-атака не меняет общего числа посылок, достигающих приемной стороны, но меняет распределение вероятностей по числам заполнения фотонов. Существующие на сегодняшний день лавинные фотодетекторы не различают числа фотонов, поэтому для обнаружения изменения распределения по числу фотонов требуется существенная модификация как протокола передачи ключей, так и самой системы[2)].

Второй путь “нейтрализации” PNS-атаки состоит в использовании протоколов, стойких относительно такой атаки. Слабость протокола BB84 относительно PNS-атаки, как видно из рассуждений, приведенных выше, состоит в том, что состояния внутри каждого

[1)] Под безусловной секретностью понимается секретность, основанная только на фундаментальных законах природы, то есть считается, что подслушиватель не ограничен никакими техническими ресурсами.

[2)] Ниже считаем, что на приемной стороне используются обычные лавинные фотодетекторы не различающие числа фотонов.

базиса ортогональны. Поэтому естественный способ видоизменения протокола состоит в том, чтобы сделать состояния внутри базисов неортогональными, соответственно, достоверно неразличимыми. Такая модификация была предложена в [3]. Оказывается, что в этом случае для достоверного знания каждого бита Еве достаточно трехфотонной компоненты (см. детали в [3]). Поэтому протокол секретен до тех пор, пока длина канала связи и потери в нем не превышают такой величины, что Ева может блокировать все одно- и двухфотонные посылки. В полном объеме стойкость подобного протокола не проанализирована.

Ранее в [4] был предложен протокол распределения ключей с фазово-временным кодированием для однофотонного источника[3]. Этот протокол не требует сколько-нибудь заметной модификации самой системы и имеет наибольшую критическую ошибку, до которой можно передавать ключи в однофотонном режиме. В данной работе сделан анализ стойкости данного протокола для случая, когда квантовые состояния не являются строго однофотонными, а представляют собой ослабленное лазерное излучение.

Оказывается, что для получения достоверной информации о каждом бите ключа Еве необходима, как минимум, пятифотонная компонента. Поэтому длина линии связи и потери должны быть таковы, чтобы Ева могла блокировать все одно-, двух-, трех-, четырех- и почти все пятифотонные посылки, чтобы знать каждый бит ключа достоверно. Однако при учете темновых отсчетов фотодетекторов на приемной стороне оказывается, что Ева не имеет возможности для PNS-атаки, поскольку для данного протокола длина линии связи, начиная с которой PNS-атака становится эффективной, больше, чем длина, на которой определяющую роль начинают играть темновые отсчеты, которые фактически и лимитируют длину линии связи.

Будет показано, что при $L_1 < L < L_5$ (L_1, L_5 – длины, начиная с которых Ева может блокировать все посылки вплоть до пятифотонных) критическая длина линии связи в этом диапазоне определяется лишь темновыми отсчетами на приемной стороне и энтропией фон Неймана источника квантовых состояний на передающей стороне.

Однофотонные информационные состояния в протоколе с фазово-временным кодированием (см. детали в [4]) в базисах $+, L$, $\times, L$ имеют вид

$$|0,+L\rangle = \cos\left(\frac{\alpha}{2}\right)|1\rangle + \sin\left(\frac{\alpha}{2}\right)|2\rangle,$$
$$|1,+L\rangle = \cos\left(\frac{\alpha}{2}\right)|1\rangle - \sin\left(\frac{\alpha}{2}\right)|2\rangle, \quad (1)$$

$$|0,\times L\rangle = -\sin\left(\frac{\alpha}{2}\right)|1\rangle + \cos\left(\frac{\alpha}{2}\right)|2\rangle,$$
$$|1,\times L\rangle = \sin\left(\frac{\alpha}{2}\right)|1\rangle + \cos\left(\frac{\alpha}{2}\right)|2\rangle, \quad (2)$$

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

$$|0,+R\rangle = \cos\left(\frac{\alpha}{2}\right)|2\rangle + \sin\left(\frac{\alpha}{2}\right)|3\rangle,$$
$$|1,+R\rangle = \cos\left(\frac{\alpha}{2}\right)|2\rangle - \sin\left(\frac{\alpha}{2}\right)|3\rangle, \quad (3)$$

$$|0,\times R\rangle = -\sin\left(\frac{\alpha}{2}\right)|2\rangle + \cos\left(\frac{\alpha}{2}\right)|3\rangle,$$
$$|1,\times R\rangle = \sin\left(\frac{\alpha}{2}\right)|2\rangle + \cos\left(\frac{\alpha}{2}\right)|3\rangle. \quad (4)$$

Здесь $|i\rangle$ – $i = 1, 2, 3$ – локализованные состояния во временных слотах 1,2,3, которые сдвинуты по времени на одинаковую величину, см. детали в [4].

Аналогично [3], выберем состояния внутри базисов L и R неортогональными $\langle 0+L|1+L\rangle = -\langle 0\times \times L|1\times L\rangle = \cos(\alpha)$, как в протоколе B92, а между базисами $+L$ и $\times L$ ($+R$ и $\times R$) частично ортогональны $\langle 0+L|0\times L\rangle = \langle 1+L|1\times L\rangle = 0$ ($\langle 0+R|0\times R\rangle = = \langle 1+R|1\times R\rangle = 0$). Аналогично и в базисе R. Информационные неоднофотонные состояния получаются ослаблением когерентного состояния. Поскольку от посылки к посылке относительная фаза в состояниях не фиксирована, то подслушиватель "видит" в канале связи усредненное по фазе когерентное состояние

$$\rho_A(i,b) = \bigoplus_{k=0}^{\infty} p_k(|i,b\rangle^{\otimes k})(^{\otimes k}\langle i,b|), \quad p_k = \frac{\mu^k}{k!},$$
$$i = 0,1, \quad b = +L, \times L, +R, \times R, \quad (5)$$

где μ – среднее число фотонов в когерентном состоянии. Рассмотрение ниже годится и для источника с произвольным распределением по числу фотонов, а не только когерентного состояния.

Перейдем теперь к измерениям на приемной стороне. Боб случайно и равновероятно выбирает измерения в одном из двух базисов. Формально измере-

[3] В определенных условиях критическая ошибка может достигать величины в 50% [4].

ния описываются следующими разложениями единицы:

$$I = A_{0,b} + A_{1,b} + A_{?,b}, \quad A_{0,b} = \frac{I - |1,b\rangle\langle 1,b|}{1 + |\langle 0,b|1,b\rangle|},$$
$$A_{1,b} = \frac{I - |0,b\rangle\langle 0,b|}{1 + |\langle 0,b|1,b\rangle|}, \quad A_{?,b} = I - A_{0,b} - A_{1,b}. \tag{6}$$

Измерения аналогичны измерениям в протоколе B92. Измерения (6) обладают тем свойством, что ненулевой результат в "канале" $A_{0,b}$ возникает только от состояния $|0,b\rangle$, и никогда от состояния $|1,b\rangle$. Аналогично для исходов в "канале" $A_{1,b}$. Отсчеты в "канале" $A_{?,b}$ отвечают результатам с неопределенным исходом, такие отсчеты отбрасываются. Вероятность отсчетов с определенным исходом есть

$$\Pr\{|0,b\rangle\langle 0,b|A_{0,b}\} = \Pr\{|1,b\rangle\langle 1,b|A_{1,b}\} = 1 - \cos(\eta). \tag{7}$$

После отбрасывания результатов с неопределенным исходом информация Боба в битах в пересчете на одну оставленную позицию составляет $I(A;B) = 1$ (при идеальных фотодетекторах). Учтем теперь неидеальность фотодетекторов.

С учетом потерь вероятность достижения информационными состояниями приемной стороны есть

$$p_{\text{detect}} = (1 - e^{-\mu} - (e^{-\mu\Gamma} - e^{-\mu}))(1 - \cos(\alpha)). \tag{8}$$

Данная величина равна доле непустых посылок. Все лавинные фотодетекторы в телекомуникационном диапазоне длин волн 1.3–1.55 мкм работают в стробируемом режиме. Фотодетектор активируется посредством подачи короткого импульса напряжения длительности 1–2 нс в момент возможного прихода информационного состояния. Темновые отсчеты с определенной вероятностью имеют место в момент стробирования независимо от прихода состояния.

Пусть квантовые эффективности фотодетекторов равны η_0 и η_1. С учетом (8) вероятность детектирования информационных состояний 0 и 1 в окне стробирования равна $\eta_{0,1}(L) = \frac{1}{2} p_{\text{detect}} \eta_{0,1}$. Темновые отсчеты возникают только в моменты стробирования, вероятность темнового отсчета во временном окне строба есть $p_{d0}^{(0)}$ и $p_{\text{dark}}^{(1)}$.

Фотоотсчеты в детекторах $\overline{D}_0$ и $\overline{D}_1$ можно разбить на следующие множества (рис.1). A_0 и A_1 – множества отсчетов от информационных состояний. D_0 и D_1 – множества темновых отсчетов соответственно в детекторе $\overline{D}_0$ и $\overline{D}_1$. Напомним, что оба детектора стробируются одновременно, поэтому темновые отсчеты могут иметь место одновременно (в одном и том же стробе) в двух фотодетекторах. A_1 – множество одновременных отсчетов *только* от информационных состояний A_0 и темновых отсчетов D_0 (аналогично для множества A_7). A_2 – множество одновременных отсчетов *только* от информационных состояний A_0 и темновых отсчетов в детекторе D_1 (аналогично для A_5). A_3 – множество одновременных отсчетов от A_0, D_0 и D_1. Аналогично для множества отсчетов A_6. A_4 – множество одновременных отсчетов *только* от D_0 и D_1. Множества A_0 и A_1 не пересекаются, поскольку Алиса посылает либо 0, либо 1.

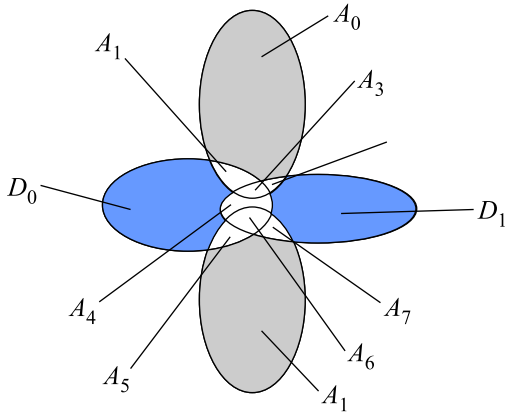

Рис.1. Различные множества событий фотоотсчетов

Одновременные события в одном временном стробе в одном детекторе от информационного состояния и темнового шума воспринимаются как один фотоотсчет. Одновременные фотоотсчеты в двух детекторах в одном временном стробе отбрасываются.

Вероятность отсчета от информационных состояний 0 и 1 равна

$$\Pr\{\text{info}\} = \Pr\{\mathrm{A_0} + \mathrm{A_1} - \mathrm{A_0} \cap \mathrm{D_1} - \mathrm{A_1} \cap \mathrm{D_0}\} = \\ = \eta_0(L) + \eta_1(L) - \eta_0(L) p_{\text{dark}}^{(0)} - \eta_1(L) p_{\text{dark}}^{(1)}. \tag{9}$$

Вероятность исходов только от темновых отсчетов равна (напомним, что одновременные отсчеты в двух детекторах отбрасываются)

$$\Pr\{\text{dark}\} =$$

$$= \Pr\{D_0 + D_1 - 2(D_0 \cap D_1 -$$

$$- A_0 \cap D_0 \cap D_1 - A_1 \cap D_0 \cap D_1) -$$

$$-(A_0 \cap D_0 - A_0 \cap D_0 \cap D_1) - (A_1 \cap D_0 - A_1 \cap D_0 \cap D_1) -$$

$$-(A_1 \cap D_1 - A_1 \cap D_0 \cap D_1) - (A_0 \cap D_1 - A_0 \cap D_0 \cap D_1)\} =$$

$$= p_{\rm dark}^{(0)} + p_{\rm dark}^{(1)} - (\eta_0(L) + \eta_1(L))(p_{\rm dark}^{(0)} + p_{\rm dark}^{(1)}) +$$

$$+4(\eta_0(L) + \eta_1(L))p_{\rm dark}^{(0)} p_{\rm dark}^{(1)} - 2p_{\rm dark}^{(0)} p_{\rm dark}^{(1)}. \qquad (10)$$

Поскольку состояния, отвечающие 0 и 1, посылаются равновероятно, то только половина из каждого непересекающегося множества темновых отсчетов будет давать правильные отсчеты. Другая половина отсчетов будет ошибочной. Для вероятности ошибки на приемной стороне у Боба имеем

$$Q(L) = \frac{\frac{1}{2}\Pr\{\text{dark}\}}{\Pr\{\text{info}\} + \Pr\{\text{dark}\}}. \qquad (11)$$

Ошибка принимает особенно простое выражение при $\eta_0(L) = \eta_1(L) = \eta(L)$, $p_{\rm dark}^{(0)} = p_{\rm dark}^{(1)} = p_{\rm dark}$. С точностью до линейных членов по $\eta(L)$, $p_{\rm dark}$, имеем

$$Q(L) = \frac{\frac{1}{2}p_{\rm dark}}{\eta(L) + p_{\rm dark}}. \qquad (12)$$

Взаимная информация между Алисой и Бобом после исправления ошибок случайными кодами не превышает пропускной способности классического симметричного бинарного канала связи с величиной ошибки $Q(L)$. Имеем

$$I(A;B) \le C_{\rm class}(Q) = 1 - H(Q(L)),$$
$$H(x) = -x\log x - (1-x)\log(1-x). \qquad (13)$$

Рассмотрим теперь действия подслушивателя. Поскольку фотодетекторы на приемной стороне не различают число фотонов, то Боб может следить лишь за сохранением общего числа посылок на приемной стороне при известной длине линии связи.

Вероятность потерь – доля посылок, исчезающих в канале связи длины L – есть

$$p_{\rm loss}(L) = \sum_{k=1}^{\infty} p_k(1 - \Gamma(L))^k, \quad \Gamma(L) = 10^{-\frac{\alpha L}{10}}; \qquad (14)$$

здесь $\alpha \approx 0.2$ дБ/км – константа затухания в одномодовом оптоволокне. Для когерентного состояния доля потерянных посылок составляет $p_{\rm loss}(L) = e^{-\mu\Gamma} - e^{-\mu}$ (при $L \to \infty$, $\Gamma(L) \to 0$, $p_{\rm loss}(L) \to 1 - e^{-\mu}$ – исходная общая доля непустых посылок).

Будем рассматривать ситуацию при больших длинах ($L > L_1$ ($p_{\rm loss}(L_1) = p_1$), когда Ева может блокировать все однофотонные посылки,[4)] при атаке на которые она неизбежно производила бы ошибки на приемной стороне. С дальнейшим ростом длины линии подслушиватель может блокировать двух, трех, ..., k-фотонные посылки. Иначе говоря, при длинах $L < L_1 < L < L_2 < L... < L_k...$ Ева может блокировать частично, а начиная с некоторой длины, полностью k-фотонные посылки. Зависимости длин L_k от среднего числа фотонов μ в когерентном состоянии приведены на рис.2.

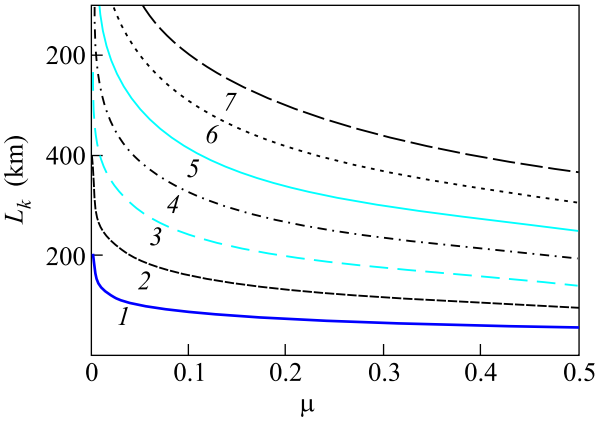

Рис.2. Зависимости длины линии L_k от среднего числа фотонов μ в когерентном состоянии, начиная с которых Ева может блокировать посылки, содержащие k фотонов

Доля оставшихся посылок при длине L, которые Ева не может блокировать и вынуждена сохранить, составляет

$$p_k(L) = p_k(1 - \theta(p_{\rm loss}(k,L))) +$$
$$+ (p_k - p_{\rm loss}(k,L))\theta(p_{\rm loss}(k,L))\theta(p_k - p_{\rm loss}(k,L)); \qquad (15)$$

здесь

$$p_{\rm loss}(k,L) = p_{\rm loss}(L) - \sum_{m=1}^{k-1} p_m.$$

Далее из каждой посылки, содержащей $k > 1$ фотонов, Ева один фотон направляет к Бобу через свой канал связи с меньшими потерями (в предельном случае вообще без потерь), а остальные оставляет у себя в квантовой памяти до процедуры разглашения базисов легитимными пользователями. Однако даже после разглашения базисов из-за неортогональности состояний внутри базиса Ева не будет достоверно знать каждый передаваемый бит[5)].

[4)] Анализ стойкости протокола в однофотонном режиме ($L < L_1$) является наиболее сложным. При длинах, L бóльших L_1, как видно из данного рассмотрения, анализ стойкости существенно упрощается.

[5)] Напомним, что в протоколе BB84, начиная с длины канала $L > L_1$, Ева знает каждый передаваемый бит после разглашения базисов, так как состояния внутри базиса ортого-

При длине линии связи $L > L_1$, после разглашения базисов, Ева имеет в каждой ячейке квантовой памяти состояние

$$\rho_E(0,b)=\bigoplus_{k=2}^{\infty} p_k(L)(|0,b\rangle^{\otimes(k-1)})(^{\otimes(k-1)}\langle 0,b|), \text{ или}$$

$$\rho_E(1,b) = \bigoplus_{k=2}^{\infty} p_k(L)(|1,b\rangle^{\otimes(k-1)})(^{\otimes(k-1)}\langle 1,b|); \tag{16}$$

здесь базис b считается известным.

Количество информации в битах на одну посылку $I(A;E)$, которое может быть получено из ансамбля квантовых состояний (16), ограничено сверху фундаментальной границей Холево, которая является достижимой и совпадает с классической пропускной способностью $\overline{C}(L)$ квантового канала связи между Алисой и Евой с информационными состояниями (16) [5,6]. Имеем

$$I(A;E) \le \overline{C}(L) = \sum_{m=2}^{\infty} \overline{p}_m(L)\overline{C}(\cos^{m-1}(\alpha)); \tag{17}$$

здесь

$$\overline{p}_m(L) = p_m(L)/N(L), \quad N(L) = \sum_{m=2}^{\infty} p_m(L),$$

$$\overline{C}(x) = -\left(\frac{1-x}{2}\right)\log\left(\frac{1-x}{2}\right) - \left(\frac{1+x}{2}\right)\log\left(\frac{1+x}{2}\right), \tag{18}$$

классическая пропускная способность квантового канала связи [5–7]. Из (17), (18) следует, что информация Евы о передаваемом ключе фактически определяется энтропией фон Неймана источника на передающей стороне Алисы, в котором распределение по числам заполнения фотонов сдвинуто на единицу, поскольку один фотон должен быть направлен на приемную сторону к Бобу.

Распространение ключей возможно [7–9], если $I(A;E) < I(A;B)$[6]. Критическая длина линии определяется как корень уравнения $I(A;E) = I(A;B)$, имеем

$$C_{\text{class}}(Q) = \overline{C}(L),$$
$$1 - H(Q(L)) = \sum_{m=2}^{\infty} \overline{p}_m(L)\overline{C}(\cos^{m-1}(\alpha)). \tag{19}$$

нальны. Поэтому данный протокол является более стойким к затуханию и обеспечивает секретность передачи ключей при бóльших длинах линии.

[6] Хорошее физическое обсуждение данного вопроса можно найти в обзоре [7] и монографии [9].

Зависимости взаимных информаций $I(A;E)$ и $I(A;B)$ от длины оптоволоконной линии связи при различной вероятности темновых отсчетов представлены на рис.3. Критическая длина линии связи, до

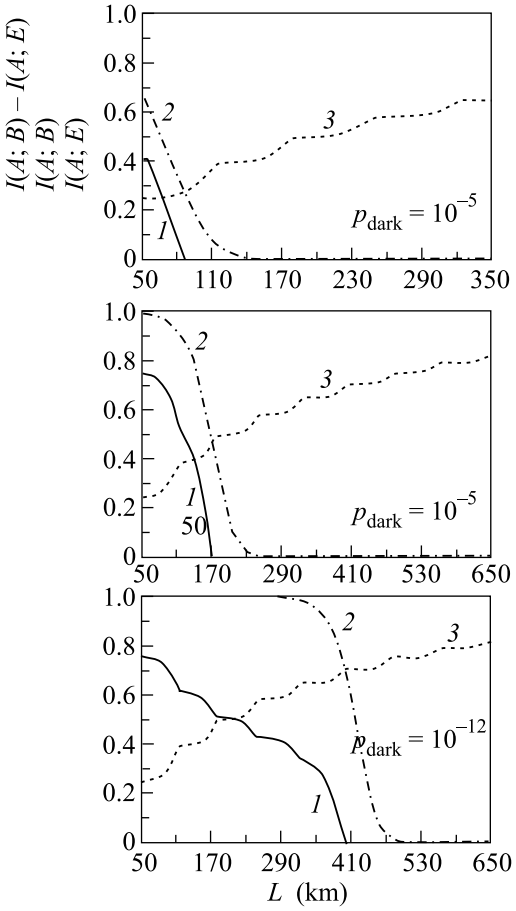

Рис.3. Кривые *1* отвечают зависимостям $I(A;B) - I(A;E)$ от длины линии связи L, кривые *2* – зависимостям $I(A;B)$ и *3* – зависимостям $I(A;E)$. Вероятности темновых отсчетов приведены непосредственно на рисунке. Квантовая эффективность фотодетекторов и среднее число фотонов в когерентном состоянии одинаковы для всех кривых и равны, соответственно, $\eta = 0.1$, $\mu = 0.2$. Угол между состояниями $\alpha = \pi/8$

которой возможно распределение ключей, определяется точкой, где разность $I(A;B) - I(A;E)$ обращается в нуль. Фактически разность $I(A;B) - I(A;E)$ представляет собой количество информации в битах, которое является ключом.

Как следует из рис.1, при вероятности темновых отсчетов $p_{\text{dark}} = 10^{-5}$ отсч/строб, предельная длина линии связи составляет ≈ 80 км. Такой уровень темновых отсчетов является типичным при охлаждении лавинных фотодетекторов до температуры ≈ -50–$60\,^{\circ}$C. При охлаждении до азотных тем-

пературу достижим уровень темновых шумов $p_{\rm dark} = 10^{-7}$ отсч/строб. Предельная длина линии связи в этом случае составляет ≈ 170 км. И, наконец, при вероятности темновых отсчетов[7] $p_{\rm dark} = 10^{-12}$ отсч/строб достижима длина в 400 км. Такой уровень темновых отсчетов достигается в ряде экспериментов для сверхпроводящих детекторов на основе NbN [10].

Сделаем в заключение одно замечание. Описанная выше стратегия дает Еве вероятностную информацию о битах ключа. Ева может в принципе использовать стратегию, которая дает ей достоверную информацию о каждом передаваемом бите. Поскольку имеется 4 базиса, $+L$, $\times L$ и $+R$, $\times R$, и внутри базисов состояния неортогональны, то для того, чтобы получить достоверную информацию, Еве необходима как минимум пятифотонная компонента. Ева использует 4 фотона для измерений, которые аналогичны (6). Пятый фотон направляется к Бобу *только* в том случае, если получен результат с определенным исходом для измерений над всеми четырьмя фотонами (исходы $A_{0,1,+L}$, $A_{0,1,\times L}$ и $A_{0,1,+R}$, $A_{0,1,\times R}$). Это дает возможность Еве после раскрытия базисов однозначно определить передаваемый бит. Если получен результат измерения с неопределенным исходом $A_{?,b}$, хотя бы для одного из четырех фотонов, то посылка блокируется. Вероятность исхода с определенным результатом для четырех фотонов – $(1-\cos(\alpha))^4$ (например, при $\alpha = \pi/8$ эта величина меньше 10^{-4}). Это означает, что Ева должна будет блокировать почти все пятифотонные посылки (долю посылок $> 1 - 10^{-4}$).

Такая стратегия возможна, если длина линии связи превышает $L > L_5$. Однако, как следует из рис.2 и 3 при типичных рабочих значениях среднего числа фотонов в состоянии $\mu = 0.1-0.2$, взаимная информация $I(A;E)$ сравнивается со взаимной информацией $I(A;B)$ при меньших длинах, чем L_5, поэтому данная атака Евы неэффективна. Уже при меньших длинах определяющую роль начинают играть темновые отсчеты, которые, по существу, определяют критическую длину.

Выражаю благодарность Академии криптографии РФ за поддержку. Работа частично поддержана проектом Российского фонда фундаментальных исследований # 08-02-00559. Выражаю также благодарность С.П.Кулику за обсуждения.

1. G. Brassard, N. Lütkenhaus, T. Mor, and B. Sanders, Phys. Rev. Lett. **85**, 1330 (2000); N. Lütkenhaus, Phys. Rev. A **61**, 052304 (2000).
2. C. H. Bennett and G. Brassard, *Quantum Cryptography: Public Key Distribution and Coin Tossing*, Proc.of IEEE Int. Conf. on Comput. Sys. and Sign. Proces., Bangalore, India, December 1984, p.175.
3. A. Acin, N. Gisin, and V. Scarani, arXiv:quant-ph/0302037.
4. С. Н. Молотков, ЖЭТФ **133**, 5 (2008).
5. А. С. Холево, *Введение в квантовую теорию информации*, серия *Современная математическая физика, вып.5*, М.: МЦНМО, 2002; Успехи математических наук **53**, 193 (1998).
6. B. Schumacher and M. D. Westmoreland, Phys. Rev. A **56**, 131 (1997).
7. М. Нильсен, И. Чанг, *Квантовые вычисления и квантовая информация*, М.: Мир, 2006; M. A. Nielsen and I. L. Chuang, *Quantum Computation and Quantum Information*, Cambridge University Press, 2000, 2001.
8. I. Csiszár and J. Körner, IEEE Trns. Inf. Theory, **24**, 339 (1978).
9. N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, quant-ph/0101098.
10. Book of Abstracts, *Single-Photon Workshop 2007, Source, Detectors, Applications and Measurements Methods*, 25–28 September 2007, INRIM, Torino, Italy.

[7] Для сверхпроводящих детекторов не требуется стробирование, поэтому данная величина является вероятностью темновых отсчетов в пересчете на длительность строба.