Письма в ЖЭТФ, том 92, вып. 7, с. 539 – 544 © 2010 г. 10 октября

Усиление стойкости фазово-временно́й квантовой криптографии блочным исправлением ошибок

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, 119899 Москва, Россия

Поступила в редакцию 5 августа 2010 г.

Рассмотрено блочное кодирование перед исправлением ошибок для протокола квантового распределения ключей с фазово-временны́м кодированием. По сравнению с другими известными протоколами квантового распределения ключей в данном случае блочное кодирование обеспечивает наилучшие результаты по допустимой критической ошибке, что делает протокол с фазово-временны́м кодированием наиболее устойчивым к внешним воздействиям.

Квантовая криптография – квантовое распределение ключей – основано на принципиальных запретах квантовой механики на достоверное различение неортогональных квантовых состояний [1]. Любое измерение неортогональных квантовых состояний с целью извлечения информации неизбежно приводит к их возмущению и ошибке на приемной стороне, что позволяет детектировать любые попытки подслушивания.

В зависимости от структуры квантовых состояний, в которые кодируются классические биты ключа 0 и 1, величина извлекаемой информации из передаваемых состояний и неизбежная ошибка на приемной стороне связаны определенным соотношением. Для каждого квантового протокола передачи ключей существует фундаментальная связь между верхней границей информации, извлекаемой из квантовых состояний, и производимой ошибкой Q на приемной стороне. При определенной величине критической ошибки Q_c взаимная информация между Алисой (передающая сторона) и Бобом (приемная сторона) сравнивается с взаимной информацией между Алисой и Евой (подслушиватель), поэтому при $Q > Q_c$ передача секретных ключей невозможна, поскольку при этом Ева знает весь передаваемый ключ.

Доказано (см., например, полное изложение в [2][1)]), что для протоколов, в которых квантовые состояния передаются в каждой посылке независимо друг от друга, наиболее мощной является коллективная атака. Данная атака сводится к следующему. В каждой посылке Ева готовит свое вспомогательное состояние, которое унитарно взаимодействует с передаваемым состоянием. После этого состояния Алисы и Евы оказываются в совместном запутанном состоянии. Свою подсистему Ева оставляет у себя в квантовой памяти, а модифицированное состояние Алисы направляет к Бобу. После посылки всей серии состояний Алисой и измерений Боба Ева производит коллективные измерения над всей последовательностью состояний в своей квантовой памяти.

Оказывается, что существует оптимальная атака Евы [2 – 4], в том смысле, что она может подобрать свое вспомогательное квантовое состояние, унитарное взаимодействие и измерения таким образом, что при данной наблюдаемой (производимой Евой на стороне Боба) ошибке Q она может извлечь максимум информации о передаваемых состояниях. В результате длина финального секретного ключа r из переданной последовательности длины n является функцией наблюдаемой ошибки Q на приемной стороне:

$$r/n = r(Q), \quad r(Q) \to 0, \quad Q \to Q_c. \qquad (1)$$

Причем функция $r(Q)$ и Q_c определяются лишь протоколом квантового распределения ключей. При $Q < Q_c$ Алиса и Боб имеют совместный секретный ключ длины $nr(Q)$ бит, про который Ева не имеет никакой информации. Если Ева начинает вторгаться в канал таким образом, что она производит ошибку $Q > Q_c$ (неважно, действуя оптимальным или иным способом), то Алиса и Боб прерывают протокол передачи ключей и решают вопрос с подслушивателем другими средствами.

Таким образом, квантовая криптография позволяет не только детектировать все попытки подслушивания, но и передавать секретные ключи, если на при-

[1)] Частичные результаты приведены в [3].

емной стороне наблюдаемая ошибка $Q < Q_c$[2]. Поэтому, чем больше критическая ошибка Q_c, до которой гарантируется секретность передаваемых ключей, тем более устойчивым считается протокол. Например, для наиболее разработанного протокола BB84 [1] критическая ошибка составляет $Q_c \approx 11\%$ [2–4]. Допустимую критическую ошибку можно увеличить, жертвуя частью распределенной битовой последовательности примерно до величины $\approx 30\%$ [5], что все равно еще далеко от теоретического предела в 50%.

Нужно отметить, что длина секретного ключа в (1) получается с учетом исправления ошибок через открытый классический канал связи и дополнительного сжатия "очищенного" ключа.

Выше речь шла о так называемых однопараметрических протоколах квантовой криптографии, когда детектирование подслушивания и длина секретного ключа зависят только от одного параметра – наблюдаемой ошибки на приемной стороне Q в битовой последовательности.

Недавно были предложены новые двухпараметрические протоколы квантового распределения ключей [4]. Одним из таких протоколов является фазово-временна́я квантовая криптография. В этом протоколе детектирование подслушивания происходит по двум параметрам – ошибке Q и вероятности отсчетов в контрольных временны́х окнах – δ. Причем важно, что при отсутствии подслушивателя неидеальности аппаратуры приводят только к ошибке Q и не дают отсчетов в контрольных временны́х окнах – $\delta = 0$. В этом протоколе длина секретного ключа является функцией двух параметров

$$r/n = r(Q, \delta). \tag{2}$$

Условие $r(Q, \delta) > 0$ определяет целую область секретности в плоскости параметров (Q, δ). Оба параметра зависят от действий подслушивателя. Однако Алиса и Боб могут прервать протокол, если величина δ отсчетов в контрольных временны́х окнах будет превышать некоторую величину, которую они могут выбрать для себя независимо от Евы. В этом случае критическая ошибка в битовой последовательности $Q_c(\delta)$ функцией отсчетов в контрольных временны́х окнах. При малых $\delta \to 0$ допустимая критическая ошибка, до которой можно передавать ключи, стремится к теоретическому пределу $Q_c(\delta \to 0) \to 1/2$. С ростом δ допустимая критическая ошибка уменьшается (является убывающей функцией δ).

[2]Нужно отметить, что Боб принципиально не может отличить ошибки от подслушивателя и несовершенства аппаратуры.

Идеальной, с точки зрения устойчивости к ошибкам при распределении ключей, была бы ситуация, когда критическая ошибка близка к теоретическому пределу $Q_c = 1/2$ и не зависела бы вообще от отсчетов в контрольных временны́х окнах. Однако целиком такой цели добиться не удается. Тем не менее, можно расширить область секретности (см. ниже) посредством предварительного блочного исправления ошибок. Идея достаточно проста. После передачи квантовых состояний и измерений на приемной стороне перед исправлением ошибок случайными шенноновскими кодами, биты в разных посылках объединяются в блоки по N одинаковых символов 0 или 1, и оставляются только блоки, когда на передающей стороне и приемной все символы в определенных посылках в результате измерений получились одинаковыми. Сами биты, естественно, не разглашаются, и блоки, где возник хотя бы один другой символ, отбрасываются. Данная процедура делается через открытый классический канал связи. То есть возникают "новые" блочные 0 и 1. После этого блочные 0 и 1 все еще содержат ошибки. Боб может получить во всех N символах неправильный исход, хотя и с меньшей вероятностью, чем в отдельной позиции. Данные ошибки затем исправляются, как и обычно, случайными шенновскими кодами. Такая процедура существенно менее экономна, чем просто исправление ошибок только случайными шенноновскими кодами, в смысле расходования переданной битовой последовательности, но зато расширяет область секретности.

Информационные квантовые состояния представляют собой суперпозицию состояний, локализованных в трех временны́х окнах 1, 2, 3 – $|1\rangle$, $|2\rangle$, $|3\rangle$[3]. Всего имеются 4 базиса. Два левых базиса – прямой $L+$, сопряженный $L\times$, в котором состояния являются суперпозицией состояний $|1\rangle$, $|2\rangle$, и аналогично два правых – $R+$, $R\times$, с состояниями натянутыми на базисные состояния $|2\rangle$, $|3\rangle$. Информационные состояния, чтобы отличать их от базисных, будем снабжать чертой сверху; имеем в левых базисах

$$\begin{aligned} |\overline{0_L^+}\rangle &= \frac{1}{\sqrt{2}}(|1\rangle + |2\rangle), \quad |\overline{1_L^+}\rangle = \frac{1}{\sqrt{2}}(|1\rangle - |2\rangle), \\ |\overline{0_L^\times}\rangle &= \frac{1}{\sqrt{2}}(|1\rangle + i|2\rangle), \quad |\overline{1_L^\times}\rangle = \frac{1}{\sqrt{2}}(|1\rangle - i|2\rangle), \end{aligned} \tag{3}$$

[3]Классические биты кодируются как в суперпозицию состояний, локализованных в разных временных окнах, так и в относительную фазу между состояниями в этих окнах. Отсюда происходит название фазово-временна́я квантовая криптография.

соответственно, в правых базисах имеем

$$|\overline{0_R^+}\rangle = \frac{1}{\sqrt{2}}(|2\rangle + |3\rangle), \quad |\overline{1_R^+}\rangle = \frac{1}{\sqrt{2}}(|2\rangle - |3\rangle),$$
$$|\overline{0_R^\times}\rangle = \frac{1}{\sqrt{2}}(|2\rangle + i|3\rangle), \quad |\overline{1_R^\times}\rangle = \frac{1}{\sqrt{2}}(|2\rangle - i|3\rangle). \tag{4}$$

Пусть вспомогательное состояние Евы $|A\rangle_E \in \in \mathcal{H}_E$. Совместная эволюция вспомогательного и информационного состояний описывается унитарным оператором Евы U_{BE}. В силу линейности проще сначала выяснить действие U_{BE} на базисные состояния, имеем (см. детали в [4])

$$\begin{gathered} U_{BE}(|1\rangle_B \otimes |A\rangle_E) = \sqrt{1-2\delta}|1\rangle_B \otimes |\psi_1^1\rangle_E + \\ + \sqrt{\delta}|2\rangle_B \otimes |\psi_2^1\rangle_E + \sqrt{\delta}|3\rangle_B \otimes |\psi_3^1\rangle_E, \\ U_{BE}(|2\rangle_B \otimes |A\rangle_E) = \sqrt{\delta}|1\rangle_B \otimes |\psi_1^2\rangle_E + \\ + \sqrt{1-2\delta}|2\rangle_B \otimes |\psi_2^2\rangle_E + \sqrt{\delta}|3\rangle_B \otimes |\psi_3^2\rangle_E, \\ U_{BE}(|3\rangle_B \otimes |A\rangle_E) = \sqrt{\delta}|1\rangle_B \otimes |\psi_1^3\rangle_E + \\ \sqrt{\delta}|2\rangle_B \otimes |\psi_2^3\rangle_E + \sqrt{1-2\delta}|3\rangle_B \otimes |\psi_3^3\rangle_E, \end{gathered} \tag{5}$$

где справедливы следующие соотношения между состояниями [4] $|\psi_i^j\rangle_E \in \mathcal{H}_E$:

$$\begin{gathered} {}_E\langle\psi_i^j|\psi_i^k\rangle_E = {}_E\langle\psi_j^i|\psi_k^i\rangle_E = 0, \\ {}_E\langle\psi_1^1|\psi_2^2\rangle_E = {}_E\langle\psi_2^2|\psi_3^3\rangle_E = \\ = {}_E\langle\psi_1^2|\psi_2^1\rangle_E = {}_E\langle\psi_2^3|\psi_3^2\rangle_E = \cos\alpha, \end{gathered} \tag{6}$$

$$Q = \frac{1-\cos\alpha}{2}.$$

Действие Евы на информационные состояния, с учетом (3) и (5), может быть представлено в виде

$$\begin{gathered} |\Psi^{0^+L}\rangle_{BE} = U_{BE}(|\overline{0_L^+}\rangle_B \otimes |A\rangle_E) = \\ = |\overline{0_L^+}\rangle_B \otimes |\varphi_1^{0La}\rangle_E + |\overline{1_L^+}\rangle_B \otimes |\varphi_2^{0La}\rangle_E + \\ + |3\rangle_B \otimes \left(\frac{|\psi_3^1\rangle_E + |\psi_3^2\rangle_E}{\sqrt{2}}\right), \end{gathered} \tag{7}$$

$$\begin{gathered} |\Psi^{1^+L}\rangle_{BE} = U_{BE}(|\overline{1_L^+}\rangle_B \otimes |A\rangle_E) = \\ = |\overline{0_L^+}\rangle_B \otimes |\varphi_1^{1La}\rangle_E + |\overline{1_L^+}\rangle_B \otimes |\varphi_2^{1La}\rangle_E + \\ + |3\rangle_B \otimes \left(\frac{|\psi_3^1\rangle_E - |\psi_3^2\rangle_E}{\sqrt{2}}\right). \end{gathered} \tag{8}$$

Аналогичное представление легко получается для состояний из левого сопряженного базиса. Причем состояния в (7), (8) выражаются через состояния в (5) следующим образом:

$$\begin{gathered} |\varphi_1^{0L}\rangle_E = \frac{1}{2}(|\psi_1^1\rangle_E + |\psi_2^1\rangle_E + |\psi_1^2\rangle_E + |\psi_2^2\rangle_E), \\ |\varphi_1^{1L}\rangle_E = \frac{1}{2}(|\psi_1^1\rangle_E - |\psi_2^1\rangle_E - |\psi_1^2\rangle_E + |\psi_2^2\rangle_E), \end{gathered} \tag{9}$$

$$\begin{gathered} |\varphi_2^{0L}\rangle_E = \frac{1}{2}(|\psi_1^1\rangle_E - |\psi_2^1\rangle_E + |\psi_1^2\rangle_E - |\psi_2^2\rangle_E), \\ |\varphi_2^{1L}\rangle_E = \frac{1}{2}(|\psi_1^1\rangle_E + |\psi_2^1\rangle_E - |\psi_1^2\rangle_E - |\psi_2^2\rangle_E), \end{gathered} \tag{10}$$

Модифицированное состояние Евы представимо в виде линейной комбинации трех однокубитных состояний $|\overline{i},\overline{j},\overline{k}\rangle_E$ $(i,j,k=0,1)$:

$$\begin{gathered} |\psi_1^1\rangle_E = \sqrt{1-2\delta}|\overline{000}\rangle_E, \\ |\psi_2^1\rangle_E = \sqrt{\delta}(\cos\alpha|\overline{110}\rangle_E - \sin\alpha|\overline{111}\rangle_E), \\ |\psi_3^1\rangle_E = \sqrt{\delta}|\overline{010}\rangle_E, \end{gathered} \tag{11}$$

$$\begin{gathered} |\psi_1^2\rangle_E = \sqrt{\delta}|\overline{110}\rangle_E, \\ |\psi_2^2\rangle_E = \sqrt{1-2\delta}(\cos\alpha|\overline{000}\rangle_E - \sin\alpha|\overline{001}\rangle_E), \\ |\psi_3^2\rangle_E = \sqrt{\delta}|\overline{100}\rangle_E, \end{gathered} \tag{12}$$

$$\begin{gathered} |\psi_3^1\rangle_E = \sqrt{\delta}|\overline{010}\rangle_E, \ |\psi_3^2\rangle_E = \sqrt{\delta}|\overline{100}\rangle_E, \\ |\psi_3^3\rangle_E = \sqrt{1-2\delta}|\overline{000}\rangle_E. \end{gathered} \tag{13}$$

С учетом (4), (5) состояния (7)–(10) могут быть получены в обоих правых базисах, которые из-за экономии места и симметрии по отношению к левым и правым базисам, не выписываем. Далее все рассуждения проводим, выписывая все выражения только для левого базиса.

Перейдем к измерениям Боба. Любое измерение в квантовой механике описывается некоторым разложением единицы ($I_B = \mathcal{P}_{L+}^0 + \mathcal{P}_{L+}^1 + |3\rangle_{BB}\langle 3|$), то есть каждому элементарному событию сопоставляется положительный эрмитов оператор. В нашем случае элементарными событиями являются: 1) событие, которое интерпретируется как логический 0, ему сопоставляется проектор $\mathcal{P}_{L+}^0 = |\overline{0_L^+}\rangle_{BB}\langle\overline{0_L^+}|$, 2) событие, которое интерпретируется как логическая 1, ему сопоставляется проектор $\mathcal{P}_{L+}^1 = |\overline{1_L^+}\rangle_{BB}\langle\overline{1_L^+}|$, 3) отсчет в контрольном временно́м окне для состояний в левых базисах – отсчет во временно́м окне 3 (проектор $|3\rangle_{BB}\langle 3|$). В отсутствие подслушивателя, отсчеты в этом временно́м окне для состояний из левых базисов отсутствуют. Эта ситуация отвечает значению $\delta = 0$. Вероятность правильного исхода у Боба, когда Алиса посылала 0 в прямом левом базисе, есть

$$\mathrm{Pr}_B(0|0) = \frac{\mathrm{Tr}_{BE}(\mathcal{P}_{L+}^0|\Psi^{0^+L}\rangle_{BEBE}\langle\Psi^{0^+L}|)}{\mathrm{Tr}_{BE}(|\Psi^{0^+L}\rangle_{BEBE}\langle\Psi^{0^+L}|)} = 1-Q, \tag{14}$$

при этом в распоряжении Евы оказывается состояние

$$\rho_E^{0,OK} = \frac{|\varphi_1^{0La}\rangle_{EE}\langle\varphi_1^{0La}|}{1-\delta} = \\ = \frac{\mathrm{Tr}_B(\mathcal{P}_{L+}^0|\Psi^{0^+L}\rangle_{BEBE}\langle\Psi^{0^+L}|)}{\mathrm{Tr}_{BE}(|\Psi^{0^+L}\rangle_{BEBE}\langle\Psi^{0^+L}|)}. \tag{15}$$

Аналогично для ошибочного исхода Боба

$$\mathrm{Pr}_B(1|0) = \frac{\mathrm{Tr}_{BE}(\mathcal{P}_{L+}^1|\Psi^{0^+L}\rangle_{BEBE}\langle\Psi^{0^+L}|)}{\mathrm{Tr}_{BE}(|\Psi^{0^+L}\rangle_{BEBE}\langle\Psi^{0^+L}|)} = Q, \tag{16}$$

и соответствующая матрица плотности Евы

$$\rho_E^{0,Err} = \frac{|\varphi_2^{0La}\rangle_{EE}\langle\varphi_2^{0La}|}{1-\delta} = \\ = \frac{\mathrm{Tr}_B(\mathcal{P}_{L+}^1|\Psi^{0^+L}\rangle_{BEBE}\langle\Psi^{0^+L}|)}{\mathrm{Tr}_{BE}(|\Psi^{0^+L}\rangle_{BEBE}\langle\Psi^{0^+L}|)}. \tag{17}$$

Полная матрица плотности Евы, когда Алиса посылала 0, с учетом (15) и (17) равна

$$\rho_E^0 = \frac{1}{2}\left(\rho_E^{0,OK} + \rho_E^{0,Err}\right). \tag{18}$$

Далее Алиса сообщает номера только тех посылок по N штук в каждой, в которых она посылала только 0 или только 1 (но, естественно, не называет, что именно она посылала). Боб сохраняет N посылок только в том случае, если в каждой из них был получен одинаковый результат (все 0, или все 1). Вероятность того, что если Алиса посылала 0, и Боб во всех N посылках получил правильный результат 0, равна (соответственно, вероятность того, что во всех N посылках Боб получил неверный исход)

$$\mathrm{Pr}(0^N|0^N) = \frac{(1-Q)^N}{(1-Q)^N+Q^N} = 1-\tilde{Q_N}, \\ \mathrm{Pr}(1^N|0^N) = \frac{Q^N}{(1-Q)^N+Q^N} = \tilde{Q_N}, \tag{19}$$

$$\rho_E^{0^{\otimes N},OK} = \left(\frac{|\varphi_1^{0La}\rangle_{EE}\langle\varphi_1^{0La}|}{1-\delta}\right)^{\otimes N} \\ \rho_E^{0^{\otimes N},Err} = \left(\frac{|\varphi_2^{0La}\rangle_{EE}\langle\varphi_2^{0La}|}{1-\delta}\right)^{\otimes N}. \tag{20}$$

Далее, полная матрица плотности Евы, когда Алиса посылала 0, есть

$$\rho_E^{0^{\otimes N}} = \frac{1}{2}\left(\rho_E^{0^{\otimes N},OK} + \rho_E^{0^{\otimes N},Err}\right). \tag{21}$$

Аналогично, когда Алиса посылала 1 в прямом левом базисе, соответствующие состояния Евы в квантовой памяти равны

$$\rho_E^{1^{\otimes N},OK} = \left(\frac{|\varphi_1^{1La}\rangle_{EE}\langle\varphi_1^{1La}|}{1-\delta}\right)^{\otimes N} \\ \rho_E^{1^{\otimes N},Err} = \left(\frac{|\varphi_2^{1La}\rangle_{EE}\langle\varphi_2^{1La}|}{1-\delta}\right)^{\otimes N}, \tag{22}$$

и полная матрица плотности Евы есть

$$\rho_E^{1^{\otimes N}} = \frac{1}{2}\left(\rho_E^{1^{\otimes N},OK} + \rho_E^{1^{\otimes N},Err}\right). \tag{23}$$

Теперь задача Евы сводится к различению матриц плотности (21) и (23).

Алиса и Боб теперь имеют последовательности новых X – Алиса и Y – Боб, строк. $X, Y = \{\tilde{0}, \tilde{1}\}^n$, n – длина последовательности новых $\tilde{0} = 0^N$ и $\tilde{1} = 1^N$ по N штук бит, причем часть из них у Боба с ошибкой. Данные ошибки должны быть исправлены через открытый канал связи. При исправлении ошибок наилучшим образом при помощи случайных шенноновских кодов [6, 7] потребуется раскрытие $nH(X|Y)$ бит классической информации через открытый канал связи [2, 4, 6, 7]. Здесь $nH(X|Y)$ – условная шенноновская энтропия. Полное количество информации (взаимная информация $I_{AB}(X;Y)$) в битах между Алисой и Бобом есть

$$I_{AB}(X;Y) = H(X) - H(X|Y) = n(1 - h(\tilde{Q_N})). \tag{24}$$

Шенноновская энтропия источника $H(X)$ в силу равновероятного выбора 0 и 1 есть $H(X) = n$, здесь бинарная энтропийная функция $h(x) = -x\log x - (1 - x)\log(1-x)$, где логарифм берется по основанию 2.

Информация Евы ограничена фундаментальной границей Холево [8], которая достижима; имеем

$$n\chi(\rho_E) = n\Bigg(S\left(\frac{\rho_E^{0^{\otimes N}} + \rho_E^{1^{\otimes N}}}{2}\right) - \\ - \frac{1}{2}S\left(\rho_E^{0^{\otimes N}}\right) - \frac{1}{2}S\left(\rho_E^{1^{\otimes N}}\right)\Bigg), \tag{25}$$

здесь $S(\rho) = -\mathrm{Tr}\{\rho\log\rho\}$ – энтропия фон Неймана.

Для вычисления энтропий фон Неймана требуются собственные числа полной матрицы плотности и

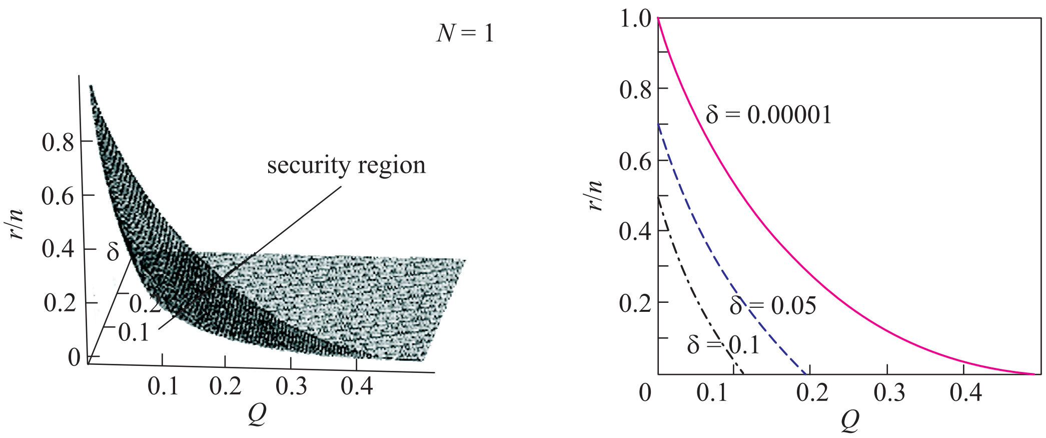

Рис.1

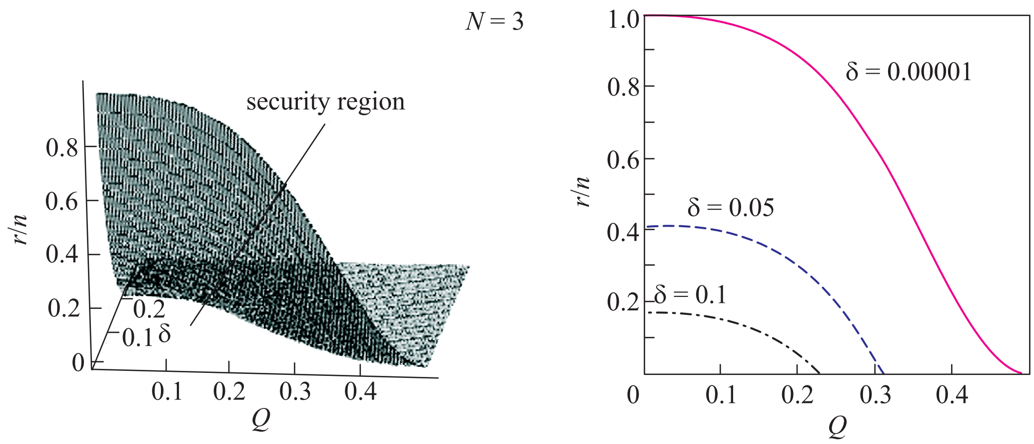

Рис.2

частичных матриц плотности в (25). Для собственных чисел полной матрицы плотности имеем

$$\lambda_{1,2} = \frac{(1-Q)^N}{(1-Q)^N + Q^N} \cdot \frac{1 \pm \varepsilon^N}{2},$$

$$\lambda_{3,4} = \frac{Q^N}{(1-Q)^N + Q^N} \cdot \frac{1 \pm \varepsilon^N}{2}, \qquad (26)$$

$$\varepsilon = \frac{(1-3\delta)}{(1-\delta)}.$$

Поскольку собственные числа частичных матриц плотности Евы $\rho_E^{0\otimes N}$, $\rho_E^{1\otimes N}$ и Боба совпадают, то

$$h(\tilde{Q}_N) = \frac{1}{2}\left(S\left(\rho_E^{0\otimes N}\right) + S\left(\rho_E^{1\otimes N}\right)\right). \qquad (27)$$

Длина финального ключа может быть представлена в виде (см., детали в [2])

$$\frac{r}{n} = 1 - S\left(\frac{\rho_E^{0\otimes N} + \rho_E^{1\otimes N}}{2}\right) = 1 - \sum_{i=1}^{4} \lambda_i \log \lambda_i =$$

$$= 1 - h(\tilde{Q}_N) - h(\tilde{\varepsilon}_N), \quad \tilde{\varepsilon}_N = \frac{1+\varepsilon^N}{2}. \qquad (28)$$

Иными словами, Ева из переданной последовательности длиной n знает долю не более, чем $n\chi(\rho_E)$ бит. В то же время Боб знает долю бит, равную (24). Разница этих двух информаций (24) и (25) составляет секретный ключ. На финальной стадии Алиса и Боб через открытый канал связи сжимают строку из n бит до строки длиной $n\frac{r}{n}$ бит при помощи универсальных хэш-функций второго порядка [9, 10]. После такого сжатия строка длиной (28) бит составляет секретный ключ, известный только Алисе и Бобу.

Результаты расчетов приведены на рис.1–3. На плоскости параметров (Q, δ) существует целая область секретности (левые части рисунков). Без предварительного блочного кодирования при исправлении ошибок (рис.1, $N = 1$) область секретности по величине отсчетов в контрольном временно́м окне

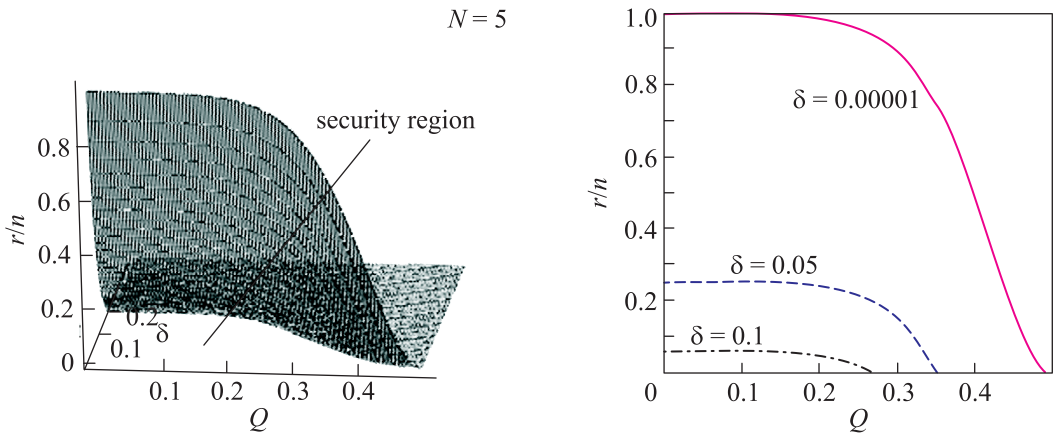

Рис.3

$\delta = 0.00001$ достигает практически теоретического предела по ошибке $Q_c = \frac{1}{2}$. При больших $\delta = 0.05$ и $\delta = 0.1$ допустимая критическая ошибка падает соответственно до $\approx 20\%$ и $\approx 11\%$ (правая часть рис.1). Предварительное блочное кодирование с длиной блока $N = 3$ и $N = 5$ (рис.2, 3) приводит к тому, что область секретности на плоскости параметров расширяется (левые части рис.2, 3) и стремится по форме к прямоугольной области. Последнее означает, что допустимая критическая ошибка все слабее с ростом длины блока N зависит от отсчетов в контрольных временны́х окнах. Как показывают расчеты, при длине блока, бо́льшей $N > 5$, область секретности практически перестает меняться. Поэтому не имеет смысла на практике увеличивать длину блока более чем до $N = 5$.

Таким образом, по сравнению с другими известными протоколами квантового распределения ключей (см., например, работу [5] и ссылки в ней) предварительное блочное кодирование обеспечивает наилучшие результаты по допустимой критической ошибке, что делает протокол с фазово-временны́м кодированием наиболее устойчивым к внешним воздействиям (включая действия подслушивателя и собственные неидеальности аппаратуры).

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

1. C. H.Bennett, G. Brassard, Proc. of IEEE Int. Conf. on Comput. Sys. and Sign. Proces., Bangalore, India, December 1984, p.175.
2. R. Renner, arXiv: quant-ph/0512258.
3. С. Н. Молотков, А. В. Тимофеев, Письма в ЖЭТФ **85**, 632 (2007).
4. Д. А. Кронберг, С. Н. Молотков, ЖЭТФ **136**, 650 (2009).
5. A. Asin, J. Bae, E. Bagan et al., Phys. Rev. A **73**, 012327 (2006); H. F. Chau, Phys. Rev. A **66**, 060302(R) (2002).
6. C. E. Shannon, Bell Syst. Tech. Jour. **27**, 397; 623 (1948).
7. Р. Галлагер, *Теория информации и надежная связь*, М.: Сов. Радио, 1974.
8. А. С. Холево, *Введение в квантовую теорию информации*, серия Современная математическая физика, вып.5, МЦНМО, Москва, 2002; Успехи математических наук **53**, 193 (1998).
9. J. L. Carter and M. N. Wegman, J. Computer and System Sciences **18**, 143 (1979).
10. C. H. Bennett, G. Brassard, C. Crépeau, and U.Maurer, IEEE Transaction on Information Theory **41**, 1915 (1995).