ЖЭТФ, 2008, том 133, вып. 1, стр. 5–24

О КРИПТОГРАФИЧЕСКОЙ СТОЙКОСТИ СИСТЕМЫ КВАНТОВОЙ КРИПТОГРАФИИ С ФАЗОВО-ВРЕМЕННЫМ КОДИРОВАНИЕМ

С. Н. Молотков*

Институт физики твердого тела Российской академии наук
142432, Черноголовка, Московская обл., Россия

Академия криптографии Российской федерации
Факультет вычислительной математики и кибернетики,
Московский государственный университет им. М. В. Ломоносова
119899, Москва, Россия

Поступила в редакцию 5 июня 2007 г.

Сделан криптоанализ нового квантового протокола распределения ключей с фазово-временным кодированием. Найдена величина критической ошибки, до которой гарантируется секретность ключей. Особенностью данного протокола является то, что критическая ошибка зависит от наблюдаемой величины отсчетов в контрольном временном слоте. При отсутствии отсчетов в контрольном временном слоте протокол гарантирует секретность ключей вплоть до 50 % ошибок в первичных ключах. В данном протоколе в определенном смысле удалось частично «развязать» ошибки, связанные с неидеальностью самой системы, в частности, с разбалансировкой оптоволоконных интерферометров и действиями подслушивателя. В отсутствие подслушивателя отсчеты в контрольном временном слоте не связаны с разбалансировкой интерферометра, что снижает требования к его стабильности.

PACS: 03.67.Dd

1. ВВЕДЕНИЕ

Квантовая криптография — распределение криптографических ключей по открытым каналам связи (либо оптоволоконному, либо через открытое пространство) — гарантирует детектирование не только попыток подслушивания, но и конфиденциальность передаваемых ключей, что принципиально позволяет реализовать системы шифрования с одноразовыми ключами [1–3]. Секретность финальных ключей гарантируется фундаментальными законами квантовой механики при условии, что ошибка на приемной стороне в первичных ключах не превосходит некоторой критической величины (Q_c), которая определяется используемым протоколом и является фундаментальной величиной для каждого протокола. Практически во всех исследованных и используемых протоколах квантового распределения ключей для детектирования подслушивания и извлечения финальных ключей достаточно знать величину ошибки в первичных ключах [4]. В более общей ситуации детектирование подслушивания должно происходить по изменению статистики фотоотсчетов по отношению к статистике на невозмущенных состояниях. Принципиально невозможно отличить, по какой причине произошло отклонение статистики отсчетов от идеальной статистики. Такое отклонение может быть вызвано как подслушивателем, так и собственными шумами и неидеальностями системы квантовой криптографии, поэтому все отклонения статистики отсчетов (или ошибки в первичных ключах) приходится списывать на действия подслушивателя. Поскольку системы квантовой криптографии работают на пределе современных технологических возможностей, то одним из способов повышения устойчивости их работы является использо-

*E-mail: molotkov@issp.ac.ru

вание квантово-криптографических протоколов распределения ключей, которые обеспечивают секретность ключей при большей критической ошибке.

Одним из способов увеличения критической ошибки, до которой гарантируется секретность распределения ключей, является использование в качестве информационных состояний квантовых систем с размерностью пространства состояний, большей двух (с числом степеней свободы, большим двух). Рост критической ошибки Q_c для подобных протоколов распределения ключей происходит по логарифмическому закону $Q_c \propto \log D$ (D — размерность пространства состояний).

Практически во всех оптоволоконных системах квантовой криптографии из-за того, что оптоволокно не сохраняет поляризацию, используется фазовый метод кодирования с применением разбалансированных оптоволоконных интерферометров Маха–Цандера на передающей и приемной станциях. Увеличение критической ошибки за счет размерности пространства состояний в этом случае неизбежно приводит к использованию многоплечевых интерферометров Маха–Цандера. Однако даже для стандартного двухплечевого интерферометра приходится использовать активную стабилизацию интерферометра (балансировку), поэтому на сегодняшний день еще никому не удалось добиться устойчивой работы многоплечевых схем. Поэтому такой путь увеличения критической ошибки не приводит к успеху [5].

Другой способ увеличения размерности пространства состояний состоит в использовании двухфотонных состояний (бифотонов). Однако такие схемы используют кодирование в поляризационные степени свободы и годятся только для передачи ключей через открытое пространство [6].

Третий способ увеличения размерности пространства состояний и критической ошибки состоит в использовании фазово-временного метода кодирования. Такие протоколы не требуют использования многоплечевых интерферометров Маха–Цандера и какой-либо модификации оптоволоконной части существующих систем, все изменения достигаются за счет небольшой модификации управляющей электроники и программного обеспечения.

Данная работа посвящена квантовому криптоанализу системы квантовой криптографии, использующей комбинированный метод фазово-временного кодирования, предложенный ранее в нашей работе [7]. В некотором смысле данный протокол квантового распределения ключей является комбинацией двух базовых протоколов BB84 [4] и B92 [8].

Для данного протокола найдена точная величина критической ошибки (с учетом коллективной атаки на передаваемый ключ и использования квантовой памяти подслушивателем), до которой гарантируется секретность ключей. Существенной особенностью этого протокола является то, что детектирование попыток подслушивания происходит не только по ошибкам в первичных ключах, но и по изменению статистики фотоотсчетов в контрольном временном слоте. Поэтому область секретности ключей зависит от двух параметров — ошибки Q в первичных ключах и изменения количества отсчетов q в контрольном временном слоте. Критическая величина ошибки зависит от наблюдаемой доли отсчетов в контрольном временном слоте — $Q_c(q)$. Это обстоятельство позволяет частично «разнести» ошибки, связанные с нестабильностью (разбалансированностью) интерферометра и действиями подслушивателя. «Разнести» в том смысле, что для протоколов, в которых детектирование попыток подслушивания происходит только по одному параметру — ошибке Q в первичных ключах, разбалансировка интерферометра также приводит к ошибке. В данном протоколе разбалансировка интерферометра приводит только к ошибке Q и не приводит к появлению отсчетов в контрольном временном слоте. Извлечение какой бы то ни было информации о передаваемом ключе подслушивателем может приводить к появлению как ошибок Q в первичных ключах, так и отсчетов в контрольном временном слоте. Поэтому, если обнаружены ошибки, но нет отсчетов в контрольном временном слоте, можно не прерывать протокол вплоть до появления 50 % ошибок.

Величина ошибки связана с видностью (V) интерференционной картины соотношением $Q = (1-V)/2$. При $Q \to 1/2$ имеет место почти полная потеря видности, однако при этом протокол все еще обеспечивает секретность, если нет отсчетов в контрольном временном слоте. Отсчеты в контрольном слоте не связаны с потерей видности, а возникают либо за счет темновых отсчетов, либо за счет действий подслушивателя.

Напомним, что $Q = 1/2$ — это предельная величина ошибки, до которой вообще возможна передача информации через бинарный классический симметричный канал связи. В данном протоколе вплоть до этой величины ошибки гарантируется еще и секретность ключей при отсутствии отсчетов в контрольном временном слоте.

2. ФОРМАЛЬНОЕ ОПИСАНИЕ МЕТОДА ФАЗОВО-ВРЕМЕННОГО КОДИРОВАНИЯ

Опишем сначала формальный протокол.

В протоколе в качестве информационных состояний используется восемь состояний по два состояния в каждом из четырех базисов, которые будем обозначать как $+L$, $\times L$, $+R$, $\times R$. Состояния имеют вид в базисе $+L$

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

в базисе $\times L$

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

в базисе $+R$

$$|0_{+R}\rangle = \frac{1}{\sqrt{2}}(|2\rangle + |3\rangle), \quad |1_{+R}\rangle = \frac{1}{\sqrt{2}}(|2\rangle - |3\rangle), \quad (3)$$

в базисе $\times R$

$$|0_{\times R}\rangle = \frac{1}{\sqrt{2}}(|2\rangle + i|3\rangle), \quad |1_{\times R}\rangle = \frac{1}{\sqrt{2}}(|2\rangle - i|3\rangle). \quad (4)$$

Здесь $|1\rangle$, $|2\rangle$ и $|3\rangle$ — ортонормированные базисные векторы (забегая вперед, отметим, что данные базисные векторы отвечают локализованным во времени однофотонным состояниям, попарно сдвинутым во времени на определенную величину). Формально пространство состояний $\mathcal{H}$ является трехмерным. Состояния внутри одного базиса ортогональны аналогично протоколу BB84 [4], а состояния из разных базисов попарно неортогональны, как в протоколе B92 [8].

Формально протокол выглядит следующим образом.

1. Алиса на передающей станции равновероятно выбирает одно из восьми состояний и направляет на приемную станцию Бобу.

2. Боб независимо от Алисы случайно и равновероятно выбирает один из четырех базисов для измерений. Более точно, Боб использует случайно одно из четырех измерений, которые описываются следующими разложениями единицы I в $\mathcal{H}$:

$$I = |0_{+L}\rangle\langle 0_{+L}| + |1_{+L}\rangle\langle 1_{+L}| + |3\rangle\langle 3|, \quad \text{измерение в базисе } +L, \quad (5)$$

$$I = |0_{\times L}\rangle\langle 0_{\times L}| + |1_{\times L}\rangle\langle 1_{\times L}| + |3\rangle\langle 3|, \quad \text{измерение в базисе } \times L, \quad (6)$$

$$I = |1\rangle\langle 1| + |1_{+R}\rangle\langle 1_{+R}| + |2_{+R}\rangle\langle 2_{+R}|, \quad \text{измерение в базисе } +R, \quad (7)$$

$$I = |1\rangle\langle 1| + |1_{\times R}\rangle\langle 1_{\times R}| + |2_{\times R}\rangle\langle 2_{\times R}|, \quad \text{измерение в базисе } \times R. \quad (8)$$

3. Боб сообщает только сам факт получения состояния.

4. После проведения серии посылок Алисой и измерений Бобом, Алиса раскрывает базисы, но не раскрывает сами состояния.

5. Боб открыто сообщает номера посылок, где базисы не совпадали. Данные посылки отбрасываются. Результаты измерений в тех посылках, в которых базисы совпадали, сохраняются. В результате измерений Боб получает 0, 1 или отсчет в контрольном временном слоте 3 (в базисе $+, \times L$) или слоте 1 (в базисе $+, \times R$). Номера посылок, где был отсчет в контрольном временном слоте через открытый классический канал, сообщаются Алисе.

6. Боб подсчитывает q — процент отсчетов в контрольных временных слотах.

7. Оценивается процент ошибок в той части посылок, где у Боба был результат 0 или 1, путем раскрытия части посылок и сравнения. Далее эта часть отбрасывается.

8. Если наблюдаемая ошибка при данном числе отсчетов в контрольных временных слотах $Q(q) < Q_c(q)$, то протокол продолжается. В противном случае протокол прерывается. Дальнейшие действия аналогичны другим протоколам [4]. Происходит распределенная коррекция ошибок в оставшейся части, если вероятность ошибки не превышает критической величины. Затем проводится сжатие очищенного ключа (усиление секретности — privacy amplification) [9].

3. ОБЩИЙ КРИТЕРИЙ СЕКРЕТНОСТИ КВАНТОВЫХ ПРОТОКОЛОВ РАСПРЕДЕЛЕНИЯ КЛЮЧЕЙ

Любой квантовый протокол распределения ключей в том и или ином виде сводится к следующему. Алиса случайно выбирает символ k из классического алфавита в соответствии с распределением вероятностей p_k и посылает соответствующее квантовое состояние $\rho_k^A = |\psi_k^A\rangle\langle\psi_k^A|$ (как правило чистое) Бобу. Боб получает возмущенное либо подслушивателем, либо шумом в квантовом канале связи и неидеальностями аппаратуры состояние ρ_k^B, которое также описывается матрицей плотности. Отображение $\mathcal{T}$ (является вполне положительным (completely positive), линейным, сохраняет след, эрмитовость), переводящее матрицы плотности в матрицы плотности является инструментом (чаще его называют супероператором) $\rho_k^B = \mathcal{T}[\rho_k^A]$ [10]. Как известно, супероператор имеет унитарное представление [11]:

$$\rho_k^B = \mathcal{T}[\rho_k^A] = \mathrm{Tr}_E\{|\psi_k^{EB}\rangle\langle\psi_k^{EB}|\} = \\ = \mathrm{Tr}_E\{U_{EB}(|\psi_k^A\rangle|0_E\rangle\langle\psi_k^A|\langle 0_E|)U_{EB}^{-1}\}. \quad (9)$$

На словах такое представление означает, что отображение матриц плотности в матрицы плотности реализуется в виде совместной эволюции, которая описывается унитарным оператором U_{EB} исходного состояния $|\psi_k^A\rangle$ и вспомогательного состояния $|0_E\rangle$ (в нашем случае — подслушивателя или среды — канала). Состояния подсистем получаются взятием частичного следа от общего, запутанного в результате совместной эволюции состояния $|\psi_k^{EB}\rangle$. Аналогично получается состояние Евы после взаимодействия с состоянием Алисы:

$$\rho_k^E = \mathrm{Tr}_B\{|\psi_k^{EB}\rangle\langle\psi_k^{EB}|\} = \\ = \mathrm{Tr}_B\{U_{EB}(|\psi_k^A\rangle|0_E\rangle\langle\psi_k^A|\langle 0_E|)U_{EB}^{-1}\}. \quad (10)$$

Существует фундаментальное ограничение, диктуемое законами квантовой механики, на количество классической информации в битах, которое может быть извлечено Бобом и Евой посредством измерений над ансамблем квантовых состояний $\{\rho_k^B, p_k\}$ и $\{\rho_k^E, p_k\}$. Согласно теореме Холево [12] (см. также [13]), взаимная информация между Алисой и Бобом, а также между Алисой и Евой не превышает величины

$$I_{AB} \le \chi^B = S(\rho^B) - \sum_k p_k S(\rho_k^B), \\ \rho^B = \sum_k p_k \rho_k^B, \quad (11)$$

$$I_{AE} \le \chi^E = S(\rho^E) - \sum_k p_k S(\rho_k^E), \\ \rho^E = \sum_k p_k \rho_k^E, \quad (12)$$

причем равенство достижимо (см. детали в работах [12, 13]). Здесь

$$S(\rho) = -\mathrm{Tr}\{\rho \log \rho\} \quad (13)$$

— энтропия фон Неймана.

Согласно теореме [14], извлечение секретного ключа Алисой и Бобом возможно, если

$$I_{AB} > I_{AE}, \quad \chi^B > \chi^E. \quad (14)$$

Поскольку состояние $|\psi_k^{EB}\rangle$ чистое, то ненулевые собственные числа матриц плотности ρ_k^B и ρ_k^E совпадают, соответственно совпадают энтропии фон Неймана. Секретное распространение ключей между Алисой и Бобом возможно, если

$$S(\rho^B) > S(\rho^E). \quad (15)$$

Отметим, что в реализациях протоколов имеется процедура согласования базисов, т. е. часть переданных состояний отбрасывается, поэтому в формулах (11)–(15) под матрицами плотности надо понимать матрицы плотности, которые остаются после этой процедуры.

4. АНАЛИЗ КРИПТОГРАФИЧЕСКОЙ СТОЙКОСТИ ПРОТОКОЛА

Наиболее общая стратегия подслушивания Евы, допускаемая законами квантовой механики, сводится к следующему. В каждой посылке Ева приготавливает свое вспомогательное состояние $|A\rangle$ (ancilla), которое на некоторое время приводится во взаимодействие с передаваемым состоянием Алисы. Такое взаимодействие описывается унитарным оператором U_{EB}, который Ева задает по своему усмотрению. После взаимодействия состояние Алисы и ancilla оказываются, вообще говоря, в запутанном (нефакторизуемом) состоянии. Возмущенное состояние Алисы направляется Бобу, а ancilla остается у Евы.

Для полного описания действия унитарного оператора U_{EB} достаточно выяснить его действие на базисные состояния $|1\rangle$, $|2\rangle$, $|3\rangle$:

$$U_{EB}(|1\rangle\otimes|A\rangle)=|\Psi_1\rangle=|\phi_1\rangle\otimes|1\rangle+|\theta_1\rangle\otimes\otimes|2\rangle+|\varphi_1\rangle\otimes|3\rangle,$$
$$U_{EB}(|2\rangle\otimes|A\rangle)=|\Psi_2\rangle=|\varphi_2\rangle\otimes|1\rangle+|\phi_2\rangle\otimes\otimes|2\rangle+|\theta_2\rangle\otimes|3\rangle,\quad(16)$$
$$U_{EB}(|3\rangle\otimes|A\rangle)=|\Psi_3\rangle=|\theta_3\rangle\otimes\otimes|1\rangle+|\varphi_3\rangle\otimes|2\rangle+|\phi_3\rangle\otimes|3\rangle.$$

Унитарность требует сохранения нормировки для каждого состояния и углов между ними:

$$\langle\Psi_i|\Psi_j\rangle=\delta_{ij},\quad i,j=1,2,3.\qquad(17)$$

Информационные состояния преобразуются следующим образом. В базисе $+L$ имеем

$$U_{EB}(|0_{+L}\rangle\otimes|A\rangle)=|0_{+L}\rangle\otimes\frac{|\Phi^+_{+L}\rangle+|\Theta^+_{+L}\rangle}{2}+$$
$$+|1_{+L}\rangle\otimes\frac{|\Phi^-_{+L}\rangle-|\Theta^-_{+L}\rangle}{2}+|3\rangle\otimes\frac{|\Psi^+_{+L}\rangle}{\sqrt{2}},\qquad(18)$$

$$U_{EB}(|1_{+L}\rangle\otimes|A\rangle)=|1_{+L}\rangle\otimes\frac{|\Phi^+_{+L}\rangle-|\Theta^+_{+L}\rangle}{2}+$$
$$+|0_{+L}\rangle\otimes\frac{|\Phi^-_{+L}\rangle+|\Theta^-_{+L}\rangle}{2}+|3\rangle\otimes\frac{|\Psi^-_{+L}\rangle}{\sqrt{2}}.\qquad(19)$$

Для базиса $\times L$ получаем

$$U_{EB}(|0_{\times L}\rangle\otimes|A\rangle)=|0_{\times L}\rangle\otimes\frac{|\Phi^+_{\times L}\rangle+|\Theta^+_{\times L}\rangle}{2}+$$
$$+|1_{\times L}\rangle\otimes\frac{|\Phi^-_{\times L}\rangle-|\Theta^-_{\times L}\rangle}{2}+|3\rangle\otimes\frac{|\Psi^+_{\times L}\rangle}{\sqrt{2}},\qquad(20)$$

$$U_{EB}(|1_{\times L}\rangle\otimes|A\rangle)=|1_{\times L}\rangle\otimes\frac{|\Phi^+_{\times L}\rangle-|\Theta^+_{\times L}\rangle}{2}+$$
$$+|0_{\times L}\rangle\otimes\frac{|\Phi^-_{\times L}\rangle+|\Theta^-_{\times L}\rangle}{2}+|3\rangle\otimes\frac{|\Psi^-_{\times L}\rangle}{\sqrt{2}}.\qquad(21)$$

Аналогично получаются возмущенные состояния для сдвинутых по времени состояний. Для состояний в базисе $+R$ находим, что

$$U_{EB}(|0_{+R}\rangle\otimes|A\rangle)=|1\rangle\otimes\frac{|\Psi^+_{+R}\rangle}{\sqrt{2}}+|0_{+R}\rangle\otimes$$
$$\otimes\frac{|\Phi^+_{+R}\rangle+|\Theta^+_{+R}\rangle}{2}+|1_{+R}\rangle\otimes\frac{|\Phi^-_{+R}\rangle-|\Theta^-_{+R}\rangle}{2},\qquad(22)$$

$$U_{EB}(|1_{+R}\rangle\otimes|A\rangle)=|1\rangle\otimes\frac{|\Psi^-_{+R}\rangle}{\sqrt{2}}+|1_{+R}\rangle\otimes$$
$$\otimes\frac{|\Phi^+_{+R}\rangle-|\Theta^+_{+R}\rangle}{2}+|0_{+R}\rangle\otimes\frac{|\Phi^-_{+R}\rangle+|\Theta^-_{+R}\rangle}{2}.\qquad(23)$$

И наконец, для состояний в базисе $\times R$ получаем

$$U_{EB}(|0_{\times R}\rangle\otimes|A\rangle)=|1\rangle\otimes\frac{|\Psi^+_{\times R}\rangle}{\sqrt{2}}+|0_{\times R}\rangle\otimes$$
$$\otimes\frac{|\Phi^+_{\times R}\rangle+|\Theta^+_{\times R}\rangle}{2}+|1_{\times R}\rangle\otimes\frac{|\Phi^-_{\times R}\rangle-|\Theta^-_{\times R}\rangle}{2},\qquad(24)$$

$$U_{EB}(|1_{\times R}\rangle\otimes|A\rangle)=|1\rangle\otimes\frac{|\Psi^-_{\times R}\rangle}{\sqrt{2}}+|1_{\times R}\rangle\otimes$$
$$\otimes\frac{|\Phi^+_{\times R}\rangle-|\Theta^+_{\times R}\rangle}{2}+|0_{\times R}\rangle\otimes\frac{|\Phi^-_{\times R}\rangle+|\Theta^-_{\times R}\rangle}{2}.\qquad(25)$$

Квантовые состояния, введенные в формулах (17)–(25), связаны с исходными (16) следующими соотношениями:

$$|\Phi^\pm_{+L}\rangle=|\phi_1\rangle\pm|\phi_2\rangle,\quad|\Theta^\pm_{+L}\rangle=|\theta_1\rangle\pm|\varphi_2\rangle,\qquad(26)$$

$$|\Phi^\pm_{\times L}\rangle=|\phi_1\rangle\pm i|\phi_2\rangle,\quad|\Theta^\pm_{\times L}\rangle=|\theta_1\rangle\pm i|\varphi_2\rangle,\qquad(27)$$

$$|\Phi^\pm_{+R}\rangle=|\phi_2\rangle\pm|\phi_3\rangle,\quad|\Theta^\pm_{+R}\rangle=|\theta_2\rangle\pm|\varphi_3\rangle,\qquad(28)$$

$$|\Phi^\pm_{\times R}\rangle=|\phi_2\rangle\pm i|\phi_3\rangle,\quad|\Theta^\pm_{\times R}\rangle=|\theta_2\rangle\pm i|\varphi_3\rangle.\qquad(29)$$

Состояния, которые определяют отсчеты в контрольном временном слоте 1 для базиса L и слоте 3 для базиса R, имеют вид

$$|\Psi^\pm_{+L}\rangle=|\theta_2\rangle\pm|\varphi_1\rangle,\quad|\Psi^\pm_{\times L}\rangle=|\theta_2\rangle\pm i|\varphi_1\rangle,\qquad(30)$$

$$|\Psi^\pm_{+R}\rangle=|\varphi_2\rangle\pm|\theta_3\rangle,\quad|\Psi^\pm_{\times R}\rangle=|\varphi_2\rangle\pm i|\theta_3\rangle,\qquad(31)$$

Для дальнейшего анализа важную роль играют соображения симметрии. Всегда можно выбрать размерность пространства состояний для $|A\rangle$ так, чтобы состояния $|\phi_i\rangle$, $|\theta_i\rangle$, $|\varphi\rangle$ лежали во взаимно ортогональных подпространствах.

Для удобства дальнейшего изложения сначала найдем точную критическую ошибку для протокола BB84, который получается из нашего протокола, если использовать в качестве информационных состояний только состояния из базиса $+L$ и $\times L$. Базисное состояние $|3\rangle$ при этом отсутствует.

4.1. Вспомогательные результаты для протокола квантового распределения ключей BB84

Результаты данного раздела являются вспомогательными. Тем не менее они представляют интерес и

сами по себе, поскольку предъявляется явная стратегия Евы, которая позволяет ей получить максимум теоретически возможной информации о передаваемом ключе при минимально производимой при этом ошибке на приемной стороне у Боба.

Ниже речь пойдет о протоколе BB84 [4], который был первым квантовым криптографическим протоколом и который является основным и наиболее исследованным. Для данного протокола известна точная величина критической ошибки $Q_c \approx 11\,\%$ [15–17][1)]. Строгие доказательства, касающиеся критической величины Q_c, скорее являются теоремами существования и не предъявляют явную оптимальную стратегию подслушивателя, при которой достигается теоретически минимально возможное значение Q_c. Точнее говоря, оптимальную стратегию в том смысле, что Ева извлекает максимум информации о ключе при данной наблюдаемой ошибке. При $Q < Q_c$ взаимная информация между легитимными пользователями Алисой и Бобом о ключе больше, чем между Алисой и Евой, $I_{AB}(Q) > I_{AE}(Q)$, что позволяет, согласно теореме [14], извлечь секретный ключ. При $Q = Q_c$ выполняется равенство $I_{AB}(Q) = I_{AE}(Q)$ и получить секретный ключ нельзя. Формально длина секретного ключа при $Q = Q_c$ обращается в нуль.

Существует множество работ, в которых рассматриваются частичные стратегии Евы. В частности, была построена оптимальная стратегия Евы для индивидуальных измерений (см. [18]), которая кратко сводится к следующему. Ева в каждой посылке использует свое квантовое вспомогательное состояние $|A\rangle$, которое унитарно взаимодействует с передаваемым состоянием. В результате передаваемое состояние и $|A\rangle$ оказываются в запутанном состоянии. Состояние $|A\rangle$ изменяется в зависимости от передаваемого состояния. Изменяется также передаваемое состояние. Затем измененное состояние Алисы направляется Бобу, а свое состояние Ева сохраняет у себя в квантовой памяти до стадии раскрытия базисов. После того как Боб провел измерения, происходит согласование базисов. Посылки, где Боб проводил измерения в не согласованном с Алисой базисе, отбрасываются. Далее Ева проводит индивидуальные измерения над каждым своим состоянием с целью извлечения классической информации о передаваемом бите Алисы. Для такой стратегии найдена критическая величина ошибки, до которой возможно распределение секретных ключей. Критическая ошибка оказывается равной $Q_c \approx 15\,\%$, что выше теоретического значения $11\,\%$. Таким образом, подобная стратегия Евы не является оптимальной в упомянутом выше смысле.

Других явных стратегий Евы, при которых получается меньший вносимый процент ошибок, неизвестно.

Здесь будет показано, что если Ева использует на последнем шаге не индивидуальные измерения над каждым своим состоянием, а коллективные сразу над всеми состояниями, то в этом случае достигается минимальная предельно допустимая ошибка, равная $11\,\%$.

Данная стратегия применима и в других протоколах, в которых имеется процедура согласования базисов. Поскольку каждая посылка не зависит от предыдущей, достаточно сначала найти общую стратегию для каждой индивидуальной посылки. Унитарное преобразование Евы зависит от ряда параметров, которые подлежат определению. Параметры унитарного преобразования определяются таким образом, чтобы Ева могла получить максимум информации о ключе при минимуме наблюдаемой у Боба ошибки. Это достигается при коллективных измерениях Евы сразу над всей последовательностью квантовых состояний, находящихся в ее квантовой памяти. Причем измерения делаются в самом конце, после процедуры коррекции ошибок Алисой и Бобом.

После вторжения Евы в канал связи состояния, которые доступны для измерений Боба на приемной стороне, описываются матрицами плотности, которые получаются взятием частичного следа по пространству состояний Евы. Имеем в базисе $\times L$ (далее в этом разделе для краткости индекс L будем опускать)

$$\rho_B(0_+) = \mathrm{Tr}\{|\Psi_{EB}(0_+)\rangle\langle\Psi_{EB}(0_+)|\} = |0_+\rangle\langle 0_+|\frac{\langle\Phi_+^+|\Phi_+^+\rangle + \langle\Theta_+^+|\Theta_+^+\rangle}{4} + |1_+\rangle\langle 1_+|\frac{\langle\Phi_+^-|\Phi_+^-\rangle + \langle\Theta_+^-|\Theta_+^-\rangle}{4}, \quad (32)$$

$$\rho_B(1_+) = \mathrm{Tr}\{|\Psi_{EB}(1_+)\rangle\langle\Psi_{EB}(1_+)|\} = |1_+\rangle\langle 1_+|\frac{\langle\Phi_+^+|\Phi_+^+\rangle + \langle\Theta_+^+|\Theta_+^+\rangle}{4} + |0_+\rangle\langle 0_+|\frac{\langle\Phi_+^-|\Phi_+^-\rangle + \langle\Theta_+^-|\Theta_+^-\rangle}{4}. \quad (33)$$

[1)] Знак $\approx$ употребляется для краткости, точное значение Q_c определяется как корень некоторого трансцендентного уравнения [14].

Аналогично для состояний в базисе $\times L$ получаем

$$\rho_B(0_\times) = \mathrm{Tr}\{|\Psi_{EB}(0_\times)\rangle\langle\Psi_{EB}(0_\times)|\} = \\ = |0_\times\rangle\langle 0_\times|(\frac{\langle\Phi_\times^+|\Phi_\times^+\rangle + \langle\Theta_\times^+|\Theta_\times^+\rangle}{4} + \\ + |1_\times\rangle\langle 1_\times|\frac{\langle\Phi_\times^-|\Phi_\times^-\rangle + \langle\Theta_\times^-|\Theta_\times^-\rangle}{4}, \quad (34)$$

$$\rho_B(1_\times) = \mathrm{Tr}\{|\Psi_{EB}(1_\times)\rangle\langle\Psi_{EB}(1_\times)|\} = \\ = |1_\times\rangle\langle 1_\times|\frac{\langle\Phi_\times^+|\Phi_\times^+\rangle + \langle\Theta_\times^+|\Theta_\times^+\rangle}{4} + \\ + |0_\times\rangle\langle 0_\times|\frac{\langle\Phi_\times^-|\Phi_\times^-\rangle + \langle\Theta_\times^-|\Theta_\times^-\rangle}{4}. \quad (35)$$

Поскольку базисы $+$ и $\times$ выбираются случайно и равновероятно, требование симметрии диктует, чтобы ошибка, производимая Евой на приемной стороне, не зависела от выбора базиса, т. е. была одинаковой в разных базисах. Кроме того, условие унитарности U_{EB} фактически сводится к сохранению нормировки и углов между $|0_+\rangle$, $|0_\times\rangle$, $|1_+\rangle$ и $|1_\times\rangle$, что приводит к условиям в базисе $+$

$$\begin{aligned}\langle\Phi_+^+|\Phi_+^-\rangle + \langle\Theta_+^+|\Theta_+^-\rangle = 0,\\ \langle\Phi_+^+|\Phi_+^-\rangle - \langle\Theta_+^+|\Theta_+^-\rangle = 0,\end{aligned} \quad (36)$$

в базисе $\times$

$$\begin{aligned}\langle\Phi_\times^+|\Phi_\times^-\rangle + \langle\Theta_\times^+|\Theta_\times^-\rangle = 0,\\ \langle\Phi_\times^+|\Phi_\times^-\rangle - \langle\Theta_\times^+|\Theta_\times^-\rangle = 0.\end{aligned} \quad (37)$$

Вероятность ошибки Q на приемной стороне у Боба дается коэффициентом при $|1_+\rangle$, когда Алисой было послано состояние $|0_+\rangle$ в базисе $+$. Аналогично для единицы в базисе $+$. Равенство ошибок в разных базисах с учетом формул (32)–(35) дает

$$Q = \frac{\langle\Phi_+^-|\Phi_+^-\rangle + \langle\Theta_+^-|\Theta_+^-\rangle}{4} = \\ = \frac{\langle\Phi_\times^-|\Phi_\times^-\rangle + \langle\Theta_\times^-|\Theta_\times^-\rangle}{4}. \quad (38)$$

Соответственно, вероятность правильного отсчета у Боба равна

$$1 - Q = \frac{\langle\Phi_+^+|\Phi_+^+\rangle + \langle\Theta_+^+|\Theta_+^+\rangle}{4} = \\ = \frac{\langle\Phi_\times^+|\Phi_\times^+\rangle + \langle\Theta_\times^+|\Theta_\times^+\rangle}{4}. \quad (39)$$

Упомянутые выше условия удовлетворяются, если модифицированные состояния Евы после взаимодействия ancilla $|A\rangle$ с состоянием Алисы выбрать в виде

$$\begin{aligned}|\phi_1\rangle = \sqrt{1-Q}|x\rangle\otimes|x\rangle,\\ |\phi_2\rangle = \sqrt{1-Q}(\cos\alpha|x\rangle\otimes|x\rangle + \sin\alpha|y\rangle\otimes|x\rangle),\end{aligned} \quad (40)$$

$$\begin{aligned}|\theta_1\rangle = \sqrt{Q}|x\rangle\otimes|y\rangle,\\ |\varphi_2\rangle = \sqrt{Q}(\cos\alpha|x\rangle\otimes|y\rangle + \sin\alpha|y\rangle\otimes|y\rangle).\end{aligned} \quad (41)$$

Здесь $|i\rangle\otimes|j\rangle$ $(i,j = x,y)$ — ортогональные нормированные базисные состояния в пространстве состояний ancilla у Евы. С учетом требований симметрии унитарный оператор, задаваемый Евой, однозначно параметризуется двумя параметрами Q, α. Угол α Ева должна выбрать так, чтобы максимизировать свою информацию о ключе при условии, что на приемной стороне у Боба будет наблюдаемый процент ошибок Q.

С учетом формул (32)–(35), (40), (41) матрица плотности на приемной стороне у Боба принимает вид (в базисе $+L$)

$$\rho_B(0_+) = (1-Q)|0_+\rangle\langle 0_+| + Q|1_+\rangle\langle 1_+|, \quad (42)$$

$$\rho_B(1_+) = (1-Q)|1_+\rangle\langle 1_+| + Q|0_+\rangle\langle 0_+|, \quad (43)$$

аналогично для 0 и 1 в базисе $\times R$.

Связь между наблюдаемой у Боба вероятностью ошибки Q и параметром α дается соотношением

$$Q = \frac{1-\cos\alpha}{2}. \quad (44)$$

4.1.1. Измерения на приемной стороне

Боб проводит измерения в каждой посылке в одном из двух сопряженных базисов. Измерение в базисе $+$ описывается разложением единицы

$$I = |0_+\rangle\langle 0_+| + |1_+\rangle\langle 1_+|, \quad (45)$$

а в базисе $\times$ — разложением

$$I = |0_\times\rangle\langle 0_\times| + |1_\times\rangle\langle 1_\times|, \quad (46)$$

которые Боб выбирает случайно и равновероятно.

После передачи всей последовательности происходит согласование базисов между Алисой и Бобом через открытый классический канал связи. Посылки, в которых базисы не совпадали, отбрасываются. Вероятности получения результатов в совпадающих базисах имеют вид

$$\Pr(0|0) = \mathrm{Tr}\{\rho_B(0_+)|0_+\rangle\langle 0_+|\} = \\ = \mathrm{Tr}\{\rho_B(0_\times)|0_\times\rangle\langle 0_\times|\} = \\ = \Pr(1|1) = \mathrm{Tr}\{\rho_B(1_+)|1_+\rangle\langle 1_+|\} = \\ \mathrm{Tr}\{\rho_B(1_\times)|1_\times\rangle\langle 1_\times|\} = 1 - Q, \quad (47)$$

$$\Pr(0|1) = \mathrm{Tr}\{\rho_B(0_+)|1_+\rangle\langle 1_+|\} = \\ = \mathrm{Tr}\{\rho_B(0_\times|1_\times\rangle\langle 1_\times|\} = \\ = \Pr(1|0) = \mathrm{Tr}\{\rho_B(1_+)|0_+\rangle\langle 0_+|\} = \\ = \mathrm{Tr}\{\rho_B(1_\times|0_\times\rangle\langle 0_\times|\} = Q. \quad (48)$$

Здесь $\Pr(i|j)$ — условная вероятность того, что Алисой был послан бит i, а Боб интерпретировал результат как бит j, Q — вероятность ошибки у Боба.

Ева пока не проводит измерения, а сохраняет свои состояния в квантовой памяти. Далее Боб раскрывает часть последовательности для оценки вероятности ошибки Q, раскрытая часть отбрасывается.

Если в базисе + Алисой был послан 0, то в результате измерений Боба в этом базисе с вероятностью $1-Q$ будет получен правильный результат 0, состояние Евы при этом будет равно

$$\frac{1}{2}\left(|\Phi_+^+\rangle + |\Theta_+^+\rangle\right), \quad (49)$$

и с вероятностью Q Бобом будет получена 1 — результат с ошибкой. Состояние Евы в этом случае имеет вид

$$\frac{1}{2}\left(|\Phi_+^-\rangle - |\Theta_+^-\rangle\right). \quad (50)$$

Аналогично для ситуации, когда Алиса посылала 1. Поскольку результат измерений Боба не разглашается, состояние Евы после измерений Боба, когда Алиса посылала 0, записывается как

$$\rho_E(0_+) = \frac{|\Phi_+^+\rangle\langle\Phi_+^+| + |\Theta_+^+\rangle\langle\Theta_+^+|}{4} + \\ + \frac{|\Phi_+^-\rangle\langle\Phi_+^-| + |\Theta_+^-\rangle\langle\Theta_+^-|}{4}; \quad (51)$$

аналогично для случая, когда Алисой была послана 1, имеем

$$\rho_E(1_+) = \frac{|\Phi_+^+\rangle\langle\Phi_+^+| + |\Theta_+^+\rangle\langle\Theta_+^+|}{4} + \\ + \frac{|\Phi_+^-\rangle\langle\Phi_+^-| + |\Theta_+^-\rangle\langle\Theta_+^-|}{4}. \quad (52)$$

Для посылок в базисе $\times$ находим

$$\rho_E(0_\times) = \frac{|\Phi_\times^+\rangle\langle\Phi_\times^+| + |\Theta_\times^+\rangle\langle\Theta_\times^+|}{4} + \\ + \frac{|\Phi_\times^-\rangle\langle\Phi_\times^-| + |\Theta_\times^-\rangle\langle\Theta_\times^-|}{4}, \quad (53)$$

аналогично для случая, когда Алисой была послана 1, имеем

$$\rho_E(1_\times) = \frac{|\Phi_\times^+\rangle\langle\Phi_\times^+| + |\Theta_\times^+\rangle\langle\Theta_\times^+|}{4} + \\ + \frac{|\Phi_\times^-\rangle\langle\Phi_\times^-| + |\Theta_\times^-\rangle\langle\Theta_\times^-|}{4}. \quad (54)$$

4.1.2. Коррекция ошибок в первичных ключах легитимными пользователями

Далее происходит распределенная коррекция ошибок у Боба. На этой стадии Алиса и Боб находятся в ситуации классического бинарного симметричного канала связи с вероятностью ошибки Q. Наиболее эффективная процедура сводится к использованию случайных кодов [19]. Пусть длина оставшейся последовательности есть n. Алиса генерирует $2^{n(C_{clas}(Q)-\delta)}$ ($\delta \to 0$ при $n \to \infty$) случайных кодовых слов. Здесь

$$C_{clas}(Q) = 1 - h(Q), \\ h(Q) = -Q\log Q - (1-Q)\log(1-Q), \quad (55)$$

— соответственно пропускная способность классического бинарного симметричного канала связи и энтропийная функция Шеннона.

Посланную битовую последовательность Алиса также включает в этот список. Далее этот список слов открыто сообщается Бобу, а значит и Еве. Согласно теореме кодирования для канала с шумом, при таком числе кодовых слов Боб с вероятностью единица выберет строку битов, посланную Алисой. Выбор осуществляется просмотром всех кодовых слов и сравнением с битовой строкой у Боба. Боб выбирает то кодовое слово, которое ближе всего в метрике Хэмминга к кодовому слову в таблице.

После раскрытия базисов шенноновская взаимная информация между Алисой и Евой, если Ева делает индивидуальные измерения, дается приведенной ниже формулой (для индивидуальных измерений ситуация для базисов + и $\times$ может рассматриваться независимо). Например, в базисе + имеем

$$I(A;E,\pi,\mathcal{M}) = \sum_{x,y}\pi_x p_{\mathcal{M}}(y|x)[\log p_{\mathcal{M}}(y|x) - \\ - \log\sum_{z=x,y}\pi_z p_{\mathcal{M}}(y|z)], \quad x,y=0,1, \quad (56)$$

где $\pi_x = \pi_y = 1/2$ — априорные распределения вероятностей для $\rho_E(0)$, $\rho_E(1)$, которые заданы Алисой; $\mathcal{M} = \{M_0, M_1\}$ — измеряющие операторы Евы. Условная вероятность, например, того, что у Евы в ячейке квантовой памяти было квантовое состояние, отвечающее 1 — $\rho_E(1)$, а результат измерения был интерпретирован как 0, имеет вид

$$p_{\mathcal{M}}(0|1) = \mathrm{Tr}\{\rho_E(1)M_0\}.$$

Согласно [12], максимальное количество классической информации, допустимое законами квантовой механики при индивидуальных измерениях, равно

$$C_1 = \max_{\pi,\mathcal{M}} I(A; E, \pi, \mathcal{M}). \quad (57)$$

Поскольку распределение априорных вероятностей π фактически задано Алисой, Ева может лишь оптимизировать измерения $\mathcal{M}$ так, чтобы уменьшить вероятность ошибки.

4.1.3. Допустимая ошибка при индивидуальных измерениях подслушивателя

Цель Евы — извлечь максимум классической информации из ансамбля квантовых состояний и произвести при этом минимально возможную ошибку Q на приемной стороне у Боба.

Если Ева делает индивидуальные измерения над каждым своим состоянием, минимизирующие ошибку различения, то это сводится после раскрытия базисов Алисой и Бобом к различению переданных битов 0 и 1 — матриц плотности $\rho_E(0_+)$ и $\rho_E(1_+)$ в базисе + или матриц плотности $\rho_E(0_\times)$ и $\rho_E(1_\times)$ в базисе $\times$. Такое измерение $\mathcal{M}$ известно (см. детали в работе [12]), ошибка различения 0 и 1 равна

$$\begin{aligned} Q_E &= \frac{1}{2}\left(1 - \sqrt{1-\varepsilon^2(Q)}\right) = \frac{1-\sin\alpha}{2} = \\ &= \frac{1}{2}\left(1 - \sqrt{1-(1-2Q)^2}\right), \\ \varepsilon(Q) &= |\langle\phi_1|\phi_2\rangle| = |\langle\theta_1|\varphi_2\rangle|. \end{aligned} \quad (58)$$

Здесь учтено, что $|\phi_{1,2}\rangle$ и $|\theta_1\rangle$, $|\varphi_2\rangle$ ортогональны, и введены обозначения

$$Q_E = p(1|0) = p(0|1), \quad C_1(\varepsilon(Q)) = C_1.$$

После проведения индивидуальных измерений Ева имеет битовую строку, в которой вероятность ошибки равна Q_E. Поскольку кодовая таблица Алисы для исправления ошибок у Боба известна также и Еве, Ева может, просматривая кодовые слова в таблице и сравнивая их со своей строкой, определить строку, которую посылала Алиса. Однако, если вероятность ошибки у Евы Q_E больше, чем вероятность ошибки у Боба Q, то, согласно сильному обращению теоремы кодирования для канала с шумом [20, 21], Ева с вероятностью единица не сможет выбрать правильное кодовое слово. Иначе говоря, Ева с вероятностью единица может различить не более $2^{nC_1(\varepsilon(Q))}$ кодовых слов. В противном случае (при $n \to \infty$) Ева с вероятностью единица выберет неправильное кодовое слово.

Таким образом, количество кодовых слов, которые может различить Ева, не превышает

$$2^{nC_{clas}(Q)} = 2^{nC_1(\varepsilon(Q))}.$$

Критическая величина ошибки определяется из равенства

$$C_{clas}(Q) = C_1(\varepsilon(Q)), \quad (59)$$

$$\begin{aligned} C_1(\varepsilon(Q)) = \frac{1}{2}\Big[&\left(1 - \sqrt{1-\varepsilon^2(Q)}\right) \times \\ &\times \log\left(1 - \sqrt{1-\varepsilon^2(Q)}\right) + \left(1 + \sqrt{1-\varepsilon^2(Q)}\right) \times \\ &\times \log\left(1 + \sqrt{1-\varepsilon^2(Q)}\right)\Big]. \end{aligned} \quad (60)$$

Здесь $C_1(\varepsilon(Q))$ — классическая пропускная способность бинарного квантового канала связи за один шаг (one shot). Фактически Ева после раскрытия базисов находится с Алисой в ситуации бинарного квантового канала связи с вероятностью ошибки Q_E.

При индивидуальных измерениях распределение ключа возможно, если

$$C_{clas}(Q) \geq C_1(\varepsilon(Q)). \quad (61)$$

Критическая величина ошибки для индивидуальных измерений Евы определяется, как корень уравнения

$$C_{clas}(Q_c) = C_1(\varepsilon(Q_c)), \quad Q_c \approx 15\,\%. \quad (62)$$

Это фактически эквивалентно равенству вероятностей ошибки:

$$\begin{aligned} Q = Q_E &= \frac{1}{2}\left(1 - \sqrt{1-\varepsilon^2(Q)}\right) = \\ &= \frac{1}{2}\left(1 - \sqrt{1-(1-2Q)^2}\right), \\ Q_c &= \frac{1}{2}\left(1 - \frac{1}{\sqrt{2}}\right) = 14.645\,\% \approx 15\,\%. \end{aligned} \quad (63)$$

4.1.4. Допустимая ошибка при коллективных измерениях подслушивателя

Ева может извлечь больше классической информации, если она будет проводить коллективные измерения сразу над всей имеющейся у нее в квантовой памяти последовательностью. Индивидуальные измерения Евы сводились фактически к различению состояний $|\phi_1\rangle$ и $|\phi_2\rangle$ (аналогично $|\theta_1\rangle$ и $|\varphi_2\rangle$), измерения сводились к проекции на два ортогональных вектора (один в плоскости на диагонали посредине между $|\phi_0\rangle$ и $|\phi_1\rangle$, второй в той же плоскости, ортогональный первому). Аналогично в подпространстве, натянутом на векторы $|\theta_1\rangle$ и $|\varphi_2\rangle$. Коллективные измерения отвечают, грубо говоря, проекциям на специальные сцепленные (запутанные) со-

стояния из n кубитов (см. ниже явный вид измеряющих операторов X_w). В этом случае соответствующая шенноновская взаимная информация, согласно [12], есть

$$I_n(A;E,\pi,\mathcal{X}) = \sum_w \pi_w p_{\mathcal{X}}(\hat{w}|w)[\log p_{\mathcal{X}}(\hat{w}|w) - \\ - \log \sum_{w'} \pi_{w'} p_{\mathcal{X}}(\hat{w}|w')]. \quad (64)$$

Здесь π_w — распределение вероятностей для последовательностей длины n состояний Евы в квантовой памяти, в каждой ячейке которой с равной вероятностью присутствует $\rho_E(0_+)$ и $\rho_E(1_+)$ (аналогично в базисе $\times$). Количество классической информации, которое может быть извлечено при коллективных измерениях (проекциях на запутанные состояния из n кубитов) по определению [12] есть

$$C_n = \max_{\pi_w,\mathcal{X}} I(A;E,\pi_w,\mathcal{X}), \quad (65)$$

поскольку априорное распределение вероятностей π_w задано Алисой, максимизация происходит по различным измерениям. Предельное значение $C_\infty = \lim_{n\to\infty} C_n$ называется классической пропускной способностью квантового канала связи.

Поскольку базисы раскрыты, набор из M битовых кодовых слов $w^{(1)}, w^{(2)}, \ldots, w^{(M)}$ ($w^{(k)} = (i_1^k, i_2^k, \ldots, i_n^k)$, $i_j^k = 0,1$) однозначно связан с квантовыми состояниями, из которых данные битовые строки могли произойти:

$$|w^{(k)}\rangle = |i_1^k(b_1)\rangle \otimes |i_2^k(b_2)\rangle \otimes \ldots \otimes |i_n^k(b_n)\rangle.$$

Здесь $|i_1^k(b_1)\rangle$ — состояние, если первый бит в k-м кодовом слове Алисы $i_1^k = 0$ и раскрытый базис в первой посылке был b_1.

Таким образом, после оглашения Алисой таблицы классических битовых кодовых слов Ева знает всю таблицу из кодовых слов квантовых состояний, но не знает, какая конкретная последовательность была послана.

Другими словами, из-за однозначной связи классических и квантовых слов, можно считать, что Алиса и Ева соединены идеальным квантовым каналом связи. Формально можно считать, что Алиса кодирует классические последовательности $w^{(k)}$ в тензорное произведение матриц плотности Евы

$$\rho_{w^{(k)}} = \rho_E(i^{k_1}(b_1)) \otimes \rho_E(i^{k_2}(b_2)) \otimes \ldots \otimes \rho_E(i^{k_n}(b_n)).$$

Число таких квантовых кодовых слов равно числу классических кодовых слов, которое выбирается Алисой в зависимости от наблюдаемой ошибки у Боба.

Ева должна использовать квантово-механические измерения с целью различения посланного Алисой кодового слова. Согласно фундаментальной теореме кодирования для квантового канала связи [8], максимальное число кодовых слов, которое Ева может различить, не более $M = 2^{n\overline{C}(\varepsilon(Q))}$, при этом Ева использует коллективные измерения сразу над всей последовательностью. Как и любое измерение, такое коллективное измерение описывается разложением единицы (см. детали в [12,13]):

$$I = \sum_{k=1}^{M} X_{w^{(k)}}, \quad X_{w^{(k)}} = \left(\sum_{l=1}^{M} PP_{w^{(l)}}P\right)^{-1/2} \times \\ \times PP_{w^{(k)}}P \left(\sum_{l=1}^{M} PP_{w^{(l)}}P\right)^{-1/2}, \quad (66)$$

где $P_{w^{(k)}}$ — проектор на типичное подпространство для оператора $\rho_{w^{(k)}}$, т. е. спектральный проектор оператора $\rho_{w^{(k)}}$, отвечающий собственным числам $\lambda_J = \lambda_{j_1}\lambda_{j_2}\ldots\lambda_{j_n}$ в интервале

$$2^{-n\left(\sum_{i=0_+,1_+,0_\times,1_\times} \frac{1}{4}S(\rho_E(i))+\delta\right)} < \lambda_J < \\ < 2^{-n\left(\sum_{i=0_+,1_+,0_\times,1_\times} \frac{1}{4}S(\rho_E(i))-\delta\right)},$$

P — проектор на типичное подпространство для оператора

$$\left(\sum_{i=0_+,1_+,0_\times,1_\times} \frac{1}{4}\rho_E(i)\right)^{\otimes n}, \\ P = \sum_{J\in Typ} |\lambda_J\rangle\langle\lambda_J|. \quad (67)$$

Здесь

$$|\lambda_J\rangle = |\lambda_{j_1}\rangle \otimes |\lambda_{j_2}\rangle \otimes \ldots \otimes |\lambda_{j_n}\rangle,$$

$|\lambda_{j_m}\rangle$ — собственные векторы оператора (67), типичное пространство — это пространство всех последовательностей, для которых

$$Typ = \Big\{ J : 2^{-n(S(\sum_{i=0_+,1_+,0_\times,1_\times} \frac{1}{4}\rho_E(i)+\delta))} < \lambda_J < \\ < 2^{-n(S(\sum_{i=0_+,1_+,0_\times,1_\times} \frac{1}{4}\rho_E(i)-\delta))} \Big\}.$$

Аналогично индивидуальным измерениям введем обозначение $\overline{C}(\varepsilon(Q)) = C_\infty$. В этом случае Ева сможет различить $2^{n\overline{C}(\varepsilon(Q))}$ кодовых слов, где

$$\overline{C}(\varepsilon(Q)) = S\sum_{i=0_+,1_+,0_\times,1_\times}\frac{1}{4}\rho_E(i) - \\ -\sum_{i=0_+,1_+,0_\times,1_\times}\frac{1}{4}S(\rho_E(i)), \\ S(\rho) = -\mathrm{Tr}\{\rho\log\rho\}. \tag{68}$$

$\overline{C}(\varepsilon(Q))$ — классическая пропускная способность квантового канала связи [12].

Для вычисления $\overline{C}(\varepsilon(Q))$ потребуются собственные числа λ_{1-4} матрицы плотности

$$\sum_{i=0_+,1_+,0_\times,1_\times}\frac{1}{4}\rho_E(i) = \frac{1}{2}\times \\ \times\begin{pmatrix} 1-Q & (1-Q)\varepsilon(Q) & 0 & 0 \\ (1-Q)\varepsilon(Q) & 1-Q & 0 & 0 \\ 0 & 0 & Q & Q\varepsilon(Q) \\ 0 & 0 & Q\varepsilon(Q) & Q \end{pmatrix}, \tag{69}$$

$$\lambda_{1,2} = \frac{1-Q}{2}\,\frac{1\pm\varepsilon(Q)}{2}, \quad \lambda_{3,4} = \frac{Q}{2}\,\frac{1\pm\varepsilon(Q)}{2}.$$

Собственные числа частичных матриц плотности $\rho_E(0_+,1_+,0_\times,1_\times)$ равны $1-Q$ и Q. При $2^{n\overline{C}(\varepsilon(Q))} \le 2^{nC_{clas}(Q)}$ возможно секретное распределение ключей между Алисой и Бобом. Учитывая связь Q и $\varepsilon(Q)$ из (8), находим

$$\overline{C}(\varepsilon(Q)) = -Q\log Q - (1-Q)\log(1-Q), \\ \varepsilon(Q) = 1-2Q. \tag{70}$$

Критическая величина ошибки

$$C_{clas}(Q_c) = \overline{C}(\varepsilon(Q_c)), \\ 1-h(Q_c) = h(Q_c), \quad Q_c \approx 11\,\%, \tag{71}$$

что совпадает с точным значением (см. [17], а также [15, 16]).

Зависимости $C_{clas}(Q)$, $\overline{C}(\varepsilon(Q))$ и $C_1(\varepsilon(Q))$ представлены на рис. 1. Точки пересечения кривой $C_{clas}(Q)$ с кривыми $\overline{C}(\varepsilon(Q))$ и $C_1(\varepsilon(Q))$ определяют критическую ошибку, до которой возможно секретное распространение ключей в случае, если Ева использует коллективные и индивидуальные измерения.

4.2. Промежуточная область ошибок $11\,\% < Q_c < 15\,\%$

Если Ева на конечном этапе проводит индивидуальные измерения, минимизирующие ошибку различения двух некоммутирующих матриц плотности,

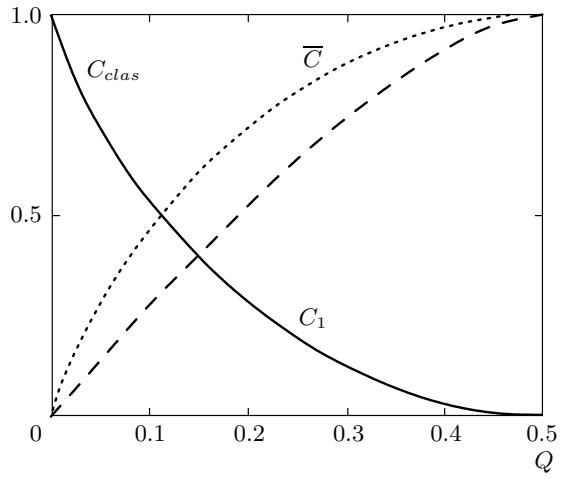

Рис. 1. Зависимости $C_{clas}(Q)$, $\overline{C}(\varepsilon(Q))$ и $C_1(\varepsilon(Q))$

это соответствует достижению пропускной способности квантового канала между Алисой и Евой за один шаг C_1. Критическая величина ошибки при этом $Q_c \approx 15\,\%$. При коллективных измерениях Евы, минимизирующих различение кодовых последовательностей матриц плотности,

$$\rho_{w^{(k)}} = \rho_E(i^{k_1}(b_1)) \otimes \rho_E(i^{k_2}(b_2)) \otimes \ldots \otimes \rho_E(i^{k_n}(b_n)),$$

при этом достигается классическая пропускная способность квантового канала связи $\overline{C}$. Допустимая критическая ошибка для протокола BB84, до которой гарантируется секретное распределение ключей, при этом равна $Q_c \approx 11\,\%$.

Что происходит в области $11\,\% < Q_c < 15\,\%$? Как было отмечено в работе [22], для квантового канала связи (точнее, канала c-q — classical-quantum, в котором классическая информация передается при помощи квантовых состояний) существует бесконечный набор классических пропускных способностей квантового канала связи. А именно, если длина кодового слова равна 1 (квантовые состояния измеряются индивидуально в каждой посылке), то максимально достижимое количество классической информации, которое можно передать при помощи квантовых состояний, не превосходит C_1 (в обозначениях [22] — $C_{1,1}$). Если длина кодового слова равна всей длине последовательности $n \to \infty$ (что отвечает коллективным измерениям над всей последовательностью), то классическая информация, извлекаемая из квантовых состояний, ограничена $\overline{C}$ (в обозначениях [22] — $C_{1,\infty}$). Длина кодового слова k может быть любой от $k=1$ до $k=\infty$, соответственно, доступное количество классической информации

не превосходит $C_{1,k}$. Если длина кодового слова k, это означает, что возможны коллективные измерения не более, чем над k квантовыми состояниями сразу. При этом $C_{1,1} < C_{1,k} < C_{1,\infty}$, критическая ошибка определяется из условия

$$\begin{gathered} C_{clas}(Q_{c,k}) = C_{1,k}(\varepsilon(Q)), \\ Q_{c,\infty} = 11\,\% < Q_{c,k} < Q_{c,1} = 15\,\%, \end{gathered} \tag{72}$$

что дает ответ на вопрос о том, что происходит в области критической ошибки между 11 % и 15 %.

Таким образом, описана явная атака на ключ, при которой достигается максимум информации Евы при минимуме наблюдаемой ошибки на приемном конце. Данная атака сводится к реализации совместной эволюции в каждой посылке состояния, передаваемого Алисой, со вспомогательным состоянием Евы. Унитарный оператор U_{EB} (16), описывающий совместную эволюцию состояния Алисы и Евы, строится явно (40), (41). По нему можно предъявить квантовую схему, которая реализует такой оператор. Далее Ева сохраняет состояния в квантовой памяти до раскрытия базисов Алисой и Бобом, и только затем проводит коллективные измерения сразу над всеми состояниями.

4.3. Связь с общим критерием секретности

Для сокращения выкладок в следующем разделе удобно получить величину критической ошибки непосредственно из общего критерия секретности для квантового протокола распределения ключей.

После раскрытия и согласования базисов Алисой и Бобом матрица плотности Евы для состояний, относящихся как к базису $+$, так и к базису $\times$, с учетом формул (16)–(31), принимает вид

$$\begin{aligned} \rho_E(+) = \rho_E(\times) = \frac{1}{4}(|\phi_1\rangle\langle\phi_1| + |\phi_2\rangle\langle\phi_2| + \\ + |\theta_1\rangle\langle\theta_1| + |\varphi_2\rangle\langle\varphi_2|). \end{aligned} \tag{73}$$

Собственные числа

$$\rho_E = \frac{1}{2}(\rho_E(+) + \rho_E(\times))$$

естественно совпадают с (69) и имеют вид

$$\begin{gathered} \lambda_1 = Q(1-Q), \quad \lambda_2 = QQ, \\ \lambda_3 = (1-Q)(1-Q), \quad \lambda_4 = (1-Q)Q. \end{gathered} \tag{74}$$

С учетом (73) находим выражение для $\chi(\rho_E)$:

$$\chi(\rho_E) = S(\rho_E) = 2h(Q). \tag{75}$$

Аналогично для матрицы плотности Боба

$$\rho_B = \frac{1}{2}(\rho_E(+) + \rho_E(\times))$$

с учетом формул (42), (43) получаем

$$\rho_B = \frac{1}{2}|1\rangle\langle 1| + \frac{1}{2}|2\rangle\langle 2|, \tag{76}$$

соответственно, оба собственных числа равны $1/2$.

Энтропия фон Неймана есть

$$\chi(\rho_B) = S(\rho_B) = 1. \tag{77}$$

Равенство выражений (75) и (77) дает критическую ошибку, до которой возможно распределение ключей:

$$S(\rho_E) = S(\rho_B), \quad 2h(Q_c) = 1, \quad Q_c \approx 11\,\%. \tag{78}$$

Если величина ошибки меньше критической, то длина секретного ключа в битах равна

$$N_{key} = n(1 - 2h(Q)). \tag{79}$$

Здесь нужно сделать одно важное замечание. Такая величина ошибки, до которой Алиса и Боб гарантируют секретность ключей, достигается, если легитимные пользователи используют случайные шенноновские коды для исправления ошибок. Такие коды практически нереализуемы, поскольку требуется экспоненциально большая таблица для кодовых слов размером $2^{nC_{clas}(Q)}$. Случайный код имеет минимально возможную избыточность (максимально кодовое расстояние). При использовании других процедур допустимая ошибка будет меньше, поскольку избыточность эффективно декодируемых кодов выше. Если применяются классические коды, исправляющие ошибки, то величина ошибки лимитируется границей Варшамова–Гильберта для таких кодов, и ограничена величиной $Q_c \approx 7.5\,\%$ [23]. Например, если используется каскадная процедура коррекции ошибок с двухсторонним обменом информацией через открытый канал связи Алисой и Бобом, то критическая величина ошибки оказывается $Q_c \approx 8.9\,\%$ [24, 25], что лучше, чем при применении других эффективно декодируемых кодов. Фактически данная ошибка следует из равенства

$$2h_{Cascade}(Q_c) = 1. \tag{80}$$

Если величина ошибки меньше критической, то длина секретного ключа в битах равна

$$N_{key} = n(1 - 2h_{Cascade}(Q)). \tag{81}$$

До тех пор пока не создано квантовой памяти, можно исходить из критической ошибки 15 %. Даже если такая квантовая память и будет создана, это не решит проблему коллективного измерения для Евы. Заметим, что на сегодняшний день реализованы лишь измерения для двухфотонных состояний (измерения в белловском базисе), причем такие измерения при экспериментальной реализации требуют использования нелинейных оптических элементов (кристаллов с нелинейной восприимчивостью второго порядка $\chi^{(2)}$, которая крайне мала и имеет порядок величины 10^{-6}). Это означает, что эффективность такого измерительного устройства также крайне мала и пропорциональна $\chi^{(2)}$. Измерения же n-фотонных состояний при применении тех же оптических элементов (других пока не предложено) будут иметь эффективность $(\chi^{(2)})^n$. В связи с этим атака с коллективными измерениями на сегодняшний день находится далеко за пределами технологических возможностей, поэтому, даже если исходить из критической ошибки 15 %, квантовая криптография имеет очень большой запас прочности.

4.4. Критическая ошибка для квантового протокола распределения ключей с фазово-временным кодированием

Вернемся теперь к протоколу с фазово-временным кодированием.

Ниже вычислим критическую ошибку сразу для коллективных измерений подслушивателя.

Для данного метода кодирования кроме требований симметрии ошибок для 0 и 1 в базисах + и × добавляются требования симметрии ошибок еще и в сдвинутых по времени относительно друг друга базисах L и R, а также равенства отсчетов в контрольном слоте 3 для базисов $+L$, $\times L$, в контрольном слоте 1 для базисов $+$, $\times R$, $\times R$. Кроме того, симметрия требует равенства отсчетов в контрольных слотах 1 и 3. Это приводит к следующим дополнительным условиям:

$$\langle\Psi^+_{+L}|\Psi^-_{+L}\rangle = \langle\Psi^+_{\times L}|\Psi^-_{\times L}\rangle = \langle\Psi^+_{+R}|\Psi^-_{+R}\rangle = \langle\Psi^+_{\times R}|\Psi^-_{\times R}\rangle = 0,$$

$$\langle\Psi^+_{+L}|\Psi^+_{+L}\rangle = \langle\Psi^-_{+L}|\Psi^-_{+L}\rangle = \langle\Psi^+_{\times L}|\Psi^+_{\times L}\rangle = \langle\Psi^-_{\times L}|\Psi^-_{\times L}\rangle = \langle\Psi^+_{+R}|\Psi^+_{+R}\rangle = \langle\Psi^-_{+R}|\Psi^-_{+R}\rangle = \langle\Psi^+_{\times R}|\Psi^+_{\times R}\rangle = \langle\Psi^-_{\times R}|\Psi^-_{\times R}\rangle.$$

Упомянутые условия приводят к следующему представлению:

$$|\phi_1\rangle = \sqrt{1-\delta^2}|x\rangle\otimes|x\rangle, \quad |\theta_1\rangle = \frac{\delta}{\sqrt{2}}|x\rangle\otimes|y\rangle, \quad |\varphi_1\rangle = \frac{\delta}{\sqrt{2}}|z\rangle\otimes|x\rangle, \tag{82}$$

$$|\varphi_2\rangle = \frac{\delta}{\sqrt{2}}(\cos\alpha|x\rangle\otimes|y\rangle + \sin\alpha|y\rangle\otimes|y\rangle),$$
$$|\phi_2\rangle = \sqrt{1-\delta^2}(\cos\alpha|x\rangle\otimes|x\rangle + \sin\alpha|y\rangle\otimes|x\rangle), \tag{83}$$
$$|\theta_2\rangle = \frac{\delta}{\sqrt{2}}(\cos\alpha|z\rangle\otimes|z\rangle + \sin\alpha|x\rangle\otimes|z\rangle),$$

$$|\theta_3\rangle = \frac{\delta}{\sqrt{2}}|y\rangle\otimes|x\rangle, \quad |\varphi_3\rangle = \frac{\delta}{\sqrt{2}}|z\rangle\otimes|z\rangle, \quad |\phi_3\rangle = \sqrt{1-\delta^2}|x\rangle\otimes|x\rangle. \tag{84}$$

Состояния Боба в базисе $+, \times L$ после подслушивания Евы принимают вид

$$\rho_B(0_{+L}) = \mathrm{Tr}\{|\Psi_{EB}(0_{+L})\rangle\langle\Psi_{EB}(0_{+L})|\} = |0_{+L}\rangle\langle 0_{+L}|\frac{\langle\Phi^+_{+L}|\Phi^+_{+L}\rangle + \langle\Theta^+_{+L}|\Theta^+_{+L}\rangle}{4} + |1_{+L}\rangle\langle 1_{+L}|\frac{\langle\Phi^-_{+L}|\Phi^-_{+L}\rangle - \langle\Theta^-_{+L}|\Theta^-_{+L}\rangle}{4} + |3\rangle\langle 3|\frac{\langle\Psi^+_{+L}|\Psi^+_{+L}\rangle}{2}, \tag{85}$$

$$\rho_B(1_{+L}) = \mathrm{Tr}\{|\Psi_{EB}(1_{+L})\rangle\langle\Psi_{EB}(1_{+L})|\} = |1_{+L}\rangle\langle 1_{+L}|\frac{\langle\Phi^+_{+L}|\Phi^+_{+L}\rangle + \langle\Theta^+_{+L}|\Theta^+_{+L}\rangle}{4} + |0_{+L}\rangle\langle 0_{+L}|\frac{\langle\Phi^-_{+L}|\Phi^-_{+L}\rangle - \langle\Theta^-_{+L}|\Theta^-_{+L}\rangle}{4} + |3\rangle\langle 3|\frac{\langle\Psi^+_{-L}|\Psi^+_{-L}\rangle}{2}, \tag{86}$$

$$\rho_B(0_{\times L}) = \mathrm{Tr}\{|\Psi_{EB}(0_{\times L})\rangle\langle\Psi_{EB}(0_{\times L})|\} = |0_{\times L}\rangle\langle 0_{\times L}|\frac{\langle\Phi^+_{\times L}|\Phi^+_{\times L}\rangle + \langle\Theta^+_{\times L}|\Theta^+_{\times L}\rangle}{4} + |1_{\times L}\rangle\langle 1_{\times L}|\frac{\langle\Phi^-_{\times L}|\Phi^-_{\times L}\rangle - \langle\Theta^-_{\times L}|\Theta^-_{\times L}\rangle}{4} + |3\rangle\langle 3|\frac{\langle\Psi^+_{+\times L}|\Psi^+_{+\times L}\rangle}{2}, \tag{87}$$

$$\rho_B(1_{\times L}) = \mathrm{Tr}\{|\Psi_{EB}(1_{\times L})\rangle\langle\Psi_{EB}(1_{\times L})|\} = \\ = |1_{\times L}\rangle\langle 1_{\times L}|\frac{\langle\Phi^+_{\times L}|\Phi^+_{\times L}\rangle + \langle\Theta^+_{\times L}|\Theta^+_{\times L}\rangle}{4} + \\ + |0_{\times L}\rangle\langle 0_{\times L}|\frac{\langle\Phi^-_{\times L}|\Phi^-_{\times L}\rangle - \langle\Theta^-_{\times L}|\Theta^-_{\times L}\rangle}{4} + \\ + |3\rangle\langle 3|\frac{\langle\Psi^+_{\times L}|\Psi^+_{\times L}\rangle}{2}. \quad (88)$$

Аналогично для базиса $+, \times R$:

$$\rho_B(0_{+R}) = \mathrm{Tr}\{|\Psi_{EB}(0_{+R})\rangle\langle\Psi_{EB}(0_{+R})|\} = \\ = |1\rangle\langle 1|\frac{\langle\Psi^+_{+R}|\Psi^+_{+R}\rangle}{2}, \\ |0_{+R}\rangle\langle 0_{+R}|\frac{\langle\Phi^+_{+R}|\Phi^+_{+R}\rangle + \langle\Theta^+_{+R}|\Theta^+_{+R}\rangle}{4} + \\ + |1_{+R}\rangle\langle 1_{+R}|\frac{\langle\Phi^-_{+R}|\Phi^-_{+R}\rangle - \langle\Theta^-_{+R}|\Theta^-_{+R}\rangle}{4}, \quad (89)$$

$$\rho_B(1_{+R}) = \mathrm{Tr}\{|\Psi_{EB}(1_{+R})\rangle\langle\Psi_{EB}(1_{+R})|\} = \\ = |1\rangle\langle 1|\frac{\langle\Psi^+_{-R}|\Psi^+_{-R}\rangle}{2} + \\ + |1_{+R}\rangle\langle 1_{+R}|\frac{\langle\Phi^+_{+R}|\Phi^+_{+R}\rangle + \langle\Theta^+_{+R}|\Theta^+_{+R}\rangle}{4} + \\ + |0_{+R}\rangle\langle 0_{+R}|\frac{\langle\Phi^-_{+R}|\Phi^-_{+R}\rangle - \langle\Theta^-_{+R}|\Theta^-_{+R}\rangle}{4}, \quad (90)$$

$$\rho_B(0_{\times R}) = \mathrm{Tr}\{|\Psi_{EB}(0_{\times R})\rangle\langle\Psi_{EB}(0_{\times R})|\} = \\ = |1\rangle\langle 1|\frac{\langle\Psi^+_{\times R}|\Psi^+_{\times R}\rangle}{2} + \\ + |0_{\times R}\rangle\langle 0_{\times R}|\frac{\langle\Phi^+_{\times R}|\Phi^+_{\times R}\rangle + \langle\Theta^+_{\times R}|\Theta^+_{\times R}\rangle}{4} + \\ + |1_{\times R}\rangle\langle 1_{\times R}|\frac{\langle\Phi^-_{\times R}|\Phi^-_{\times R}\rangle - \langle\Theta^-_{\times R}|\Theta^-_{\times R}\rangle}{4}, \quad (91)$$

$$\rho_B(1_{\times R}) = \mathrm{Tr}\{|\Psi_{EB}(1_{\times R})\rangle\langle\Psi_{EB}(1_{\times R})|\} = \\ = |1\rangle\langle 1|\frac{\langle\Psi^+_{\times R}|\Psi^+_{\times R}\rangle}{2} + \\ + |1_{\times R}\rangle\langle 1_{\times R}|\frac{\langle\Phi^+_{\times R}|\Phi^+_{\times R}\rangle + \langle\Theta^+_{\times R}|\Theta^+_{\times R}\rangle}{4} + \\ + |0_{\times R}\rangle\langle 0_{\times R}|\frac{\langle\Phi^-_{\times R}|\Phi^-_{\times R}\rangle - \langle\Theta^-_{\times R}|\Theta^-_{\times R}\rangle}{4}. \quad (92)$$

Окончательно получаем (в базисе $+L$)

$$\rho_B(0_{+L}) = |0_{+L}\rangle\langle 0_{+L}|\frac{(1-q)(1+\cos\alpha)}{2} + \\ + |1_{+L}\rangle\langle 1_{+L}|\frac{(1-q)(1-\cos\alpha)}{2} + |3\rangle\langle 3|q, \quad (93)$$

$$\rho_B(1_{+L}) = |1_{+L}\rangle\langle 1_{+L}|\frac{(1-q)(1+\cos\alpha)}{2} + \\ + |0_{+L}\rangle\langle 0_{+L}|\frac{(1-q)(1-\cos\alpha)}{2} + |3\rangle\langle 3|q. \quad (94)$$

Аналогичное выражение имеют матрицы плотности в базисе $\times L$.

Для сдвинутого по времени базиса $+R$ находим

$$\rho_B(0_{+R}) = |1\rangle\langle 1|q + |0_{+R}\rangle\langle 0_{+R}|\frac{(1-q)(1+\cos\alpha)}{2} + \\ + |1_{+R}\rangle\langle 1_{+R}|\frac{(1-q)(1-\cos\alpha)}{2}, \quad (95)$$

$$\rho_B(1_{+R}) = |1\rangle\langle 1|q + |1_{+R}\rangle\langle 1_{+R}|\frac{(1-q)(1+\cos\alpha)}{2} + \\ + |0_{+R}\rangle\langle 0_{+R}|\frac{(1-q)(1-\cos\alpha)}{2}. \quad (96)$$

Аналогично для базиса $\times R$.

Боб выполняет измерения, которые описываются разложением единицы (5)–(8). Вероятность отсчетов в контрольных слотах 3 (в базисе $+, \times L$) и 1 (в базисе $+, \times R$) равна

$$q = \delta^2/2. \quad (97)$$

Поскольку заранее неизвестен базис L или R, подслушивание неизбежно приводит к появлению отсчетов в контрольном слоте 3, если использовался базис $+, \times L$, и появлению отсчетов в временном слоте 1, если Алиса посылала состояния в базисе $+, \times R$. Боб сообщает Алисе те посылки, в которых он получил отсчеты в контрольных слотах (после раскрытия Алисой базисов $+$ или $\times$). Величина ошибки 0 или 1, как следует из формул (93)–(96), дается выражением

$$Q = \frac{(1-q)(1-\cos\alpha)}{2(1-q)} = \frac{1-\cos\alpha}{2}, \\ \cos\alpha = 1 - 2Q, \quad (98)$$

где вид знаменателя определяется тем, что полное пространство событий представляет собой исходы, интерпретируемые как 0 или 1, и отсчеты в контрольных временных слотах (1 или 3 в зависимости от выбранного Алисой базиса). Соотношение (98) дает связь между наблюдаемой ошибкой у Боба и параметрами унитарного преобразования U_{EB}, осуществляемого Евой.

После раскрытия и согласования базисов Алисой и Бобом матрица плотности состояний Евы, относящихся как к базису $+L$, так и к базису $\times L$, норми-

рованная на количество отсчетов в канале 0 и 1, с учетом формул (93)–(96) принимает вид

$$\rho_E(+L) = \rho_E(\times L) = \\ = \frac{|\phi_1\rangle\langle\phi_1| + |\phi_2\rangle\langle\phi_2| + |\theta_1\rangle\langle\theta_1| + |\varphi_2\rangle\langle\varphi_2|}{4(1-q)}. \quad (99)$$

Аналогично для базисов $+R$ и $\times R$

$$\rho_E(+R) = \rho_E(\times R) = \\ = \frac{|\phi_2\rangle\langle\phi_2| + |\phi_3\rangle\langle\phi_3| + |\theta_2\rangle\langle\theta_2| + |\varphi_3\rangle\langle\varphi_3|}{4(1-q)}. \quad (100)$$

Матрицы плотности Боба в базисах $+L$ и $\times L$ равны

$$\rho_B(+L) = \rho_B(\times L) = \frac{1}{2}|1\rangle\langle 1| + \frac{1}{2}|2\rangle\langle 2|. \quad (101)$$

Аналогично для базисов $+R$ и $\times R$

$$\rho_B(+R) = \rho_B(\times R) = \frac{1}{2}|2\rangle\langle 2| + \frac{1}{2}|3\rangle\langle 3|. \quad (102)$$

Собственные числа матриц

$$\rho_E(L) = \frac{1}{2}(\rho_E(+L) + \rho_E(\times L)),$$

$$\rho_E(R) = \frac{1}{2}(\rho_E(+R) + \rho_E(\times R)),$$

естественно, совпадают и имеют вид

$$\lambda_1 = \eta(1-Q), \quad \lambda_2 = \eta Q, \\ \lambda_3 = (1-\eta)(1-Q), \quad \lambda_4 = (1-\eta)Q, \quad (103)$$

где

$$\eta = \frac{q}{1-q}. \quad (104)$$

С учетом формул (99)–(100) находим выражение для $\chi(\rho_E)$:

$$\chi(\rho_E) = S(\rho_E) = h(\eta) + h(Q). \quad (105)$$

Аналогично для матрицы плотности Боба

$$\rho_B(L) = \frac{1}{2}(\rho_B(+L) + \rho_B(\times L)),$$

$$\rho_B(R) = \frac{1}{2}(\rho_B(+R) + \rho_B(\times R))$$

с учетом соотношений (93)–(98) получаем

$$\rho_B(L) = \frac{1}{2}|1\rangle\langle 1| + \frac{1}{2}|2\rangle\langle 2|, \\ \rho_B(R) = \frac{1}{2}|2\rangle\langle 2| + \frac{1}{2}|3\rangle\langle 3|, \quad (106)$$

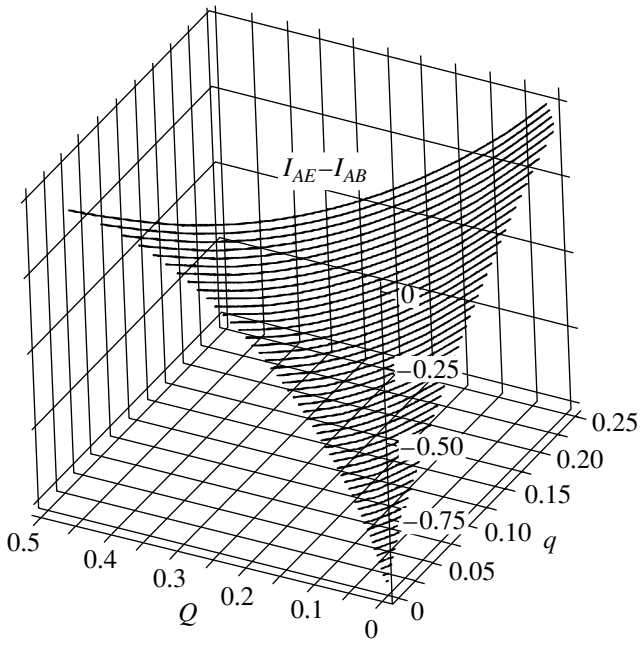

Рис. 2. Зависимости $I_{AE}(Q,q) - I_{AB}(Q,q)$

соответственно оба собственных числа равны $1/2$.

Энтропия фон Неймана есть

$$\chi(\rho_B) = S(\rho_B) = 1. \quad (107)$$

Равенство выражений (105) и (107) дает критическую ошибку, до которой возможно распределение ключей (см. уравнение для критической ошибки для протокола BB84 (78)):

$$S(\rho_E) = S(\rho_B), \quad h(\eta_c) + h(Q_c) = 1. \quad (108)$$

Зависимости $I_{AE}(Q,q) - I_{AB}(Q,q)$ приведены на рис. 2. На рис. 3 представлены зависимости $I_{AE}(Q,q) - I_{AB}(Q,q)$ при фиксированной вероятности отсчетов q в контрольных слотах, которая связана с параметром η соотношением (104).

Если величина ошибки меньше критической, то длина секретного ключа в битах равна

$$N_{key} = n(1 - h(\eta) - h(Q)). \quad (109)$$

Величина допустимой ошибки определяется числом отсчетов в контрольном временном слоте — $Q_c(q)$.

Важное свойство данного протокола состоит в том, что при нулевых отсчетах в контрольном временном слоте, в котором $h(\eta) = 0$, $q = 1/3$, $\delta = \sqrt{2/3}$, допустимая критическая ошибка, до кото-

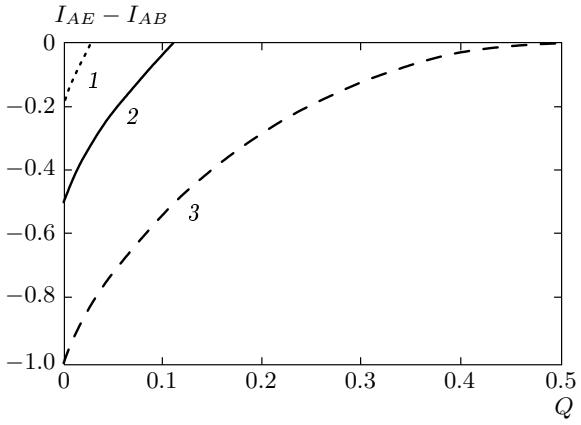

Рис. 3. Зависимости $I_{AE}(Q,q) - I_{AB}(Q,q)$ при фиксированной вероятности отсчетов q в контрольных слотах, $q = 0.2$ (*1*), 0.1 (*2*), 0 (*3*)

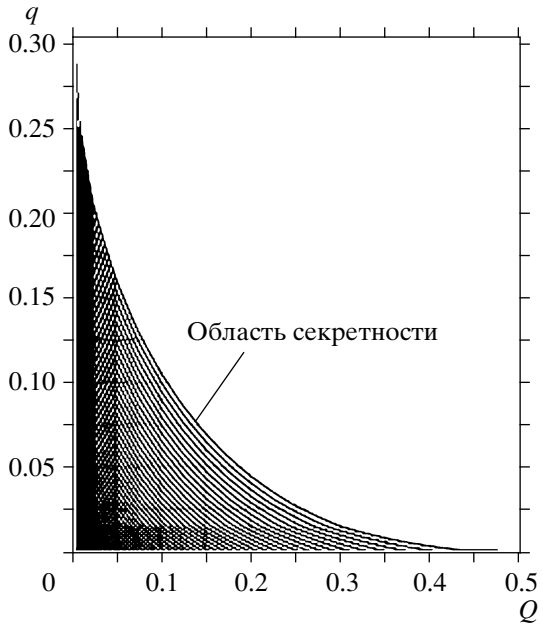

Рис. 4. Область секретности протокола с фазово-временным кодированием в плоскости параметров (Q,q)

рой гарантируется секретность ключей, определяется условием

$$h(Q_c) = 1, \quad Q_c = 1/2. \tag{110}$$

Как известно, до ошибки $Q_c = 1/2$ в бинарном классическом канале связи возможна безошибочная передача информации. В данном квантовом протоколе распределения ключей гарантируется не только возможность безошибочной передачи (ключей), но и их секретность.

В отсутствие подслушивателя отсчеты, например, в слоте 3, когда Алиса посылала состояния в базисе $+, \times L$, могут возникать практически только из-за темновых отсчетов и не связаны с разбалансировкой интерферометра.

На рис. 4 изображена область секретности протокола с фазово-временным кодированием в плоскости параметров (Q,q), которая позволяет определить критическую величину ошибки $Q_c(q)$ как функцию наблюдаемой вероятности контрольных отсчетов q.

5. ОПТОВОЛОКОННАЯ РЕАЛИЗАЦИЯ КВАНТОВОГО РАСПРЕДЕЛЕНИЯ КЛЮЧЕЙ С ФАЗОВО-ВРЕМЕННЫМ КОДИРОВАНИЕМ

Опишем теперь оптоволоконную реализацию данного протокола. Она представлена на рис. 5. Система состоит из лазера, двух разбалансированных оптоволоконных интерферометров Маха–Цандера с разностью длин плеч по времени T, двух фазовых модуляторов и двух лавинных фотодетекторов, работающих в стробируемом режиме. На рис. 5 не показаны лазер, который генерирует короткие классические импульсы, используемые для синхронизации (привязки по времени) однофотонных состояний в каждой посылке, и аттенюатор.

5.1. Приготовление информационных состояний

Алиса запускает лазер, который генерирует короткие импульсы в каждой посылке. При этом случайно и равновероятно генерируется одно из двух состояний, сдвинутых по времени на величину T, равную разности длинного и короткого плеч интерферометра Маха–Цандера. На данной стадии Алиса, по-существу, выбирает базис L или R. Обозначим данную пару состояний как $|0_L\rangle$ и $|1_R\rangle$. Состояния $|0_L\rangle$ и $|1_R\rangle$ отличаются друг от друга лишь сдвигом по времени на величину T ($|1_R\rangle = U(T)|0_L\rangle$, $U(T)$ — оператор трансляции по времени на T). Далее, как несложно убедиться, после прохождения через интерферометр Маха–Цандера на одном из его выходов данные состояния преобразуются в следующую пару состояний:

$$|0_L\rangle \to \frac{1}{\sqrt{2}}(|1\rangle + |2\rangle), \quad |1_R\rangle \to \frac{1}{\sqrt{2}}(|2\rangle + |3\rangle). \tag{111}$$

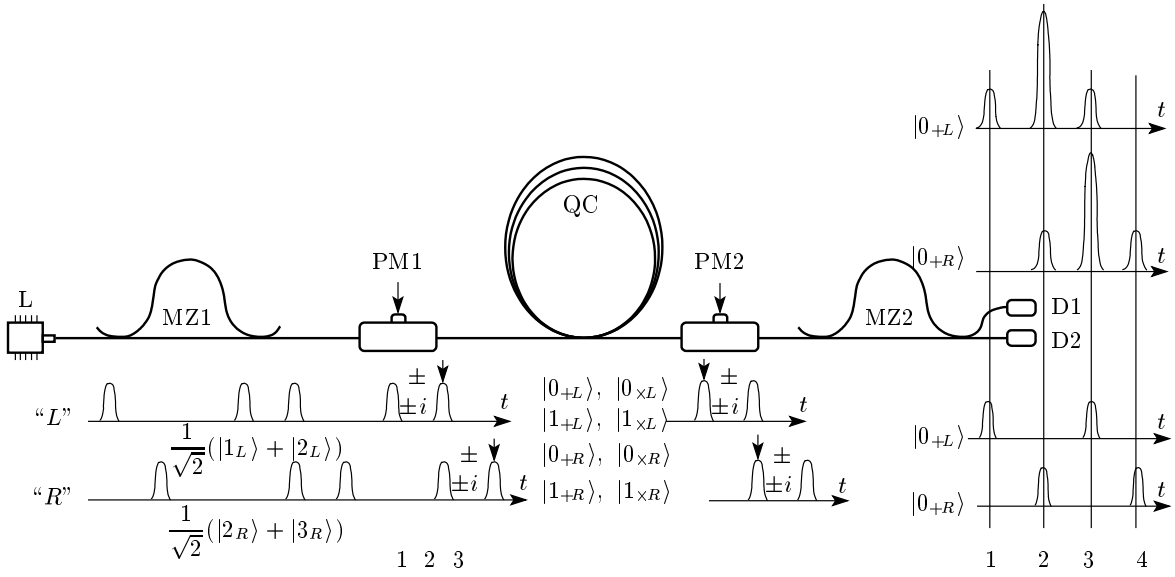

Рис. 5. Оптоволоконная схема квантовой криптографии с фазово-временным кодированием. MZ1, MZ2 — разбалансированные интерферометры Маха – Цандера; PM1, PM2 — фазовые модуляторы; QC — квантовый канал; L — лазер, D1, D2 — лавинные фотодетекторы, 1, 2, 3, 4 — временные окна

Каждое состояние в (111) представляет собой суперпозицию состояний $|1\rangle$, $|2\rangle$ и $|2\rangle$, $|3\rangle$, локализованных соответственно во временных окнах 1, 2, 3 (рис. 5). Временные окна 1, 2, 3 последовательно отстоят друг от друга на временной интервал T, равный разности длинного и короткого плеч интерферометра Маха – Цандера.

При прохождении состояний (111) через фазовый модулятор Алиса прикладывает на короткое время напряжение к модулятору, которое приводит к появлению дополнительной разности фаз между «половинками» состояний в суперпозиции

$$-\frac{1}{\sqrt{2}}(|1\rangle + e^{i\phi_A}|1\rangle), \quad \frac{1}{\sqrt{2}}(|2\rangle + e^{i\phi_A}|3\rangle).$$

Физически приложение напряжения к фазовому модулятору на время, когда в нем присутствует одна из «половинок» состояния, представляющего суперпозицию локализованных во временных окнах состояний, изменяет показатель преломления среды, что и приводит к появлению дополнительной разности фаз между «половинками» в суперпозиции. Такое включение фазовых модуляторов впервые было использовано в работе [26] (в предыдущих оптоволоконных реализациях протокола BB84 фазовые модуляторы включались в длинные плечи интерферометра Маха – Цандера на приемном и передающем концах). Возможны два варианта приложения напряжения, которые с точки зрения квантового криптографического протокола эквивалентны, поскольку имеет смысл только относительная разность фаз между «половинками» в суперпозиции. В первом варианте напряжение прикладывается во временном окне 1 (к передней «половинке» в случае $\frac{1}{\sqrt{2}}(|1\rangle + |2\rangle)$, и к задней в случае состояния $\frac{1}{\sqrt{2}}(|2\rangle + |3\rangle)$). Во втором варианте напряжение на модулятор прикладывается во временном окне 1, если Алиса генерирует состояние $\frac{1}{\sqrt{2}}(|1\rangle + |2\rangle)$, и во временном окне 2, если Алиса генерирует состояние $\frac{1}{\sqrt{2}}(|2\rangle + |3\rangle)$. Для определенности будем считать, что Алиса действует по второму варианту и выбирает случайно и равновероятно напряжение на модуляторе, которое приводит к относительной разности фаз в соответствии с табл. 1.

После ослабления состояния посылаются в канал связи.

5.2. Измерение информационных состояний

На приемной стороне Боб случайно, равновероятно и независимо от Алисы прикладывает напряжение на фазовый модулятор, которое приводит к дополнительной относительной разности фаз $\phi_B = 0$

Таблица 1

Бит	Фаза Алисы ϕ_A	Состояние в базисе L	Состояние в базисе R	Фаза Боба ϕ_B
0	0	$\|0_{+L}\rangle$	$\|0_{+R}\rangle$	0
1	π	$\|1_{+L}\rangle$	$\|1_{+R}\rangle$	0
0	$\pi/2$	$\|0_{\times L}\rangle$	$\|0_{\times R}\rangle$	$\pi/2$
1	$3\pi/2$	$\|1_{\times L}\rangle$	$\|1_{\times R}\rangle$	$\pi/2$

или $\phi_B = \pi/2$. Способ подачи напряжения на модулятор такой же, как на передающей стороне. Перед входом в интерферометр Маха–Цандера на приемной стороне состояния после фазового модулятора имеют вид

$$\frac{1}{\sqrt{2}}(|1\rangle + e^{i(\phi_A-\phi_B)}|2\rangle), \quad \text{базис } L, \tag{112}$$

$$\frac{1}{\sqrt{2}}(|2\rangle + e^{i(\phi_A-\phi_B)}|3\rangle), \quad \text{базис } R. \tag{113}$$

Далее происходит согласование базисов по открытому каналу связи. Для каждой посылки Алиса сообщает базисы, которые она использовала, но не сообщает значения бита. В каждом базисе имеются два значения бита, которые не раскрываются публично. Боб оставляет измерения только в тех посылках, где базисы совпадали. Соответствие базисов (относительной фазы в суперпозиции) у Алисы и Боба приведено в табл. 1.

Для неотбрасываемых посылок, в которых базисы совпадают, на детекторы (D1 и D2) поступают состояния, приведенные в табл. 2.

Измерения проводятся путем стробирования детекторов D1 и D2 во временных окнах 2 и 3, которые выбираются случайно. После стадии согласования базисов по открытому каналу связи между Алисой и Бобом Боб однозначно может идентифицировать передаваемые значения битов. Например, в отсутствие подслушивателя при передаче состояния $|0_{+L}\rangle$ отсчеты для состояний в базисе $+L$ будут иметь место только во временном окне 2 в детекторе D1, и никогда в окне 2 в детекторе D2. Фактически, преобразование состояний при помощи фазового модулятора и интерферометра на приемной стороне и детектирование в определенных временных окнах детекторами D1, D2 эквивалентно использованию измерений (16).

Измерения в контрольных временных окнах отвечают измерениям на приемной стороне во временном слоте 1 для состояний в базисах $+L$ и $\times L$ и,

Таблица 2

Бит	Состояние Алисы	Состояние Боба	Детектор Боба
0	$\|0_{+L}\rangle$	$\frac{1}{8}(\|1\rangle + 2\|2\rangle + \|3\rangle)$	D1
1	$\|1_{+L}\rangle$	$\frac{1}{8}(\|1\rangle + \|3\rangle)$	D2
0	$\|0_{\times L}\rangle$	$\frac{1}{8}(\|1\rangle + \|3\rangle)$	D1
1	$\|1_{\times L}\rangle$	$\frac{1}{8}(\|1\rangle + 2\|2\rangle + \|3\rangle)$	D2
0	$\|0_{+R}\rangle$	$\frac{1}{8}(\|2\rangle + \|4\rangle)$	D1
1	$\|1_{+R}\rangle$	$\frac{1}{8}(\|2\rangle + \|4\rangle)$	D2
0	$\|0_{\times R}\rangle$	$\frac{1}{8}(\|2\rangle + 2\|3\rangle + \|4\rangle)$	D1
1	$\|1_{\times R}\rangle$	$\frac{1}{8}(\|2\rangle + 2\|3\rangle + \|4\rangle)$	D2

соответственно, во временном слоте 4 для состояний в базисах $+R$ и $\times R$. Для невозмущенных состояний, например, для состояний в базисах $+L$ и $\times L$, никогда не будет отсчетов во временном окне 4. В отсутствие подслушивателя разбалансировка интерферометра приведет к ошибочным отсчетам во временном слоте 2, но никогда не приведет к отсчетам во временном слоте 4. Аналогично для состояний в базисах $+R$ и $\times R$. Разбалансировка интерферометра приведет к ошибочным отсчетам в слоте 3, но не приведет к отсчетам в контрольном слоте 1.

Таким образом, в данном протоколе удается частично разделить ошибки от подслушивателя и ошибки от разбалансировки интерферометра.

6. ЗАКЛЮЧЕНИЕ

Резюмируем полученные результаты. Анализ криптографической стойкости предложенного ранее в работе [7] квантового протокола распределения ключей с фазово-временным кодированием показывает, что существенной особенностью протокола является то, что детектирование попыток подслушивания происходит не только по ошибкам в первичных ключах, но и по изменению статистики фотоотсчетов в контрольных временных слотах. Данный протокол, в отличие от предыдущих, является двухпараметрическим. Детектирование попыток подслушивания происходит по изменению статистики отсчетов, которая описывается двумя параметрами Q (вероятность ошибок, отвечающих отсчетам в канале для 0 и 1) и q (вероятность отсчетов в контрольных временных слотах).

Таким образом, область секретности протокола зависит от двух параметров — ошибки в первичных ключах, Q, и изменения количества отсчетов в контрольном временном слоте, q. Критическая величина ошибки зависит от наблюдаемой доли отсчетов в контрольных временных слотах — $Q_c(q)$.

Данное обстоятельство является принципиально важным, поскольку позволяет частично «разнести» ошибки, связанные с собственными неидеальностями аппаратуры (нестабильностью интерферометра) и действиями подслушивателя. «Разнести» в том смысле, что для протоколов, в которых детектирование подслушивателя происходит только по одному параметру — ошибке в первичных ключах Q, разбалансировка интерферометра также приводит к ошибке. В данном протоколе разбалансировка интерферометра приводит только к ошибке Q и не приводит к появлению отсчетов в контрольных временных слотах.

Величина ошибки связана с видностью V

$$V = \frac{I_{D_1} - I_{D_2}}{I_{D_1} + I_{D_2}},$$

(I_{D_1,D_2} — доля отсчетов соответственно в детекторе D1 и D2, см. рис. 5) интерференционной картины соотношением

$$Q = \frac{1 - V}{2},$$

где при $Q \to 1/2$ имеет место полная потеря видности, однако при этом протокол все еще секретен, если нет отсчетов в контрольном временном слоте 1 или 4. Отсчеты в контрольных слотах не связаны с потерей видности, а возникают либо за счет темновых отсчетов, либо за счет действий подслушивателя.

Таким образом, если обнаружены ошибки, но нет отсчетов в контрольном временном слоте, то можно не прерывать протокол вплоть до 50 % ошибок.

Автор выражает благодарность Академии криптографии РФ за поддержку. Работа выполнена при частичной поддержке РФФИ (грант № 05-02-17387).

ЛИТЕРАТУРА

1. G. S. Vernam, J. Amer. Inst. Elect. Eng. **55**, 109 (1926).
2. В. А. Котельников, Отчет 18 июня, Москва (1941).
3. C. E. Shannon, Bell Syst. Tech. J. **28**, 658 (1949).
4. C. H. Bennett and G. Brassard, in *Proc. of IEEE Int. Conf. on Comput. Sys. and Sign. Proces.*, Bangalore, India (1984), p. 175.
5. H. Bechmann-Pasquinucci and W. Tittel, Phys. Rev. A **61**, 062308 (2000).
6. С. П. Кулик, Г. А. Масленников, Е. В. Морева, ЖЭТФ **129**, 814 (2006).
7. С. П. Кулик, С. Н. Молотков, А. П. Маккавеев, Письма в ЖЭТФ **85**, 354 (2007).
8. C. H. Bennett, Phys. Rev. Lett. **68**, 3121 (1992).
9. C. H. Bennett, G. Brassard, C. Crépeau, and U. Maurer, *Generalized Privacy Amplification*, IEEE Trans. Inf. Theory **41**, 1915 (1995).
10. K. Kraus, *States, Effects and Operations*, Springer-Verlag, Berlin (1983).
11. M. Nielsen and I. Chuang, *Quantum Computation and Quantum Information*, Cambridge Univ. Press, Cambridge (2000).
12. А. С. Холево, УМН **53**, 193 (1998); *Введение в квантовую теорию информации*, сер. *Современная математическая физика*, вып. 5, МЦНМО, Москва (2002).
13. R. Jozsa and B. Schumacher, J. Mod. Opt. **41**, 2343 (1994); P. Hausladen, R. Jozsa, B. Schumacher, M. Westmoreland, and W. K. Wootters, Phys. Rev. A **54**, 1869 (1996); B. Schumacher and M. D. Westmoreland, Phys. Rev. A **56**, 131 (1997).
14. I. Csiszár and J. Körner, IEEE Trans. Inf. Theory **24**, 339 (1978).
15. D. Mayers and A. Yao, E-print archives, quant-ph/9802025.

16. E. Biham, M. Boyer, P. O. Boykin, T. Mor, and V. Roychowdhury, E-print archives, quant-ph/9912053.

17. P. W. Shor and J. Preskill, E-print archives, quant-ph/0003004.

18. C. A. Fuchs, N. Gisin, R. Griffiths, Chi-Sheng Niu, and A. Peres, Phys. Rev. A **56**, 1163 (1997).

19. C. E. Shannon, Bell Syst. Tech. J. **27**, 397; **27**, 623 (1948).

20. Р. Галлагер, *Теория информации и надежная связь*, Сов. радио, Москва (1974), с. 719.

21. I. Csiszár and J. Körner, *Information Theory: Coding Theorems for Discrete Memoryless Systems*, Akademiai, Kiado–Budapest, (1981).

22. P. Shor, E-print archives, quant-ph/0304102.

23. E. J. Mac Williams and N. J. A. Sloane, *The Theory of Error-Correcting Codes*, North-Holland Publ. Comp., Amsterdam, New York, Oxford (1977).

24. G. Brassard and L. Salvail, Advances in Cryptology — Proc. Eurocrypt'93, Lofthus, Springer-Verlag (1993), p. 410; Lect. Notes Comp. Sci. **765**, 410 (1994).

25. А. В. Тимофеев, С. Н. Молотков, Письма в ЖЭТФ **82**, 868 (2005); А. В. Тимофеев, Д. И. Помозов, А. П. Маккавеев, С. Н. Молотков, ЖЭТФ **131**, 771 (2007).

26. Y. Nambu, K. Yoshino, and A. Tomita, E-print archives, quant-ph/0603041.