Письма в ЖЭТФ, том 89, вып. 7, с. 432 – 438 © 2009 г. 10 апреля

Квантовое распределение ключей в однофотонном режиме с неортогональными состояниями внутри базиса

Д. А. Кронберг[+], *С.Н.Молотков*[+*▽]

[+] *Институт физики твердого тела РАН, 142432 Черноголовка, Московская обл., Россия*

[*] *Академия криптографии Российской Федерации*

[▽] *Факультет вычислительной математики и кибернетики, МГУ им. М.В. Ломоносова, 119992 Москва, Россия*

Поступила в редакцию 11 ноября 2008 г.

После переработки 2 марта 2009 г.

Протокол квантового распределения ключей с неортогональными состояниями внутри базиса является обобщением известного протокола распределения ключей BB84. При произвольных значениях угла между информационными состояниями найдена критическая ошибка и длина секретного ключа для протокола с неортогональными базисными состояниями. Построена явная оптимальная атака на передаваемый ключ, которая максимизирует информацию подслушивателя при наблюдаемой на приемной стороне ошибке.

PACS: 03.65.Hk, 03.67.Dd

Одна из главных проблем квантовой криптографии состоит в том, что источник квантовых состояний не является строго однофотонным. Данное обстоятельство вместе с потерями в квантовом канале связи приводит к невозможности передачи ключей при длине линии связи больше некоторой критической величины. После открытия PNS-атаки [1] (Photon Number Splitting Attack) секретность основных протоколов квантового распределения ключей для каналов связи с потерями оказалась под вопросом. Гарантированно секретное распределение ключей для протоколов с ортогональными состояниями внутри базиса, например, такого как BB84 [2], оказывается невозможным. Это связано с тем, что подслушиватель может задерживать свои измерения до стадии раскрытия базисов легитимными пользователями. После раскрытия базисов подслушиватель делает измерения в уже известном базисе, и если состояния внутри базиса ортогональны (достоверно различимы), то можно получить полную информацию о ключе, не производя ошибок на приемной стороне.

Один из способов решения проблемы состоит в том, чтобы сделать состояния внутри базисов неортогональными – достоверно неразличимыми даже при раскрытом известном базисе. Одним из таких протоколов квантового распределения ключей является протокол SARG04, предложенный в [3]. Стойкость данного протокола [4] и более сложных протоколов, например, протокола с фазово-временным кодированием [5], при больших длинах линии связи анализировалась в ряде работ. Однако, насколько нам известно, полный анализ стойкости протокола ввиду сложности при длине линии связи меньше критической величины и строго однофотонном источнике при произвольных углах между информационными состояниями внутри базисов до сих пор не сделан.

После передачи серии квантовых состояний Алисой, измерений их Бобом и интерпретации результатов измерений на приемной стороне, Алиса и Боб имеют битовые строки X и Y, причем строка Боба содержит ошибки. Ева имеет в своем распоряжении вспомогательную квантовую систему (ρ_n^E), которая была запутана с состоянием Алисы (Боба). Поскольку Алиса посылает в каждой посылке состояния независимо друг от друга, то матрица плотности Евы может быть представлена в виде тензорного произведения матриц плотности возмущенного состояния Евы в каждой посылке $\rho_n^E = \rho^E \otimes \rho^E \ldots \otimes \rho^E$. Степень корреляции между битовыми строками Алисы и Боба описывается взаимной информацией $nI_{AB}(X;Y)$ [6 – 9]. Для исправления ошибок Алиса и Боб должны обменяться информацией через открытый классический канал связи. Чтобы получить идентичные битовые строки с вероятностью, сколь угодно близкой к единице при длинной последовательности, необходимо выдать через открытый канал не менее $nH(X|Y)$ бит информации ($nH(X|Y)$ – условная шенноновская энтропия X при данном Y [6, 9]). Данная информация доступна Еве. На данном этапе информация Евы ограничена величиной $n(H(X|Y)+\chi(\rho_n^E))$ ($\chi(\rho_n^E)$ – фундаментальная величина Холево [7], которая дает верхнюю границу классической информа-

ции, которая может быть извлечена Евой из квантового ансамбля ρ_n^E). Чтобы удалить эту информацию у Евы, Алиса и Боб используют процедуру усиления секретности [10, 11] – сжатия ключа. Цель усиления секретности ключа состоит в том, чтобы из битовой строки длины n, о которой Ева имеет частичную информацию, получить битовую строку меньшей длины – $n(H(X) - H(X|Y) - \chi(\rho_n^E))$ бит, о которой Ева, в асимптотическом пределе больших n, не будет иметь никакой информации. Данная строка является финальным секретным ключом. Таким образом, распределение секретных ключей возможно, если $I_{AB}(X;Y) = H(X) - H(X|Y) > \chi(\rho_n^E)$. Длина секретного ключа в пересчете на посылку оказывается равной[1)] [12]

$$r = H(X) - H(X|Y) - \max_{\rho^E \in \Gamma\{Q\}} \chi(\rho^E), \qquad (1)$$

где максимум берется по множеству матриц плотности $\Gamma\{Q\}$, которые дают наблюдаемую ошибку Q на приемной стороне Боба.

Информационные квантовые состояния. В протоколе используются два базиса, которые обозначаются как a и b. Важно, что состояния внутри базисов неортогональны и состояния в разных базисах получаются друг из друга зеркальным отражением [4]. Состояния в базисах a и b имеют вид

$$|0_a\rangle = \begin{pmatrix} \cos\frac{\eta}{2} \\ \sin\frac{\eta}{2} \end{pmatrix}, \quad |1_a\rangle = \begin{pmatrix} \cos\frac{\eta}{2} \\ -\sin\frac{\eta}{2} \end{pmatrix},$$
$$|0_b\rangle = \begin{pmatrix} \sin\frac{\eta}{2} \\ -\cos\frac{\eta}{2} \end{pmatrix}, \quad |1_b\rangle = \begin{pmatrix} \sin\frac{\eta}{2} \\ \cos\frac{\eta}{2} \end{pmatrix}. \qquad (2)$$

Для дальнейшего понимания важно, что состояния, отвечающие одинаковым значениям бита 0 (соответственно 1) из разных базисов, ортогональны $\langle 0_a|0_b\rangle = 0$ ($\langle 1_a|1_b\rangle = 0$), а состояния, отвечающие 0 и 1 внутри одного базиса, неортогональны (2).

Действия подслушивателя. До подслушивания в квантовом канале невозмущенное, посланное Алисой, состояние описывается матрицей плотности в $\mathcal{H}_A$ для чистого состояния (2) – $\rho_A^{i_m} = |i_m\rangle\langle i_m|$, $i_m = 0_{a,b}, 1_{a,b}$ – индекс состояния Алисы. После вторжения Евы в квантовый канал, возмущенное состояние Алисы также описывается матрицей плотности в $\mathcal{H}_A$, но, вообще говоря, для смешанного состояния – $\tilde\rho_A^{i_m}$. Далее, любое преобразование $\mathcal{T}(...)$, переводящее матрицы плотности в матрицы плотности $\tilde\rho_A^{i_m} = \mathcal{T}(\rho_A^{i_m})$, является супероператором (часто также называемое квантовой операцией или инструментом, см. [7, 8] и ссылки там). Любой супероператор унитарно представим [7, 8], то есть может быть представлен как

$$\tilde\rho_A^{i_m} = \mathrm{Tr}_E\{U(|i_m\rangle\langle i_m| \otimes |E\rangle_E\ {}_E\langle E|)U^{-1}\} = \mathrm{Tr}_E\{|\Psi^{i_m}\rangle_{AE}\ {}_{AE}\langle\Psi^{i_m}|\}, \qquad (3)$$
$$|\Psi^{i_m}\rangle_{AE} = U(|i_m\rangle \otimes |E\rangle),$$

где $|E\rangle_E$ – некоторое чистое состояние в $\mathcal{H}_E$, U – унитарный оператор эволюции, действующий в $\mathcal{H}_A \otimes \mathcal{H}_E$. Такое представление неоднозначно, то есть в нем имеется свобода.

Цель Евы состоит в том, чтобы выбрать свою квантовую систему $|E\rangle$ (пространство состояний $\mathcal{H}_E$) и взаимодействие (унитарный оператор U) таким образом, чтобы в конце протокола получить максимально возможное количество информации о ключе при данной наблюдаемой ошибке Q на приемной стороне Боба. Выясним вид возмущенных матриц плотности для возмущенного состояния $\tilde\rho_A^{0_a}$. Любую матрицу плотности можно привести к диагональному виду, общий вид возмущенной матрицы плотности Алисы в пространстве $\mathcal{H}_A$ размерности 2 есть

$$\tilde\rho_A^{0_a} = \lambda_0^{(a)}|\lambda_0^{(a)}\rangle\langle\lambda_0^{(a)}| + \lambda_1^{(a)}|\lambda_1^{(a)}\rangle\langle\lambda_1^{(a)}|, \qquad (4)$$

здесь $|\lambda_0^{(a)}\rangle$, $|\lambda_1^{(a)}\rangle$ – пара ортогональных собственных векторов в пространстве $\mathcal{H}_A$, в том же двумерном пространстве ("плоскости") лежит пара исходных ортогональных векторов $|0_a\rangle$ и $|0_b\rangle$. Аналогично для состояния возмущенного $\tilde\rho_A^{0_b}$ имеем

$$\tilde\rho_A^{0_b} = \lambda_0^{(b)}|\lambda_0^{(b)}\rangle\langle\lambda_0^{(b)}| + \lambda_1^{(b)}|\lambda_1^{(b)}\rangle\langle\lambda_1^{(b)}|, \qquad (5)$$

здесь также $|\lambda_0^{(b)}\rangle$, $|\lambda_1^{(b)}\rangle$ – пара ортогональных собственных векторов в "плоскости" $\mathcal{H}_A$. Воспользуемся соображениями симметрии между $|0_a\rangle$ и $|0_b\rangle$.

Поворот в "плоскости" $\mathcal{H}_A$ на $\pi/2$ переводит *ортогональные* (2) состояния друг в друга ($|0_a\rangle \to |0_b\rangle$),

[1)] Отметим, что при построении оптимальной атаки Евы может быть использована другая процедура оптимизации, предложенная в [12], где исходно в каждой посылке Алиса готовит максимально запутанное состояние (EPR-состояние) составной системы AB и посылает подсистему B к Бобу. Делая измерение над своей подсистемой A, Алиса фиксирует состояние Боба. Общее выражение для длины секретного ключа при $n \to \infty$ в этом случае имеет вид $r = \min_{\rho_{AB} \in \Gamma\{Q\}}(H(X|E) - H(X|Y))$, где $H(X|E)$, $H(X|Y)$ – условные энтропии фон Неймана, вычисленные для матриц плотности $\rho_{XYE} = \mathcal{T}_{XYE \leftarrow ABE}(\rho_{ABE}^{\otimes n})$. Здесь ρ_{ABE} – матрица плотности, отвечающая чистому состоянию тройной составной системы (Алиса, Боб, Ева), ρ_{AB} – матрица плотности Алисы и Боба, получающаяся из ρ_{ABE} взятием частичного следа по состояниям Евы. Отображение $\mathcal{T}_{XYE \leftarrow ABE}$ описывает преобразование матрицы плотности тройной составной системы при процедурах коррекции ошибок и усиления секретности. Можно показать, что оба способа оптимизации приводят к одинаковым результатам.

при этом повороте $\tilde{\rho}_A^{0_a} \to \tilde{\rho}_A^{0_b}$. Соответственно, ортогональные собственные векторы $|\lambda_0^{(a)}\rangle$ и $|\lambda_1^{(a)}\rangle$ ($|\lambda_0^{(b)}\rangle$ и $|\lambda_1^{(b)}\rangle$) переходят друг в друга. Соображения симметрии между $\tilde{\rho}_A^{0_a}$ и $\tilde{\rho}_A^{0_b}$ диктуют, что при таком повороте функциональная структура состояний должна сохраниться. *Ортогональность* собственных векторов и соображения симметрии позволяют записать возмущенные матрицы плотности в виде

$$\tilde{\rho}_A^{0_a} = (1-p)|\lambda_0\rangle\langle\lambda_0| + p|\lambda_1\rangle\langle\lambda_1|, \qquad (6)$$

$$\tilde{\rho}_A^{0_b} = p|\lambda_0\rangle\langle\lambda_0| + (1-p)|\lambda_1\rangle\langle\lambda_1|, \qquad (7)$$

здесь $|\lambda_0\rangle$ и $|\lambda_1\rangle$ – ортогональные векторы в "плоскости" $\mathcal{H}_A$ (лишние индексы опущены). Собственные числа, в сумме дающие единицу ($\lambda_0^{(a,b)} + \lambda_1^{(a,b)} = 1$), обозначены как $\lambda_0^{(a)} = \lambda_1^{(b)} = 1-p$ и $\lambda_1^{(a)} = \lambda_0^{(b)} = p$.

Ориентация пары ортогональных векторов $|\lambda_0\rangle$, $|\lambda_1\rangle$ относительно другой пары ортогональных векторов $|0_a\rangle$, $|0_b\rangle$ в "плоскости" $\mathcal{H}_A$ пока не фиксирована. Здесь опять помогают соображения симметрии. Вероятность ошибки, производимая Евой в базисах a и b, должна быть одинаковой. Поскольку измерения на приемной стороне Боба фактически сводятся к проектированию на векторы $|0_{a,b}\rangle$ и $|1_{a,b}\rangle$ (см. ниже)[2)], то это обстоятельство приводит к тому, что в качестве векторов $|\lambda_0\rangle$ и $|\lambda_1\rangle$ следует выбрать ортогональные векторы $|0_a\rangle$, $|0_b\rangle$. Таким образом, векторы $|0_a\rangle$, $|0_b\rangle$ являются *собственными* векторами частичных матриц плотности $\tilde{\rho}_A^{0_a}$ и $\tilde{\rho}_A^{0_b}$.

Далее, для того, чтобы выяснить совместное действие унитарного оператора на произвольное передаваемое состояние и состояние Евы, достаточно описать действие U на базисные состояния в $\mathcal{H}_A$. Действие на другие состояния может быть получено по линейности U. Любое чистое состояние в $\mathcal{H}_A \otimes \mathcal{H}_E$ может быть разложено всевозможным тензорным произведением линейно независимых векторов в $\mathcal{H}_A \otimes \otimes \mathcal{H}_E$. Имеем

$$|\Psi^{0_a}\rangle_{AE} = U(|0_a\rangle \otimes |E\rangle) = \\ = \sqrt{1-p}|0_a\rangle \otimes |\overline{\psi}_{0a}\rangle + \sqrt{p}|0_b\rangle \otimes |\overline{\theta}_{0b}\rangle, \qquad (8)$$

здесь $|\overline{\psi}_{0a}\rangle$ и $|\overline{\theta}_{0b}\rangle$ – пара нормированных векторов в $\mathcal{H}_E$. Разложение Шмидта [7, 8] (см. также [14]) *гарантирует*, что если векторы $|0_a\rangle$, $|0_b\rangle$ являются *собственными* векторами частичной матрицы плотности (4) $\tilde{\rho}_A^{0_a}$, то векторы $|\overline{\psi}_{0a}\rangle$ и $|\overline{\theta}_{0b}\rangle$ *автоматически будут собственными, а значит, и ортогональными векторами* частичной матрицы плотности $\rho_E^{0_a} = \mathrm{Tr}_A\{|\Psi^{0_a}\rangle_{AE\ AE}\langle\Psi^{0_a}|\}$, то есть $\langle\overline{\psi}_{0a}|\overline{\theta}_{0b}\rangle = 0$.

Аналогично может быть представлено разложение для второго состояния в $\mathcal{H}_A \otimes \mathcal{H}_E$; имеем

$$|\Psi^{0_b}\rangle_{AE} = U(|0_b\rangle \otimes |E\rangle) = \\ = \sqrt{p}|0_a\rangle \otimes |\overline{\theta}_{0a}\rangle + \sqrt{1-p}|0_b\rangle \otimes |\overline{\psi}_{0b}\rangle, \qquad (9)$$

где, вообще говоря, *другой* набор ортогональных базисных векторов в $\mathcal{H}_E$ ($\langle\overline{\psi}_{0b}|\overline{\theta}_{0a}\rangle = 0$).

Для того чтобы ситуация стала более содержательной, нужно установить соотношения между двумя ортогональными базисами в $\mathcal{H}_E$. Для этого воспользуемся унитарностью оператора совместной эволюции U. Условие унитарности требует сохранения скалярного произведения (углов) между векторами состояний до и после взаимодействия. Изначально векторы $|0_a\rangle \otimes |E\rangle$ и $|0_b\rangle \otimes |E\rangle$ ортогональны, после совместной эволюции векторы $|\Psi^{0_a}\rangle_{AE}$ и $|\Psi^{0_b}\rangle_{AE}$ также должны остаться ортогональными, с учетом (8), (9) имеем

$${}_{AB}\langle\Psi^{0_a}|\Psi^{0_b}\rangle_{AE} = \\ = (1-p)0 \cdot \langle\overline{\psi}_{0a}|\overline{\psi}_{0b}\rangle + p0 \cdot \langle\overline{\theta}_{0b}|\overline{\theta}_{0a}\rangle + \\ + \sqrt{(1-p)p}(\langle\overline{\psi}_{0a}|\overline{\theta}_{0a}\rangle + \langle\overline{\theta}_{0b}|\overline{\psi}_{0b}\rangle) = 0, \qquad (10)$$

откуда следует, что должно быть $\langle\overline{\psi}_{0a}|\overline{\theta}_{0a}\rangle + \langle\overline{\theta}_{0b}|\overline{\psi}_{0b}\rangle = 0$. Кроме того, соотношения симметрии между базисами и состояниями $|0_a\rangle$ и $|0_b\rangle$ диктуют, чтобы $\langle\overline{\psi}_{0a}|\overline{\theta}_{0a}\rangle = \langle\overline{\psi}_{0b}|\overline{\theta}_{0b}\rangle$, откуда вместе с (10) следует, что состояния $\langle\overline{\psi}_{0a}|\overline{\theta}_{0a}\rangle = \langle\overline{\psi}_{0b}|\overline{\theta}_{0b}\rangle = 0$ попарно ортогональны. Далее, поскольку коэффициенты в скалярном произведении (10) перед $\langle\overline{\psi}_{0a}|\overline{\psi}_{0b}\rangle$ и $\langle\overline{\theta}_{0b}|\overline{\theta}_{0a}\rangle$ равны нулю, то нет никаких оснований считать их ортогональными. Углы между этими базисными векторами из разных базисов могут быть любыми. Обозначим соответствующие скалярные произведения как

$$\langle\overline{\psi}_{0a}|\overline{\psi}_{0b}\rangle = c_\psi, \quad \langle\overline{\theta}_{0b}|\overline{\theta}_{0a}\rangle = c_\theta. \qquad (11)$$

Аналогично, как сделано выше для $|0_a\rangle$ и $|0_b\rangle$, можно провести рассуждения для пары ортогональных векторов $|1_a\rangle$ и $|1_b\rangle$. По линейности U можно получить действие Евы на состояния $|1_a\rangle$ и $|1_b\rangle$; имеем

$$|\Psi^{1_a}\rangle = U(|1_a\rangle \otimes |E\rangle) = \\ = \sqrt{1-p}|1_a\rangle \otimes |\overline{\psi}_{1a}\rangle + \sqrt{p}|1_b\rangle \otimes |\overline{\theta}_{1b}\rangle, \qquad (12)$$

[2)] Геометрически это очевидно, но в этом можно убедиться прямым вычислением: если угол между двумя ортогональными базисами оставить произвольным, то при дальнейшем вычислении ошибки по формулам (20), (21) можно увидеть, что этот угол должен быть нулем. То есть базисы совпадают.

$$|\Psi^{1_b}\rangle = U(|1_b\rangle \otimes |E\rangle) = \\ = \sqrt{p}|1_a\rangle \otimes |\overline{\theta}_{1a}\rangle + \sqrt{1-p}|1_b\rangle \otimes |\overline{\psi}_{1b}\rangle. \quad (13)$$

Далее удобно ввести новые нормированные векторы, связанные с исходными соотношениями:

$$|\psi_{0,1,a,b}\rangle = \sqrt{1-p}|\overline{\psi}_{0,1,a,b}\rangle, \quad |\theta_{0,1,a,b}\rangle = \sqrt{p}|\overline{\theta}_{0,1,a,b}\rangle. \quad (14)$$

Для сокращения выкладок обозначим $|\psi_{0,1,a,b}\rangle = \sqrt{1-p}|\overline{\psi}_{0,1,a,b}\rangle$ и $|\theta_{0,1,a,b}\rangle = \sqrt{p}|\overline{\theta}_{0,1,a,b}\rangle$.

Теперь может быть найдена связь между $|\overline{\psi}_{0a,b}\rangle$, $|\overline{\theta}_{0a,b}\rangle$ и $|\overline{\psi}_{1a,b}\rangle$, $|\overline{\theta}_{1a,b}\rangle$ в базисах a и b. Для этого выразим состояния $|1_a\rangle$ и $|1_b\rangle$ через разложение по паре ортогональных состояний $|0_a\rangle$ и $|0_b\rangle$, выбранных в качестве базиса в $\mathcal{H}_A$; имеем

$$|1_a\rangle = c_\eta|0_a\rangle + s_\eta|0_b\rangle, \quad |1_b\rangle = s_\eta|0_a\rangle - c_\eta|0_b\rangle, \\ \sin(\eta) = s_\eta, \quad \cos(\eta) = c_\eta. \quad (15)$$

Используя (2) и (8), (9), для состояний подслушивателя получаем

$$|\psi_{1a}\rangle = c_\eta^2|\psi_{0a}\rangle + s_\eta^2|\psi_{0b}\rangle + c_\eta s_\eta(|\theta_{0a}\rangle + |\theta_{0b}\rangle), \\ |\theta_{1a}\rangle = -c_\eta^2|\theta_{0a}\rangle + s_\eta^2|\theta_{0b}\rangle + c_\eta s_\eta(|\psi_{0a}\rangle - |\psi_{0b}\rangle), \quad (16)$$

$$|\psi_{1b}\rangle = s_\eta^2|\psi_{0a}\rangle + c_\eta^2|\psi_{0b}\rangle - c_\eta s_\eta(|\theta_{0a}\rangle + |\theta_{0b}\rangle), \\ |\theta_{1b}\rangle = s_\eta^2|\theta_{0a}\rangle - c_\eta^2|\theta_{0b}\rangle + c_\eta s_\eta(|\psi_{0a}\rangle - |\psi_{0b}\rangle). \quad (17)$$

Далее, с учетом (16), (17) находим

$$\langle\psi_{0a}|\theta_{1b}\rangle = c_\eta s_\eta(\langle\psi_{0a}|\psi_{0a}\rangle - \langle\psi_{0a}|\psi_{0b}\rangle), \\ \langle\psi_{1a}|\theta_{0b}\rangle = c_\eta s_\eta(\langle\theta_{0a}|\theta_{0a}\rangle + \langle\theta_{0a}|\theta_{0b}\rangle). \quad (18)$$

С учетом выражений (12), (13) находим связь между скалярными произведениями векторов (18) в пространстве Евы $\mathcal{H}_E$; имеем

$$c_\theta = \frac{(1-p)(1-c_\psi)}{p} - 1. \quad (19)$$

Таким образом, атака Евы на передаваемые состояния полностью описывается заданием унитарного оператора совместной эволюции U. Данный оператор параметризуется в итоге двумя параметрами c_ψ и p, которые в дальнейшем должны быть выбраны так, чтобы Ева могла получить максимум информации о финальном ключе при наблюдаемой ошибке на приемной стороне Боба.

Измерения на приемной стороне. Любые измерения над квантовой системой описываются разложением единицы [7,8] в пространстве состояний $\mathcal{H}_B$, в базисе a имеем

$$I_B = M_{0a} + M_{1a} + M_{a?}, \\ M_{0a} = \frac{I_B - |1_a\rangle\langle 1_a|}{1+c_\eta} = \frac{|1_b\rangle\langle 1_b|}{1+c_\eta}, \\ M_{1a} = \frac{I_B - |0_a\rangle\langle 0_a|}{1+c_\eta} = \frac{|0_b\rangle\langle 0_b|}{1+c_\eta}, \quad (20)$$

где I_B – единичный оператор в $\mathcal{H}_B$. Операторнозначные меры M_{0a} и M_{1a} описывают исходы с определенным результатом, а $M_{?a}$ – исходы с неопределенным результатом. Аналогичные выражения для измеряющих операторов имеют место в базисе b; они получаются из (20) заменой индексов $a \to b$ и $b \to a$ соответственно.

Условная вероятность того, что Алисой исходно послано состояние $|i_m\rangle$ ($i = 0,1$ в базисе $m = a,b$), а результат измерения интерпретирован как $j = 0,1$ при измерении в согласованном базисе m у Боба, равна

$$\Pr(i_m|j_m) = \mathrm{Tr}_{BE}\{|\Psi^{i_m}\rangle_{BE\ BE}\langle\Psi^{i_m}|(M_{j_m}\otimes I_E)\} = \\ \mathrm{Tr}_B\{\rho_B^{i_m} M_{j_m}\}, \quad (21)$$

где $\rho_B^{i_m} = \mathrm{Tr}_E\{|\Psi^{i_m}\rangle_{BE\ BE}\langle\Psi^{i_m}|\}$ – матрица плотности, доступная для измерений на приемной стороне, дается частичным следом совместного запутанного состояния по пространству состояний Евы. Единичный оператор в (21) отражает тот факт, что пока Ева не проводит измерения над своей подсистемой.

Ошибка на приемной стороне – отношение числа неправильных отсчетов к полному числу – имеет вид

$$Q = \frac{\Pr(0a|1a)+\Pr(1a|0a)}{\Pr(0a|0a)+\Pr(1a|1a)+\Pr(0a|1a)+\Pr(1a|0a)} = \\ = \frac{p}{(1-p)s_\eta^2 + (c_\eta^2+1)p}. \quad (22)$$

Такое же выражение для ошибки имеет место для состояний в базисе b. Данное соотношение позволяет Еве связать p, параметризующий ее унитарный оператор с наблюдаемой ошибкой на приемной стороне Боба. Структура информационных состояний такова, что наблюдаемая ошибка Боба Q (соответственно, информация Боба о ключе) не зависит от второго параметра c_ψ, описывающего унитарный оператор Евы. Однако информация Евы о ключе зависит как от Q (p), так и от c_ψ (данный параметр определяет угол между состояниями Евы, от которого зависит различимость этих состояний).

Измерения и информация подслушивателя о ключе. После измерений Боба и отбрасывания отсчетов с неопределенным результатом, для ненормированной матрицы плотности подслушивателя получаем

$$\rho_E^{i_m} = \mathrm{Tr}_B\{|\Psi^{i_m}\rangle_{BE\ BE}\langle\Psi^{i_m}|M_{0_m}\} + \\ + \mathrm{Tr}_B\{|\Psi^{i_m}\rangle_{BE\ BE}\langle\Psi^{i_m}|M_{1_m}\}. \quad (23)$$

Первое слагаемое описывает вклад в матрицу плотности Евы, если у Боба был результат в "канале регистрации" M_{0_m}, соответственно, второе – когда отсчет был в "канале регистрации" M_{1_m}. Для нормированной матрицы плотности находим

$$\rho_E^a = \frac{\rho_E^{0a} + \rho_E^{1a}}{\mathrm{Tr}\{\rho_E^{0a} + \rho_E^{1a}\}} = \frac{1}{2}\frac{\rho_E^{0a} + \rho_E^{1a}}{(1-p)s_\eta^2 + (c_\eta^2+1)p}, \quad (24)$$

где

$$\rho_E^{0a} = s_\eta^2(1-p)|\overline{\psi}_{0a}\rangle\langle\overline{\psi}_{0a}| - \\ - c_\eta\ s_\eta\sqrt{(1-p)p}(|\overline{\psi}_{0a}\rangle\langle\overline{\theta}_{0b}| + |\overline{\theta}_{0b}\rangle\langle\overline{\psi}_{0a}|) + \\ + (c_\eta^2+1)|\overline{\theta}_{0b}\rangle\langle\overline{\theta}_{0b}|, \quad (25)$$

$$\rho_E^{1a} = s_\eta^2(1-p)|\overline{\psi}_{1a}\rangle\langle\overline{\psi}_{1a}| - \\ - c_\eta s_\eta\sqrt{(1-p)p}(|\overline{\psi}_{1a}\rangle\langle\overline{\theta}_{1b}| + |\overline{\theta}_{1b}\rangle\langle\overline{\psi}_{1a}|) + \\ + (c_\eta^2+1)|\overline{\theta}_{1b}\rangle\langle\overline{\theta}_{1b}|. \quad (26)$$

Выражения для матрицы плотности Евы в базисе b получаются из (25), (26) заменой индексов $a \to b$ и $b \to a$.

Таким образом, Ева имеет в квантовой памяти последовательность квантовых состояний

$$\rho_E^{i_1 m_1} \otimes \rho_E^{i_2 m_2} \otimes \ldots \otimes \rho_E^{i_n m_n}. \quad (27)$$

Информация Евы ограничена фундаментальной величиной Холево [7]:

$$\chi(Q, c_\psi) = S(\rho_E^a) - \frac{1}{2}(S(\rho_E^{0a}) + S(\rho_E^{1a})), \quad (28)$$

где $S(\rho) = -\mathrm{Tr}\{\rho\log\rho\}$ – энтропия фон Неймана. Величина Холево (28) дает верхнюю границу классической информации в битах, которая может быть извлечена из ансамбля квантовых состояний (27). Данная граница является достижимой и достигается на коллективных измерениях [7].

Для вычисления величины Холево в (28) требуются собственные числа матрицы плотности ρ_E^a. Оператор $\rho_E^a - \lambda I_B$, определяющий собственные числа в базисе состояний $|\overline{\psi}_{0a}\rangle$, $|\overline{\theta}_{0b}\rangle$, $|\overline{\psi}_{1a}\rangle$, $|\overline{\theta}_{1b}\rangle$, задается следующими матричными элементами:

$$a = \langle\overline{\psi}_{0a}|\rho_E^a|\overline{\psi}_{0a}\rangle = \frac{s_\eta^2 p\langle\overline{\psi}_{0a}|\overline{\psi}_{0a}\rangle^2(1+c_\psi) - 2c_\eta s_\eta\sqrt{p(1-p)}\langle\overline{\psi}_{0a}|\overline{\theta}_{1b}\rangle\langle\overline{\psi}_{0a}|\overline{\psi}_{1a}\rangle + (c_\eta^2+1)\langle\overline{\psi}_{0a}|\overline{\theta}_{1b}\rangle)}{2[s_\eta^2(1-p)) + (c_\eta^2+1)p]}, \quad (29)$$

$$b = \langle\overline{\theta}_{0b}|\rho_E^a|\overline{\theta}_{0b}\rangle = \frac{s_\eta^2(1-p)\langle\overline{\theta}_{0b}|\overline{\psi}_{1a}\rangle^2 - 2c_\eta s_\eta\sqrt{p(1-p)}\langle\overline{\theta}_{0b}|\overline{\theta}_{1b}\rangle\langle\overline{\psi}_{1a}|\overline{\theta}_{0b}\rangle + (c_\eta^2+1)(\langle\overline{\theta}_{0b}|\overline{\theta}_{1b}\rangle^2 + \langle\overline{\theta}_{0b}|\overline{\theta}_{1b}\rangle^2)}{2[s_\eta^2(1-p)) + (c_\eta^2+1)p]}, \quad (30)$$

$$G = \langle\overline{\psi}_{0a}|\rho_E^a|\overline{\psi}_{1a}\rangle = \quad (31)$$

$$\frac{s_\eta^2(1-p)(\langle\overline{\psi}_{0a}|\overline{\psi}_{0a}\rangle\langle\overline{\psi}_{0a}|\overline{\psi}_{1a}\rangle + \langle\overline{\psi}_{1a}|\overline{\psi}_{1a}\rangle\langle\overline{\psi}_{0a}|\overline{\psi}_{1a}\rangle) - c_\eta s_\eta\sqrt{p(1-p)}(\langle\overline{\psi}_{0a}|\overline{\psi}_{0b}\rangle\langle\overline{\theta}_{0b}|\overline{\psi}_{1a}\rangle + \langle\overline{\psi}_{0a}|\overline{\theta}_{1b}\rangle\langle\overline{\psi}_{0a}|\overline{\psi}_{1a}\rangle)}{2[s_\eta^2(1-p)) + (c_\eta^2+1)p]}$$

$$C = \langle\overline{\psi}_{1a}|\rho_E^a|\overline{\theta}_{1b}\rangle = \quad (32)$$

$$= \frac{s_\eta^2(1-p)\langle\overline{\psi}_{0a}|\overline{\psi}_{1a}\rangle\langle\overline{\psi}_{1a}|\overline{\theta}_{0b}\rangle - c_\eta s_\eta[\sqrt{p(1-p)}(\langle\overline{\psi}_{0a}|\overline{\psi}_{0a}\rangle\langle\overline{\theta}_{0b}|\overline{\theta}_{0b}\rangle + \langle\overline{\psi}_{0a}|\overline{\theta}_{1b}\rangle\langle\overline{\psi}_{1a}|\overline{\theta}_{0b}\rangle) + \langle\overline{\psi}_{0a}|\overline{\theta}_{1b}\rangle\langle\overline{\psi}_{1a}|\overline{\theta}_{0b}\rangle]+}{2[s_\eta^2(1-p)) + (c_\eta^2+1)p]} \times$$

$$\times\frac{(c_\eta^2+1)\langle\overline{\psi}_{0a}|\overline{\theta}_{1b}\rangle\langle\overline{\theta}_{1b}|\overline{\theta}_{0b}\rangle}{2[s_\eta^2(1-p)) + (c_\eta^2+1)p]},$$

$$D = \langle\overline{\psi}_{0a}|\rho_E^a|\overline{\theta}_{1b}\rangle = \frac{s_\eta^2(1-p)\langle\overline{\psi}_{1a}|\overline{\psi}_{1a}\rangle\langle\overline{\psi}_{1a}|\overline{\theta}_{0b}\rangle - 2c_\eta s_\eta[\sqrt{p(1-p)}\langle\overline{\psi}_{1a}|\overline{\psi}_{0a}\rangle\langle\overline{\theta}_{0b}|\overline{\theta}_{0b}\rangle + \langle\overline{\psi}_{1a}|\overline{\psi}_{1a}\rangle\langle\overline{\theta}_{1b}|\overline{\theta}_{0b}\rangle]+}{2[s_\eta^2(1-p)+(c_\eta^2+1)p]} \times \tag{33}$$

$$\times\frac{(c_\eta^2+1)\langle\overline{\psi}_{1a}|\overline{\theta}_{0b}\rangle\langle\overline{\theta}_{0b}|\overline{\theta}_{0b}\rangle}{2[s_\eta^2(1-p)+(c_\eta^2+1)p]}.$$

Окончательно имеем

$$\begin{pmatrix} a-\lambda & G-\lambda\cdot p_{(\psi,\psi)} & C & D-\lambda\cdot p_{(\psi,\theta)} \\ G-\lambda\cdot p_{(\psi,\psi)} & a-\lambda & D-\lambda p_{(\psi,\theta)} & C \\ C & D-\lambda\cdot p_{(\psi,\theta)} & b-\lambda & F-\lambda\cdot p_{(\theta,\theta)} \\ D-\lambda\cdot p_{(\psi,\theta)} & C & F-\lambda\cdot p_{(\theta,\theta)} & b-\lambda \end{pmatrix}, \tag{34}$$

где

$$p_{(\psi,\psi)} = c_\eta^2 + s_\eta^2 c_\psi, \quad p_{(\theta,\theta)} = s_\eta^2 c_\theta - c_\eta^2, \quad p_{(\psi,\theta)} = c_\eta s_\eta(1-c_\psi)\sqrt{\frac{1-p}{p}}. \tag{35}$$

Индексы относятся к состояниям, по которым вычисляются матричные элементы. Все величины в (29)–(34) являются функциями Q, c_ψ и η, из экономии места аргументы не выписываем. Вычисление детерминанта матрицы (34) приводит к уравнению 4-й степени общего вида, корни которого являются собственными числами матрицы плотности ρ_E^a. Имеются известные явные аналитические выражения для корней. Ввиду громоздкости они здесь не приводятся. Пусть собственные числа матрицы (34) есть $\lambda_{1,2,3,4}$. Далее,

$$\begin{aligned} S(\rho_E^a) &= -\sum_{i=1}^{4}\lambda_i\log\lambda_i, \\ S(\rho_E^{0a}) = S(\rho_E^{1a}) &= -\overline{\lambda}_1\log\overline{\lambda}_1 - \overline{\lambda}_2\log\overline{\lambda}_2; \end{aligned} \tag{36}$$

здесь $\overline{\lambda}_{1,2}$ – собственные числа частичной матрицы плотности (25), (26)

$$\overline{\lambda}_{1,2} = \frac{e_1+e_2 \pm \sqrt{(e_1-e_2)^2+4\gamma^2}}{2}, \tag{37}$$

$$\begin{aligned} e_1 &= \frac{s_\eta^2(1-p(Q))}{s_\eta^2(1-p(Q))+(c_\eta^2+1)p(Q)}, \\ e_2 &= \frac{(c_\eta^2+1)p(Q)}{s_\eta^2(1-p(Q))+(c_\eta^2+1)p(Q)}, \end{aligned} \tag{38}$$

$$\gamma = \frac{\sqrt{p(Q)(1-p(Q))}}{s_\eta^2(1-p(Q))+(c_\eta^2+1)p(Q)}. \tag{39}$$

Зависимость p от Q дается соотношением (22).

Критическая ошибка и длина секретного ключа. Критическая ошибка Q_c, до которой можно передавать ключи и гарантировать их секретность с учетом (1) и (23), определяется уравнением

$$1 - h(Q_c) = \max_{c_\psi}\chi(Q_c, c_\psi), \tag{40}$$

где параметр c_ψ определяется Евой так, чтобы максимизировать свою информацию о ключе. Длина секретного ключа, который может быть получен из последовательности длины n, определяется как

$$r = n(1 - h(Q) - \max_{c_\psi}\chi(Q, c_\psi)). \tag{41}$$

Максимизация информации Евы проводится по одной переменной c_ψ. Зависимости $1-h(Q)$ и $\max_{c_\psi}\chi(Q,c_\psi)$ как функции наблюдаемой ошибки на приемной стороне при оптимальном значении c_ψ, которое находилось численно, представлены на рис.1 при различных значениях угла η (формула (2)) между информационными состояниями. Значения угла между состояниями указаны на рис.1a, b.

На рис.2a приведена зависимость $1-h(Q)-\chi(Q,c_\psi)$ на плоскости параметров (Q,c_ψ). Указана область, где $|c_\theta| > 1$, и решения отсутствуют. На рис.2b приведена зависимость критической ошибки, до которой возможно распространение секретных ключей, как функция угла η между состояниями внутри базисов.

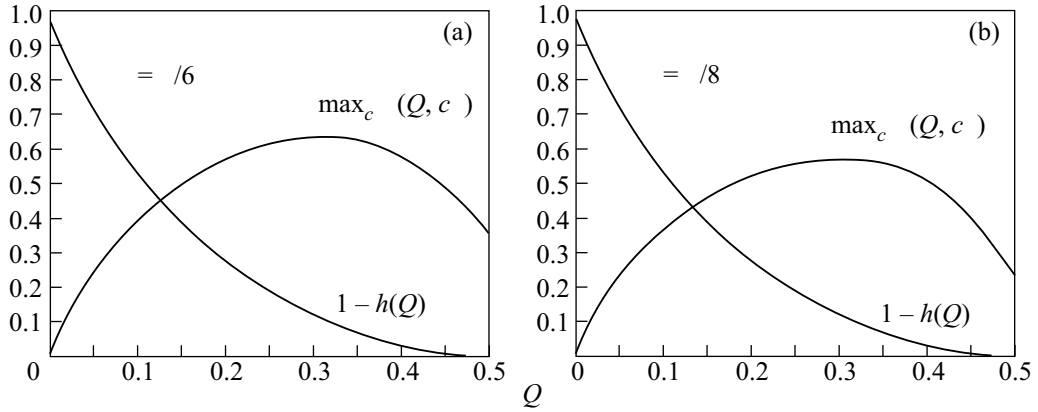

Рис.1

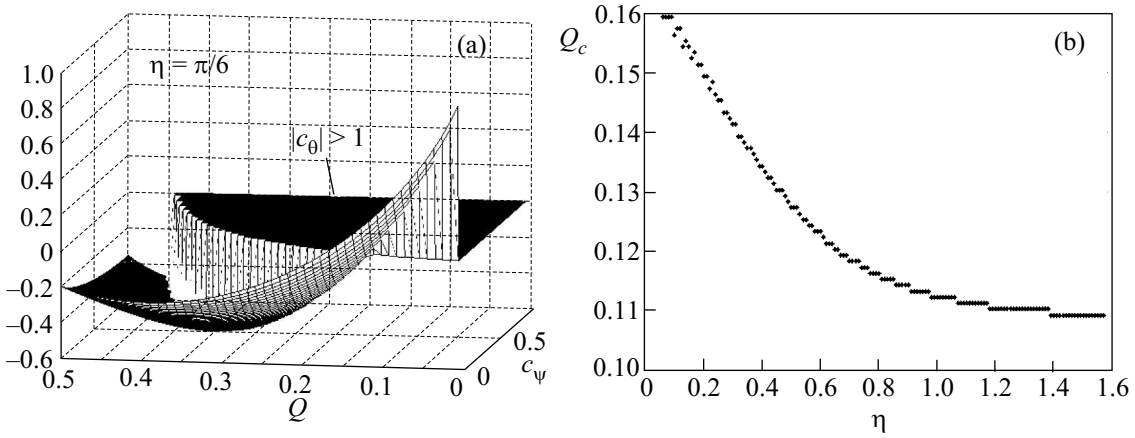

Рис.2

Один из авторов (С.Н.М.) выражает благодарность Академии криптографии Российской Федерации за поддержку. Работа частично поддержана проектом Российского фонда фундаментальных исследований # 08-02-00559.

1. G. Brassard, N. Lütkenhaus, T. Mor, and B. Sanders, Phys. Rev. Lett., **85**, 1330 (2000); N.Lütkenhaus, Phys. Rev. A **61**, 052304 (2000).
2. C. H. Bennett, G. Brassard, *Quantum Cryptography: Public Key Distribution and Coin Tossing*, Proc.of IEEE Int. Conf. on Comput. Sys. and Sign. Proces., Bangalore, India, December 1984, p. 175.
3. V. Scarani, A. Acin, G. Ribordy, and N. Gisin, Phys. Rev. Lett. **92**, 057901-1 (2004).
4. C. Branciard, N. Gisin, B. Kraus, and V. Scarani, Phys. Rev. A **72**, 032301 (2005).
5. С. Н. Молотков, ЖЭТФ **133**, 5 (2008); Письма в ЖЭТФ **88**, 315 (2008).
6. C. E. Shannon, Bell Syst. Tech. Jour. **27**, 397; 623 (1948).
7. А. С. Холево, *Введение в квантовую теорию информации*, серия *Современная математическая физика*, вып.5, М.: МЦНМО, 2002; Успехи математических наук **53**, 193 (1998).
8. M. Nielsen and I. Chuang, *Quantum Computation and Quantum Information*, Cambridge University Press, 2001; (М.Нильсен, И.Чанг, *Квантовые вычисления и квантовая информация*, М.: Мир, 2006).
9. Р. Галлагер, *Теория информации и надежная связь*, М.: Сов. Радио, 1974.
10. C. H. Bennett, G. Brassard, C. Crépeau, and U. Maurer, IEEE Transaction on Information Theory, **41**, 1915 (1995).
11. J. L. Carter and M. N. Wegman, J. of Computer and System Sciences **18**, 143 (1979).
12. R. Renner, arXiv: quant-ph/0512258.
13. С. Н. Молотков, А. В. Тимофеев, Письма в ЖЭТФ **85**, 632 (2007).
14. М. А. Наймарк, Известия АН СССР (математическая серия) **4**, 277 (1940).