Письма в ЖЭТФ, том 88, вып. 10, с. 791 – 796

Существует ли фундаментальный предел дальности передачи ключей в квантовой криптографии?

С. Н. Молотков

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

Академия Криптографии Российской Федерации, 121552 Москва, Россия

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

Поступила в редакцию 19 августа 2008 г.

После переработки 30 сентября 2008 г.

Существует ли фундаментальный предел дальности передачи ключей в квантовой криптографии? Существуют ли квантовые протоколы распределения ключей, которые позволяют приблизиться к данному пределу и насколько близко? Ответ на первый вопрос звучит как: и "да", и "нет". Оказывается, что ответить на первый вопрос можно в самом общем виде, не аппелируя к конкретному протоколу квантового распределения ключей и его реализации. Ответ на второй вопрос дается предъявлением конкретного протокола, для которого дальность передачи близка к теоретическому пределу, а достижение данной границы ограничивается уже не самим квантовым протоколом распределения ключей, а нашими возможностями по коррекции ошибок *классическими кодами*.

PACS: 03.67.Dd, 03.65.Hk

Квантовая криптография, или более точно, квантовое распределение криптографических ключей предназначено для передачи ключей между пространственно удаленными пользователями [1]. В дальнейшем ключи могут использоваться в различных системах шифрования или аутентификации. Секретность передаваемых ключей основана не на предполагаемых технических или вычислительных ограничениях подслушивателя, а на фундаментальных законах природы – квантовой механики[1)]. Более точно, секретность ключей базируется на двух фундаментальных запретах квантовой теории: 1) невозможности копирования неизвестного квантового состояния [5]; 2) невозможности достоверного различения неортогональных квантовых состояний [6]. Данные запреты фактически являются следствием соотношений неопределенности Гайзенберга, которые в самой общей формулировке сводятся к известному математическому факту, что пара некоммутирующих эрмитовых операторов не может иметь общей системы собственных векторов.

Расстояние, на которое можно передавать ключи и гарантировать их безусловную секретность, определяется многими факторами и прежде всего неидеальностями системы. Источники квантовых состояний не являются строго однофотонными, детекторы также имеют собственные темновые шумы и не единичную квантовую эффективность, квантовый канал связи имеет потери. Кроме того, дальность определяется и самим квантовым протоколом распределения ключей – алгоритмом действий легитимных пользователей, который определяет информационные квантовые состояния, их приготовление, измерение, интерпретацию результатов измерений, согласование базисов, оценку вероятности ошибок на приемной стороне, коррекцию ошибок через открытый аутентичный классический канал связи, сжатие – усиление секретности "очищенных" ключей.

Доказательство стойкости (секретности) систем квантовой криптографии, с учетом упомянутых факторов, является крайне сложной задачей, которую приходится решать каждый раз заново для каждого квантового протокола распределения ключей и его конкретной технической реализации (см., например, обзоры [7, 8]). В связи с этим возникает вопрос о том, имеются ли принципиальные ограничения на длину передачи секретных ключей?

Важно, что для ответа на вопрос можно не апеллировать к конкретному протоколу квантового распределения ключей, поэтому рассуждения будут годиться для любого протокола в том смысле, что предельная дальность для любого протокола не может превысить данную границу. Нужно подчеркнуть, что данная граница определяется фундаментальными

[1)] Секретность, основанную на фундаментальных законах природы, принято называть безусловной, в отличие от совершенной секретности, основанной на шифровании в режиме одноразового блокнота (one time pad) [2 – 4].

ограничениями на безошибочную передачу информации через неидеальный канал связи. Длина канала, на которую можно передавать информацию с вероятностью ошибки декодирования, стремящейся к нулю в асимптотическом пределе длинных последовательностей, естественно, зависит от физических параметров канала связи (потерь в квантовом канале связи, темновых шумов и квантовой эффективности детекторов). *Причина, по которой в принципе невозможно передать секретный ключ на длину, большую критической при данных физических параметрах канала связи, является фундаментальной и определяется принципиальной невозможностью исправить классические ошибки в битовой последовательности, если длина линии превышает критическую величину.*

Сначала уточним исходные посылки, которые будут использоваться в дальнейшем. Для установления теоретического предела дальности будем считать, что источник квантовых состояний строго однофотонный. Это наилучшая ситуация для легитимных пользователей и наихудшая для подслушивателя. Будем считать, что квантовый канал связи имеет потери с константой затухания α $[db/km]$. Также считаем, что детекторы на приемной стороне неидеальные – имеют квантовую эффективность $\eta \leq 1$ и собственные темновые шумы с вероятностью p_{dark} [counts/gate]. Предельный переход к идеальным детекторам и идеальному каналу связи осуществляется, если положить $\alpha = 0$, $\eta = 1$, $p_{\text{dark}} = 0$.

Доля секретных бит в финальном ключе, согласно [9][2)], определяется как

$$r/n = \min_{\text{all attack}} \{I(A;B) - I(A;E)\}, \quad n \to \infty; \qquad (1)$$

здесь $I(A;B)$ – взаимная информации для легитимных пользователей (Алиса, Боб), $I(A;E)$ – взаимная информация между подслушивателем (Евой) и Алисой. Минимум вычисляется по всевозможным атакам Евы на передаваемый ключ.

Выражение (1) для длины финального секретного ключа r неформально означает следующее. Перед стадией коррекции ошибок Алиса и Боб имеют битовую строку длины n, причем строка Боба содержит ошибки с вероятностью Q. Независимо от квантового протокола распределения ключей, после передачи квантовых состояний и оценки вероятности ошибки легитимным пользователями необходимо исправить ошибки на приемной стороне. На этой стадии протокола легитимные пользователи находятся в ситуации *бинарного классического канала связи с вероятностью ошибки Q.*

Фундаментальный результат классической теории информации (прямая теорема кодирования для канала с шумом) [12–14] гласит, что существует классический код, исправляющий ошибки со "скоростью" R, сколь угодно близкой к $C(Q)$ при достаточно большом n[3)]:

$$R = \frac{k}{n} < C_{\text{class}}(Q) = \\ = 1 - h(Q) = 1 + Q\log Q + (1-Q)\log(1-Q), \qquad (2)$$

где $C_{\text{class}}(Q)$ – пропускная способность бинарного классического канала связи. Причем всегда

$$I(A;B) \leq C_{\text{class}}(Q). \qquad (3)$$

На словах (2), (3) означают, что из последовательности длиной n, содержащей ошибки с вероятностью Q, можно извлечь не более $n \cdot C_{\text{class}}(Q)$ бит, не содержащих ошибок (точнее, с вероятностью ошибки, стремящейся к 0 при $n \to \infty$), если использовать при исправлении ошибок самый оптимальный код с длиной кодового слова n. Иначе говоря, в этом коде может быть не более $k < n \cdot C_{\text{class}}(Q)$ информационных символов, остальные проверочные.

Далее, применительно к квантовой криптографии. Исправление ошибок через открытый канал связи означает, что из n бит для того, чтобы исправить ошибки, Алиса должна выдать через открытый классический канал связи не менее $n-k$ бит проверочной информации. Данная информация доступна Еве и впоследствии должна быть удалена из исходной последовательности длины n. Кроме того, из последовательности длины n необходимо удалить информацию $I(A;E)$, которую Ева получила во время передачи квантовых состояний.

Таким образом, после коррекции ошибок Алиса и Боб имеют идентичные строки бит длины n, строка у Боба уже не содержит ошибок. Однако Еве теперь известно количество информации не менее $n - k + n \cdot I(A;E) = n(1 - C_{\text{class}}(Q) + I(A;E))$. Удаление этой информации у Евы достигается процедурой хэширования (сжатия) последовательности при помощи универсальных хэш-функций второго порядка [15, 16]. Длина r секретного ключа в битах при этом не более

$$n - n(1 - C_{\text{class}}(Q) + I(A;E)) = n(C_{\text{class}}(Q) - I(A;E)) \qquad (4)$$

[2)] Существуют другие более тонкие критерии на длину ключа, см., например [10,11], которые, тем не менее, приводят к тому же окончательному выражению.

[3)] Здесь под "скоростью" ($R = k/n$) кода, как обычно [12–14], понимается отношение числа информационных символов в коде к длине кодового слова.

бит. После данных процедур, как можно показать [16], информация Евы о ключе длиной, определяемой (4), сколь угодно мала.

Критическая длина линии связи определяется из условия обращения в нуль длины ($r = 0$) секретного ключа. Наилучшая ситуация для легитимных пользователей и наихудшая для подслушивателя имеет место, когда $I(A;E) = 0$. Фактически это условие означает, что подслушиватель не получает никакой информации о передаваемом ключе из квантового канала связи. Информацию о битовой строке Алисы и Боба подслушиватель получает только из открытого классического канала связи, выдаваемой легитимными пользователями при коррекции ошибок.

Данное обстоятельство качественно можно понять следующим образом. Алиса и Боб открыто выбирают корректирующий код и оглашают таблицу из 2^k кодовых слов. Длина каждого кодового слова n бит. Поэтому после оглашения таблицы кодовых слов Ева должна выбирать не из пространства 2^n всевозможных битовых строк, а только из пространства битовых строк размером 2^k. Чем лучше код, то есть чем меньше избыточность кода (чем больше k), тем меньшее количество информации легитимные пользователи выдают в открытый канал связи. Исправление ошибок в бинарном канале связи теоретически возможно вплоть до ошибки $Q < 1/2$. Теоретический предел Шеннона дает фактически нижнюю границу избыточности кода при данной ошибке Q, которая необходима, чтобы можно было исправить ошибки со стремящейся к нулю ошибкой декодирования (различения кодовых слов) в асимптотическом пределе длинных последовательностей ($n \to \infty$). При $Q \to 1/2$ число информационных символов $k \to 0$, а контрольных, соответственно, к n.

Проблема состоит в том, что наилучший код известен на уровне теоремы существования. Доказано, что такой код существует, но неизвестно конструктивных и эффективных алгоритмов для явного построения такого кода.

Условие $I(A;E) = 0$ будет давать верхнюю границу длины линии связи для передачи секретных ключей. При условии $I(A;E) = 0$ ошибки на приемной стороне возникают только из-за затухания и неидеальности детекторов[4)].

Далее требуется связать ошибку Q с длиной линии связи. Ошибка на приемной стороне может быть представлена в виде (см. детали по учету темновых отсчетов, например, в [17])

$$Q = \frac{\frac{1}{2}p_{\mathrm{dark}}}{\eta \cdot 10^{-\frac{\alpha \cdot L}{10}} + p_{\mathrm{dark}}}, \qquad (5)$$

здесь L – длина квантового канала связи, $\eta \cdot 10^{-\frac{\alpha \cdot L}{10}}$ – вероятность детектирования информационных квантовых состояний[5)]. При $L \to \infty$, $Q \to 1/2$, то есть на приемной стороне, регистрируются фактически случайные собственные темновые шумы детекторов. При $p_{\mathrm{dark}} = 0$, $Q = 0$ никаких ошибок в принимаемой битовой последовательности нет (даже при квантовой эффективности $\eta < 1$).

Таким образом, легитимные пользователи, по крайней мере теоретически, могут исправить ошибки, вплоть до $Q = 1/2$. Комбинируя (2) и (5), получаем для длины квантового канала связи (для дальнейшего удобно, как это обычно делается, представить $p_{\mathrm{dark}} = 10^{-d}$)

$$L = \frac{10}{\alpha}d + \frac{10}{\alpha}\log_{10}(\eta) - \frac{10}{\alpha}\log_{10}\left(\frac{1-2Q}{2Q}\right). \qquad (6)$$

Зависимости длины передачи ключей от показателя экспоненты вероятности темновых отсчетов приведены на рис.1 при различных значениях критической ошибки Q.

Формула (6) дает зависимость длины передачи ключей от параметров системы. Если бы существовал квантовый протокол распределения ключей с критической ошибкой $Q = 1/2$, то не было бы формальных ограничений на длину передачи ключей. Поскольку даже при неидеальных детекторах и потерях в квантовом канале связи можно *теоретически* достичь любой длины передачи за счет последнего слагаемого, которое стремится к бесконечности при $Q \to 1/2$. Однако данная возможность чисто теоретическая, поскольку если бы был известен квантовый протокол распределения ключей с критической ошибкой $Q = 1/2$, даже в этом случае требуется наличие конструктивно и эффективно реализуемого классического кода, исправляющего ошибки, когда последние сколь угодно близки к $1/2$. Дело в том, что зависимость длины от ошибки слабая – логарифмическая.

[4)] Здесь мы не учитываем ошибки, возникающие из-за неидеальностей оптоволоконной части (например, разбалансировки интерферометров и т.д.), поскольку с такими неидеальностями можно эффективно бороться. Ясно, что их учет может только уменьшить предельную длину передачи ключей. Напомним, что в принципе невозможно отличить ошибки от неидеальностей системы от ошибок, производимых подслушивателем.

[5)] Строго говоря, под затуханием надо понимать не только потери в самой линии связи, но и потери в оптоволоконных соединениях. Будем считать, что эти потери учтены в совокупной квантовой эффективности η.

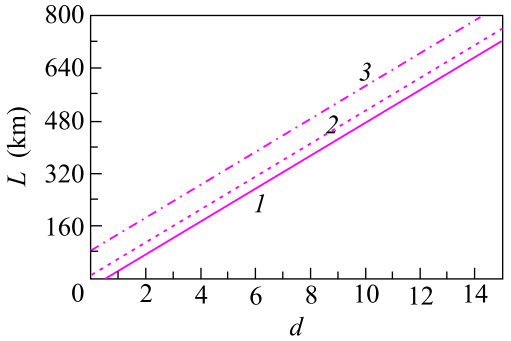

Рис.1. Зависимости длины передачи ключей от показателя экспоненты темновых отсчетов d при различных значениях критической ошибки Q. Линия *1* – $Q = 11\%$, *2* – $Q = 30\%$, *3* – $Q = 49\%$. Значение квантовой эффективности фотодетекторов $\eta = 100\%$, показатель затухания в оптоволокне взят стандартным, $\alpha = 0.2$ $[db/km]$, для одномодового волокна SMF-28

Последнее означает, что для того, чтобы увеличить длину передачи в 2 раза (за счет последнего слагаемого), требуется уметь приблизиться к границе ошибки в 1/2 в сто раз ближе. Известные классические коды перестают работать при гораздо меньшей величине ошибки. Например, наиболее эффективная из известных каскадная процедура коррекции ошибок [18], используемая в различных реализациях систем квантовой криптографии, перестает исправлять ошибки уже при $\approx 20 - 25\%$ в лучшем случае. Корректирующая способность других известных кодов также начинает "заваливаться" примерно при том же проценте ошибок [19, 20]. Наиболее перспективными являются так называемые турбокоды, а также коды с низкой плотностью проверок на четность, которые на сегодняшний день позволяют наиболее близко приблизиться к шенноновскому пределу по ошибке (см., например, [21]). Ответ и "да" и "нет" на поставленный выше вопрос, в части "нет", звучит как – нет формальных ограничений на длину передачи ключей. Однако в практической плоскости получаем ответ, что такие ограничения существуют. Неизвестен квантовый протокол распределения ключей *для неидеальной системы* с критической ошибкой $Q = 1/2$. Такой протокол известен только *для идеальной системы*. Если бы такой протокол и существовал для неидеальной системы, то все равно им нельзя воспользоваться в полной мере для увеличения длины передачи, поскольку приближение к $Q = 1/2$ требует конструктивного умения исправлять классические ошибки экспоненциально, близкие к критической величине, что практически невозможно.

Для широко известных протоколов квантового распределения ключей критическая ошибка находится в районе 10%. Например, для самого известного протокола распределения ключей BB84 критическая ошибка составляет $\approx 11\%$ [22–24].

Как следует из (6), зависимость длины передачи от квантовой эффективности детекторов также слабая – логарифмическая. Наиболее критическая зависимость от показателя экспоненты для вероятности темновых отсчетов – линейная. Зависимость длины от константы потерь в канале – обратно пропорциональная.

Для оптоволоконных систем квантовой криптографии фактически единственными параметрами, за счет которых можно увеличить длину, являются темновые отсчеты, поскольку минимальное значение константы потерь на длине волны 1535 нм $\alpha = 0.2$ $[db/km]$ фиксировано материалом кварцевого оптоволокна.

Протокол, который для *идеальной* системы имеет критическую ошибку 50%, в принципе существует. Уравнение, которое определяет критическую ошибку в отсутствие темновых шумов, имеет вид (см. детали в [25])

$$1 - h(Q) = h(\zeta), \tag{7}$$

где ζ – вероятность отсчетов в контрольном временном окне. При идеальных детекторах отсчеты в контрольном временном слоте возникают только из-за действий подслушивателя. Для идеальных детекторов критическая ошибка дается уравнением

$$1 - h(Q) = 0 \tag{8}$$

и равна, соответственно, $Q = 1/2$ для идеальной системы. В отсутствие подслушивателя[6)], но при наличии собственных темновых шумов детекторов, величину ζ, как показывает подробный анализ, необходимо заменить на p_{dark}. Критическая длина определяется уравнением (6) с Q из формулы (7). При малых p_{dark} длина линии передачи определяется формулой (6) с заменой критической ошибки $Q = 1/2 \to \approx$ $\approx (1/2 - p_{\text{dark}}/\ln(2))$.

Сделаем некоторые численные оценки различных вкладов в длину передачи.

1) *Вклад первого слагаемого.* Типичные вероятности темновых отсчетов составляют $p_{\text{dark}} = 10^{-5}$ при охлаждении лавинных детекторов элементами Пельтье до температур $-50{-}60\,^{\circ}$C; $p_{\text{dark}} = 10^{-7}$ при охлаждении детекторов до температуры жидкого азота; $p_{\text{dark}} = 10^{-13}$ для лучших сверхпроводящих де-

[6)] Именно в этом случае достигается максимальная длина передачи.

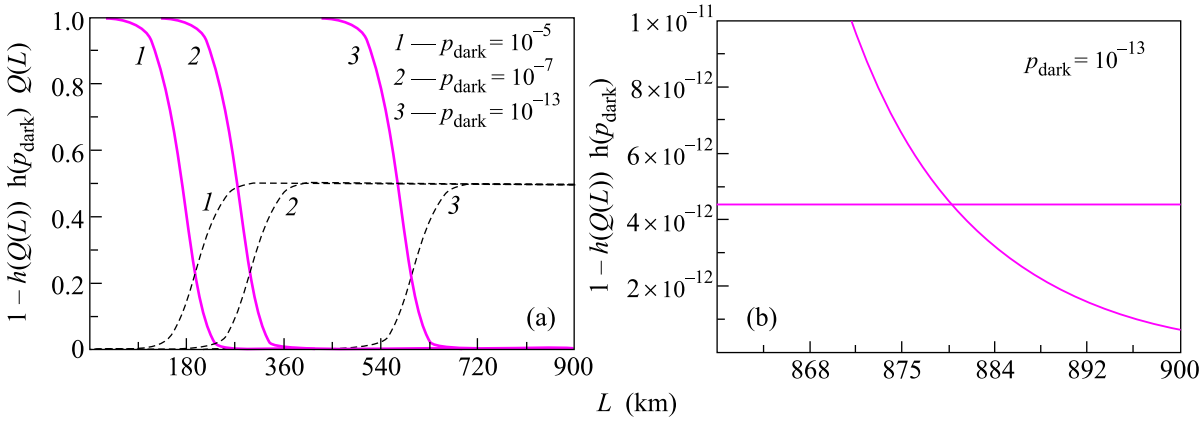

Рис.2. (a) Сплошные линии – зависимости взаимной информации легитимных пользователей $(1 - h(Q(L))$ от длины линии связи; пунктирные линии – зависимости ошибки на приемной стороне (см. ф-лу (4)); сплошные горизонтальные линии (в данном масштабе практически совпадающие с осью абсцисс) – энтропийная функция $h(p_{\rm dark}))$ при разных значениях вероятности темновых отсчетов $p_{\rm dark}$. Критическая длина линии связи определяется точкой пересечения $1 - h(Q(L))$ и $h(p_{\rm dark})$. Квантовая эффективность детекторов взята равной $\eta = 10\%$. (b) Зависимости $1 - h(Q(L))$ и $h(p_{\rm dark})$ от длины линии связи, критическая длина определяется точкой пересечения этих функций

текторов при охлаждении до температуры жидкого гелия. Длины передачи, соответственно, равны $L = 250$; 350; 650 км. Типичные значения квантовой эффективности детекторов составляют $\eta = 10\%$ (для сверхпроводящих детекторов эта величина относится только к рекордным значениям и не является на сегодняшний день типичной) [26].

2) *Вклад второго слагаемого* уменьшает предельную длину на 50 км, что дает, соответственно, $L = 200$; 300; 600 км.

3) *Вклад третьего слагаемого* зависит от квантового протокола распределения ключей, например, для протокола BB48 $Q \approx 11\%$. При такой критической ошибке этот вклад еще отрицателен и равен ≈ -27.5 км, он становится положительным, если критическая ошибка собственно самого протокола становится $Q > 25\%$. В итоге, критическая длина линии связи уменьшается до $L \approx 172.5$; 272.5; 572.5 км.

Критическая длина протокола с фазово-временным кодированием [25] может быть найдена графически (рис.2) и составляет соответственно $L \approx 290$; 435; 880 км. Для достижения данных предельных длин необходимо уметь исправлять ошибки соответственно до величин $Q = 1/2 - 2 \cdot 10^{-4}$; $Q = 1/2 - 2.5 \cdot 10^{-6}$; $Q = 1/2 - 4.5 \cdot 10^{-12}$. Однако конструктивно и эффективно реализуемые классические коды, исправляющих ошибки с такой эффективностью, на сегодняшний день неизвестны.

Таким образом, проблема состоит не в том, что нет хорошего квантового протокола распределения ключей, который обеспечивает теоретически большую дальность передачи секретных ключей, а в том, что в полной мере невозможно воспользоваться возможностями[7)], которые дает квантовая часть протокола, поскольку достижение предельных длин передачи ключей лимитируется *классической частью протокола*.

Выражаю благодарность Академии Криптографии Российской Федерации за поддержку. Работа частично поддержана проектом Российского фонда фундаментальных исследований # 08-02-00559. Выражаю также благодарность С.С. Назину и С.П. Кулику за ряд полезных обсуждений.

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. G. S. Vernam, J. Amer. Inst. Elect. Eng. **55**, 109 (1926).
3. В. А. Котельников, Отчет 18 июня 1941 г.
4. C. E. Shannon, Bell Syst. Tech. Jour. **28**, 658 (1949).
5. W. K. Wootters and W. H. Zurek, Nature **299**, 802 (1982).
6. C. H. Bennett, Phys. Rev. Lett. **68**, 3121 (1992).
7. N. Gisin, G. Ribordy, W.Tittel, and H. Zbinden, Rev. Mod. Phys. **74**, 145 (2002).
8. V. Scarani, H. Btchmann-Pasquinucci, N. J. Cerf et al., arXiv: [quant-ph] 0802.4155.

[7)] Как видно из рис.2а (кривая *1*), если нет ограничений на исправление ошибок, то можно "дотянуться" до длины $L \approx 290$ км. Однако при способности исправлять ошибки до величины 20–25% длина оказывается ≈ 180 км.

9. I. Csiszár and J. Körner, IEEE Trns. Inf. Theory **24**, 339 (1978).
10. B. Kraus, N. Gisin, and R. Renner, Phys. Rev. Lett. **95**, 080501 (2005).
11. I. Devetak and A. Winter, Proc. Royal Soc. A **461**, 207 (2005).
12. C. E. Shannon, Bell Syst. Tech. Jour. **27**, 397; 623 (1948).
13. Р. Галлагер, *Теория информации и надежная связь*, М.: "Советское радио", 1974, p. 719.
14. I. Csiszár and J.Körner, *Information Theory: Coding Theorems for Discreter Memoryless Systems*, Akademiai, Kiado–Budapest, 1981.
15. J. L. Carter and M. N. Wegman, J. of Computer and System Sciences **18**, 143 (1979).
16. C. H. Bennett, G. Brassard, C. Crépeau, and U. Maurer, IEEE Transaction on Information Theory **41**, 1915 (1995).
17. С. Н. Молотков, Письма в ЖЭТФ **88**, 315 (2008).
18. G. Brassard and L. Salvail, *Secret Key Reconciliation by Public Discussion*, EUROCRYPT 410-423 (1993); Lecture Notes in Computer Science **765**, 410 (1994).
19. E. J. Mac Williams and N. J. A. Sloane, *The Theory of Error-Correcting Codes*, North-Holland Publ. Company, Amsterdam, New York, Oxord, 1977.
20. W. W. Peterson and E. J. Weldon, *Error-Correcting Codes*, The MIT Press, Cambridge, Massachusetts, London, England, 1972.
21. R. H. Morelos-Zaragoza, *The Art of Error Correcting Codes*, John Wiley&Sons Ltd., 2002.
22. D. Mayers, JACM **48**, 351 (2001).
23. P. W. Shor and J. Preskill, Phys. Rev. Lett. **85**, 441 (2000).
24. С. Н. Молотков, А. В. Тимофеев, Письма в ЖЭТФ **85**, 632 (2007).
25. С. Н. Молотков, ЖЭТФ **133**, 5 (2008).
26. Book of Abstracts, *Single-Photon Workshop 2007, Source, Detectors, Applications and Measurements Methods*, 25–28 September 2007, INRIM, Torino, Italy.