Письма в ЖЭТФ, том 90, вып. 7, с. 597 – 603 © 2009 г. 10 октября

Об одном асимптотическом свойстве квантовой криптографии на временны́х сдвигах

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, Москва, Россия

Поступила в редакцию 22 июня 2009 г.

После переработки 7 августа 2009 г.

Один из основных результатов классической теории информации состоит в том, что безошибочная передача информации возможна даже через неидеальный бинарный канал связи с шумом вплоть до величины ошибки $Q_c = \frac{1}{2}$. Существует фундаментальный и практически важный вопрос о том, могут ли ограничения квантовой механики обеспечить не только безошибочную передачу классической информации при помощи квантовых состояний, но еще и гарантировать секретность передаваемых ключей вплоть до теоретического предела по ошибке Q_c. Показано, что секретная передача ключей принципиально возможна вплоть до значения ошибки Q_c в асимптотическом пределе большого числа базисов.

PACS: 03.65.Hk, 03.67.Dd

Квантовая информатика находится на пересечении двух наиболее значительных теорий прошлого века – квантовой механики и теории информации. Классическая теория информации занимается обработкой и передачей информации при помощи объектов (сигналов), описывающихся законами классической физики. Одним из наиболее практически важных и повседневно используемых достижений классической теории информации является тот факт, что информацию можно передавать без искажений через неидеальные каналы связи [1]. Внесение некоторой избыточности в исходную информацию, которая зависит от степени искажений в канале связи, позволяет корректировать возникающие ошибки и передавать исходную информацию без ошибок. Без коррекции ошибок ни один вид современных телекоммуникаций, от интернета до спутниковой связи, был бы невозможен.

В квантовой теории информации передача информации осуществляется посредством квантовых состояний. Оказалось, что в квантовом случае, несмотря на бóльшую "хрупкость" квантовых состояний по сравнению с классическими сигналами, также возможна передача квантовых объектов как таковых без искажений через неидеальные каналы связи с помощью квантовых кодов, корректирующих ошибки [2]. Кроме передачи квантовых состояний как таковых, возможна передача классической информации, "закодированной" в квантовые состояния. В этом случае символам классического алфавита на передающей стороне сопоставляются квантовые состояния. На приемной стороне извлечение "закодированной" в квантовые состояния информации производится путем квантово-механических измерений. Фундаментальные физические ограничения на измеримость квантовых состояний позволяют передавать конфиденциальную информацию по открытым и доступным для модификации квантовым каналам связи [3].

Для классического бинарного канала связи предельное возмущение (ошибка Q_c), до которой можно передавать информацию без потерь в асимптотическом пределе длинных последовательностей ($n \to \infty$), составляет $Q_c = \frac{1}{2}$ [1,4]. Для исправления ошибок при $Q < Q_c$ требуется использовать не менее $k/n \approx h(Q)$ $(h(Q) = -Q\log Q - (1-Q)\log(1-Q))$ контрольных символов, соответственно, доля полезных информационных символов составляет не более $(n-k)/n \approx (1-h(Q))$. Ошибки, естественно, имеют место и в контрольных символах, в которых они также исправляются. При $Q \to \frac{1}{2}$ вся последовательность из n бит расходуется на исправление ошибок, доля полезных информационных символов стремится к нулю, и информацию передавать невозможно. То есть ошибка $Q_c = \frac{1}{2}$ является теоретическим пределом.

Существует фундаментальный и практически важный вопрос о том, могут ли ограничения квантовой механики обеспечить не только безошибочную передачу классической информации при помощи

квантовых состояний, но еще и гарантировать секретность передаваемых ключей вплоть до теоретического предела по ошибке $Q_c = \frac{1}{2}$. На первый взгляд, такая ситуация кажется принципиально невозможной по следующим соображениям. В квантовой криптографии получение любого количества информации подслушивателем из передаваемых квантовых состояний неизбежно приводит к их возмущению и ошибке на приемной стороне [3, 5]. Ошибки исправляются через открытый канал связи, доступный для подслушивателя. Поэтому кроме информации, полученной при измерении квантовых состояний, подслушиватель получает дополнительно информацию при коррекции ошибок. Информация, выдаваемая через открытый канал связи, при коррекции ошибок при $Q \to \frac{1}{2}$ уже сама по себе стремится к n битам. Поэтому с учетом информации, полученной при измерении квантовых состояний, подслушиватель будет иметь полную информацию о переданном ключе уже при меньших значениях Q. *Все известные до настоящего времени системы квантовой криптографии существенно не дотягивают по критической ошибке до теоретического значения* $Q_c = \frac{1}{2}$ [6–14].

Ниже будет показано, что секретная передача ключей принципиально возможна вплоть до теоретического значения ошибки Q_c, что является основным результатом данной работы. Это связано с тем, что приведенные выше рассуждения неявно подразумевают, что извлечение информации из квантовых состояний подслушивателем приводит только к появлению ошибки Q. Если детектирование попыток подслушивания осуществляется еще по дополнительному параметру – отсчетам в контрольных временных окнах q, то в этом случае длина секретного ключа оказывается равной

$$r/n = 1 - h(Q) - h(q(N)), \tag{1}$$

где $q(N) \to 0$ при $N \to \infty$, соответственно, $h(q(N)) \to 0$ (N – число базисов, см. далее), и длина секретного ключа переходит в

$$r/n \to (1 - h(Q)), \tag{2}$$

что совпадает с пропускной способностью классического бинарного канала связи. Длина секретного ключа обращается в нуль при $Q = \frac{1}{2}$.

Любое квантовое распределение ключей состоит из следующих шагов.

Приготовление квантовых состояний. Алиса случайно и равновероятно выбирает базис b, а затем случайно и равновероятно символ классического алфавита x^b (как правило, бинарного) и сопоставляет ему квантовое состояние, которое направляется через квантовый канал связи на приемную сторону к Бобу:

$$\{b\} \to \{x^b, p_X^b(x)\} \to \{\sigma_A^{x,b} = |\varphi^{x,b}\rangle_{A\,A}\langle\varphi^{x,b}|\}. \tag{3}$$

Вторжение в квантовый канал связи подслушивателем. Наиболее общая атака подслушивателя (Евы) сводится к следующему [14, 15]. В каждой посылке Ева готовит свое вспомогательное квантовое состояние $|E\rangle_E$, которое описывает исходное состояние прибора Евы. Данное состояние Евы (прибор) на время приводится во взаимодействие с передаваемым состоянием. Совместная эволюция двух состояний описывается унитарным оператором U_{AE}. В результате совместной эволюции передаваемого Алисой состояния $|\varphi^{x,b}\rangle_A$ и вспомогательного состояния Евы $|E\rangle_E$ возникает совместное, вообще говоря, запутанное состояние $|\Psi^{x,b}\rangle_{AE}$. Затем подсистема A направляется к Бобу, модифицированная подсистема E остается в распоряжении Евы и используется в дальнейшем для измерений.

Для совместной матрицы плотности Алиса-Ева в каждой посылке имеем

$$\begin{gathered}\sigma_{AE}^{x,b} = |\Psi^{x,b}\rangle_{AE\;\;AE}\langle\Psi^{x,b}|,\\ |\Psi^{x,b}\rangle_{AE} = U_{AE}(|\varphi^{x,b}\rangle_A \otimes |E\rangle_E).\end{gathered} \tag{4}$$

Измерения на приемной стороне. После измерений на приемной стороне, которые, как правило производятся в ортогональном базисе $\{|y^b\rangle\}$ ($y^b = 0, 1$), совместная матрица плотности Боб-Ева переходит в новую, зависящую от исхода измерений. Любое преобразование матриц плотности в матрицы плотности описывается отображением (супероператором), которое сохраняет эрмитовость, след и является вполне положительным [2]. Применительно к нашему случаю, изменение совместной матрицы плотности после измерений дается супероператором

$$\begin{aligned}\sigma_{BE}^{x,y,b} &= \mathcal{T}_{YE\leftarrow BE}(\sigma_{BE}^{x,b}) = \mathcal{T}_{Y\leftarrow B} \otimes I_E(\sigma_{BE}^{x,b}) =\\ &= \sum_y \mathcal{P}^{y,b}(\sigma_{BE}^{x,b})\mathcal{P}^{y,b}, \quad \mathcal{P}^{y,b} = |y^b\rangle_{BB}\langle y^b|,\end{aligned} \tag{5}$$

где I_E – единичный оператор, отражающий тот факт, что Ева не производит никаких действий. Все ее измерения производятся в самом конце протокола. С учетом (4), (5) имеем

$$\sigma_{BE}^{x,y,b} = \sum_y |y^b\rangle_{BB}\langle y^b|\Psi^{x,b}\rangle_{BE\;\;BE}\langle\Psi^{x,b}|y^b\rangle_{BB}\langle y^b|. \tag{6}$$

После измерений Алиса и Боб связаны классическим каналом связи с переходными вероятностями (после согласования базисов индекс b опускаем)

$$\{x, p_X(x)\} \to \{y, p_{X|Y}(x|y)\},$$
$$p_{X|Y}(x|y) = \mathrm{Tr}_E\{{}_B\langle y|\Psi^{x,b}\rangle_{BEBE}\langle\Psi^{x,b}|y\rangle_B\}, \tag{7}$$

а Алиса-Ева – классически квантовым каналом связи

$$\{x, p_X(x)\} \to \{\sigma_E^x, p_X(x)\},$$
$$\sigma_E^x = \sum_y {}_B\langle y|\Psi^{x,b}\rangle_{BEBE}\langle\Psi^{x,b}|y\rangle_B. \tag{8}$$

Вероятность ошибки для канала Алиса-Боб определяется как

$$Q = \sum_{x\neq y=0,1} p_X(x)p_{X|Y}(x|y). \tag{9}$$

Предельная длина секретного ключа, которая может быть получена из последовательности длины n после усиления секретности (privacy amplification [16] – сжатия при помощи универсальных хзш-функций второго порядка [17]), не превосходит (см.,например, [14])

$$r/n = \min_{\sigma_{BE}\in\Gamma(Q)}(C_{1,1}(\sigma_B) - C_{1,\infty}(\sigma_E)),$$
$$\sigma_{BE} = \sum_{x,y} p_X(x)\sigma_{BE}^{x,y}, \tag{10}$$

где минимум берется по всем совместным матрицам плотности Боб-Ева, которые дают наблюдаемую ошибку Q на приемной стороне. Матрица плотности, описывающая общее состояние Боба и Евы есть σ_{BE}. Поскольку Боб и Ева имеют доступ только к своим квантовым подсистемам, то состояния этих квантовых подсистем, как обычно, даются частными матрицами плотности $\sigma_B = \mathrm{Tr}_E\{\sigma_{BE}\}$ и $\sigma_E = \mathrm{Tr}_B\{\sigma_{BE}\}$, которые получаются из общей матрицы плотности σ_{BE} взятием частичного следа по пространству состояний Боба и Евы, соответственно.

Максимум классической информации, которая может быть получена из квантового канала связи, определяется классическими пропускными способностями квантового канала. В отличие от классического канала связи, без памяти для квантового канала связи существует бесконечный набор классических пропускных способностей квантового канала связи [18–20]. Это связано с тем, что количество классической информации, которое может быть извлечено из ансамбля квантовых состояний, зависит от измерений на приемной стороне. Пропускные способности обычно обозначаются как $C_{1,k}$ $(k = 1, ..\infty)$. Первый индекс 1 означает, что состояния в каждой посылке посылаются независимо от других посылок.

Возможны индивидуальные измерения над каждым отдельным состоянием в каждой отдельной посылке. Такие оптимальные измерения (оптимальные в смысле минимизации ошибки различения отдельных квантовых состояний) приводят к пропускной способности $C_{1,1}$. Если используются измерения, которые минимизируют ошибку различения квантовых состояний в паре посылок, то из ансамбля квантовых состояний можно извлечь $C_{1,2}$ бит информации, и т.д. Имеет место $C_{1,1} < C_{1,2}, ... < C_{1,\infty}$ [18–20]. Оказывается, что максимум классической информации может быть получен, если использовать измерения, которые минимизируют ошибку различения целых последовательностей из n состояний. Для достижении этой величины необходимо иметь квантовую память. При $n \to \infty$ это приводит к так называемой классической пропускной способности квантового канала связи $C_{1,\infty}$ [20, 21].

Из (10) видно, что для достижения теоретического предела по ошибке требуется эффективное обращение в нуль второго слагаемого в (10) $\min_{\sigma_{BE}\in\Gamma(Q)}(C_{1,\infty}(\sigma_E)) \to 0$ по некоторому параметру протокола независящему от ошибки Q. Таким параметром является отношение числа отсчетов в контрольных временны́х окнах к отсчетам в информационных временны́х окнах.

Переходим к формулировке протокола квантового распределения ключей, обладающего таким свойством.

Информационные состояния представляют собой суперпозицию двух локализованных во временны́х окнах состояний (рис.1)

$$|0_i^b\rangle_B = \frac{1}{\sqrt{2}}(|i\rangle_B + \overline{b}|i+1\rangle_B),$$
$$|1_i^b\rangle_B = \frac{1}{\sqrt{2}}(|i\rangle_B - \overline{b}|i+1\rangle_B); \tag{11}$$

здесь индекс b – i-го временно́го базиса, который принимает значения $b = +, \overline{b} = 1$, $b = \times, \overline{b} = i$. В каждом временно́м базисе i (рис.1) имеется еще два внутренних базиса, состояния внутри каждого базиса $b = +$ и $b = \times$ попарно ортогональны, а между базисами – попарно неортогональны. Все состояния из соседних временны́х базисов с i и $i \pm 1$ также попарно неортогональны (рис.1) за счет перекрытия в общем временно́м окне. Число временны́х базисов обозначим как N.

Атака Евы полностью описывается заданием унитарного оператора U_{BE} [14]. Цель Евы состоит в том, чтобы сконструировать такой U_{BE}, чтобы в конце протокола получить максимум информации при

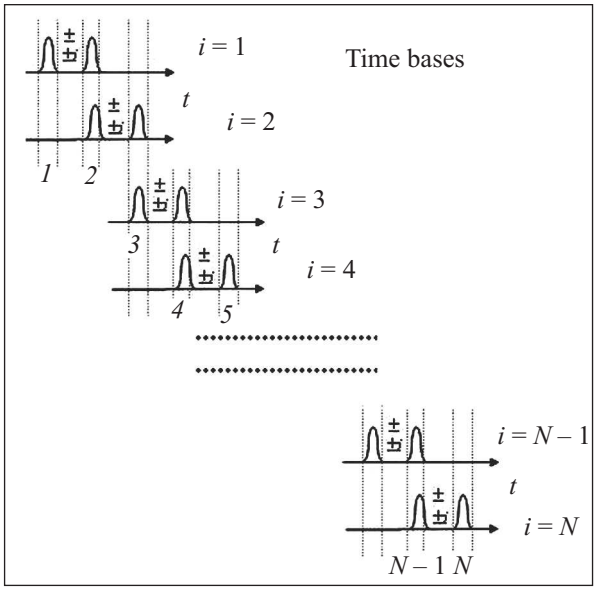

Рис.1. Структура информационных состояний

наблюдаемых контрольных параметрах на приемной стороне Боба.

Имеем

$$|\tilde{i}\rangle_{BE} = U_{BE}(|i\rangle_B \otimes |E\rangle_E) = \sum_{j=1}^{N} |j\rangle_B \otimes |\phi_i^j\rangle_E. \quad (12)$$

Выражение (12) представляет собой разложение вектора запутанного состояния по ортогональным базисным векторам в $\mathcal{H}_B \otimes \mathcal{H}_E$. Базисные векторы $|\phi_i^j\rangle_E$ ортогональны между собой при фиксированном i ${}_E\langle\phi_i^j|\phi_i^k\rangle_E = |\phi_i^j|^2\delta_{j,k}$. Условие сохранения нормировки требует, чтобы $\sum_j {}_E\langle\phi_i^j|\phi_i^j\rangle_E = 1$ при $\forall i$. При различных i векторы $|\phi_i^j\rangle_E$, вообще говоря, не обязаны быть попарно ортогональными, выяснением этого займемся ниже.

Для возмущенных Евой информационных состояний, с учетом (11), (12), получаем (далее для экономии места индекс базиса, пока он не потребуется, опускаем)

$$|\Psi_0^i\rangle_{BE} = |0^i\rangle_B \otimes |\Phi^{i+}\rangle_E + |1^i\rangle_B \otimes |\Theta^{i+}\rangle_E + \sum_{j\neq i,i+1}^{N} |j\rangle_B \otimes |\phi_i^{j+}\rangle_E, \quad (13)$$

$$|\Psi_1^i\rangle_{BE} = |0^i\rangle_B \otimes |\Theta^{i-}\rangle_E + |1^i\rangle_B \otimes |\Phi^{i-}\rangle_E + \sum_{j\neq i,i+1}^{N} |j\rangle_B \otimes |\phi_i^{j-}\rangle_E, \quad (14)$$

$$|\Phi^{i\pm}\rangle_E = \frac{1}{2}\left(|\phi_i^i\rangle \pm |\phi_{i+1}^{i+1}\rangle_E \pm (|\phi_{i+1}^i\rangle + |\phi_i^{i+1}\rangle_E)\right),$$

$$|\Theta^{i\pm}\rangle_E = \frac{1}{2}\left(|\phi_i^i\rangle - |\phi_{i+1}^{i+1}\rangle_E \pm (|\phi_{i+1}^i\rangle - |\phi_i^{i+1}\rangle_E)\right), \quad (15)$$

$$|\phi^{i\pm}\rangle_E = \frac{1}{\sqrt{2}}\left(|\phi_i^j\rangle \pm |\phi_{i+1}^j\rangle_E\right). \quad (16)$$

Выражения (13), (14) относятся к состояниям в базисе $+, i$, для других базисов состояния получаются аналогично. Боб осуществляет измерения в случайно выбранном базисе – временном базисе. Измерение при выбранном временном базисе (индексе i) дается разложением единицы:

$$I_B = |0^i\rangle_{BB}\langle 0^i| + |1^i\rangle_{BB}\langle 1^i| + \sum_{j\neq i,i+1}^{N} |j\rangle_{BB}\langle j|. \quad (17)$$

Такое измерение при совпадающих базисах Алисы и Боба для *возмущенных* состояний даст отсчеты как в информационных временны́х окнах (первые два слагаемых), так и в контрольных окнах. В контрольных временны́х никогда не будет отсчетов на невозмущенных состояниях[1)].

Оптоволоконная реализация, поясняющая работу квантового протокола распределения ключей, приведена на рис.2.

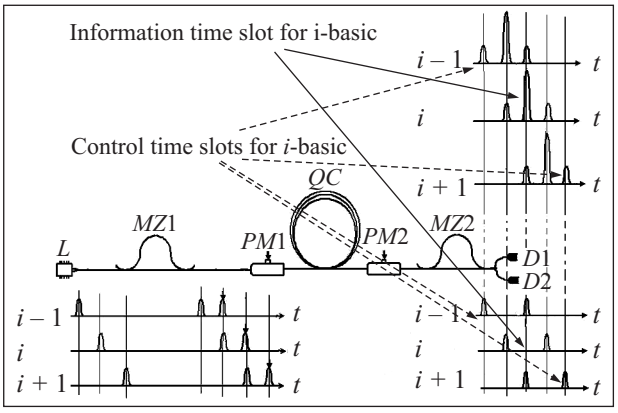

Рис.2. Оптоволоконная реализация: L – лазер, $MZ1$, $MZ2$ — разбалансированные (с разной оптической длиной плеч) и идентичные оптоволоконные интерферометры Маха-Цандера, $PM1$, $PM2$ – фазовые модуляторы, QC – оптоволоконный квантовый канал связи. Показано приготовление информационных квантовых состояний в трех соседних базисах с номерами $i-1$, i, $i+1$.

[1)] Детали экспериментальной реализации измерений в оптоволоконном варианте см. в [22].

Совместная матрица плотности Боб-Ева нормированная на число отсчетов в информационных временны́х окнах, с учетом (14)–(17) принимает вид

$$\tilde{\sigma}_{BE}^{i,\,0,1} = (\mathcal{P}_B^i \otimes I_E)|\Psi_{0,1}^i\rangle_{BE\ BE}\langle\Psi_{0,1}^i|(\mathcal{P}_B^i \otimes I_E) = \\ = |\tilde{\Psi}_{0,1}^i\rangle_{BE\ BE}\langle\tilde{\Psi}_{0,1}^i|, \tag{18}$$

$$|\tilde{\Psi}_0^i\rangle_{BE} = |0^i\rangle_B \otimes |\Phi^{i+}\rangle_E + |1^i\rangle_B \otimes |\Theta^{i+}\rangle_E, \\ |\tilde{\Psi}_1^i\rangle_{BE} = |0^i\rangle_B \otimes |\Theta^{i-}\rangle_E + |1^i\rangle_B \otimes |\Phi^{i-}\rangle_E, \tag{19}$$

$$\mathcal{P}_B^i = I_B - \sum_{j\neq i,i+1}^{N} |j\rangle_{BB}\langle j| \tag{20}$$

Частичные матрицы плотности, к которым имеют доступ Боб и Ева, даются частичным следом. С учетом (18), (19) имеем

$$\overline{\sigma}_B^{i\ 0,1} = \frac{\mathrm{Tr}_E\{\tilde{\sigma}_{BE}^{i,\,0,1}\}}{\mathrm{Tr}_{BE}\{\tilde{\sigma}_{BE}^{i,\,0,1}\}}, \quad \overline{\sigma}_E^{i\ 0,1} = \frac{\mathrm{Tr}_B\{\tilde{\sigma}_{BE}^{i,\,0,1}\}}{\mathrm{Tr}_{BE}\{\tilde{\sigma}_{BE}^{i,\,0,1}\}}. \tag{21}$$

Таким образом, Боб и Ева имеют дело с квантовыми ансамблями $\{\frac{1}{2}, \overline{\sigma}_B^{i\ 0,1}\}$ и $\{\frac{1}{2}, \overline{\sigma}_E^{i\ 0,1}\}$, априорные вероятности посылки 0 и 1 Алисой равны $\frac{1}{2}$. Количество информации, которое может быть получено Бобом и Евой из доступных им квантовых ансамблей, может быть выражено через соответствующие пропускные способности. Канал Алиса – Боб – классический канал, при индивидуальных ортогональных измерениях в каждой посылке пропускная способность этого канала совпадает с одношаговой пропускной способностью, которая выражается через энтропию фон Неймана по формуле Холево [21]:

$$C_{1,1}(\overline{\sigma}_B^{i\ 0,1}) = S\left(\frac{\overline{\sigma}_B^{i\ 0} + \overline{\sigma}_B^{i\ 1}}{2}\right) - \frac{1}{2}\left(S\left(\overline{\sigma}_B^{i\ 0}\right) + S(\overline{\sigma}_B^{i\ 1})\right), \tag{22}$$

Максимум информации Евы совпадает с классической пропускной способностью квантового канала Алиса – Ева и дается аналогичной формулой

$$C_{1,\infty}(\overline{\sigma}_E^{i\ 0,1}) = S\left(\frac{\overline{\sigma}_E^{i\ 0} + \overline{\sigma}_E^{i\ 1}}{2}\right) - \frac{1}{2}\left(S(\overline{\sigma}_E^{i\ 0}) + S(\overline{\sigma}_E^{i\ 1})\right). \tag{23}$$

Причем данная пропускная способность достигается на коллективных измерениях Евы (см. [21]). Энтропия фон Неймана, по определению, $S(\sigma) = -\mathrm{Tr}\{\sigma\log\sigma\} = -\sum_k \lambda_k \log\lambda_k$ (λ_k – собственные числа матрицы плотности). Поскольку состояния (13), (14) чистые, то собственные числа частичных матриц плотности и энтропии фон Неймана совпадают: $S(\overline{\sigma}_E^{i\ 0}) = S(\overline{\sigma}_B^{i0})$. С учетом этого, выражение для длины ключа принимает вид

$$\frac{r}{n} = \min_{\overline{\sigma}_{BE}\in\Gamma(Q)} \left(S\left(\frac{\overline{\sigma}_B^{i\ 0} + \overline{\sigma}_B^{i\ 1}}{2}\right) - S\left(\frac{\overline{\sigma}_E^{i\ 0} + \overline{\sigma}_E^{i\ 1}}{2}\right)\right). \tag{24}$$

Для дальнейшего нужен явный вид матриц плотности. Займемся теперь детальным вычислением матриц плотности. После измерений (17) матрица плотности Боба принимает вид

$$\sigma_B^{i\ 0} = |0^i\rangle_{BB}\langle 0^i|_E\langle\Phi^{i+}|\Phi^{i+}\rangle_E + \\ + |1^i\rangle_{BB}\langle 1^i|_E\langle\Theta^{i+}|\Theta^{i+}\rangle_E + \\ + \sum_{j\neq i,i+1}^{N} |j\rangle_{BB}\langle j|_E\langle\phi_i^{j+}|\phi_i^{j+}\rangle_E, \tag{25}$$

$$\sigma_B^{i\ 1} = |0^i\rangle_{BB}\langle 0^i|_E\langle\Theta^{i-}|\Theta^{i-}\rangle_E + \\ + |1^i\rangle_{BB}\langle 1^i|_E\langle\Phi^{i-}|\Phi^{i-}\rangle_E + \\ + \sum_{j\neq i,i+1}^{N} |j\rangle_{BB}\langle j|_E\langle\phi_i^{j-}|\phi_i^{j-}\rangle_E. \tag{26}$$

С учетом (20), (25), (26) для матрицы плотности Боба в (21) имеем

$$\overline{\sigma}_B^i = \frac{1}{2}\left(\overline{\sigma}_B^{i\ 0} + \overline{\sigma}_B^{i\ 1}\right) = \frac{1}{2}\left(|0^i\rangle_{BB}\langle 0^i| + |1^i\rangle_{BB}\langle 1^i|\right). \tag{27}$$

Матрица плотности Евы (21), с учетом (20), (25), (26), имеет вид

$$\sigma_E^i = \frac{1}{2}\left(\sigma_E^{i\ 0} + \sigma_E^{i\ 1}\right) = \tag{28}$$

$$\frac{(|\phi_i^i\rangle_{EE}\langle\phi_i^i| + |\phi_{i+1}^{i+1}\rangle_{EE}\langle\phi_{i+1}^{i+1}|) + (|\phi_i^{i+1}\rangle_{EE}\langle\phi_i^{i+1}| + |\phi_{i+1}^i\rangle_{EE}\langle\phi_{i+1}^i|)}{|\phi_i^i|^2 + |\phi_{i+1}^{i+1}|^2 + |\phi_i^{i+1}|^2 + |\phi_{i+1}^i|^2}.$$

Для вычисления информации Евы необходимо знать структуру ее состояний $|\phi_i^j\rangle_E$. Для этого воспользуемся свойством унитарности U_{BE}. Унитарность сохраняет скалярное произведение между состояниями, что означает ${}_{BE}\langle\tilde{i}|\tilde{i'}\rangle_{BE} = 0$. Использование (12)–(14) дает

$$0 = {}_{BE}\langle\tilde{i}|\tilde{i'}\rangle_{BE} = \sum_j {}_B\langle j|j\rangle_{BE}\langle\phi_i^j|\phi_{i'}^j\rangle_E + \\ + \sum_{j\neq j'} {}_B\langle j|j'\rangle_{BE}\langle\phi_i^j|\phi_{i'}^{j'}\rangle_E. \tag{29}$$

Для большей наглядности удобно представить компоненты состояний Евы в виде таблицы

ϕ_1^1	ϕ_1^2	ϕ_1^3	...	ϕ_1^{N-2}	ϕ_1^{N-1}	ϕ_1^N
ϕ_2^1	ϕ_2^2	ϕ_2^3	...	ϕ_2^{N-2}	ϕ_2^{N-1}	ϕ_2^N
ϕ_3^1	ϕ_3^2	ϕ_3^3	...	ϕ_3^{N-2}	ϕ_3^{N-1}	ϕ_3^N
...	...	...	...	...	...	...
ϕ_{N-2}^1	ϕ_{N-2}^2	ϕ_{N-2}^3	...	ϕ_{N-2}^{N-2}	ϕ_{N-2}^{N-1}	ϕ_{N-2}^N
ϕ_{N-1}^1	ϕ_{N-1}^2	ϕ_{N-1}^3	...	ϕ_{N-1}^{N-1}	ϕ_{N-1}^{N-1}	ϕ_{N-1}^N
ϕ_N^1	ϕ_N^2	ϕ_N^3	...	ϕ_N^{N-2}	ϕ_N^{N-1}	ϕ_N^N

(30)

Векторы в (29), (30) из разных клеток одного столбца (одинаковом индексе j) можно выбрать, за счет выбора достаточной размерности пространства состояний Евы, попарно ортогональными, поскольку скалярное произведение ${}_E\langle\phi_i^j|\phi_{i'}^j\rangle_E$ стоит сомножителем при ненулевом слагаемом ${}_B\langle j|j\rangle_B = 1$. Напомним (см. (29)), что векторы из разных клеток одной строки попарно ортогональны. Скалярные произведения во второй сумме (29), содержащие векторы из разных столбцов и разных строк ($j \neq j'$ и $i \neq i'$), стоят сомножителем перед нулем – ${}_B\langle j|j'\rangle_B = 0$. Поэтому такие скалярные произведения нельзя считать нулевыми. В матрицу плотности Евы (28) входят только векторы с индексами j, j' и i, i', отличающимися на единицу. Кроме того, векторы в первой скобке числителя (28) и векторы во второй скобке числителя попарно ортогональны. То есть матрица плотности (28) в базисе четырех векторов, фигурирующих в числителе, имеет блочно-диагональный вид из двух матриц 2×2. Скалярные произведения векторов внутри каждой скобки обозначим как ${}_E\langle\phi_i^i|\phi_{i+1}^{i+1}\rangle_E = |\phi_i^i||\phi_{i+1}^{i+1}|\cos\ alpha_i$ и ${}_E\langle\phi_i^{i+1}|\phi_{i+1}^i\rangle_E = |\phi_{i+1}^i||\phi_i^{i+1}|\ cos\beta_i$.

Далее, поскольку энтропия фон Неймана – выпуклая функция, максимум информации Евы о ключе по всем временным базисам (индексам i) достигается в случае, когда информация в каждом базисе одинакова и не зависит от i. Как видно из структуры таблицы и матрицы плотности Евы, это приводит к равенству модулей векторов на главной диагонали. Аналогичное условие независимости от номера базиса дает равенство модулей векторов над главной и под главной диагональю $|\phi_i^{i+1}| = |\phi_{i+1}^i|$. Для выяснения этой величины остается воспользоваться условием нормировки в каждой строке $\sum_{j=1}^N |\phi_i^j|^2 = 1$. Равенство модулей всех недиагональных элементов и условие нормировки, дают

$$|\phi_i^j|^2 = \frac{q}{N-1}, \quad j \neq i,$$
$$|\phi_i^i|^2 = 1-q, \quad \eta(N) = 1 - \frac{1-\frac{N-2}{N-1}q}{1-\frac{N-3}{N-1}q}. \tag{31}$$

Величина $q/(N-1)$ имеет смысл вероятности отсчетов в контрольных временны́х окнах (напомним, что в отсутствие подслушивателя данная величина должна быть равна 0). Здесь также введена величина $\eta(N)$, имеющая смысл отношения вероятностей отсчетов в контрольных и информационных временны́х окнах.

Осталось определить углы между состояниями ${}_E\langle\phi_i^i|\phi_{i+1}^{i+1}\rangle_E$ и ${}_E\langle\phi_i^{i+1}|\phi_{i+1}^i\rangle_E$. С учетом (31) находим собственные числа матрицы плотности (28) и информацию Евы – энтропию фон Неймана в (24). Собственные числа $\lambda_1 = (1-\eta(N))(1-Q_1)$, $\lambda_2 = (1-\eta(N))Q_1$ и $\lambda_3 = \eta(N)(1-Q_2)$, $\lambda_4 = \eta Q_2$, где введены обозначения $Q_{1,2} = \frac{1}{2}(1-\cos\alpha_{1,2})$. Для информации Евы находим

$$h(\eta(N)) + (1-\eta(N))h(Q_1) + \eta(N)h(Q_2). \tag{32}$$

Как несложно проверить, из-за выпуклости $h(x)$ и того, что собственные числа в сумме равны единице, максимум (32) достигается при $Q_1 = Q_2 = Q$. С учетом этого обстоятельства находим

$$S\left(\frac{\overline{\sigma}_E^{i\,0} + \overline{\sigma}_E^{i\,1}}{2}\right) = h(\eta(N)) + h(Q). \tag{33}$$

Смысл величины Q становится ясен из записи матрицы плотности Боба. Нормированная на информационные временны́е окна матрица плотности Боба в (21) принимает вид

$$\overline{\sigma}_B^0 = \frac{1}{2}\left((1-Q)|0\rangle_{BB}\langle 0| + Q|1\rangle_{BB}\langle 1|\right),$$
$$\overline{\sigma}_B^1 = \frac{1}{2}\left(Q|0\rangle_{BB}\langle 0| + (1-Q)|1\rangle_{BB}\langle 1|\right). \tag{34}$$

Из (34) следует, что величина Q имеет смысл ошибки в информационной последовательности Боба. Величина $\eta(N)$ имеет смысл отношения вероятности отсчетов в информационных временны́х окнах к вероятности отсчетов в контрольных временны́х окнах.

Окончательно для длины секретного ключа, с учетом (23), (33), (34), получаем

$$r/n = 1 - h(Q) - h(\eta(N)). \tag{35}$$

Зависимости длины ключа на плоскости параметров (Q, η) приведены на рис.3 для разного числа базисов. Как видно из рис.3, в асимптотическом пределе большого числа базисов длина секретного ключа перестает зависеть от η и остается только зависимость от Q. Из правого нижнего графика видно, что длина ключа выходит на зависимость (2) – пропускную способность бинарного классического канала связи, то есть

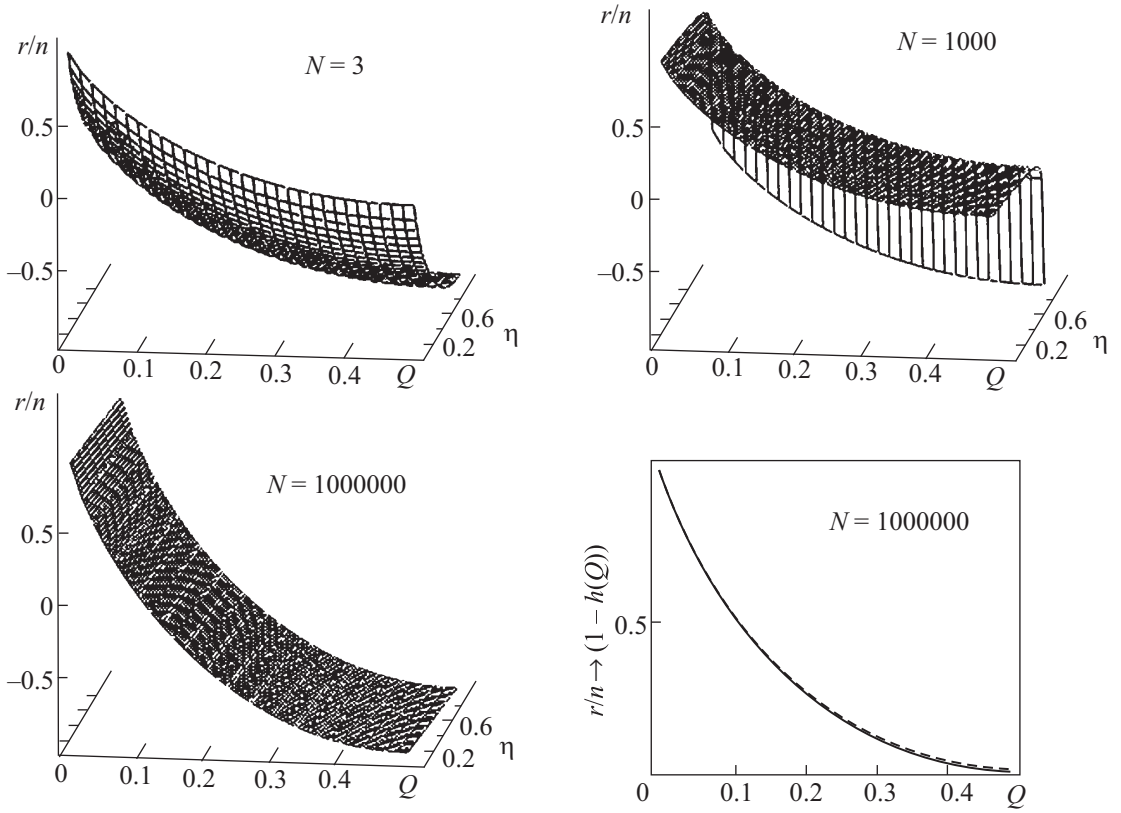

Рис.3. Длина ключа как функция $(Q, \eta(N))$ для разного числа базисов N. Число базисов N указано на графиках

шенноновский предел, который определяет возможность безошибочной передачи информации. В данном случае гарантируется еще и секретность передаваемых ключей.

Выражаю благодарность коллегам по Академии Криптографии Российской Федерации за постоянную поддержку. Работа частично поддержана проектом Российского фонда фундаментальных исследований # 08-02-00559.

1. C. E. Shannon, Bell Syst. Tech. Jour. **27**, 397; 623 (1948).
2. 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).
3. C. H. Bennett and G.Brassard, *Quantum Cryptography: Public Key Distribution and Coin Tossing*, Proc.of IEEE Int. Conf. on Comput. Sys. and Sign. Proces., Bangalore, India, December 1984, p. 175.
4. Р. Галлагер, *Теория информации и надежная связь*, М.: Сов. Радио, 1974.
5. C. H. Bennett, Phys. Rev. Lett. **68**, 3121 (1992).
6. H. F. Chau, Phys. Rev. A **66**, 060302-1 (2002).
7. A. Acin, J. Bae, E. Bagan et al., Phys. Rev. A **73**,012327-1 (2006).
8. N. Gisin and S.Wolf, Phys. Rev. Lett. **83**, 4200 (1999).
9. G. Smith, J. M. Renes, and J. A. Smolin, arXiv: quant-ph 0607018.
10. G. M. Nikolopoulos, K. S. Ranade, and G. Alber, Phys. Rev. A **73**, 032325-1 (2006).
11. C. Branciard, N. Gisin, B. Kraus, and V. Scarani, Phys. Rev. A **72**, 032301-1 (2005).
12. J. Bae and A. Acin, arXiv: quant-ph 0610048.
13. S. Watanabe, R. Matsumoto, and T. Uyematsu, arXiv: quant-ph 0705.2904.
14. R. Renner, arXiv: quant-ph/0512258.
15. B. Kraus, N. Gisin, and R. Renner, Phys. Rev. Lett. **95**, 080501 (2005).
16. C. H. Bennett, G. Brassard, C. Crépeau, and U. Maurer, IEEE Transaction on Information Theory **41**, 1915 (1995).
17. J. L. Carter, M. N. Wegman, **18**, 143 (1979).
18. C. H. Bennett, P. W. Shor, IEEE Trans. Inform. Theory **44**, 2724 91998).
19. P. Shor, arXiv:quant-ph/0304102.
20. A. S. Holevo, *Statistical Structure of Quantum Theory*, Springer-Verlag, Berlin, Heidelberg, New York, London, Paris, Tokyo, Hong Kong, Barselona, Budapest, (2001).
21. А. С. Холево, Введение в квантовую теорию информации, серия Современная математическая физика, вып.5, МЦНМО, Москва, 2002; Успехи математических наук **53**, 193 (1998).
22. С. П. Кулик, С. Н. Молотков, А. П. Маккавеев, Письма в ЖЭТФ **95**, 324 (2007).