Письма в ЖЭТФ, том 85, вып. 10, с. 632 – 637 © 2007 г. 25 мая

Явная атака на ключ в квантовой криптографии (протокол BB84), достигающая теоретического предела ошибки $Q_c \approx 11\%$

С. Н. Молотков[+*▽], *А. В. Тимофеев*[▽]

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

[*] *Академия Криптографии РФ*

[▽] *Факультет вычислительной математики и кибернетики, МГУ им. М.В. Ломоносова, 119899 Москва, Россия*

Поступила в редакцию 27 февраля 2007 г.

После переработки 17 апреля 2007 г.

Приведена явная атака на передаваемый ключ по квантовому криптографическому протоколу BB84. При данной атаке достигается теоретически возможный максимум информации подслушивателя (Евы) о ключе при минимально возможной ошибке Q на приемном конце. Максимум информации Евы достигается при коллективных измерениях, которые строятся явно и которые Ева производит в самом конце протокола. Выяснено, что происходит в интервале критической ошибки между $11\% < Q_c < 15\%$.

PACS: 03.65.Bz, 03.67.Db

Квантовая криптография – система распределения криптографических ключей по открытым каналам связи обеспечивает секретность передаваемых ключей. Причем гарантии секретности ключей основаны на фундаментальных законах природы – квантовой механики, а не на технических или вычислительных ограничениях подслушивателя. Квантовая криптография обеспечивает не только детектирование попыток подслушивания, но и секретность передаваемых ключей, если процент ошибок (в более общей ситуации изменение статистики результатов измерений) на приемной стороне не превосходит некоторой критической величины, которая определяется квантовым криптографическим протоколом. Первой задачей теории является определение критической величины ошибки, до которой гарантируется секретность передаваемых ключей. Вторая задача состоит в вычислении длины финального ключа при данном наблюдаемом проценте ошибок, если он ниже критической величины. Еще один вопрос, ответ на который фактически объединяет ответы на первые два, сводится к тому, какова оптимальная стратегия подслушивателя, при которой извлекается максимально возможное количество информации подслушивателем о ключе при данной наблюдаемой ошибке на приемной стороне. При этом считается, что действия подслушивателя ограничены лишь фундаментальными законами природы. И было бы совсем хорошо, если бы удалось явно предъявить оптимальную стратегию подслушивателя. К сожалению, до сегодняшнего для ни для одного квантового криптографического протокола такая стратегия не была предъявлена.

Ниже речь пойдет о протоколе BB84 [1], который был первым квантовым криптографическим протоколом и который является основным и наиболее исследованным. Для данного протокола известна точная величина критической ошибки $Q_c \approx 11\%$ [2–4][1)]. Строгие доказательства о критической величине 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, и Алисой и Евой: $I_{AB}(Q) > I_{AE}(Q)$, что позволяет, согласно теореме [5], извлечь секретный ключ. При $Q = Q_c$ $I_{AB}(Q) = I_{AE}(Q)$, 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. [6]), которая на словах сводится к следующему. Ева в каждой посылке использует свое квантовое вспомогательное состояние $|A\rangle$ (ancilla), которое унитарно взаимодействует

[1)] Знак $\approx$ употребляется для краткости, точное значение Q_c определяется как корень некоторого трансцендентного уравнения [4].

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 к Бобу, а свое состояние Ева сохраняет у себя в квантовой памяти до стадии раскрытия базисов. После того как Боб произвел измерения, происходит согласование базисов. То есть посылки, где Боб производил измерения в не согласованным с Алисой базисе, отбрасываются. Далее Ева производит *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 в 11%. То есть подобная стратегия Евы не является оптимальной в упомянутом выше смысле. Никаких других явных стратегий Евы, при которых получается меньший вносимый процент ошибок, неизвестно.

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 в 11%.

В протоколе BB84 используется два сопряженных базиса, в которые кодируются биты передаваемого ключа $\{0,1\} \to \{|x\rangle, |y\rangle\}$ и $\{0,1\} \to \{|u\rangle = \frac{1}{\sqrt{2}}(|x\rangle + |y\rangle), |v\rangle = \frac{1}{\sqrt{2}}(|x\rangle - |y\rangle)\}$. Внутри каждого базиса состояния ортогональны, а состояния из разных базисов попарно неортогональны.

В каждой посылке Ева использует свое вспомогательное состояние $|A\rangle$, которое унитарно взаимодействует с передаваемым состоянием:

$$U(|x\rangle \otimes |A\rangle) = |X\rangle, \quad U(|y\rangle \otimes |A\rangle) = |Y\rangle. \tag{1}$$

В силу линейности квантовой механики, для состояний из сопряженного базиса имеем

$$\begin{aligned} U(|u\rangle \otimes |A\rangle) = |U\rangle = \frac{1}{\sqrt{2}}(|X\rangle + |Y\rangle), \\ U(|v\rangle \otimes |A\rangle) = |V\rangle = \frac{1}{\sqrt{2}}(|X\rangle - |Y\rangle). \end{aligned} \tag{2}$$

Можно показать, что при индивидуальных измерениях Евы оптимальна симметричная стратегия, в которой подслушивание приводит к тому, что к каждому состоянию из данного базиса примешивается другое состояние из того же базиса [6]. Имеем:

$$|X\rangle = \sqrt{1-Q}|x\rangle \otimes |\phi_x\rangle + \sqrt{Q}|y\rangle \otimes |\theta_x\rangle, \tag{3}$$

$$|Y\rangle = \sqrt{1-Q}|y\rangle \otimes |\phi_y\rangle + \sqrt{Q}|x\rangle \otimes |\theta_y\rangle,$$

и для сопряженного базиса:

$$|U\rangle = \sqrt{1-Q}|u\rangle \otimes |\phi_u\rangle + \sqrt{Q}|v\rangle \otimes |\theta_v\rangle, \tag{4}$$

$$|V\rangle = \sqrt{1-Q}|v\rangle \otimes |\phi_v\rangle + \sqrt{Q}|u\rangle \otimes |\theta_v\rangle,$$

здесь $|\phi_{x,y,u,v}\rangle$ и $|\theta_{x,y,u,v}\rangle$ – состояния Евы. К этим состояниям предъявляется лишь требование по нормировке и сохранению унитарности:

$$\langle X|Y\rangle = \langle x|y\rangle, \quad \langle U|V\rangle = \langle u|v\rangle. \tag{5}$$

Размерность пространства состояний для $|A\rangle$ может быть выбрана любой. Если размерность пространства состояний равна 4 (или выше), то компоненты состояний могут быть сделаны ортогональными, то есть $|\phi_{x,y,u,v}\rangle \perp |\theta_{x,y,u,v}\rangle$. Далее, условие симметричности атаки (ошибки в разных базисах, возникающие от подслушивания Евы одинаковы), линейности (1) и унитарности дает связь между разными состояниями:

$$2\sqrt{1-Q}|\phi_u\rangle = \sqrt{1-Q}(|\phi_x\rangle + |\phi_y\rangle) + \sqrt{Q}(|\theta_x\rangle + |\theta_y\rangle), \tag{6}$$

$$2\sqrt{Q}|\theta_u\rangle = \sqrt{1-Q}(|\phi_x\rangle - |\phi_y\rangle) + \sqrt{Q}(|\theta_y\rangle - |\theta_x\rangle). \tag{7}$$

Для симметричной атаки [6] скалярные произведения $\langle\phi_x|\phi_y\rangle$ и $\langle\theta_x|\theta_y\rangle$ могут быть выбраны вещественными. Кроме того, максимум информации Евы достигается при $\langle\phi_x|\phi_y\rangle = \langle\theta_x|\theta_y\rangle = \cos(\alpha)$. То есть атака параметризуется лишь двумя параметрами Q и α. Остается связать эти два параметра. Имеем

$$1 - Q = \frac{1 + \langle\theta_x|\theta_y\rangle}{2 - \langle\phi_x|\phi_y\rangle + \langle\theta_x|\theta_y\rangle} = \frac{1 + \cos(\alpha)}{2}. \tag{8}$$

Если Алиса посылала состояния $\{|x\rangle, |y\rangle\}$, то состояния Боба получаются взятием частичного следа по пространству состояний Евы (соответственно, состояния Евы получаются взятием частичного следа по пространству состояний Боба) и имеют вид

$$|x\rangle \to \rho_x^{\mathrm{Eve}} = (1-Q)|\phi_x\rangle\langle\phi_x| + Q|\theta_x\rangle\langle\theta_x| \to$$

$$\to \rho_x^{\mathrm{Bob}} = (1-Q)|x\rangle\langle x| + Q|y\rangle\langle y|, \tag{9}$$

$$|y\rangle \to \rho_y^{\mathrm{Eve}} = (1-Q)|\phi_y\rangle\langle\phi_y| + Q|\theta_y\rangle\langle\theta_y| \to$$

$$\to \rho_y^{\mathrm{Bob}} = (1-Q)|y\rangle\langle y| + Q|x\rangle\langle x|.$$

Аналогично для сопряженного базиса $\{|u\rangle|v\rangle\}$

$$|u\rangle \to \rho_u^{\mathrm{Eve}} = (1-Q)|\phi_u\rangle\langle\phi_u| + Q|\theta_u\rangle\langle\theta_u| \to$$

$$\to \rho_u^{\mathrm{Bob}} = (1-Q)|u\rangle\langle u| + Q|v\rangle\langle v|, \qquad (10)$$

$$|v\rangle \to \rho_v^{\mathrm{Eve}} = (1-Q)|\phi_v\rangle\langle\phi_v| + Q|\theta_v\rangle\langle\theta_v| \to$$

$$\to \rho_v^{\mathrm{Bob}} = (1-Q)|v\rangle\langle v| + Q|u\rangle\langle u|,$$

Боб производит измерения в каждой посылке в одном из двух сопряженных базисов $\{|x\rangle, |y\rangle\}$ или $\{|u\rangle, |v\rangle\}$, которые он выбирает случайно и независимо от Алисы. После измерений происходит согласование базисов между Алисой и Бобом. Посылки, в которых базисы не совпадали, отбрасываются. Вероятность получения результатов в совпадающих базисах есть

$$\Pr(0|0)=\mathrm{Tr}\{\rho_x^{\mathrm{Bob}}|x\rangle\langle x|\}=\mathrm{Tr}\{\rho_u^{\mathrm{Bob}}|u\rangle\langle u|\}=\Pr(1|1)=$$
$$= \mathrm{Tr}\{\rho_y^{\mathrm{Bob}}|y\rangle\langle y|\} = \mathrm{Tr}\{\rho_v^{\mathrm{Bob}}|v\rangle\langle v|\} = 1-Q, \qquad (11)$$

$$\Pr(0|1)=\mathrm{Tr}\{\rho_x^{\mathrm{Bob}}|y\rangle\langle y|\}=\mathrm{Tr}\{\rho_u^{\mathrm{Bob}}|v\rangle\langle v|\}=\Pr(1|0)=$$
$$\mathrm{Tr}\{\rho_y^{\mathrm{Bob}}|x\rangle\langle x|\} = \mathrm{Tr}\{\rho_v^{\mathrm{Bob}}|u\rangle\langle u|\} = Q. \qquad (12)$$

Здесь $\Pr(i|j)$ – вероятность того, что Алисой был послан бит i, а Боб интерпретировал результат как бит j, Q – вероятность ошибки у Боба. Ева пока не производит измерения, а сохраняет свои состояния в квантовой памяти. Далее Боб раскрывает часть последовательности для оценки вероятности ошибки Q, раскрытая часть отбрасывается.

После этого 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 [7]. Пусть длина оставшейся последовательности есть n. Алиса генерирует $2^{n(C_{\mathrm{clas}}(Q)-\delta)}$ ($\delta \to 0$ при $n \to \infty$) случайных кодовых слов. Здесь

$$C_{\mathrm{clas}}(Q) = 1 - h(Q),$$
$$h(Q) = -Q\log Q - (1-Q)\log(1-Q) \qquad (13)$$

– 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 бит, 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 последовательности бит у Боба.

После раскрытия базисов шенноновская взаимная информация между Алисой и Евой, если Ева делает индивидуальные измерения, дается формулой (для индивидуальных измерений ситуация для базисов $+$ и $\times$ может рассматриваться независимо) π_x:

$$I(A;E,\pi,\mathcal{M}) = \sum_{x,\,y} \pi_x p_{\mathcal{M}}(y|x)[\log p_{\mathcal{M}}(y|x) -$$
$$- \log \sum_{z\,=\,x,\,y} \pi_z p_{\mathcal{M}}(y|z)], \qquad (14)$$

где $\pi_x = \pi_y = 1/2$ – априорные распределения вероятностей для $\rho_{x,y}^{\mathrm{Eve}}$, которые заданы Алисой, $\mathcal{M} = \{M_x, M_y\}$ – измеряющие операторы Евы. Далее условная вероятность, например, $p_{\mathcal{M}}(y|x) = \mathrm{Tr}\{\rho_y^{\mathrm{Eve}} \cdot M_x\}$, того, что было у Евы в ячейке квантовой памяти было квантовое состояние, отвечающее $1-\rho_y^{\mathrm{Eve}}$, а результат измерения был интерпретирован как 0.

Согласно [8], максимальное количество классической информации, допустимое законами квантовой механики при индивидуальных измерениях,

$$C_1 = \max_{\pi,\mathcal{M}} I(A;E,\pi,\mathcal{M}), \qquad (15)$$

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

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 ρ_x^{Eve} и ρ_y^{Eve} в базисе (x,y) или матриц плотности ρ_u^{Eve} и ρ_v^{Eve} в базисе (u,v). Такое измерение $\mathcal{M}$ известно (см. детали в [8]), ошибка различения 0 и 1 есть

$$Q_E = \frac{1}{2}\left(1 - \sqrt{1-\varepsilon^2(Q)}\right) = \frac{1-\sin\alpha}{2} =$$
$$= \frac{1}{2}\left(1 - \sqrt{1-(1-2Q)^2}\right), \quad \varepsilon(Q) = |\langle\phi_x|\phi_y\rangle|, \qquad (16)$$

здесь учтено, что $|\phi_i\rangle$ и $|\theta_j\rangle$ ортогональны, и введено обозначение $Q_E = p(x|y) = p(y|x)$, а также $C_1(\varepsilon(Q)) = C_1$.

Количество кодовых слов, которые может различить Ева, не превышает $2^{nC_{\rm clas}(Q)} = 2^{nC_1(\varepsilon(Q))}$, где

$$C_{\rm clas}(Q) = C_1(\varepsilon(Q)), \tag{17}$$

$$C_1(\varepsilon(Q)) = \\ = \frac{1}{2}\Big[(1-\sqrt{1-\varepsilon^2(Q)})\log(1-\sqrt{1-\varepsilon^2(Q)}) + \\ + (1+\sqrt{1-\varepsilon^2(Q)})\log(1+\sqrt{1-\varepsilon^2(Q)})\Big], \tag{18}$$

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. Тот факт, что Алиса сообщает открыто набор кодовых слов, означает, что известны и сами состояния в каждой кодовой последовательности, но не известно, какая из них была послана. Цель Евы извлечь классическую информацию.

При индивидуальных измерениях распределение ключа возможно, если

$$C_{\rm clas}(Q) \geq C_1(\varepsilon(Q)). \tag{19}$$

Критическая величина ошибки для индивидуальных измерений Евы определяется как корень уравнения

$$C_{\rm clas}(Q_c) = C_1(\varepsilon(Q_c)), \quad Q_c \approx 15\%. \tag{20}$$

Ева может извлечь больше классической информации, если она будет проводить коллективные измерения сразу над всей последовательностью. Индивидуальные измерения Евы сводились фактически к различению состояний $|\phi_x$ и ϕ_y (аналогично $|\phi_u$ и ϕ_v), измерения сводились к проекции на два ортогональных вектора (один в плоскости на диагонали посредине между $|\phi_x$ и ϕ_y, второй в той же плоскости, ортогональный первому). Коллективные измерения отвечают, грубо говоря, проекции на специальные сцепленные (запутанные) состояния из n кубитов (см. ниже, явный вид измеряющих операторов X_w). В этом случае соответствующая шенноновская взаимная информация, согласно [8], есть

$$I_n(A;E,\pi,\mathcal{X}) = \sum_w \pi_w p_{\mathcal{X}}(\hat{w}|w)[\log p_{\mathcal{X}}(\hat{w}|w) - \\ - \log\sum_{w'}\pi_{w'}p_{\mathcal{X}}(\hat{w}|w')]; \tag{21}$$

здесь π_w – распределение вероятностей для последовательности длины n (состояний Евы в регистре квантовой памяти, в каждой ячейке которого с равной вероятностью присутствует ρ_x^{Eve} и ρ_y^{Eve} (в базисе +). Количество классической информации, которое может быть извлечено при коллективных измерениях (проекциях на запутанные состояния из n кубитов), по определению [8] есть

$$C_n = \max_{\pi_w,\mathcal{X}} I(A;E,\pi_w,\mathcal{X}), \tag{22}$$

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

Далее 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

$$\overline{C}(\varepsilon(Q)) = S(\sum_{i=x,y,u,v}\frac{1}{4}\rho_i^{\rm Eve}) - \sum_{i=x,y,u,v}\frac{1}{4}S(\rho_i^{\rm Eve}), \\ S(\rho) = -{\rm Tr}\{\rho\log\rho\}. \tag{23}$$

$\overline{C}(\varepsilon(Q))$ – *классическая пропускная способность квантового канала связи* [8].

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

$$\sum_{i=x,y,u,v}\frac{1}{4}\rho_i^{\rm Eve} = \\ = \frac{1}{2}\begin{pmatrix} 1-Q & (1-Q)\varepsilon(Q) & 0 & 0 \\ (1-Q)\varepsilon(Q) & 1-Q & 0 & 0 \\ 0 & 0 & Q & Q\varepsilon(Q) \\ 0 & 0 & Q\varepsilon(Q) & Q \end{pmatrix}, \tag{24}$$

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

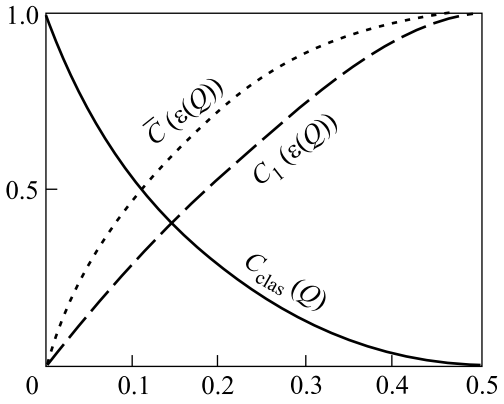
Собственные числа частичных матриц плотности $\rho_{x,y,u,v}^{Eve}$ равны $1-Q$ и Q. При $2^{n\overline{C}(\varepsilon(Q))} \leq 2^{nC_{\rm clas}(Q)}$ возможно секретное распределение ключей между Алисой и Бобом. Учитывая связь Q и $\varepsilon(Q)$ из (8), находим

$$\overline{C}(\varepsilon(Q)) = -Q\log Q - (1-Q)\log(1-Q), \ \varepsilon(Q) = 1-2Q. \tag{25}$$

Критическая величина ошибки

$$C_{clas}(Q_c) = \overline{C}(\varepsilon(Q_c)), \ 1-h(Q_c) = h(Q_c) \ Q_c \approx 11\%, \tag{26}$$

что совпадает с точным значением [4].



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

Подчеркнем, что такая величина ошибки достигается, если легитимные пользователи используют случайный шенноновский код для исправления ошибок. Такой код практически нереализуем, поскольку требует экспоненциально большой таблицы для кодовых слов размером $2^{nC_{\rm clas}(Q)}$. Случайный код имеет минимально возможную избыточность (максимально кодовое расстояние). При использовании других процедур критическая ошибка будет меньше, поскольку избыточность конструктивных кодов выше. Например, если используется каскадная процедура коррекции ошибок, то критическая величина ошибки оказывается $Q_c \approx 8.9\%$ [9], что лучше, чем при использовании других конструктивных эффективно декодируемых кодов, для которых $Q_c \approx 7.5\%$ [2, 3].

Если величина ошибки меньше критической, то длина ключа в битах есть

$$N_{\rm key} = n(1 - 2h(Q)). \qquad (27)$$

Поясним несколько более подробно, что означает, что Алиса и Ева после раскрытия базисов и выбора кодовых слов для исправления ошибок у Боба, связаны квантовым каналом связи.

Поскольку базисы раскрыты, то набор из M битовых кодовых слов $w^{(1)}, w^{(2)}, ...w^{(M)}$ ($w^{(k)} = (i_1^k, i_2^k, ...i_n^k)$, $i_j^k = 0, 1$) однозначно связан с квантовыми состояниями, из которых данные битовые строки могли произойти: $|w^{(k)}\rangle = |i_1^k(b_1)\rangle \otimes |i_2^k(b_2)\rangle .... \otimes |i_n^k(b_1)\rangle$. Здесь, например, $|i_1^k(b_1)\rangle = |x\rangle$, если первый бит в k-м кодовом слове Алисы $i_1^k = 0$ и раскрытый базис в первой посылке был $b_1 = \{x, y\}$.

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: $\rho_{w^{(k)}} = \rho^{\rm Eve}_{i^k_1(b_1)} \otimes \rho^{\rm Eve}_{i^k_2(b_2)} \cdots \otimes \rho^{\rm Eve}_{i^k_n(b_n)}$. Число таких квантовых кодовых слов равно числу классических кодовых слов, которое выбирается Алисой в зависимости от наблюдаемой ошибки у Боба.

Ева должна использовать квантовомеханические 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 [8]):

$$I = \sum_{k=1}^{M} X_{w^{(k)}},$$
$$X_{w^{(k)}} = \left(\sum_{l=1}^{M} P P_{w^{(l)}} P\right)^{-1/2} \times \qquad (28)$$
$$\times P P_{w^{(k)}} P \left(\sum_{l=1}^{M} P P_{w^{(l)}} P\right)^{-1/2},$$

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

$$2^{-n(\sum_{i=x,y,u,v} \frac{1}{4} S(\rho_i^{\rm Eve}) + \delta)} < \lambda_J < 2^{-n(\sum_{i=x,y,u,v} \frac{1}{4} S(\rho_i^{\rm Eve}) - \delta)}.$$

Далее, P – проектор на типичное подпространство для оператора $(\sum_{i=x,y,u,v} \frac{1}{4}\rho_i^{Eve})^{\otimes n}$, где

$$P = \sum_{J \in Typ} |\lambda_J\rangle\langle\lambda_J|; \qquad (29)$$

здесь $|\lambda_J\rangle = |\lambda_{j_1}\rangle \otimes |\lambda_{j_2}\rangle \otimes .... \otimes |\lambda_{j_n}\rangle$, $|\lambda_{j_m}\rangle$ – собственные векторы оператора (24) и типичное пространст-

во – это пространство всех последовательностей, для которых

$$\mathrm{Typ} = \{J : 2^{-n(S(\sum_{i=s,y,u,v}\frac{1}{4}\rho_i^{\mathrm{Eve}}+\delta))} < \lambda_J < 2^{-n(S(\sum_{i=s,y,u,v}\frac{1}{4}\rho_i^{\mathrm{Eve}}-\delta))}\}.$$

Таким образом, описана явная атака на ключ, при которой достигается максимум информации Евы при минимуме наблюдаемой ошибки на приемном конце.

Если Ева на конечном этапе производит индивидуальные измерения, то это соответствует достижению пропускной способности квантового канала между Алисой и Евой за один шаг C_1 (one shot). Критическая величина ошибки при этом $Q_c \approx 15\%$. При коллективных измерениях Евы достигается классическая пропускная способность квантового канала связи $\overline{C}$. Критическая ошибка при этом $Q_c \approx 11\%$.

Что происходит в области $11\% < Q_c < 15\%$?

Как было отмечено в работе [11], для квантового канала связи (точнее c-q – classical-quantum, канала, 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 [11] $C_{1,1}$). 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 [11] $C_{1,\infty}$). 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, то 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

$$\begin{gathered} C_{\mathrm{clas}}(Q_{c,k}) = C_{1,k}(\varepsilon(Q)), \\ Q_{c,\infty}(11\%) < Q_{c,k} < Q_{c,1}(15\%), \end{gathered} \tag{30}$$

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

До тех пор, пока не создано квантовой памяти можно исходить из критической ошибки в 15%. Даже если такая квантовая память и будет создана, это еще не решает 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, если использовать те же оптические элементы (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 в 15%, квантовая криптография имеет очень большой запас прочности.

Один из авторов (С.Н.М.) благодарит Академию криптографии РФ за поддержку. Работа поддержана проектом Российского фонда фундаментальных исследований # 05-02-17387.

1. C. H. Bennett and G. Brassard, Proc. of IEEE Int. Conf. on Comput. Sys. and Sign. Proces., Bangalore, India, December 1984, p. 175.
2. D. Mayers and A. Yao, arXiv:quant-ph/9802025.
3. E. Biham, M. Boyer, P. O. Boykin et al., arXiv:quant-ph/9912053.
4. P. W. Shor and J. Preskill, arXiv:quant-ph/0003004.
5. I. Csiszár and J. Körner, IEEE Trns. Inf. Theory, **24**, 339 (1978).
6. C. A. Fuchs, N. Gisin, R. Griffiths et al., Phys. Rev. A **56**, 1163 (1997).
7. C. E. Shannon, Bell Syst. Tech. Jour. **27**, 397, 623 (1948).
8. А. С. Холево, Проблемы передачи информации **8**, 63 (1972); **15**, 3 (1979); Успехи математических наук **53**, 193 (1998); *Введение в квантовую теорию информации*, серия *Современная математическая физика*, вып. 5, МЦНМО, Москва, 2002.
9. А. В. Тимофеев, С. Н. Молотков, Письма в ЖЭТФ **82**, 868 (2005).
10. R. Griffiths and Chi-Sheng Niu, Phys. Rev. A **56**, 1173 (1997).
11. P. Shor, arXiv:quant-ph/0304102.