Письма в ЖЭТФ, том 80, вып. 8, с. 639 – 644 © 2004 г. 25 октября

О коллективной атаке на ключ в квантовой криптографии на двух неортогональных состояниях

С. Н. Молотков

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

Факультет вычислительной математики и кибернетики, МГУ им. М. В. Ломоносова, 119899 Москва, Россия

Поступила в редакцию 21 сентября 2004 г.

Рассмотрена "коллективная" атака на ключ и прослежена ее связь с классической пропускной способностью квантового канала связи. Показано также, что допустимая вероятность ошибок у легитимных пользователей, до которой возможно извлечение секретного ключа, уменьшается более чем в два раза по сравнению с "прозрачным" подслушиванием и индивидуальными измерениями.

PACS: 03.67.Dt, 42.50.−p, 89.70.+c

Квантовое распространение ключа (квантовая криптография) позволяет организовать секретную передачу ключа таким образом, что можно гарантировать его секретность на уровне фундаментальных законов природы – квантовой механики [1 – 3].

Различные стратегии подслушивания можно условно разделить на следующие.

1) Стратегия "непрозрачного" (opaque) подслушивания, часто также называемая прием-перепосылка, сводится к измерению непосредственно передаваемого состояния, а затем перепосылке нового состояния в зависимости от результата измерения.

2) При стратегии индивидуального "прозрачного" (translucent) подслушивания подслушиватель в каждой посылке использует свое вспомогательное состояние, которое на время приводится во взаимодействие с передаваемым состоянием. После взаимодействия передаваемое и вспомогательное состояния оказываются в общем запутанном состоянии. Далее подслушиватель производит измерение в каждой посылке над своим вспомогательным состоянием, а информационное состояние направляется на приемный конец к легитимному пользователю.

3) При "коллективной" атаке подслушиватель действует аналогично предыдущему случаю, но с той разницей, что сохраняет свои вспомогательные состояния в квантовой памяти и не производит измерения до тех пор, пока не будут переданы все состояния легитимным пользователем и не закончится обмен по открытому каналу с целью исправления ошибок и усиления секретности. Только после этого подслушиватель производит измерения коллективно сразу над всеми своими состояниями.

4) И наконец, самая общая и, по-видимому, самая эффективная атака (joint attack) аналогична предыдущей с той лишь разницей, что подслушиватель использует единое вспомогательное состояние из гильбертова пространства состояний большой размерности, с которым взаимодействуют передаваемые состояния и все измерения над которым также производятся в самом конце.

В данной работе будет рассмотрена "коллективная" атака на ключ и прослежена ее связь с классической пропускной способностью квантового канала связи.

Концептуально наиболее простой является квантовая криптография на двух неортогональных состояниях (протокол B92) [2]. Секретность данного протокола исследовалась в целом ряде работ [4 – 9] для различных измерений на приемном конце. Коллективные измерения рассматривались для данного протокола обмена лишь для достаточно частного случая – определения бита четности [10].

Протокол для легитимных пользователей выглядит стандартным образом. В качестве информационных состояний используется пара неортогональных однофотонных состояний: $0 \to |u\rangle$, $1 \to |v\rangle$. Далее следуем обозначениям [4], что будет удобно при сравнении результатов:

$$\langle u|v\rangle = \sin(2\alpha), \quad \langle e_0|e_1\rangle = 0, \tag{1}$$

где $|e_0\rangle$ и $|e_1\rangle$ – ортонормированные базисные векторы в пространстве, натянутом на $|u\rangle$ и $|v\rangle$ (см. рис.1). На приемном конце всегда используется одно и то же измерение, которое описывается разложением единицы:

$$\mathcal{A}_u = \frac{(I - |v\rangle\langle v|)}{1 + \langle u|v\rangle}, \quad \mathcal{A}_v = \frac{(I - |u\rangle\langle u|)}{1 + \langle u|v\rangle}, \tag{2}$$
$$\mathcal{A}_? = I - \mathcal{A}_u - \mathcal{A}_v.$$

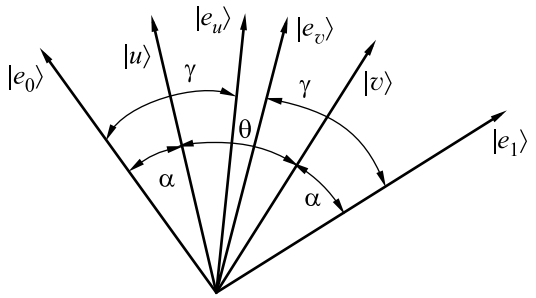

Рис.1

Пространство результатов на приемном конце состоит из трех событий: 0, 1, ?, вероятности которых на входных состояниях $|u\rangle$, $|v\rangle$ равны

$$\mathrm{Tr}_B\{|u\rangle\langle u|\mathcal{A}_v\} = \mathrm{Tr}_B\{|v\rangle\langle v|\mathcal{A}_u\} = 0,$$
$$\mathrm{Tr}_B\{|u\rangle\langle u|\mathcal{A}_u\} = \mathrm{Tr}_B\{|v\rangle\langle v|\mathcal{A}_v\} = 1-\cos(\theta), \quad (3)$$
$$\mathrm{Tr}_B\{|u\rangle\langle u|\mathcal{A}_?\} = \mathrm{Tr}_B\{|v\rangle\langle v|\mathcal{A}_?\} = \cos(\theta).$$

Индекс B означает взятие следа по пространству состояний на приемном конце[1)]. Исходы 0 и 1 являются исходами с определенным результатом (conclusive). То есть срабатывание в канале $\mathcal{A}_u$ может быть лишь на состоянии $|u\rangle$ и никогда на входном состоянии $|v\rangle$, и наоборот. Отсчеты в канале $\mathcal{A}_?$ являются исходами с неопределенным результатом (inconclusive), поскольку могут иметь место как на входном состоянии $|u\rangle$, так и на состоянии $|v\rangle$.

В дальнейшем действия легитимных пользователей сводятся к следующему. Alice равновероятно посылает к Bob состояния $|u\rangle$ и $|v\rangle$, Bob производит измерения (2). После передачи достаточно длинной последовательности Bob через открытый классический канал сообщает, в каких посылках у него были результаты измерений с неопределенным исходом. Эти посылки отбрасываются. Далее сообщается примерно половина случайно выбранных битов и оценивается вероятность ошибки Q. Данные раскрытые позиции затем отбрасываются. При длинной последовательности в нераскрытой части последовательности вероятность ошибки совпадает с Q. Если $Q < Q_c$, пользователи исправляют ошибки и извлекают секретный ключ.

Действия Eve сводятся к следующему. В каждой посылке Eve готовит свое вспомогательное состояние $|e\rangle$, которое взаимодействует с передаваемым состоянием. Совместная эволюция описывается как (см. рис.1, [4])

$$|u\rangle\otimes|e\rangle \to U(|u\rangle\otimes|e\rangle) = \\ = a|u\rangle\otimes|e_u\rangle + b|v\rangle\otimes|e_v\rangle = |\phi_1\rangle, \quad (4)$$

$$|v\rangle\otimes|e\rangle \to U(|v\rangle\otimes|e\rangle) = \\ = b|u\rangle\otimes|e_u\rangle + a|v\rangle\otimes|e_v\rangle = |\phi_2\rangle; \quad (5)$$

здесь $|e_u\rangle$, $|e_v\rangle$ – состояния в пространстве, натянутом на $|u\rangle$ и $|v\rangle$, a и b – вещественные коэффициенты, которые могут выбираться подслушивателем (фактически определяются оператором совместной унитарной эволюции).

Eve сохраняет свои модифицированные состояния в квантовой памяти и не производит никаких измерений до тех пор, пока легитимные пользователи не завершат весь обмен информацией как по квантовому, так и классическому каналам.

Bob производит индивидуальные измерения над состояниями в каждой посылке. Состояния, которые "видит" Bob, даются взятием частичного следа по подпространству состояний Eve. Имеем для входного состояния $|u\rangle$:

$$\rho(|u\rangle) = \mathrm{Tr}_E\{|\phi_1\rangle\langle\phi_1|\} = \\ = a^2|u\rangle\langle u| + ab\sin(2\gamma)(|u\rangle\langle v| + |v\rangle\langle u|) + b^2|v\rangle\langle v|, \quad (6)$$

и, соответственно, для входного состояния $|v\rangle$:

$$\rho(|v\rangle) = \mathrm{Tr}_E\{|\phi_2\rangle\langle\phi_2|\} = \\ = b^2|u\rangle\langle u| + ab\sin(2\gamma)(|u\rangle\langle v| + |v\rangle\langle u|) + a^2|v\rangle\langle v|. \quad (7)$$

Для вероятностей исходов на приемном конце с учетом (4)–(7) получаем (правый символ отвечает посланному состоянию, а левый – интерпретации результата измерений)

$$\Pr\{0|0\} = \mathrm{Tr}_B\{\mathcal{A}_u\rho(|u\rangle)\} = a^2(1-\sin(2\alpha)), \quad (8)$$

$$\Pr\{1|0\} = \mathrm{Tr}_B\{\mathcal{A}_v\rho(|u\rangle)\} = b^2(1-\sin(2\alpha)), \quad (9)$$

$$\Pr\{?|0\} = \mathrm{Tr}_B\{\mathcal{A}_?\rho(|u\rangle)\} = 1-(a^2+b^2)(1-\sin(2\alpha)), \quad (10)$$

и аналогично для остальных переходных вероятностей

$$\Pr\{1|1\} = \Pr\{0|0\}, \quad \Pr\{0|1\} = \Pr\{1|0\}, \\ \Pr\{?|1\} = \Pr\{?|0\}. \quad (11)$$

[1)] Для краткости, как это обычно делается, будем обозначать передающий узел и принимающий, соответственно, Alice и Bob, а подслушивателя – Eve (Eavesdropper).

Легитимные пользователи отбрасывают посылки, где были зафиксированы inconclusive исходы. Вероятности правильно интерпретируемых ($\Pr\{1|1\}, \Pr\{0|0\}$) и ошибочно интерпретируемых ($\Pr\{0|1\}, \Pr\{1|0\}$) исходов соответственно равны

$$Q_{OK} = \frac{a^2}{a^2+b^2}, \tag{12}$$

$$Q = \frac{b^2}{a^2+b^2}. \tag{13}$$

Eve также выбрасывает из квантовой памяти состояния в тех позициях, где Bob получил inconclusive исход.

Далее Alice и Bob случайной выборкой раскрывают примерно половину своих битовых последовательностей и оценивают вероятность ошибки Q. В результате у Eve остаются состояния только в тех позициях, в которых Bob получил conclusive исход. Состояния в этих позициях, которые "видит" Eve после измерений Bob, даются следующими матрицами плотности (ненормированными):

$$\rho_E^{OK}(|u\rangle) = \mathrm{Tr}_B\{\sqrt{\mathcal{A}_u}|\phi_1\rangle\langle\phi_1\sqrt{\mathcal{A}_u}\} = (1-Q)|e_u\rangle\langle e_u|, \tag{14}$$

поскольку операторы $\mathcal{A}_u$ и $\mathcal{A}_v$ с точностью до нормировки являются ортогональными проекторами. Формула (14) означает, что в ячейке квантовой памяти у Eve находится состояние $|u\rangle$, а у Bob измерение дало правильный исход, который соответствует входному состоянию $|u\rangle$, посланному Alice. Соответственно, в ячейке памяти у Eve будет находиться состояние

$$\rho_E^{Q}(|u\rangle) = \mathrm{Tr}_B\{\sqrt{\mathcal{A}_v}|\phi_1\rangle\langle\phi_1|\sqrt{\mathcal{A}_v}\} = Q|e_v\rangle\langle e_v|, \tag{15}$$

если исход измерения у Bob на входном состоянии $|u\rangle$ был с ошибкой. Аналогично имеем для входного состояния $|v\rangle$

$$\rho_E^{OK}(|v\rangle) = \mathrm{Tr}_B\{\sqrt{\mathcal{A}_v}|\phi_2\rangle\langle\phi_2|\sqrt{\mathcal{A}_v}\} = (1-Q)|e_v\rangle\langle e_v|, \tag{16}$$

$$\rho_E^{Q}(|v\rangle) = \mathrm{Tr}_B\{\sqrt{\mathcal{A}_u}|\phi_2\rangle\langle\phi_2|\sqrt{\mathcal{A}_u}\} = Q|e_u\rangle\langle e_u|. \tag{17}$$

Имеется соответствие один в один между правильными и ошибочными позициями у Bob и у Eve, в том смысле, что в той позиции, где измерения у Bob дали conclusive исход и были правильно интерпретированы, например, Alice послано состояние $|u\rangle$, и Bob интерпретировал его как 0, то у Eve в соответствующей позиции будет состояние $\rho_E^{OK}(|u\rangle)$. В той позиции у Bob, где был conclusive исход, но состояние интерпретировано ошибочно (послано Alice $|u\rangle$, а Bob интерпретировал его как 1), у Eve в этой позиции будет неправильное состояние, отвечающее $1-\rho_E^{Q}(|u\rangle)$, а не 0. Аналогично для посланного состояния $|v\rangle$.

Разумеется, положения ошибочных позиций неизвестны Bob и Eve. Разница на этот момент между Bob и Eve состоит в том, что у Bob информация в оставленных позициях представлена в классическом виде (битов 0 и 1), а у Eve в виде квантовых состояний, отвечающих классическим битам у Bob. Eve будет пытаться определить секретный ключ, используя квантовомеханические измерения, и решающие правила, в результате применения которых ее уже классическая битовая последовательность будет наиболее близка к ключевой последовательности у Alice и Bob.

Фактически, Eve имеет лишь чистые состояния $|u\rangle$ или $|v\rangle$ в каждой ячейке квантовой памяти, которые находятся с вероятностью $1/2$.

К данному моменту легитимные пользователи имеют классические битовые строки, а Eve – регистр квантовой памяти с состояниями. Далее будем рассуждать, используя случайные кодовые слова, как известно [11,12], именно на таких случайных кодах достигается шенноновский предел. Поскольку Alice и Bob находятся в ситуации классического симметричного бинарного канала с вероятностью ошибки Q, то они могут через открытый канал сгенерировать набор случайных кодовых слов, состоящий из M кодовых слов, таких, которые бы при декодировании позволяли с вероятностью единица исправить ошибки. Формально эта процедура сводится к тому, что Alice считает нераскрытую часть длиной n посланной ей битовой строки первым кодовым словом, случайным образом генерирует еще $M-1$ кодовых слов длиной n и открыто сообщает все M кодовых слов Bob.

Обозначим такой набор кодовых слов как $w^1, w^2, \ldots w^M$, каждое кодовое слово представляет собой бинарную строку длиной n, $w^i = \{i_1, i_2, \ldots i_n\}$, $i_k = 0, 1$. Избыточность кода (при случайных кодовых словах фактически число кодовых слов) должна быть такова, чтобы он исправлял ошибки, встречающиеся с частотой Q, с вероятностью единица. Это возможно, если число кодовых слов не превосходит [11,12]

$$M < 2^{n[H(Q)-\delta]},$$

$$I_{AB}(Q) = H(Q) = 1 + Q\log(Q) + (1-Q)\log(1-Q), \tag{18}$$

где $H(Q)$ – пропускная способность бинарного симметричного канала. Вероятность ошибки по всем кодовым словам не превосходит [12]

$$p_{AB}(n,M) \le 2\varepsilon + (M-1)2^{n[H(Q)-\delta]} \to 0 \qquad (19)$$

при условии (18).

Цель Eve "привязаться" к классическим кодовым словам, открыто анонсированным Alice. Затем по классическим кодовым словам построить решающие правила для квантовомеханических измерений, чтобы с максимальной вероятностью получить правильное кодовое слово, которое отвечает ключу. Каждому классическому кодовому слову у Alice и Bob, $w^i = \{i_1, i_2, \dots i_n\}$, Eve сопоставляет $|\psi_{w^i}\rangle = |e_{i_1}\rangle \otimes |e_{i_2}\rangle \dots \otimes |e_{i_n}\rangle$, где $|e_{i_k}\rangle = |e_u\rangle$ при $i_k = 0$ и $|e_{i_k}\rangle = |e_v\rangle$ при $i_k = 1$. Фактически, для каждого классического кодового слова каждой позиции слова 0 или 1 Eve сопоставляет квантовые состояния $|e_u\rangle$ или $|e_v\rangle$, которые неортогональны. Если бы состояния были ортогональны, то Eve могла бы их достоверно различить, то есть вписать в соответствующие позиции 0 или 1, и иметь такую же битовую строку, как и Bob. Однако из-за неортогональности состояний они достоверно неразличимы и при измерении Eve будет иметь дополнительную ошибку по сравнению с Bob. Eve может осуществлять индивидуальные измерения [13] состояний в каждой позиции и интерпретировать результат как 0 или 1. Ошибка будет меньше, если Eve будет делать коллективные измерения [14], используя описанные ниже измеряющие операторы.

Поскольку кодовые слова выбираются случайно и независимо друг от друга, вероятность появления отдельного кодового слова (см. детали в [14])

$$\Pr\{w = (i_1, i_2, \dots i_n)\} = p_{i_1} \cdot p_{i_2} \cdot \dots p_{i_n} = \frac{1}{2^n},$$

$$p_{i_k} = \frac{1}{2}, \qquad (20)$$

то математическое ожидание $\rho_{w^i} = |\psi_{w^i}\rangle\langle\psi_{w^i}|$

$$\mathbf{E}(\rho_{w^i}) = \sum_{i_1,i_2,\dots i_n} p_{i_1} \cdot p_{i_2} \dots p_{i_n} |e_{i_1}\rangle\langle e_{i_1}| \otimes \dots \otimes |e_{i_n}\rangle\langle e_{i_n}| = \rho_E^{\otimes n}, \qquad (21)$$

где

$$\rho_E = \frac{1}{2}|e_u\rangle\langle e_u| + \frac{1}{2}|e_v\rangle\langle e_v| \qquad (22)$$

– матрица плотности, описывающая состояния квантовой памяти.

Далее Eve использует декодирование квантовых кодовых слов (по сути осуществляет их перевод в классические битовые строки), используя решающее правило, которое задается измеряющими операторами:

$$\mathcal{X}_k = |\tilde{\psi}_{w^k}\rangle\langle\tilde{\psi}_{w^k}|, \quad |\tilde{\psi}_{w^k}\rangle = \mathcal{P}|\psi_{w^k}\rangle, \qquad (23)$$

где $\mathcal{P}$ – проектор на типичное подпространство матрицы плотности $\rho_E^{\otimes n}$:

$$\mathcal{P} = \sum_{J\in B} |\lambda_J\rangle\langle\lambda_J|, \quad |\lambda_J\rangle = |\lambda_{j_1}\rangle \otimes |\lambda_{j_2}\rangle \dots \otimes |\lambda_{j_n}\rangle, \qquad (24)$$

$|\lambda_{j_k}\rangle$ – собственные векторы ρ_E, и $\lambda_J = \lambda_{j_1} \cdot \lambda_{j_2} \dots \lambda_{j_n}$ – собственные числа ρ_E. Типичное подпространство матрицы плотности определено как

$$B = \{J : 2^{-n[H(\rho_E)+\delta]} < \lambda_J < 2^{-n[H(\rho_E)-\delta]}\}, \qquad (25)$$

для которого выполнены условия (см. [14])

$$\|\rho_E^{\otimes n}\mathcal{P}\| < 2^{-n[H(\rho_E)-\delta]}, \quad \mathrm{Tr}\{\rho_E^{\otimes n}(1-\mathcal{P}\} < \varepsilon. \qquad (26)$$

Величина $H(\rho_E)$ является энтропией фон Неймана, и в нашем случае по сути совпадает с классической пропускной способностью бинарного квантового канала связи [14]:

$$\overline{C}(\rho_E) = H(\rho_E) = -\mathrm{Tr}\{\rho_E \log \rho_E\} = -\lambda_1 \log\lambda_1 - \lambda_2 \log\lambda_2 =$$

$$= -\left(\frac{1-\sin(2\gamma)}{2}\right)\log\left(\frac{1-\sin(2\gamma)}{2}\right) - \left(\frac{1+\sin(2\gamma)}{2}\right)\log\left(\frac{1+\sin(2\gamma)}{2}\right), \qquad (27)$$

где $\lambda_{1,2} = (1 \pm \sin(2\gamma))/2$ – собственные числа ρ_E.

Ошибка Eve при декодировании M кодовых слов, сгенерированных Alice, есть [14]

$$p_E(n,M) \le 2\mathrm{Tr}\{\rho^{\otimes n}(1-\mathcal{P})\} + (M-1)\mathrm{Tr}\{(\rho^{\otimes n}\mathcal{P})^2\} \le 2\varepsilon + (M-1)2^{[H(\rho_E)-\delta]}, \qquad (28)$$

а ошибка при декодировании легитимными пользователями есть [12]

$$p_{AB}(n,M) \le 2\varepsilon + (M-1)2^{n[H(Q)-\delta]}. \qquad (29)$$

Таким образом, если

$$H(Q) > H(\rho_E) = \overline{C}(\rho_E), \qquad (30)$$

и легитимные пользователи выбирают число кодовых слов $M < 2^{n[H(Q)-\delta]}$, то их ошибка при декодировании экспоненциально по n стремится к нулю, а ошибка Eve имеет конечную величину (стремится к единице). Другими словами, при условии (18) Alice и Bob имеют после декодирования одинаковую (с вероятностью единица) строку бит – секретный ключ, а Eve с вероятностью единица не знает данную строку.

Величина $\overline{C}(\rho_E)$ является *классической пропускной способностью бинарного квантового канала связи* [13,14]. Если бы Eve делала оптимальные, в смысле минимальности ошибки различения пары неортогональных состояний, индивидуальные измерения, то вместо $\overline{C}(\rho_E)$ фигурировала бы *классическая пропускная способность бинарного квантового канала связи за один шаг (one shot)* [14], равная

$$C_1(\rho_E) = \frac{1}{2}\Big[(1+\sqrt{1-\sin^2(2\gamma)})] \times \\ \times \log(1+\sqrt{1-\sin^2(2\gamma)}) + \\ + (1-\sqrt{1-\sin^2(2\gamma)})]\log(1-\sqrt{1-\sin^2(2\gamma)})\Big], \quad (31)$$

которая никогда не превосходит (27), $C_1(\rho_E) < \overline{C}(\rho_E)$.

Передача секретного ключа возможна, если при данной величине ошибки Q у легитимных пользователей величина пропускной способности классического бинарного симметричного канала между Alice и Bob превышает величину классической пропускной способности бинарного квантового канала для Eve. Для окончательного ответа оставалось связать величину $\overline{C}(\rho_E)$ (фактически $\sin(2\gamma)$) с параметрами a, b, Q и $\sin(2\alpha)$ – углом между сигнальными состояниями, выбираемыми легитимными пользователями.

Получим эту связь. Условия унитарности и нормировки состояний $|\phi_{1,2}\rangle$ в (4), (5) приводят к условиям

$$\sin(2\alpha) = 2ab + (a^2+b^2)\sin(2\alpha)\sin(2\gamma), \\ a^2+b^2+2ab\sin(2\alpha)\sin(2\gamma) = 1. \quad (32)$$

Для $\sin(2\gamma)$ получаем

$$\sin(2\gamma) = \frac{\sqrt{1-(1-2Q)^2}-\sin(2\alpha)}{\sin(2\alpha)[\sqrt{1-(1-2Q)^2}\sin(2\alpha)-1]}. \quad (33)$$

Перейдем к обсуждению результатов. Как известно [15,16], передача секретного ключа возможна, если выполнено условие

$$C_s \geq \max I_{AB} - I_{AE}, I_{AB} - I_{BE} > 0, \quad (34)$$

где C_s – секретная пропускная способность канала между Alice и Bob в присутствии подслушивателя (количество бит секретного ключа на одну посылку, которое могут передать легитимные пользователи в пределе длинной последовательности). I_{AB}, I_{AE}, I_{BE} – максимальная величина (при атаке Eve и выбранных сигнальных состояниях и измерениях на приемном конце) взаимной информации между легитимными пользователями Alice и Bob, между Alice и Eve, и между Bob и Eve, соответственно. При индивидуальных измерениях Eve (см. ниже) величина $I_{AE} \leq I_{BE}$, поэтому условие (34) сводится к

$$C_s \geq I_{AB} - I_{AE} > 0. \quad (35)$$

Величины I_{AE} и I_{BE} определяются величиной ошибки Q_{AE} и Q_{BE} в каналах Alice-Eve и Bob-Eve, соответственно. Имеем с учетом (6)–(13) (см. подробности в [4,5])

$$Q_{AE} = Q\cos^2\gamma + (1-Q)\sin^2\gamma, \quad Q_{BE} = \sin^2\gamma \quad (36)$$

и

$$I_{AE} = 1 + Q_{AE}\log Q_{AE} + (1-Q_{AE})\log(1-Q_{AE}), \\ I_{BE} = 1 + Q_{BE}\log Q_{BE} + (1-Q_{BE})\log(1-Q_{BE}). \quad (37)$$

Обратим внимание на то, что при коллективной атаке есть только одна взаимная информация между Eve и обоими легитимными пользователями, то есть формально $I_{AE} = I_{BE} = \overline{C}(\rho_E)$. В этом случае условие (34) сводится к

$$C_s \geq I_{AB} - \overline{C}(\rho_E) > 0, \quad I_{AB} \geq \overline{C}(\rho_E). \quad (38)$$

На рис.2 приведены графики величин (левая половина) I_{AB}, I_{AE}, I_{BE} для прозрачного индивидуального подслушивания и $\overline{C}(\rho_E)$ для коллективной атаки, соответственно, как функции ошибки Q, производимой Eve в канале между легитимными пользователями. Значения угла перекрытия между сигнальными состояниями $|u\rangle$: и $|v\rangle$ (a) – $\alpha = \pi/16$, (b) – $\alpha = \pi/8$, (c) – $\alpha = \pi/5$. Видно, что при коллективной атаке на ключ критическая величина ошибки, до которой гарантируется распространение секретного ключа, примерно вдвое меньше, чем при индивидуальных измерениях Eve, то есть коллективная атака является существенно более эффективной для Eve. На правой половине рис.2 приведены значения секретной пропускной способности (38), умноженной на долю conclusive исходов. При малых углах перекрытия между сигнальными состояниями (большей

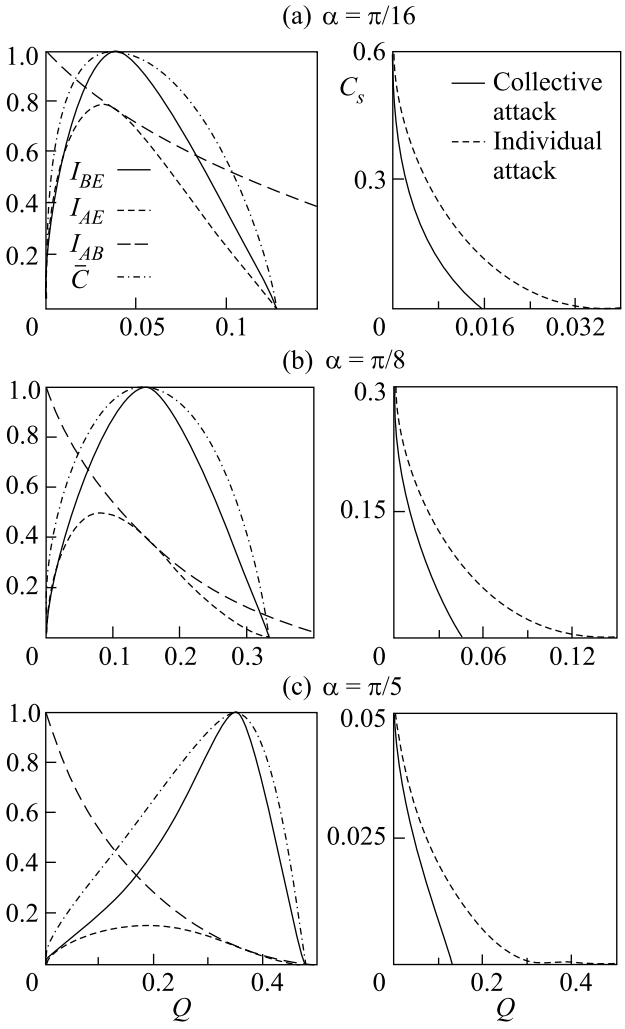

Рис.2

различимости неортогональных состояний) величина секретной пропускной способности, например, для $\alpha = \pi/16$, достаточно велика (Q мало, $C_s \sim 0.6$, примерно каждый второй бит из исходной последовательности является секретным), однако величина критической ошибки не более 1.5 %. При больших углах перекрытия, когда неортогональные состояния более неразличимы, например, $\alpha = \pi/5$, величина критической ошибки $\approx$ 11 %, однако при этом секретная пропускная способность крайне мала. Секретными являются лишь 5 % бит из исходной переданной последовательности.

Работа поддержана Академией криптографии РФ, Российским фондом фундаментальных исследований (проект # 02-02-16289), а также междисциплинарным проектом МГУ.

1. S. Wiesner, SIGACT News **15**, 78 (1983).
2. C. H. Bennett and G. Brassard, *Proc.of IEEE Int. Conf. on Comput. Sys. and Sign. Proces.*, Bangalore, India, December 1984, p.175; C. H. Bennett, Phys. Rev. Lett. **68**, 3121 (1992).
3. W. K. Wootters and W. H. Zurek, Nature **299**, 802 (1982).
4. A. K. Ekert, B. Huttner, G. M. Palma, and A. Peres, Phys. Rev. **A50**, 1047 (1994).
5. H. E. Brandt, J. M. Myer, and S. J. Lomonaco Jr., Phys. Rev. **A56**, 4456 (1997).
6. B. A. Slutsky, R. Rao, Pang-Chen Sun, and Y. Fainman, Phys. Rev., **A57**, 2383 (1998).
7. K. Tamaki, M. Koashi, and N. Imoto, quant-ph/0212161.
8. K. Tamaki, M. Koashi, and N. Imoto, quant-ph/0212162.
9. K. Tamaki and N. Lutkenhaus, quant-ph/0308048.
10. E. Biham and T. Mor, Phys. Rev. Lett. **78**, 2256 (1997); **79**, 4034 (1997).
11. C. E. Shannon, Bell Syst. Tech. Jour. **27**, 397; 623 (1948).
12. Р. Галлагер, *Теория информации и надежная связь*, М.: Советское радио, 1974.
13. А. С. Холево, *Введение в квантовую теорию информации*, серия *Современная математическая физика*, вып.5, М.: МЦНМО, 2002.
14. А. С. Холево, Проблемы передачи информации **8**, 63 (1972); **15**, 3 (1979); Успехи математических наук **53**, 193 (1998).
15. I. Csiszár and J. Körner, IEEE Trns. Inf. Theory **24**, 339 (1978).
16. D. Maurer, IEEE Trns. Inf. Theory, **39**, 733 (1993).