PACS 03.67.Dd; 03.67.Pp

Квантовая криптография: индивидуальный перехват с учетом протокола коррекции ошибок

Д.Б.Хорошко

Протокол квантового распределения ключа BB84 в комбинации с протоколом повторения для коррекции ошибок проанализирован с точки зрения защищенности от индивидуального перехвата, опирающегося на квантовую память. Показано, что простое знание протокола коррекции ошибок изменяет оптимальную атаку и снабжает перехватчика дополнительной информацией о распределяемом ключе.

***Ключевые слова**: квантовая криптография, квантовая память.*

В течение последнего десятилетия были найдены критерии безусловной защищенности для многих протоколов квантовой криптографии, что сделало возможным обеспечение их защиты от атак любого типа [1 – 3]. Однако значительный интерес до сих пор привлекают к себе критерии защищенности от простейшего, и поэтому наиболее легко реализуемого класса атак – индивидуальных атак. Этот интерес связан с тем, что защищенность от таких атак достигается при значительно более высокой скорости генерации ключа, нежели безусловная защищенность.

Анализ защищенности от индивидуальных атак до сих пор был основан на неявном предположении о том, что перехватчик – Ева – при совершении квантового измерения, являющегося частью любого процесса перехвата, не получает выгоды от знания протокола коррекции ошибок (ПКО), используемого законными пользователями – Алисой и Бобом – для генерации идентичных ключей [3, 4]. Мы показываем, что в общем случае это не так и что знание a priori ПКО позволяет Еве увеличить ее информацию о ключе даже при индивидуальной атаке.

Для иллюстрации мы рассматриваем простейший протокол квантового распределения ключа BB84 с простейшим ПКО – протоколом тройного повторения. Любой протокол квантового распределения ключа состоит из двух этапов: квантовой передачи данных и их классической обработки. Передача осуществляется путем пересылки двухуровневых систем (кубитов) по квантовому каналу. В коммерческих реализациях квантовой криптографии в качестве кубитов используются одиночные фотоны, а в качестве канала – оптическое волокно. Напомним порядок квантовой передачи данных по протоколу BB84 [5]. Один из пользователей (Алиса) генерирует два случайных, равномерно распределенных бита – a и r. В зависимости от результата она приготавливает кубит в одном из четырех квантовых состояний ($|0\rangle$, $|1\rangle$, $|\bar{0}\rangle$ и $|\bar{1}\rangle$), причем два первых и два последних состояния попарно ортогональны, а связь между парами состояний задается соотношениями

$$|\bar{0}\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle), \quad (1)$$

$$|\bar{1}\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle). \quad (2)$$

Состояния $|0\rangle$ и $|\bar{0}\rangle$ соответствуют $a = 0$, состояния $|1\rangle$ и $|\bar{1}\rangle$ – $a = 1$. При $r = 0$ Алиса использует базис $\{|0\rangle, |1\rangle\}$, при $r = 1$ – базис $\{|\bar{0}\rangle, |\bar{1}\rangle\}$. Созданное состояние пересылается по квантовому каналу другому пользователю – Бобу, который генерирует случайный бит r' и в зависимости от его значения настраивает аппаратуру на измерение состояния кубита в базисе $\{|0\rangle, |1\rangle\}$ при $r' = 0$ или в базисе $\{|\bar{0}\rangle, |\bar{1}\rangle\}$ при $r' = 1$. В результате измерения Боб получает значение бита b, которое равно 0 при получении результата измерения $|0\rangle$ или $|\bar{0}\rangle$, и 1 при получении результата измерения $|1\rangle$ или $|\bar{1}\rangle$. Очевидно, что в отсутствие ошибок передачи и измерения биты a и b должны совпадать каждый раз, когда совпадают биты r и r'.

Описанная процедура повторяется $2n + 2\delta$ раз, где n и δ – натуральные числа, причем $1 \ll \delta \ll n$, в результате чего составляются так называемые сырые последовательности данных – битов a у Алисы и соответствующих битов b у Боба. Затем начинается классическая обработка сырых последовательностей, координируемая путем сообщения по классическому каналу связи (например, локальной сети), не защищенному от пассивного перехвата.

Первая стадия классической обработки – согласование базисов – состоит в раскрытии последовательностей битов r и r', которые Алиса и Боб пересылают друг другу по классическому каналу связи. После этого обе стороны оставляют только те биты сырой последовательности, которые соответствуют совпадению r и r'. Таких битов будет $n + \delta$ (асимптотически в пределе больших n), и они составят так называемые просеянные последовательности.

Вторая стадия – оценка ошибки – состоит в генерации Алисой случайного множества из δ номеров от 1 до $n + \delta$ и в пересылке этого множества Бобу вместе со значениями битов просеянной последовательности, имеющими соответствующие номера. Боб находит значения битов с соответствующими номерами в своей просеянной после-

Д.Б.Хорошко. Институт физики им. Б.И.Степанова НАНБ, Белоруссия, 220072 Минск, просп. Независимости, 68;
e-mail: dhoroshko@rambler.ru

Поступила в редакцию 5 июля 2007 г.

довательности и сравнивает эти значения со значениями битов Алисы. На основе этого сравнения Боб вычисляет долю несовпадающих битов Q в случайной выборке длиной δ. Эта доля принимается обеими сторонами за оценку уровня ошибки в квантовом канале связи. Биты, участвовавшие в случайной выборке, удаляются из просеянных последовательностей, которые после этого приобретают длину n битов.

Третья стадия классической обработки информации состоит в коррекции ошибок. Для этого стороны обмениваются некоторой информацией по классическому каналу связи. Процесс коррекции ошибок может быть односторонним, когда только Алиса посылает информацию Бобу (или наоборот), или двусторонним, при котором идет интерактивный обмен информацией. Наиболее просты для анализа односторонние ПКО, которыми мы и ограничимся в данной работе.

Согласно теореме Шеннона стандартной теории информации [6], число битов, которые Алисе следует переслать для коррекции Qn ошибок в просеянном ключе Боба длиной n, асимптотически равно $nh_2(Q)$, где

$$h_2(x) = -x\log_2 x - (1-x)\log_2(1-x) \tag{3}$$

– бинарная H-функция Больцмана. В конкретном ПКО будет использовано немногим большее число пересылаемых битов. В результате выполнения ПКО пользователи получат идентичные (с высокой вероятностью) исправленные последовательности длиной n битов. При разработке ПКО следует учитывать, что вся пересылаемая информация попадает к перехватчику Еве, которая может пассивно прослушивать классический канал. Таким образом, с каждым ПКО связана некоторая информация I_{ec} об исправленном ключе, поступающая к Еве. Эта информация «суммируется» Евой с информацией I_{qt}, полученной при перехвате в квантовом канале на этапе квантовой передачи. Данное суммирование не является простой арифметической операцией в силу того, что информация I_{qt} может быть не классической, а квантовой, что возможно для Евы, обладающей квантовой памятью.

Последней стадией классической обработки информации является процедура усиления секретности. Она состоит в отображении путем случайного хеширования исправленной последовательности длиной n на окончательную последовательность длиной $m \leqslant n$, которая уже может быть использована как криптографический ключ [7]. Длина этого ключа m дается специальной теорией, в которой в качестве входного параметра используется доступный Еве верхний предел классической информации I_{qt+ec} об исправленной последовательности Алисы и Боба.

В том случае, когда Ева не обладает квантовой памятью, способной хранить квантовую информацию в течение времени между квантовой передачей и классической обработкой, выражение для длины секретного ключа имеет особенно простой вид. При этом информация Евы о просеянной последовательности Алисы I_{qt} является просто числом (взаимной информацией по Шеннону), которое оценивается моделированием процесса перехвата. При уровне ошибок Q информация Боба о просеянной последовательности Алисы есть $I_B = n[1-h_2(Q)]$. Из теоремы Чисара – Кернера [8] следует, что существуют такие коды, которые асимптотически обеспечивают получение

$$m = I_B - I_{qt} \tag{4}$$

битов ключа, информация Евы о котором асимптотически стремится к нулю. Коды, о которых идет речь, по сути объединяют коды коррекции ошибок и процедуру усиление секретности.

Существует также возможность иной стратегии перехвата, не попадающей в область применимости теоремы Чисара – Кернера, что обеспечивается наличием у Евы достаточно долговременной квантовой памяти. В настоящей работе мы рассмотрим, как информация о ПКО позволяет Еве эффективно суммировать квантовую (I_{qt}) и классическую (I_{ec}) информацию. Следует отметить, что полезность квантовой памяти для перехвата – хорошо осознаваемый факт, детально исследованный с теоретико-информационной точки зрения [9]. Однако при таком подходе, во-первых, не рассматриваются конкретные протоколы перехвата информации, а во-вторых, предполагается, что у Евы существует не только квантовая память, но и, фактически, квантовый компьютер, позволяющий осуществлять коллективное измерение многих кубитов. В настоящей работе рассмотрен случай наличия у Евы квантовой памяти, но не квантового компьютера, что достаточно для индивидуальной атаки. Эффективное использование информации, получаемой на стадии коррекции ошибок, при таком ограниченном арсенале средств перехвата до сих пор не рассматривалось. Подобный подход кажется нам тем более уместным, что прогресс в области квантовой памяти в настоящее время сильно опережает прогресс в области квантовых компьютеров. Кроме того, такой подход опирается на конструктивное описание процесса перехвата, а не просто на доказательство его возможности.

Для иллюстрации принципа перехвата в данной работе мы рассматриваем один из простейших ПКО – протокол тройного повторения, который работает следующим образом. Алиса разбивает нули своей просеянной последовательности случайным образом на блоки по три бита. Так же она поступает с единицами. Все блоки расставляются в случайном порядке. Алиса сообщает Бобу номера битов в каждой тройке и записывает их значения как биты своей исправленной последовательности. Боб выделяет из своей просеянной последовательности биты с соответствующими номерами, выбирает то значение, которое в тройке представлено большинством, и записывает его в свою исправленную последовательность. При низком уровне ошибок исправленные последовательности Алисы и Боба будут почти идентичными. Несовпадение может возникнуть только в тех случаях, когда два или все три бита в одном блоке содержат ошибки, откуда вероятность ошибки в исправленной последовательности

$$Q_B = 3(1-Q)Q^2 + Q^3. \tag{5}$$

При типичном уровне ошибок в просеянной последовательности 10^{-2} уровень ошибок в исправленной последовательности будет порядка 10^{-4}. Если такой уровень ошибок неудовлетворителен, вслед за протоколом тройного повторения может быть применен другой ПКО, доводящий вероятность ошибки до требуемого уровня.

Перейдем к описанию действий Евы по перехвату информации [4]. К каждому кубиту X, следующему по квантовому каналу, Ева присоединяет пробную четырехуровневую систему A в начальном состоянии $|\chi\rangle_A$ и со-

вершает над обеими системами унитарное преобразование U:

$$|0\rangle_X|\chi\rangle_A \to \sqrt{1-Q}\,|0\rangle_X|A\rangle_A + \sqrt{Q}\,|1\rangle_X|B\rangle_A, \tag{6}$$

$$|1\rangle_X|\chi\rangle_A \to \sqrt{1-Q}\,|1\rangle_X|C\rangle_A + \sqrt{Q}\,|0\rangle_X|D\rangle_A, \tag{7}$$

где состояния четырехуровневой пробы $|A\rangle_A$ и $|C\rangle_A$ принадлежат единому двумерному подпространству H_{AC}, а состояния $|B\rangle_A$ и $|D\rangle_A$ – единому двумерному подпространству H_{BD}, причем $H_{AC}\perp H_{BD}$, а Q и есть уровень ошибок, вносимых Евой в квантовый канал. Традиционно предполагается, что все ошибки в квантовом канале связаны с перехватом. Кроме того,

$$\langle A|C\rangle = \langle B|D\rangle = \cos\varphi = 1-2Q. \tag{8}$$

Нетрудно найти, что описанное выше унитарное преобразование U можно также записать в виде

$$|\bar{0}\rangle_X|\chi\rangle_A \to \sqrt{1-Q}\,|\bar{0}\rangle_X|A'\rangle_A + \sqrt{Q}\,|\bar{1}\rangle_X|B'\rangle_A, \tag{9}$$

$$|\bar{1}\rangle_X|\chi\rangle_A \to \sqrt{1-Q}\,|\bar{1}\rangle_X|C'\rangle_A + \sqrt{Q}\,|\bar{0}\rangle_X|D'\rangle_A, \tag{10}$$

где состояния $|A'\rangle_A$ и $|C'\rangle_A$ также принадлежат единому двумерному подпространству H'_{AC}, а состояния $|B'\rangle_A$ и $|D'\rangle_A$ – единому двумерному подпространству H'_{BD}, причем $H'_{AC}\perp H'_{BD}$. Кроме того,

$$\langle A'|C'\rangle = \langle B'|D'\rangle = \cos\varphi = 1-2Q. \tag{11}$$

После осуществления взаимодействия Ева позволяет кубиту X двигаться дальше по квантовому каналу, а пробную систему A помещает в квантовую память. Так Ева поступает со всеми $2n+2\delta$ кубитами, после чего ее квантовая память содержит такое же количество пробных систем. На стадии согласования базисов Ева перехватывает в классическом канале последовательности битов r и r' и отбрасывает все пробные системы, для которых биты в этих последовательностях различны. На стадии оценки ошибки Ева перехватывает в классическом канале номера δ битов случайной выборки и отбрасывает соответствующие пробные системы. После этого она применяет к каждой пробной системе, которой соответствует $r = r' = 1$, унитарное преобразование V, отображающее штрихованные состояния на нештрихованные: $V|Z'\rangle = |Z\rangle$, где Z принимает значения A, B, C, D. Затем каждая пробная система подвергается проективному измерению, различающему ортогональные подпространства H_{AC} и H_{BD}. Обнаружение подпространства H_{AC}, вероятность чего равна $1-Q$, означает, что данный бит в последовательности Боба – тот же, что и у Алисы. Обнаружение подпространства H_{BD}, вероятность чего равна Q, означает, что данный бит в последовательности Боба – ошибочный. В последнем случае Ева применяет к пробной системе унитарное преобразование W, удовлетворяющее соотношениям $W|B\rangle = |A\rangle$, $W|D\rangle = |C\rangle$. В результате перед стадией коррекции ошибок Ева обладает последовательностью из n систем, каждая из которых находится либо в состоянии $|A\rangle$, либо в состоянии $|C\rangle$, соответствующем 0 и 1 в просеянной последовательности Алисы.

Стандартный подход к анализу индивидуального перехвата основывается на предположении, что в момент перехвата Ева производит измерение своих пробных систем. Доказано [4], что в этом случае оптимальной стратегией для Евы будет проективное измерение каждой пробной системы в «симметрично расставленном» базисе (straddling basis), т. е. в базисе, который в подпространстве H_{AC} состоит из ортогональных векторов $\{|\zeta_0\rangle, |\zeta_1\rangle\}$, составляющих равные углы γ с векторами $|A\rangle$ и $|C\rangle$ (рис.1). Получив результат $|\zeta_0\rangle$, Ева записывает 0 в свою перехваченную последовательность, получив результат $|\zeta_1\rangle$, она записывает 1. Вероятность ошибки q при определении значения бита из рис.1 и (8) нетрудно найти:

$$q = \sin^2\gamma = \frac{1}{2}\left[1 - \sqrt{1-(1-2Q)^2}\right]. \tag{12}$$

На стадии коррекции ошибок Ева перехватывает данные о разбиении просеянной последовательности на блоки, и таким же образом разбивает на тройки битов свою перехваченную последовательность. Далее, подобно Бобу, она выбирает то значение, которое в тройке представлено большинством, и записывает его в свою исправленную последовательность. Вероятность ошибки Евы в определении значения блока $q_{\text{в}} = 3(1-q)\,q^2 + q^3$, а ее информация об исправленной последовательности (в расчете на один бит)

$$I_{\text{E}}^{(\text{s})} = 1 - h_2(q_{\text{в}}). \tag{13}$$

Оптимальность стандартной атаки обеспечивается тем фактом, что измерение в симметрично расставленном базисе является оптимальным для того, чтобы различить два неортогональных чистых состояния. Предположим теперь, что Ева сохранила свои пробные системы в квантовой памяти до стадии коррекции ошибок. Перехватив в классическом канале данные о разбиении просеянной последовательности на блоки, она разбивает свои пробные системы таким же образом. Теперь каждый блок из трех пробных систем находится либо в состоянии $|A\rangle|A\rangle|A\rangle$, либо в состоянии $|C\rangle|C\rangle|C\rangle$. Известно, что в классе индивидуальных измерений различать эти два состояния лучше всего в базисе, составляющем неодинаковые углы с векторами $|A\rangle$ и $|C\rangle$ [10]. Естественно предположить, что и оптимальный индивидуальный перехват будет связан с тем же базисом.

Рассмотрим проективное измерение подпространства H_{AC} в базисе $\{|\xi_0\rangle, |\xi_1\rangle\}$, для которого выполняются соотношения $\langle\xi_0|A\rangle = \cos\alpha$, $\langle\xi_1|C\rangle = \cos\beta$, причем в общем случае $\alpha \neq \beta$ (рис.2). Угол α будет служить парамет-

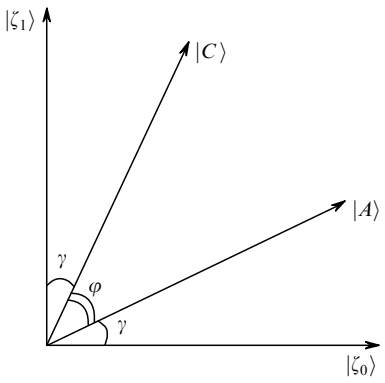

Рис.1. Базис измерения, используемый для того, чтобы различить состояния $|A\rangle$ и $|C\rangle$ при стандартной индивидуальной атаке на протокол BB84.

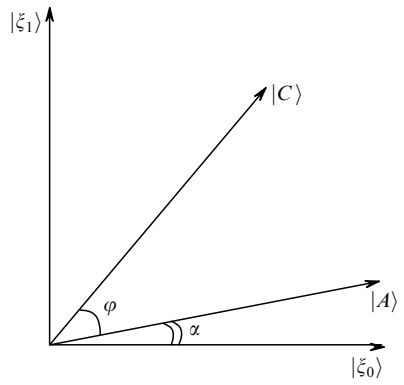

Рис.2. Базис измерения, используемый для того, чтобы различить состояния $|A\rangle$ и $|C\rangle$ при оптимизированной с учетом протокола коррекции ошибок индивидуальной атаке на протокол BB84.

ром, задающим базис, а $\beta = \pi/2 - \varphi - \alpha$. Ева подвергает описанному измерению все три пробных системы в блоке. Получив результат $|\xi_0\rangle$ и $|\xi_1\rangle$, Ева записывает 0 и 1 в свою перехваченную последовательность. Вероятность правильного определения значения 0 есть $p_0 = \cos^2\alpha$. Вероятность ошибки при определении 1 есть $q_1 = \cos^2(\alpha + \varphi)$. Далее Ева присваивает биту исправленной последовательности значение 0 только в том случае, когда все три бита в блоке равны нулю. В противном случае этому биту присваивается значение 1. Таким образом, вероятность правильно определить значение бита при перехвате блока Алисы из трех нулей равна p_0^3, а вероятность ошибки при перехвате блока из трех единиц равна q_1^3. Соответственно информация Евы об исправленной последовательности

$$I_E^{\alpha} = 1 - [h_2(p_0^3) + h_2(q_1^3)]/2\,. \tag{14}$$

Максимальное значение данного выражения при изменении угла α от 0 до $\pi/4 - \varphi/2$

$$I_E^{(m)} = \max_{\alpha} I_E^{\alpha} \tag{15}$$

может быть без труда рассчитано численно, что определяет максимально доступную Еве информацию об исправленной последовательности при оптимальном выборе базиса измерения, соответствующего некоторому углу α_m. На рис.3 приведены зависимости от Q величины $I_E^{(m)}$ вместе с информацией Евы при стандартной атаке $I_E^{(s)}$ и информацией Боба об исправленной последовательности Алисы $I_B = 1 - h_2(Q_B)$. Отчетливо видно, что перехват с учетом ПКО более информативен.

Следует отметить, что для проведения атаки, оптимизированной с учетом ПКО, Ева не нуждается в сохранении пробных систем до стадии коррекции ошибок, если ПКО был ей известен еще на стадии квантовой передачи. Сразу после стадии согласования базисов она может измерить свои системы в базисе, соответствующем углу α_m, а определение значений блоков отложить до стадии коррекции ошибок. Таким образом, оптимизация использует не саму корректирующую информацию, а только знание о конкретном выборе ПКО. Отсюда следует и метод защиты от рассмотренной атаки. В системах квантового распределения ключа можно рекомендовать шифровать ПКО при помощи специального короткого ключа. Например, перед началом квантовой передачи можно условиться о протоколе N-кратного повторения, а величину N сообщить только на стадии коррекции ошибок. Тогда в силу того, что разным значениям N соответствуют разные углы оптимального измерения α_m, Ева не сможет оптимизировать свое измерение без привлечения более долговременной квантовой памяти.

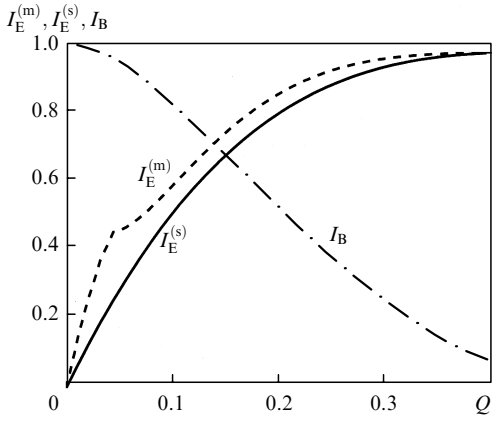

Рис.3. Зависимости количества перехваченной информации об исправленном ключе I от уровня ошибок Q в просеянном ключе при индивидуальной атаке на протокол BB84 с кодом тройного повторения для коррекции ошибок.

Итак, мы показали, что при атаке на линию квантовой криптографии знание перехватчиком протокола, выбранного пользователями для коррекции ошибок, позволяет ему оптимизировать свою атаку таким образом, чтобы увеличить количество перехваченной информации. Эта возможность была продемонстрирована на примере атаки простейшего класса – индивидуальной атаки, и было показано, что она не требует дополнительных ресурсов квантовой памяти по сравнению со стандартной индивидуальной атакой. Дальнейшее рассмотрение индивидуального перехвата с учетом протокола коррекции ошибок, опирающееся на расчет информации по Шеннону, содержится в [11].

Автор благодарит за поддержку данного исследования фонд INTAS и Европейскую комиссию (Specific Targeted Research Project EQUIND, Engineered Quantum Information in Nanostructured Diamond, funded by the FP6 IST directorate as contract number 034368).

1. Килин С.Я. *УФН*, **169**, 507 (1999).
2. Kilin S.Ya., in *Progress in Optics* (Amsterdam: Elsevier, 2001, Vol. 42, p. 1).
3. Gisin N., Ribordy G., Tittel W., Zbinden H. *Rev. Mod. Phys.*, **74**, 145 (2002).
4. Fuchs C. A., Gisin N., Griffiths R. B., Niu C.-S., Peres A. *Phys. Rev. A*, **56**, 1163 (1997).
5. Bennett C. H., Brassard G., in *Proc. of IEEE Intern. Conf. on Computers, Systems and Signal Processing* (New York: IEEE, 1984, p. 175).
6. Shannon C.E. *Bell Syst. Techn. J.*, **27**, 379 (1948).
7. Maurer U. M. *IEEE Trans. Inf. Theory*, **39**, 733 (1993).
8. Csiszar I., Korner J. *IEEE Trans. Inf. Theory*, **24**, 339 (1978).
9. Koenig R., Maurer U., Renner R. *IEEE Trans. Inf. Theory*, **51**, 2391 (2005).
10. Fuchs C. A. *Preprint of Los-Alamos National Laboratory*; quant-ph/9601020.
11. Horoshko D. *Proc. SPIE Int. Soc. Opt. Eng.*, **6726**, 67263Q (2007).