Письма в ЖЭТФ, том 101, вып. 8, с. 637 – 643

О секретности волоконных систем квантовой криптографии без контроля интенсивности квазиоднофотонных когерентных состояний

С. Н. Молотков[1)]

Институт физики твердого тела РАН, 142432 Черноголовка, Россия

Академия криптографии РФ, 121552 Москва, Россия

Факультет вычислительной математики и кибернетики, МГУ им. Ломоносова, 119991 Москва, Россия

Поступила в редакцию 9 февраля 2015 г.

После переработки 10 марта 2015 г.

Внутренние потери в системах квантовой криптографии могут использоваться при атаках подслушивателя. В результате для ряда протоколов невозможно обеспечить секретность ключей. Эта проблема может быть преодолена путем использования геометрически однородных когерентных состояний с бóльшим числом базисов. При числе базисов $N_b/2 = 4$ и числе состояний $N_b = 8$ удается гарантировать секретность ключей даже без контроля интенсивности входных состояний.

DOI: 10.7868/S0370274X15080135

Введение. Системы квантовой криптографии предназначены для распределения секретных криптографических ключей через открытый и доступный для пассивного и активного вторжения квантовый канал связи. Классический аутентичный вспомогательный канал связи, служащий для обмена классической информацией между легитимными пользователями: при согласовании базисов (если этого требует протокол), коррекции ошибок в первичных ключах, финального сжатия (хэширования – усиления секретности) очищенных ключей также доступен для прослушивания. Секретность ключей в квантовой криптографии гарантируется фундаментальными запретами квантовой механики на различимость неортогональных квантовых состояний. На сегодняшний день строго доказана секретность протокола BB84 [1] для случая строго однофотонного источника квантовых состояний и конечных длин передаваемых последовательностей. Доказательство [2] основано на фундаментальных энтропийных соотношениях неопределенностей и не использует предположений о атаках подслушивателя на передаваемые ключи. В реальной ситуации квантовые состояния являются квазиоднофотонными ослабленными когерентными состояниями. Кроме того, потери в канале связи вместе с квазиоднофотонными состояниями, открывают возможности для новых атак, которые отсутствуют в однофотонном случае.

Протокол BB84 в реальных системах использует 4 когерентных состояния, по два состояния в каждом базисе. В базисе + состояния равны $0 \to |\alpha\rangle$, $1 \to |-\alpha\rangle$, в базисе $\times$ – $0 \to |i\alpha\rangle$, $1 \to |-i\alpha\rangle$. Комплексные параметры α_i $(i = 0, 1, 2, 3)$, описывающие информационные состояния, равномерно расположены на окружности в комплексной плоскости. Как будет показано ниже, протокол BB84 не может гарантировать секретность ключей в реальных системах при наличии потерь в канале и неизбежных потерях внутри приемника. Поэтому необходимо использовать протоколы с большим числом информационных состояний и базисов.

Одним из таких протоколов является протокол на геометрически однородых состояниях (протокол BB84 – частный случай семейства таких протоколов). Оказывается, что числа базисов $N_b/2 = 4$ уже достаточно для гарантии секретности ключей в реальных системах. Информационными состояниями являются геометрически однородные когерентные состояния вида $|\alpha_j\rangle$, получающиеся геометрическим сдвигом (унитарным поворотом U^j, $U^N = I$) $|\alpha_j\rangle = U^j|\alpha\rangle$, где $\alpha_j = e^{i\frac{2\pi}{N_b}j}\alpha$ $(j = 0, 1, ..., N_b - 1)$. В протоколе используется $N_b/2 = 4$ базиса. В каждом базисе имеется пара неортогональных состояний с $|\alpha_j\rangle$ и $|\alpha_{j+1}\rangle$, отвечающих 0 и 1.

Критерий корректности и секретности ключей. Любой протокол квантового распределения ключей состоит из следующих стадий: 1) передача квантовых состояний от Алисы к Бобу и их измерение на приемной стороне (если,

[1)]e-mail:???

как в протоколе BB84 это требуется, то еще и согласование базисов – отбрасывание или фиксирование посылок, в которых базисы не совпадали или совпадали); 2) оценка вероятности ошибки и исправление ошибок через открытый классический канал; 3) оценка информации Евы при наблюдаемой ошибке на приемной стороне, ее изменение после исправления ошибок и последующее сжатие (усиление секретности) очищенных ключей.

Ситуация Алиса–Боб–Ева после стадии 1 описывается совместной матрицей плотности $\rho^n_{XX'E}$, где X^n, X'^n – битовые строки Алисы и Боба (последняя, возможно, с ошибками), $\rho^n_E = \mathrm{Tr}_{XX'}\{\rho^n_{XX'E}\}$ – квантовая система, доступная Еве. Учитывая информацию, которую Ева получила из квантового канала связи, и дополнительную классическую информацию при коррекции ошибок из классического канала связи, Алиса и Боб производят сжатие очищенных ключей, чтобы Ева не имела никакой информации о финальном секретном ключе. Протокол должен удовлетворять критерию корректности и секретности [3]. Корректность: ключи Алисы и Боба после исправления ошибок должны быть идентичными с заданной вероятностью $\varepsilon_{\mathrm{corr}}$,

$$\Pr[X^n \neq X'^n] < \varepsilon_{\mathrm{corr}}, \tag{1}$$

где X^n и X'^n – битовые строки Алисы и Боба после исправления ошибок.

Неформально протокол секретен, если битовая строка Алисы X^n не коррелирована с квантовой системой Евы ρ^n_E. На формальном языке отсутствие корреляций между строкой Алисы и квантовой системой Евы означает, что совместная матрица плотности Алиса–Ева (ρ^n_{XE}) распадается на произведение матриц плотности двух систем, ($\rho^n_U \otimes \rho^n_E$) (идеальная ситуация). Здесь ρ^n_U – матрица плотности Алисы, описывающая равномерное распределение классических битовых строк: $\rho^n_U = \frac{1}{2^n}\sum_{i_1,i_2,\ldots,i_n=0,1} |i_1\rangle\langle i_1| \otimes \otimes |i_2\rangle\langle i_2| \otimes \ldots \otimes |i_n\rangle\langle i_n|$.

Мерой секретности ключей является следовое расстояние между реальной матрицей плотности Алиса–Ева (ρ^n_{XE}) и некоррелированными матрицами плотности Алиса–Ева ($\rho^n_U \otimes \rho^n_E$) (*идеальная ситуация*). Протокол должен гарантировать, что следовое расстояние Δ между данными матрицами плотности может быть сделано меньше наперед заданной величины $\varepsilon_{\mathrm{secr}}$:

$$\Delta = \frac{1}{2}||\rho^n_{XE} - \rho^n_U \otimes \rho^n_E||_1 < \varepsilon_{\mathrm{secr}}, \tag{2}$$

где, по определению, следовое расстояние между двумя операторами равно $||\rho_1 - \rho_2||_1 = \mathrm{Tr}\{|\rho_1 - \rho_2|\} = \mathrm{Tr}\{\sqrt{(\rho_1 - \rho_2)^2}\}$. В этом случае протокол называется $\varepsilon_{\mathrm{secr}}$-секретным. Часть информации Ева получает из квантового канала, атакуя передаваемые квантовые состояния. При коррекции ошибок через классический канал передается классическая корректирующая информация, которая также доступна Еве. Кроме того, после исправления ошибок происходит сжатие ключей через открытый классический канал: Алиса передает информацию о функции хэширования. Данные обстоятельства должны быть учтены в формуле (2). Их учет дает лемма об остатке хэширования [4] (Left over Hash Lemma). Согласно лемме об остатке хэширования после коррекции ошибок и сжатия очищенного ключа универсальными хэш-функциями второго порядка [5] следовое расстояние становится равным

$$\Delta = \frac{1}{2}\sqrt{2^{-[H^{\varepsilon}_{\min}(X^n|C^nE^n) - R_n]}}, \tag{3}$$

где $H^{\varepsilon}_{\min}(X^n|C^nE^n)$ – сглаженная условная min-энтропия, а C^n включает в себя корректирующую информацию, переданную Алисой через открытый канал к Бобу. По определению, $H^{\varepsilon}_{\min}(X^n|C^nE^n) = \sup_{\tilde{\rho}^n_{CE}} H_{\min}(\tilde{\rho}^n_{XCE}|\tilde{\rho}^n_{CE})$, где $H_{\min}(\tilde{\rho}^n_{XCE}|\tilde{\rho}^n_{CE}) = -\log\lambda$, λ – минимальное число, такое, что $\lambda I_X \otimes \tilde{\rho}^n_{CE} - \tilde{\rho}^n_{XCE} > 0$, $||\tilde{\rho}^n_{CE} - \rho^n_{CE}||_1 < \varepsilon$. При этом мы считаем, что $\mathrm{Tr}(\tilde{\rho}^n_{CE}) = 1$. Протокол является ε-секретным [3], если длина финального секретного ключа

$$R_n \leq H^{\varepsilon}_{\min}(X^n|C^nE^n) - 2\log(1/2\varepsilon). \tag{4}$$

Для $H^{\varepsilon}_{\min}(X^n|C^nE^n)$ может быть получена оценка [3]

$$H^{\varepsilon}_{\min}(X^n|C^nE^n) \geq H^{\varepsilon}_{\min}(X^n|E^n) - \mathrm{leak}_n - 2\log(1/2\varepsilon), \tag{5}$$

где leak_n – классическая информация в битах, переданная через открытый канал при коррекции ошибок, которая определяется только процедурой коррекции. Формула (5) имеет интуитивно прозрачную интерпретацию. Величина $H^{\varepsilon}_{\min}(X^n|C^nE^n)$ отображает дефицит информации, которой не хватает Еве, имеющей квантовую систему E и классическую информацию $C(\rho^n_{CE})$, чтобы целиком знать битовую строку Алисы.

В асимптотическом пределе длинных последовательностей ($n \to \infty$, откуда автоматически $\varepsilon \to 0$) сглаженная энтропия стремится к условной энтропии фон Неймана [3] (в классическом случае энтропии Шеннона), $H^{\varepsilon}_{\min}(X^n|C^nE^n) \to H(X^n|C^nE^n)$, которая имеет смысл дефицита информации Евы. Неформально сглаженная условная энтропия $H^{\varepsilon}_{\min}(X^n|C^nE^n)$ имеет смысл дефицита информации Евы требующейся для того, чтобы целиком

знать битовую строку X^n при условии, что она имеет квантовую систему E^n вместе с классической информацией C^n, переданной через классический канал при коррекции ошибок. Грубо говоря, $H^{\varepsilon}_{\min}(X^n|C^nE^n)$ равно числу бит, не известных Еве после всех стадий протокола. Неравенство (5) позволяет разделить информацию Евы, полученную из квантового и классического каналов связи.

Упомянутая выше интерпретация имеет место, если матрицы плотности известны точно (например, в асимптотическом пределе). В реальной ситуации при конечных длинах последовательностей можно получить лишь оценку матриц плотности с некоторой точностью по отношению к истинной матрице плотности. Можно гарантировать только близость к истинной матрице плотности с точностью ε в смысле следового расстояния. Сглаженная энтропия $H^{\varepsilon}_{\min}(X^n|C^nE^n)$ является нижней границей дефицита информации Евы по множеству матриц плотности, которые ε-близки к истинной матрице плотности.

Однофотонный случай. Для протокола BB84 однофотонный случай является особым. В этом случае теорема о запрете клонирования гарантирует, что любое получение информации о передаваемых неортогональных состояниях подслушивателем будет приводить к возмущению состояний и появлению ошибок на приемной стороне. Замечательный результат [2] состоит в использовании фундаментальных энтропийных соотношений неопределенностей для сглаженных энтропий для трехчастичной матрицы плотности $\rho^n_{XX'E}$ Алиса–Боб–Ева:

$$\frac{1}{n}\left[H^{\varepsilon}_{\min}(X^n|E^n) + H^{\varepsilon}_{\max}(Z^n|Z'^n)\right] \geq 2\log(1/c),$$
$$c = |\langle 0(X)|0(Z)\rangle| = 1/\sqrt{2}, \tag{6}$$

где $|0(X,Z)\rangle$ – информационные состояния в прямом (X) и сопряженном (Z) базисе. Правая часть (6) не зависит от матрицы плотности $\rho^n_{XX'E}$ и определяется *только* самим протоколом BB84. Величина $H^{\varepsilon}_{\max}(Z^n|Z'^n)$ является чисто классической и определяет минимальное количество бит информации, необходимое для исправления ошибок в битовой строке Боба Z'^n. Она связана с ошибкой Q. Кроме того, из-за симметрии протокола относительно базисов X и Z имеем $H^{\varepsilon}_{\max}(Z^n|Z'^n) = H^{\varepsilon}_{\max}(X^n|X'^n)$. Данный факт и соотношения (6) позволяют выразить $H^{\varepsilon}_{\min}(X^n|E^n)$ через $H^{\varepsilon}_{\max}(X^n|X'^n)$: $H^{\varepsilon}_{\min}(X^n|E^n) > > 1 - H^{\varepsilon}_{\max}(X^n|X'^n)$. Длина секретного ключа

$$R_n \leq 1 - 2H^{\varepsilon}_{\max}(X^n|X'^n). \tag{7}$$

В асимптотическом пределе $n \to \infty$ сглаженная энтропия стремится к условной энтропии Шеннона, $H^{\varepsilon}_{\max}(X^n|X'^n) \to nH(X|X')$, и $\mathrm{leak}_n \to nH(X|X')$. Для бинарного канала с ошибкой Q имеем $\mathrm{leak}_n = nh(Q)$. В этом пределе формула (7) дает знаменитое уравнение для критической ошибки протокола BB84, до которой гарантируется секретное распределение ключей: $1 = 2h(Q_c)$, $Q_c \approx 11\,\%$ [6]. *Фундаментальные энтропийные соотношения неопределенностей* (6) *для однофотонных состояний позволяют связать утечку информации к Еве с наблюдаемой ошибкой на приемной стороне и избавляют от перебора всевозможных атак Евы и выбора среди них оптимальной.* Заметим, что оптимальную атаку можно построить явно [7]. *К сожалению, этот замечательный фундаментальный результат* [2] *не может быть перенесен на реальные системы квантовой криптографии. Главная трудность состоит в оценке* $H^{\varepsilon}_{\min}(X^n|E^n)$, *которая содержит в себе всю информацию о атаках Евы.*

Секретность в квазиоднофотонном случае когерентных состояний. Ситуация радикально меняется, если в качестве информационных используются квазиоднофотонные когерентные состояния. Набор из N_b состояний является линейно независимым, что служит необходимым и достаточным условием существования UM (Unambiguous Measurements) измерений. Если канал имеет потери, то подслушиватель, проводя UM-измерения, разрывает его в двух местах (вблизи Алисы и Боба). С вероятностью $1 - \Pr(?)$ может быть получен определенный исход (разрыв вблизи Алисы). В этом случае Ева перепосылает правильные состояния к Бобу (от второго разрыва). Если получен неопределенный исход (с вероятностью $\Pr(?)$), то Ева ничего не перепосылает. При вероятности потерь в канале $\Pr[\mathrm{Loss(ch)}] > \Pr(?)$ подслушиватель знает весь ключ, не производит ошибок на приемной стороне и не детектируется. Таким образом, начиная с определенной длины канала (и потерь), ключ не является секретным.

Такая оценка является не верной. Принципиально важно учитывать не только потери в канале связи, но и потери в приемной части системы. Ниже под потерями будут пониматься полные потери в данной последовательности как отношение числа посланных и зарегистрированных посылок, $\Pr(\mathrm{Loss}) = \frac{N_{\mathrm{registr}}}{N_{\mathrm{send}}}$. Даже при $\Pr[\mathrm{Loss(ch)}] < \Pr(?)$ Ева может проводить UM-измерения, используя потери внутри приемной части. Полные потери определяются квантовой эффективностью детектора ($\eta \approx 0.1{-}0.25$), средним числом фотонов ($\mu \approx 0.1{-}0.25$) в когерентном со-

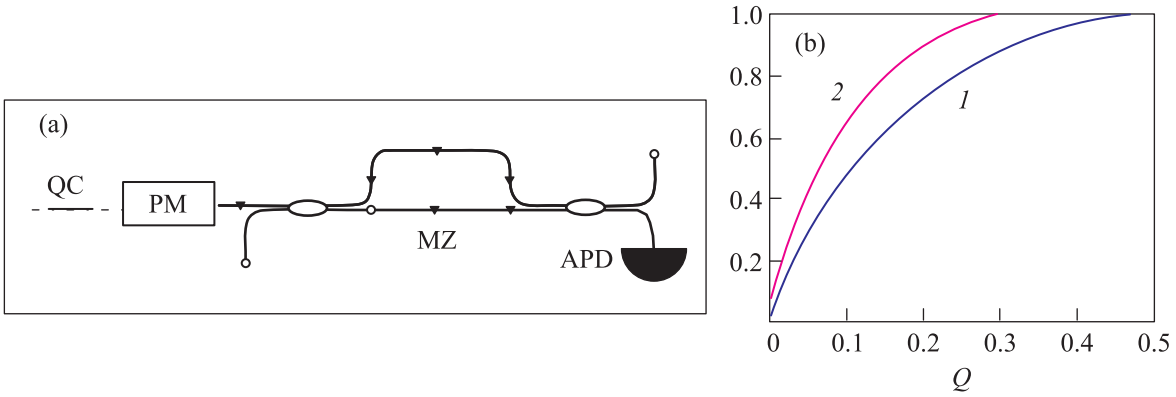

Рис. 1. (a) – Схема приемной части волоконной системы квантовой криптографии: PM – фазовый модулятор, APD – лавинный однофотонный детектор, MZ – интерферометр Маха–Цандера, QC – квантовый канал. (b) – Кривая *1* – бинарная энтропийная функция Шеннона $h(Q)$, кривая *2* – функция $\mathrm{leak}_{\infty}^{\mathrm{Ham}}(Q)$ (см. текст)

стоянии, потерями в приемной оптической части и потерями в канале. Заметим, что внутренние потери $1-\eta\cdot\mu\approx 1-10^{-2}$, что эквивалентно потерям при длине линии на волокне SMF-28 в 100 км. Кажется, что не имея доступа к приемной части системы, Ева не может скомпенсировать внутренние потери. Однако это не так. Ева может скомпенсировать потери внутри системы, посылая более интенсивные состояния так, чтобы каждая перепосланная посылка после UM-измерений была зарегистрирована. Для реальных лавинных детекторов среднее число фотонов непосредственно на самом детекторе, достаточное для гарантированной регистрации, составляет $\mu\approx 50{-}60$ [8]. Конечно, перепосыл более интенсивных правильных состояний для протоколов с базисами приведет к одновременным отсчетам в двух лавинных детекторах в посылках, где базисы Алисы и Боба не совпадали, и не приведет к ошибочным отсчетам там, где базисы совпадали. Изменение темпа двойных отсчетов требует пересчета на утечку информации к Еве. Однако поскольку лавинные детекторы не различают среднее число фотонов, изменение темпа отсчета требует дополнительных предположений о темпе отсчета от числа фотонов, что является неприемлемым. На таких предположениях фактически базируется протокол Decoy State [9]. Данные предположения неизбежно будут входить в длину финального секретного ключа. Даже если закрыть глаза на это обстоятельство, то требуется решить задачу пересчета числа двойных отсчетов лавинных детекторов на утечку информации к Еве. Такая задача является крайне сложной и до сих пор внятно не решена.

Требования к формуле длины секретного ключа. Длина секретного ключа должна зависеть только от: 1) наблюдаемой ошибки на приемной стороне, 2) числа посланных и зарегистрированных состояний при совпадающих базисах, 3) структуры квантового состояния, посланного в канал связи. Внутренними параметрами являются квантовая эффективность детекторов, вероятность темновых шумов, число двойных отсчетов. Потери во внутренней оптической части и канале не должны фигурировать в длине секретного ключа, поскольку они неизвестны и могут меняться в каждой посылке.

Протокол квантового распределения ключей без контроля интенсивности. Информационными состояниями являются геометрически однородные когерентные состояния [10], ослабленные до квазиоднофотонного уровня. Среднее число фотонов в состоянии $\mu=|\alpha|^2$. Число информационных состояний задается числом базисов N_b ($N_b/2=2,3,4,...$). В каждом базисе имеется пара неортогональных состояний $|\varphi_{ib}\rangle=|\alpha_j\rangle$, отвечающих 0 и 1 ($i=0,1$, $b=1,...,N_b/2$ – индекс базиса). Любое i-е состояние получается унитарным поворотом: $|\alpha_i\rangle=U^i|\alpha_0\rangle$, где $\alpha_i=\alpha e^{i\varphi_i}$ ($i=0,...,N_b-1$). Информационными состояниями являются геометрически однородные когерентные состояния вида $|\alpha_j\rangle$, получающиеся унитарным поворотом U^j, $U^{N_b}=I$, $|\alpha_j\rangle=U^j|\alpha\rangle$, где $\alpha_j=e^{i\frac{2\pi}{N_b}j}\alpha$ ($j=0,1,...,N_b-1$). Измерительная схема приемной части содержит один детектор (рис. 1). При этом двойные отсчеты автоматически не учитываются. Она с одним детектором устойчива к активным атакам типа ослепления и mismatch лавинных детекторов. Она может быть реализована как в однопроходном, так и в двухпроходном вариантах.

Атака с UM-измерениями. Обсудим атаку с UM-измерениями и получим длину секретного ключа в асимптотическом пределе. Ева проводит UM-измерения в доле δ посылок. В $\delta\cdot[1-\Pr(?)]$ по-

сылок она получает определенный результат, а в $\delta \cdot \Pr(?)$ – неопределенный. Далее Ева отбрасывает эти посылки. В посылках, где получен определенный исход, Ева перепосылает более интенсивные когерентные состояния $|\alpha^* e^{i\varphi_i}\rangle$, которые гарантированно регистрируются. В остальных $1-\delta$ посылках она производит индивидуальные измерения, пытаясь различить состояния с минимальной вероятностью ошибки. Пусть результат измерения интерпретирован как $|\alpha e^{i\varphi_i}\rangle$ (возможно, с ошибкой). Затем Ева перепосылает вместо исходных квазиоднофотонных более интенсивные состояния $|\alpha^* e^{i\varphi_i}\rangle$, чтобы преодолеть потери в приемной части. Структура геометрически однородных состояний определяет вероятность неопределенного исхода, для которой имеется точное решение [11]:

$$\Pr(?) = 1 - \min_r \left| \sum_{j=0}^{N_b-1} e^{\mu\left(e^{i\frac{2\pi j}{N_b}}-1\right)} e^{-i\frac{2\pi jr}{N_b}} \right|, \; 0 \le r \le N_b - 1. \tag{8}$$

Длина секретного ключа в асимптотическом пределе. Получим длину секретного ключа в асимптотическом пределе $n \to \infty$. После согласования базисов она равна

$$R_n = H(X^n|E^n) - \mathrm{leak}_n. \tag{9}$$

Пусть n – число посланных посылок, в которых базисы совпадали, а $n[1-\Pr(\mathrm{Loss})]$ – число зарегистрированных посылок:

$$n[1-\Pr(\mathrm{Loss})] = n\delta\cdot[1-\Pr(?)]+n(1-\delta),\; n\to\infty, \tag{10}$$

где первое слагаемое – число посылок, для которых имел место определенный исход, второе – число посылок, в которых используются индивидуальные измерения. Здесь важно отметить, что *UM-атака возможна даже при условии, что вероятность полных потерь* $\Pr(\mathrm{Loss})$ *меньше вероятности неопределенного исхода* $\Pr(?)$. *Оптимальная доля посылок, в которой Ева делает UM-измерения, составляет* $\delta = \Pr(\mathrm{Loss})/\Pr(?) \le 1$. *Критическое значение* $\delta_c = 1$ ($\Pr(\mathrm{Loss}) = \Pr(?)$). *В этом случае Ева знает весь ключ и не производит ошибок на приемной стороне.* Находим

$$R_\infty = \lim_{n\to\infty}\frac{R_n}{n} = [1-\Pr(\mathrm{Loss})](1-\mathrm{leak}_\infty) - \\ -[1-\Pr(\mathrm{Loss},?)]\,C_1(N_b) - \Pr(\mathrm{Loss},?)\,[1-\Pr(?)], \tag{11}$$

где $\Pr(\mathrm{Loss},?) = \Pr(\mathrm{Loss})/\Pr(?)$. Подчеркнем, что *оценка утечки информации* $H(X^n|E^n)$ *к Еве не связана с оценкой вероятности ошибки*, как в однофотонном случае (6), (7). *Для* $H(X^n|E^n)$ *используется верхняя консервативная оценка.* Для исправления ошибок в шенноновском пределе требуется передача через открытый канал $\mathrm{leak}_\infty^{\mathrm{Shan}}(Q) = h(Q)$ бит на позицию, где Q – оценка вероятности ошибки [12]. В реальной ситуации используются конструктивные процедуры коррекции ошибок. Например, для процедуры, основанной на кодах Хэмминга, с дополнительной проверкой на четность и длиной кодового слова $(2^m - m - 1, m)$, $m = 3, 4, 5$, зависящей от вероятности ошибки (в среднем одна ошибка на блок), требуется раскрытие $(n \to \infty)$ $\mathrm{leak}_\infty^{\mathrm{Ham}}(Q) = 1 - \left(0.99827e^{-Q/0.112922} - 0.06851\right)$ бит [8]. В формуле (11) фигурируют только наблюдаемые величины: полные потери $\Pr(\mathrm{Loss})$, число раскрытых бит при коррекции leak_∞, вероятность неопределенного исхода $\Pr(?)$ и классическая пропускная способность квантового канала за один шаг (one shot) $C_1(N_b)$, которые зависят только от структуры информационных состояний. Длина ключа, вычисленная по формуле (11), приведена на рис. 2.

Длина секретного ключа при конечных длинах передаваемых последовательностей. Вычислим длину секретного ключа в пределе конечных переданных последовательностей. Здесь число n имеет тот же смысл, что и выше. В зависимости от оценки ошибки Q выбирается некоторый классический корректирующий код. Пусть $n\cdot\mathrm{leak}(n,Q)$ – число бит, переданных через открытый канал при коррекции ошибок для данной конкретной последовательности длины n. После исправления ошибок требуется проверить идентичность очищенных ключей у Алисы (X_A) и Боба (X_B). Одна из процедур состоит в сравнении через открытый канал бита четности X_A и X_B со случайной строкой X_rand той же длины: $\mathrm{Parity}(X_{rand} \oplus X_A)$, $\mathrm{Parity}(X_\mathrm{rand} \oplus X_\mathrm{B})$. Случайная строка генерируется открыто. Если биты четности после выполнения данной процедуры M раз совпадают, то вероятность того, что очищенные ключи не равны, $\Pr[X_\mathrm{A} \ne X_\mathrm{B}] < 1/2^M$. После этих стадий Ева получает $n\cdot\mathrm{leak}(n,Q)+M$ бит информации, которые будут удалены из ключа на стадии усиления секретности. Если длина финального ключа

$$R_n \le H_{\min}^{\varepsilon}(\rho_{XE}^n|\rho_E^n) - n\cdot\mathrm{leak}(n,Q) - M - \\ - 2\log(1/2\varepsilon), \quad \varepsilon = \varepsilon_? + \varepsilon_c, \tag{12}$$

то ключ является ε-секретным.

Напомним, что n посылок относятся к случаю, когда базисы у Алисы и Боба уже согласованы (одинаковы). С учетом супераддитивности сглаженной min-энтропии получаем (детали см. в [3])

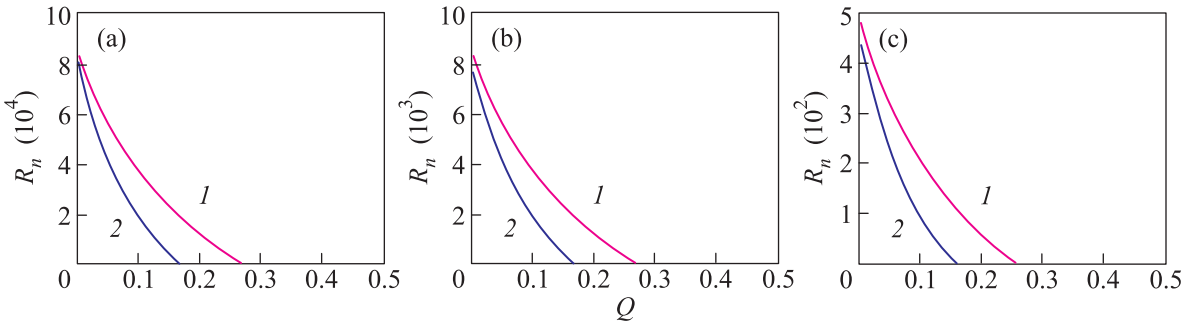

Рис. 2. Длина секретного ключа в асимптотическом пределе при различных потерях для протокола на геометрически однородных состояниях, $N_b = 8$ – число состояний, $N_b/2 = 4$ – число базисов. Кривые *1* – коррекция ошибок случайными кодами Шеннона, *2* – кодами Хэмминга (см. текст). Потери Pr(Loss) = 0.99 (a), 0.999 (b) и 0.9999 (c). Число переданных бит при совпадающих базисах $n = 10^7$, $\mu = 0.4$

$$H_{\min}^{\varepsilon_? + \varepsilon_c}(\rho_{XE}^n|\rho_E^n) = \\ = H_{\min}^{\varepsilon_? + \varepsilon_c}(\rho_{XE}^{n\cdot\delta} \otimes \rho_{XE}^{n\cdot(1-\delta)}|\rho_E^{n\cdot\delta} \otimes \rho_E^{n\cdot(1-\delta)}) > \\ > H_{\min}^{\varepsilon_?}(\rho_{XE}^{n\cdot\delta}|\rho_E^{n\cdot\delta}) + H_{\min}^{\varepsilon_c}(\rho_{XE}^{n\cdot(1-\delta)}|\rho_{XE}^{n\cdot(1-\delta)}). \quad (13)$$

Оценка энтропии $H_{\min}^{\varepsilon}(\rho_{XE}^{n\cdot\delta}|\rho_E^{n\cdot\delta})$ для части UM-измерений сводится к ситуации классического бинарного канала *с блокированием* (не путать с каналом со стиранием). Вероятность стирающего исхода есть Pr(?). Получаем

$$H_{\min}^{\varepsilon_?}(\rho_{XE}^{\otimes n\cdot\delta}|\rho_E^{\otimes n\cdot\delta}) > n_\delta\,[H(\rho_{XE}|\rho_E) - \delta_?] = \\ = n_\delta\,[\Pr(?) - \delta_?]\,, \quad n_\delta = n\cdot\delta, \quad n_? = n\cdot\Pr(?), \quad (14)$$

где $\delta_? = \log(5)\sqrt{2\log(1/2\varepsilon_?)/n_\delta}$. В оставшейся части посылок $n\cdot(1-\delta)$ Ева производит индивидуальные измерения:

$$H_{\min}^{\varepsilon_c}(\rho_{XE}^{\otimes[n\cdot(1-\delta)]}|\rho_E^{\otimes[n\cdot(1-\delta)]} > \\ > (n-n_\delta)\,[H(\rho_{XE}|\rho_E) - \delta_c] = \\ = (n-n_\delta)\,[1 - C_1(N_b) - \delta_c]\,, \quad (15)$$

где $\delta_c = \log(5)\sqrt{2\log(1/2\varepsilon_c)/(n-n_\delta)}$. При этом в нашем случае величина $H(\rho_{XE}|\rho_E)$ ограничена величиной $1 - C_1(N_b)$. Здесь принята консервативная оценка в пользу Евы. Величина $C_1(N_b)$ должна вычисляться для квантового ансамбля из N_b состояний еще до раскрытия базисов. Будем считать в пользу Евы, что базис ей известен и ей остается различить пару состояний внутри базиса. При этом $H(\rho_{XE}|\rho_E) \geq H(\rho_{XEB}|\rho_{EB})$ (здесь ρ_{XEB}, ρ_{EB} – матрицы плотности при известном базисе). Кроме того, в (15) входит пропускная способность за один шаг, а не величина Холево (пропускная способность $\overline{C}(N_b)$) [13]. Это связано со свойством двойственности квантовых каналов связи [14, 15]. Величина $\overline{C}(N_b)$ достигается на коллективных измерениях на заранее известной кодовой таблице из последовательности квантовых состояний. В нашем случае такой таблицы нет и Ева должна различать квантовые состояния "на ходу" [16]. Свойство двойственности для квантовых каналов приводит к тому, что коллективные измерения без кодовой таблицы не дают большей информации, чем оптимальные индивидуальные. Для двух состояний пропускная способность за один шаг имеет вид [13] $C_1(N_b) = (\xi^- \log \xi^- + \xi^+ \log \xi^+)/2$, где $\xi^\pm = 1 \pm \sqrt{1-\varepsilon_b^2}$, $\varepsilon_b = |\langle\alpha_i|\alpha_{i+1}\rangle|$ – скалярное произведение состояний внутри одного базиса.

В итоге длина секретного ключа равна

$$\frac{R_n}{n} = (1 - \Pr(\text{Loss}))[1 - \text{leak}(n,Q) - M] - \\ - [1 - \Pr(\text{Loss},?)]\,[C_1(N_b) + \delta_c] - \\ - \Pr(\text{Loss},?)\,[1 - \Pr(?) + \delta_?]\,, \quad (16)$$

где $n[1 - \Pr(?)][\text{leak}(n,Q) + M]$ – число реально раскрытых бит для данной последовательности длины $n[1-\Pr(?)]$ (число зарегистрированных отсчетов при совпадающих базисах). Результаты вычислений длины секретного ключа приведены на рис. 3.

Заключение. Внутренние потери в любой системе квантовой криптографии составляют порядка $1 - \eta\cdot\mu \approx 1 - 10^{-2}$ даже при нулевой длине канала связи. Подслушиватель может использовать данные потери при атаках на ключ, перепосылая более интенсивные состояния, чтобы скомпенсировать эти потери. В результате протоколы с малым числом информационных состояний, например BB84 и аналогичные не могут обеспечить секретность ключей. Причина связана с малой вероятностью неопределенного исхода Pr(?). Для протокола с восемью состояниями вероятность неопределенного исхода $\Pr(?) \approx (1 - 10^{-6}) - (1 - 10^{-8})$ (при $\mu = 0.4$–0.25), что позволяет обеспечить секретность при потерях в канале $1 - 10^{-4}$. Кроме того, здесь не требуется контролировать интенсивность входных состояний на приемной

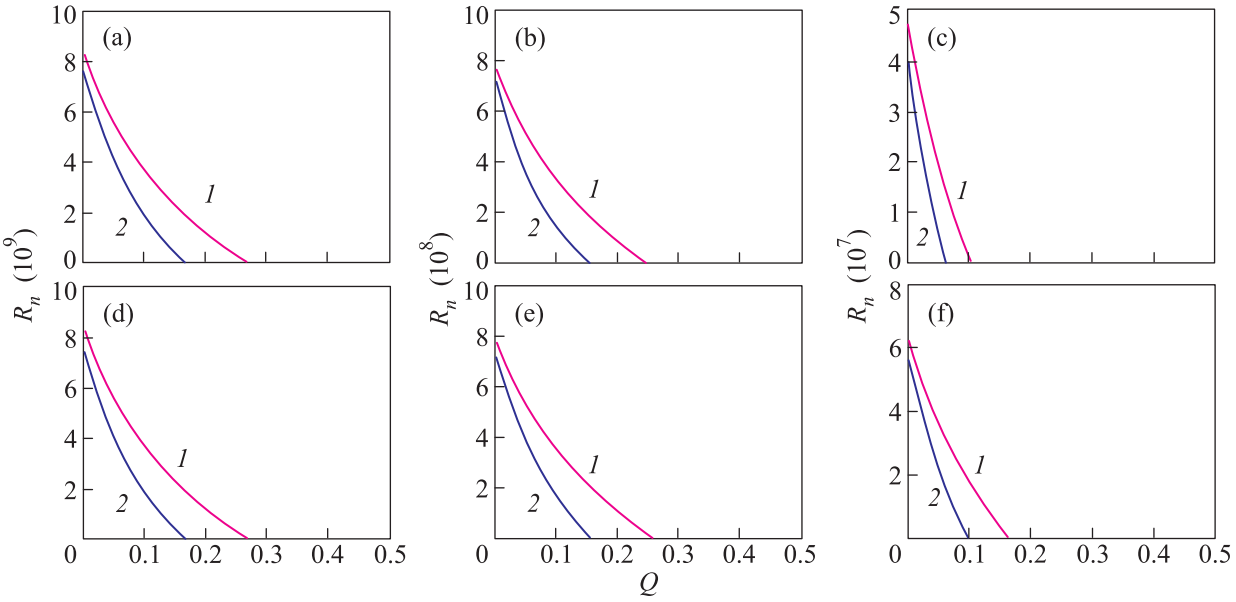

Рис. 3. Длина секретного ключа при конечной длине последовательности при различных потерях для протокола на геометрически однородных состояниях, $N_b = 8$ – число состояний, $N_b/2 = 4$ – число базисов. Кривые *1* – коррекция ошибок случайными кодами Шеннона, *2* – кодами Хэмминга (см. текст). Потери Pr(Loss) = 0.99 (a, d), 0.999 (b, e), 0.9999 (c, f). Число переданных бит при совпадающих базисах $n = 10^{12}$, $\mu = 0.4$. Параметры $\varepsilon_? = \varepsilon_c = 10^{-32}$ (a–c) и 10^{-9} (d–f)

стороне и, соответственно, пересчитывать изменение темпа двойных отсчетов в утечку информации к подслушивателю.

Автор выражает благодарность коллегам по Академии криптографии РФ за постоянную поддержку, а также С.П. Кулику и А.Н. Климову за многочисленные плодотворные обсуждения.

1. 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.
2. M. Tomamichel, C. C. Wen Lim, N. Gisin, and R. Renner, Nat. Comm. **3**, 634 (2011).
3. R. Renner, arXiv/quant-ph: 0512258.
4. M. Tomamichel, C. Schaffner, A. Smith, and R. Renner, arXiv/quant-ph:10022436.
5. J. L. Carter and M. N. Wegman, J. Comput. Sys. Sci. **18**, 143 (1979).
6. P. Shor and J. Preskill, Phys. Rev. Lett. **85**, 441 (2000).
7. С. Н. Молотков, А. В. Тимофеев, Письма в ЖЭТФ **85**, 632 (2007).
8. А. Н. Климов, частное сообщение.
9. W.-Y. Hwang, Phys. Rev. Lett. **91**, 057901-1 (2003).
10. С. Н. Молотков, Письма в ЖЭТФ **95**, 361 (2012).
11. A. Chefles, arXiv/quant-ph: 9807022; A. Chefles and S. M. Barnett, arXiv/quant-ph: 9807023.
12. Р. Галлагер, *Теория информации и надежная связь*, Сов. радио (1974) [R. G. Gallager, *Information Theory and Reliable Communication*, Wiley, N.Y. (1968)].
13. А. С. Холево, *Введение в квантовую теорию информации*, сер. *Современная математическая физика*, МЦНМО, М. (2002), вып. 5; Успехи мат. наук. **53**, 193 (1998).
14. A. S. Holevo, arXiv:quant-ph/1103.2615.
15. M. D'A.Giacomo, M. D'Ariano, and M. F. Sacchi, arXiv:quant-ph/11031972.
16. Д. А. Кронберг, С. Н. Молотков, Письма в ЖЭТФ **100**, 305 (2014).