Письма в ЖЭТФ, том 81, вып. 11, с. 733 – 738 © 2005 г. 10 июня

О предельно допустимой ошибке и степени сжатия ключа 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, 119992 Москва, Россия

Поступила в редакцию 11 апреля 2005 г.

После переработки 11 мая 2005 г.

Найдена предельно допустимая величина вероятности ошибки на приемном конце, до которой возможно распространение секретного ключа. Данный результат учитывает всевозможные атаки на передаваемый ключ, в том числе с использованием большой квантовой памяти и способности подслушивателя выполнять коллективные измерения сразу над всей передаваемой последовательностью квантовых состояний. Величина критической ошибки не зависит от параметров конкретной атаки и определяется лишь через степень перекрытия информационных состояний $\varepsilon = |\langle u_1|u_0\rangle|$ и фундаментальные функции классической и квантовой теории информации ($H(Q)$ – пропускную способность классического бинарного канала связи, и классическую пропускную способность бинарного квантового канала связи – $\overline{C}(\varepsilon)$). Степень сжатия ключа после коррекции ошибок также выражается лишь через классическую пропускную способность квантового канала связи $\overline{C}(\varepsilon)$.

PACS: 03.67.Dt, 42.50.−p, 89.70.+c

Квантовая криптография – секретное распространение ключей, основана фактически на фундаментальном соотношении неопределенностей Гейзенберга [1]. Точнее, на том факте, что пара наблюдаемых, которым отвечают некоммутирующие эрмитовы операторы, не может иметь общих собственных векторов состояний. В качестве наблюдаемых в квантовой криптографии выступают, по сути, операторы матриц плотности. Для квантовой криптографии [2], где в качестве информационных состояний берется пара неортогональных состояний $0 \leftrightarrow |u_0\rangle$, $1 \leftrightarrow |u_1\rangle$, наблюдаемыми являются матрицы плотности $\rho_0 = |u_0\rangle\langle u_0|$ и $\rho_1 = |u_1\rangle\langle u_1|$. Некоммутативность операторов означает неортогональность состояний $|u_0\rangle$ и $|u_1\rangle$ ($\langle u_1|u_0\rangle \neq 0$). Вторым фундаментальным запретом квантовой механики является запрет на копирование заранее неизвестного квантового состояния [3].

Принципиально важным следствием для квантовой криптографии упомянутых выше запретов является то, что не существует в принципе измерений, которые бы позволяли с достоверностью (вероятностью единица) отличать одно неортогональное состояние от другого. Поэтому любые попытки подслушивания (измерения) передаваемых квантовых состояний приводят к их изменению, что неизбежно ведет к изменению статистики измерений на приемном конце по сравнению со статистикой измерений на невозмущенных состояниях. Если бы квантовая механика позволяла только детектировать сам факт подслушивания, то это было бы бесполезно для передачи секретных ключей. Однако законы квантовой механики гарантируют не только детектирование факта подслушивания, но и позволяют (и это есть главный интерес для криптографии) гарантировать секретность ключей при условии, что изменения статистики на возмущенных состояниях не превышают некоторой критической величины. Разумеется, возмущение состояний может возникать и без подслушивателя за счет шумов в канале связи. В этом смысле невозможно отличить действия подслушивателя от шума. Важно только, чтобы возмущение состояний не превышало некоторой критической величины. Критическая величина ошибки, до которой возможно распространение секретного ключа, является индивидуальной величиной для каждого протокола квантовой криптографии. Существует два базовых протокола квантовой криптографии – BB84 [1] и B92 [2] на двух неортогональных состояниях. Все остальные протоколы являются производными от двух базовых. Вычисление величины критической ошибки является нетривиальной задачей. Точная величина ошибки известна для протокола BB84. Первое строгое и достаточно сложное доказательство было получено в [4] (см. также [5]). Позднее это доказательство было упрощено в [6] с использованием квантовых кодов. Для протокола B92, несмотря на его концептуальную простоту, оно до сих пор отсутствует.

Ниже будет приведен набросок доказательства секретности протокола B92, основанный на точных границах для классической пропускной способности квантового канала связи.

Протокол выглядит стандартным образом. Alice случайно и равновероятно (с априорными вероятностями $\pi_0 = \pi_1 = 1/2$) выбирает 0 или 1 и посылает в канал связи, соответственно, $|u_0\rangle$ или $|u_1\rangle$. Bob производит измерения последовательно над каждым состоянием, измерение описывается разложением единицы:

$$I = A_0 + A_1 + A_?, \quad A_0 = \frac{I - |u_1\rangle\langle u_1|}{1 + \langle u_0|u_1\rangle}, \\ A_1 = \frac{I - |u_0\rangle\langle u_0|}{1 + \langle u_0|u_1\rangle}, \quad A_? = I - A_0 - A_1. \tag{1}$$

При таком измерении возможны три исхода, которые интерпретируются Bob как 0,1 и ?. Результат измерения в канале A_0 никогда не имеет место на состоянии $|u_1\rangle$. Соответственно, исход в канале A_1 никогда не возможен на состоянии $|u_0\rangle$. Исход ? интерпретируется как неопределенный результат, поскольку отсчет в канале $A_?$ может иметь место как на состоянии $|u_0\rangle$, так и на состоянии $|u_1\rangle$.

Наиболее общая стратегия Eve сводится к тому, что она выбирает некоторое вспомогательное состояние $|A\rangle \in \mathcal{H}$ достаточно большой размерности, далее накапливает всю переданную Alice последовательность квантовых состояний длиной n, при этом пока ничего не посылая Bob. И приводит во взаимодействие со всеми состояниями:

$$\mathcal{U}(|u_{i_1}\rangle \otimes |u_{i_2}\rangle \otimes ...|u_{i_n}\rangle \otimes |A\rangle) = |\Phi_{i_1,i_2,..i_n,A}\rangle, \tag{2}$$

где состояние $|\Phi_{i_1,i_2..i_n,A}\rangle$ является запутанным по всем состояниям $|u_{i_k}\rangle$ и исходному состоянию Eve $|A\rangle$. Далее, не производя никаких измерений, Eve последовательно перепосылает состояния $|u_{i_k}\rangle$ к Bob. Bob производит последовательно измерения (1) над каждым состоянием. Возникает последовательность исходов в каналах измерения $A_{0,1,?}$. После измерений над всей последовательностью состояние Eve оказывается следующим

$$\mathrm{Tr}_{Bob}\{\sqrt{A_{j_n}}\sqrt{A_{j_{n-1}}}...\sqrt{A_{j_1}}\mathcal{U}(\rho_{i_1} \otimes \rho_{i_2} \otimes \\ \otimes ...\rho_{i_n} \otimes |A\rangle\langle A|)\mathcal{U}^+\sqrt{A_{j_1}}\sqrt{A_{j_2}}...\sqrt{A_{j_n}}\} = \\ = \rho^{Eve}_{i_1,i_2...i_n}(j_1, j_2, ...j_n), \tag{3}$$

где

$$\rho_{i_k} = |u_{i_k}\rangle\langle u_{i_k}|, \quad j_k = 0, 1, ?. \tag{4}$$

Bob может получить как исходы в каналах $A_{0,1}$, которые интерпретируются как 0 и1, так и результаты с неопределенным исходом $A_?$. Исходы с неопределенным результатом отбрасываются путем обмена информацией Bob с Alice через открытый канал связи, через который Bob сообщает номера позиций, где такой результат был получен. Eve, имея информацию из открытого канала связи, также "вычеркивает" эти позиции. Фактически для этого достаточно взять частичный след по степеням свободы в состоянии $|\Phi_{i_1,i_2..i_n,A}\rangle$, которые связаны с номерами $j_k?$, где $j_k?$ – номера позиции с исходом ?. В результате состояние Eve оказывается следующим:

$$\mathrm{Tr}_{j_{k_1}?,j_{k_2}?,...j_{k_n}?}\{\rho^{Eve}_{i_1,i_2...i_n}(j_1, j_2, ...j_n)\} = \\ = \rho^{Eve}_{\underbrace{i_1,i_2...i_n}_{\text{нет}_{k_1,...k_n}}} \underbrace{(j_1, j_2, ...j_n)}_{\text{нет}_{j_{k_1}?,...j_{k_n}?}}. \tag{5}$$

После проведения измерений Bob и отбрасывания результатов с неопределенным исходом (?) участники протокола оказываются в следующей ситуации. Alice знает, какие состояния она посылала, Eve имеет матрицу плотности, а Bob битовую строку

$$|\mathbf{u}\rangle_\mathbf{i} = \underbrace{|u_{i_1}\rangle \otimes ... \otimes |u_{i_n}\rangle}_{(i_1,.....i_n)} \to \rho^{Eve}_{i_1,i_2...i_n}(j_1, j_2, ...j_n) \to \\ \to (j_1, ...j_n), \quad j_k, i_k = 0, 1. \tag{6}$$

Здесь считается, что произведена перенумерация индексов после отбрасывания исходов ?, и длина оставшейся строки обозначена тем же символом n, что и ранее. В некоторых позициях у Bob имеются ошибки. Несоответствие индексов посылаемых состояний и полученных результатов для некоторых индексов $i_k \neq j_k$ возникает за счет возмущения состояний, передаваемых Alice подслушивателем. Вероятность ошибочных позиций выясняется Alice и Bob через открытый канал связи путем оглашения случайной выборки позиций и их содержимого (примерно половины n). Доля несоответствия дает величину вероятности ошибки Q. Затем раскрытые позиции отбрасываются. Eve также отбрасывает состояния, относящиеся к этим позициям, так как это было обсуждено выше.

С этого момента цель Alice и Bob получить секретный ключ путем исправления ошибок в нераскрытой части последовательности посредством обсуждений через открытый канал связи. Если вероятность ошибок $Q < Q_c$ меньше критической величины, которую еще нужно установить, то протокол продолжается, в противном случае, $Q > Q_c$, протокол прерывается.

Фактически цель Eve состоит в том, чтобы посредством квантовомеханических измерений над $\rho^{Eve}_{i_1,i_2...i_n}(j_1, j_2, ...j_n)$ "привязаться" к битовой строке Alice $(i_1, i_2, ...i_n)$, то есть различить конкретную матрицу плотности $\rho^{Eve}_{i_1,i_2...i_n}(j_1, j_2, ...j_n)$ из множест-

ва 2^n других матриц плотности, которым отвечают другие наборы индексов $(i_1, i_2, ...i_n)$ при заданных $(j_1, j_2, ..., j_n)$. Мерой близости матрицы плотности Eve и посланной Alice является величина (fidelity)

$$F(|\mathbf{u}\rangle_{\mathbf{i}}, \rho^{Eve}) = \tag{7}$$

$$= \mathrm{Tr}_{Eve}\{\sqrt{|\mathbf{u}\rangle_{\mathbf{ii}}\langle\mathbf{u}|}\rho^{Eve}_{i_1,i_2...i_n}(j_1, j_2, ..., j_n)\sqrt{|\mathbf{u}\rangle_{\mathbf{ii}}\langle\mathbf{u}|}\} \leq 1,$$

причем $F(|\mathbf{u}\rangle_{\mathbf{i}}, \rho^{Eve}) = 1$ тогда и только тогда, когда

$$\rho^{Eve}_{i_1,i_2...i_n}(j_1, j_2, ..., j_n) = |\mathbf{u}\rangle_{\mathbf{ii}}\langle\mathbf{u}|. \tag{8}$$

При подслушивании всегда

$$\rho^{Eve}_{i_1,i_2...i_n}(j_1, j_2, ..., j_n) \neq |\mathbf{u}\rangle_{\mathbf{ii}}\langle\mathbf{u}|, \tag{9}$$

поскольку в противном случае это бы противоречило теореме о запрете на копирование (no cloning), то есть Eve могла бы получать информацию о неортогональных состояниях без их возмущения. Состояние Eve в результате взаимодействия не может точно совпадать с передаваемым состоянием. Для этого достаточно рассмотреть попарно все передаваемые Alice состояния. Пусть пара таких состояний $|\mathbf{u}\rangle_{\mathbf{i}}$ и $|\mathbf{u}\rangle_{\mathbf{m}}$. В результате совместной эволюции и дальнейшего взятия следа по переменным Bob, имеем $\rho^{Eve}_{i_1,i_2...i_n}(j_1, j_2, ...j_n)$ и $\rho^{Eve}_{m_1,m_2...m_n}(j_1, j_2, ...j_n)$. Причем скалярное произведение между этими двумя состояниями Eve $\mathrm{Tr}\{\rho^{Eve}_{i_1,i_2...i_n}(j_1, j_2, \ldots j_n)\rho^{Eve}_{m_1,m_2...m_n}(j_1, j_2, \ldots j_n)\} \leq$ $\leq |_{\mathbf{i}}\langle\mathbf{u}|\mathbf{u}\rangle_{\mathbf{m}}|^2$, то есть перекрытие состояний у Eve не может стать меньше, чем у исходных состояний, посланных Alice. Уменьшение скалярного произведения (увеличение угла) означало бы увеличение различимости состояний по сравнению с исходными. Если бы такое было возможно, то используя свои новые состояния опять как входные для унитарного преобразования, можно было бы еще увеличить угол между ними (увеличить различимость), и т.д. до их полной (достоверной) различимости, что противоречило бы теореме [2]. Таким образом, "уступая" в пользу Eve, можно считать: лучшее, что может иметь Eve, так это исходные состояния, посланные Alice. Максимум классической информации, которые может извлечь Eve из этих состояний, ограничено *классической пропускной способностью квантового канала связи, которая в данном случае совпадает с энтропией фон Неймана.*

Консервативная оценка, завышающая получение информации Eve в ее пользу, сводится к равенству (8).

Перейдем теперь к вычислению критической величины ошибку Q_c, до которой возможно распространение секретного ключа между Alice и Bob. Приведем набросок доказательства в шенноновском пределе. На данной стадии Alice и Bob имеют битовые строки, причем вероятность ошибки у Bob есть Q. Такая ситуация отвечает симметричному классическому бинарному каналу связи между Alice и Bob. Далее Alice случайно в соответствии с равновероятным распределением на множестве всех 2^n битовых строк длины n генерирует $M_{AB} - 1$ строк и помещает M_{AB} строк вместе с переданной строкой $(i_1, i_2...i_n)$ в открытый и доступный всем справочник:

$$\left\{\begin{array}{c} l_1, l_2, ...l_n \\ r_1, r_2, ...r_n \\ ..... \\ \underline{i_1, i_2, ...i_n} \\ k_1, k_2, ...k_n \end{array}\right\} = M_{AB} \leq 2^{n[H(Q)-\delta]}, \tag{10}$$

$$\delta \to 0, \quad n \to \infty,$$

где

$$H(Q) = 1 + Q\log Q + (1-Q)\log(1-Q) \tag{11}$$

пропускная способность классического бинарного симметричного канала связи.

Если $M_{AB} \leq 2^{n[H(Q)-\delta]}$, то, согласно прямой теореме кодирования для бинарного классического канала связи, Bob с вероятностью единица выберет из множества M_{AB} строк правильную строку $(i_1, i_2, ...i_n)$. Фактически Bob должен сравнить все M_{AB} строк со своей и выбрать ту, которая наиболее близка к его строке в смысле расстояния Хэмминга (имеет отличие в минимальном числе позиций) [7, 8]. После этого Alice и Bob будут иметь с вероятностью единица одинаковые битовые строки, то есть вероятность неправильного декодирования по всем кодовым словам

$$P_e(n, M_{AB}) < (M_{AB} - 1)2^{-n[H(Q)-\delta]} < \varepsilon(n, M_{AB}) \to 0 \tag{12}$$

стремится к нулю при $n \to \infty$ и при условии, что $M_{AB} \leq 2^{n[H(Q)-\delta]}$.

Перейдем теперь к Eve. Открытое оглашение Alice в "справочнике" набора кодовых слов (10) говорит Eve о том, что могла быть послана одна из строк квантовых состояний $|u_{a_1}\rangle \otimes |u_{a_2}\rangle \otimes ...|u_{a_n}\rangle$, соответствующая одному из наборов индексов $(a_1, a_2, ..., a_n)$, сгенерированных Alice в (10). Фактически Eve должна отличить одну единственную правильную строку $|\mathbf{u_i}\rangle$ из набора M_{AB} кодовых строк, посланную Alice. Прямая теорема кодирования для *классической пропускной способности квантового канала связи* [9] гласит (см. также [10]), что вероятность правильного декодирования (различения) равна единице (Eve сможет узнать правильную строку), если число кодовых слов $M_{Eve} \leq 2^{n[\overline{C}(\varepsilon)-\delta]}$, где $\overline{C}()$ – *классическая про-*

пускная способность квантового канала связи, впервые доказанная в [9], которая в нашем случае равна

$$\overline{C}(\varepsilon) = -\left(\frac{1-\varepsilon}{2}\right)\log\left(\frac{1-\varepsilon}{2}\right) - \left(\frac{1+\varepsilon}{2}\right)\log\left(\frac{1+\varepsilon}{2}\right), \quad \varepsilon = |\langle u_0|u_1\rangle|. \qquad (13)$$

Недавно доказанная теорема так называемого сильного обращения теоремы кодирования для квантовых каналов связи [11] гласит, что если число кодовых слов $M_{Eve} > 2^{n[\overline{C}(\varepsilon)-\delta]}$, то вероятность правильного декодирования (различения нужной строки) равна нулю. Точнее, вероятность правильного декодирования стремится к нулю, соответственно, вероятность ошибки стремится к единице как

$$P_e(n, M_{Eve}) > 1 - 2^{-n\cdot\alpha\cdot(\overline{C}(\varepsilon))} \to 1, \qquad (14)$$

где $\alpha(\overline{C}(\varepsilon))$ – некоторая функция.

Это означает, что при условии $M_{AB} > M_{Eve}$ Eve не сможет узнать строку бит у Alice и Bob, в то же время Bob сумеет с вероятностью единица исправить ошибки в своей строке, вызванные подслушивателем, и будет иметь одинаковую с Alice строку бит, которую не будет знать Eve. Данная строка является общим секретным ключом Alice и Bob. Таким образом, критическая величина ошибки, до которой возможно распространение секретного ключа, определяется из условия

$$\overline{C}(\varepsilon) = H(Q_c); \qquad (15)$$

Q_c выражается лишь через фундаментальные величины и учитывает всевозможные атаки Eve на передаваемый ключ. При условии (15) квантовая криптография гарантирует секретность ключа, даже если у Eve имеется квантовая память большого размера и если Eve может делать коллективные измерения (фактически, экспериментально реализовать проекцию на сцепленные (запутанные) состояния).

Предыдущие рассуждения, которые использовались при генерации секретного ключа при $Q < Q_c$, не являются конструктивными, поскольку используют идеологию случайного кодирования Шеннона и требуют экспоненциально большого блокнота из кодовых слов. При случайном кодировании достигается максимальная длина ключа, то есть ошибки у Bob исправляются самым эффективным способом. Все остальные, конструктивно реализуемые методы исправления ошибок, дают меньшую длину финального секретного ключа. Однако для квантовой криптографии не столь важна эффективность в смысле длины ключа, а важнее гарантировать, что финальный ключ является секретным. Секретность на формальном языке означает, что взаимная информация между ключом легитимных пользователей и Eve, которая имеет конкретную битовую строку, экспоненциально мала по любому наперед выбранному параметру секретности. Поэтому после исправления ошибок в битовой строке Bob легитимные пользователи используют процедуру сжатия ключа. После сжатия (случайного хэширования) ключа возникает финальный секретный ключ, и Eve имеет о нем сколь угодно малую информацию. Это обстоятельство гарантируется строгой математической теоремой [12], которая носит название теоремы об усилении секретности (privacy amplification theorem).

Пусть $x \in X$ – случайная величина с распределением $P_X(x)$, и $R(X)$ – энтропия Реньи второго порядка

$$R(X) = -\log P_c(X), \quad P_c(X) = \sum_{x\in X} P_X^2(x), \qquad (16)$$

где $P_c(X)$ – вероятность коллизий, то есть вероятность того, что в двух последовательных испытаниях случайная величина примет одно и то же значение. Аналогичные соотношения имеют место для условных распределений

$$R(X|Y) = -\sum_{y\in Y} P_Y(y) R(X|Y=y). \qquad (17)$$

Для дальнейшего при вычислении взаимной информации Eve о ключе важны следующие соотношения между энтропией Шеннона $H(X)$ и энтропией Реньи $R(X)$:

$$R(X) \le H(X), \; H(X) = -\sum_{x\in X} P_X(x)\log P_X(x), \quad R(X|Y) \le H(X|Y). \qquad (18)$$

Пусть теперь $g \in G$ – случайная величина с равномерным распределением на множестве универсальных хэш-функций G второго порядка [13], $g: X = \{0,1\}^n \to \{0,1\}^r$ и $K = G(x)$, тогда имеет место

$$H(K|G) \ge R(K|G) \ge r - \log(1 + 2^{r-R(X)}) \ge r - \frac{2^{r-R(x)}}{\ln(2)}, \qquad (19)$$

где $H(K|G) = H(G(X)|G)$ – средняя условная энтропия Шеннона. Здесь хэш-функция сама является случайной величиной.

Применительно к задачам квантовой криптографии важно следующее следствие теоремы. Пусть имеется совместное распределение вероятностей P_{XY}, которое, вообще говоря неизвестно. Здесь $X = \{0,1\}^n$ – множество битовых строк у легитимных пользователей Alice и Bob, которые после коррекции ошибок у них уже одинаковые, а $Y = \{0,1\}^c$ – множество битовых строк у Eve. Если

энтропия Реньи $R(X|Y=y)=c$ и если Alice и Bob выбирают хэш-значения от своих (одинаковых) строк $K=G(X)$ в качестве секретного ключа, причем хэш-функция из $\{0,1\}^n \to \{0,1\}^r$ выбирается случайно и равновероятно из G, то имеет место

$$H(K|G,Y=y) \geq R(K|G,Y=y) \geq \\ \geq r - \log(1+2^{r-c}) \geq r - \frac{2^{r-c}}{\ln(2)}, \qquad (20)$$

то есть информация Eve о ключе экспоненциально мала по параметру $c-r$. Условная энтропия Реньи $R(X|Y=y)$ выражается через условные вероятности $P_{X|Y}(X=x|Y=y)$ уже после коррекции ошибок в ключе. Условная вероятность $P_{X|Y}(X=x|Y=y)$ – вероятность того, что данная конкретная битовая последовательность Eve $Y=y$ произошла из некоторой битовой строки у Alice и Bob $X=x$.

Для взаимной информации Eve о секретном ключе имеем

$$I(K;GY) = H(K) - H(K|GY) \leq \frac{2^{-s}}{\ln(2)}, \quad H(K)=r, \qquad (21)$$

где s – параметр секретности, который выбирается легитимными пользователями. Если после коррекции ошибок оставалась строка длиной n, то длина оставшегося ключа определяется как

$$r = c - s, \qquad (22)$$

что и определяет степень сжатия ключа после коррекции ошибок. Энтропия Шеннона $H(K)$, по сути, есть энтропия равномерно распределенной случайной величины на множестве финальных ключей $K=\{0,1\}^r$, равномерность обеспечивается универсальностью хэш-функции.

Теперь задача сводится к получению границы для условной энтропии Реньи (17). Получим эту фундаментальную границу, которая определяется другой фундаментальной величиной – *классической пропускной способностью квантового канала связи* [9].

Если используются процедуры исправления ошибок, например, *Binary* [14] или *Cascade с выбрасыванием ошибочных бит* [15], то после коррекции ошибок все участники протокола оказываются в ситуации

$$|\mathbf{u}\rangle_{\mathbf{i}} = \underbrace{|u_{i_1}\rangle \otimes ... \otimes |u_{i_n}\rangle}_{(i_1,.....i_n)} \to \rho^{Eve}_{i_1,i_2...i_n}(i_1,i_2,...i_n) \to \\ \to (i_1,....i_n), \quad i_k = 0,1. \qquad (23)$$

Здесь n – длина оставшейся строки уже после коррекции ошибок. Alice и Bob имеют одинаковые битовые строки, имеется однозначное соответствие между состояниями, которые посылала Alice $|u_{i_k}\rangle$ и битами у Bob $i_k \leftrightarrow |u_{i_k}\rangle$. Eve имеет матрицу плотности квантовых состояний, из которой ей еще предстоит посредством измерений получить битовую строку. Консервативная оценка в пользу Eve сводится к тому, что наиболее близкая матрица плотности Eve к передаваемой Alice последовательности квантовых состояний будет, если $\rho^{Eve}_{i_1,i_2...i_n}(i_1,i_2,...i_n) = \rho_{i_1} \otimes \rho_{i_2} \otimes ... \otimes \rho_{i_n}$, где $\rho_{i_k} = |u_{i_k}\rangle\langle u_{i_k}|$ (по сути, для этого проводятся рассуждения аналогичные предыдущим при выводе (7)–(9)).

Цель Eve – узнать набор индексов $y=(j_1,j_2,...j_n)$ посредством квантовомеханических измерений. Число областей декодирования (множество индексов y), которые Eve может декодировать при больших n с нулевой вероятностью ошибки, не превосходит $2^{n\overline{C}(\varepsilon)}$. При этом число кодовых слов, которые находятся в каждой области декодирования и, соответственно, декодируются в одно кодовое слово – набор индексов $y=(j_1,j_2,...j_n)$, равно $2^n/2^{n\overline{C}(\varepsilon)}$. Далее, измерения с $2^{n\overline{C}(\varepsilon)}$ исходами описываются разложением единицы

$$I = \sum_{y\in Y} X_y, \quad y \in Y = \{0,1\}^t, \quad t = n\overline{C}(\varepsilon), \qquad (24)$$

где X_y – измеряющие операторы, "привязанные" к области декодирования y. Условная вероятность того, что Alice была послана последовательность состояний $\rho_x = \rho_{i_1} \otimes \rho_{i_2} \otimes ... \otimes \rho_{i_n}$ $(x=(i_1,i_2...i_n))$, а Eve получила результат $y=(j_1,j_2,...j_n)$, есть

$$P_{X|Y}(X=x|Y=y) = \mathrm{Tr}\{\rho_x \cdot X_y\}. \qquad (25)$$

Поскольку Alice посылает состояния в каждой посылке, равновероятно, то $P_X(x)=1/2^n$. Далее имеем

$$P_{X|Y}(X|Y=y) = \\ = \sum_{x\in X_y} P_X(x) P_{X|Y}(X=x|Y=y) = \\ = \frac{1}{2^n}\sum_{x\in X_y} P_{X|Y}(X=x|Y=y) = \frac{2^{n\overline{C}(\varepsilon)}}{2^n}. \qquad (26)$$

Здесь X_y – множество слов, посланных Alice, которые при измерениях Eve декодируются в одно и то же кодовое слово – набор индексов $y=(j_1,j_2,...j_n)$.

Перейдем теперь к степени сжатия ключа (см. детали в [12–16]). Пусть Alice и Bob выбирают в качестве секретного ключа сжатую случайной универсальной хэш-функцией $G: X=\{0,1\}^n \to K=\{0,1\}^r$ строку из r бит – $K=G(X)$. Если значение r выбирается равным $r=n-t-s=n(1-\overline{C}(\varepsilon))-s$, где s – параметр секретности, то взаимная информация Eve о ключе

$$I(K;GY) \leq 2^{-s}/\ln(2). \qquad (27)$$

Вероятность коллизий и условная энтропия Реньи в этом случае равны

$$P_c(X|Y=y) = \frac{2^n}{2^{n\overline{C}(\varepsilon)}} \left(\frac{2^{n\overline{C}(\varepsilon)}}{2^n} \right)^2 ,$$
$$R(X|Y=y) = -\log(P_c(X|Y=y)) = n(1-\overline{C}(\varepsilon)). \quad (28)$$

Грубо говоря, условная энтропия Реньи дает количество бит на строку, которые Eve не знает с вероятностью единица. Eve знает с вероятностью единица число на строку не более $n\overline{C}(\varepsilon)$ – длина строки умноженная на *классическую пропускную способность квантового канала связи*. И, соответственно, с вероятностью единица не знает $n(1-\overline{C}(\varepsilon))$ бит, такое количество бит из строки после хэширования может быть использовано как секретный ключ.

Величина перекрытия состояний (степень их различимости) $\langle u_0|u_1\rangle$ выбирается легитимными пользователями в начале протокола и считается всем известной. Данная величина является независимой от наблюдаемой величины вероятности ошибки Q. В этом смысле не существует оптимального значения степени перекрытия. Нужно только заметить, что увеличение степени перекрытия приводит к увеличению количества исходов с неопределенным исходом на приемном конце, которые отбрасываются, что снижает скорость генерации ключа.

Таким образом, протокол B92 обеспечивает секретность ключа при условии, что наблюдаемая ошибка на приемном конце у Bob не превышает критической величины, определяемой условием (15). Данный результат учитывает всевозможные атаки Eve на передаваемый ключ, в том числе с использованием большой квантовой памяти и способности выполнять коллективные измерения сразу над всей переданной последовательностью (так называемые проекции на запутанные или, по терминологии [9], сцепленные состояния). Величина критической ошибки не зависит от параметров конкретной атаки и определяется лишь через степень перекрытия информационных состояний $\varepsilon = |\langle u_1|u_0\rangle|$ и фундаментальные функции классической и квантовой теории информации ($H(Q)$ – пропускную способность классического бинарного канала связи, и классическую пропускную способность бинарного квантового канала связи – $\overline{C}(\varepsilon)$). Степень сжатия ключа после коррекции ошибок также выражается лишь через классическую пропускную способность квантового канала связи $\overline{C}(\varepsilon)$.

Отметим в заключение, что если Eve может делать лишь индивидуальные измерения над состоянием в каждой посылке, то величина критической ошибки, до которой возможно распространение секретного ключа, будет определяться так называемой классической пропускной способностью квантового канала за один шаг (one shot) [9], которая равна

$$C_1(\varepsilon) = \tfrac{1}{2}\left[(1+\sqrt{1-\varepsilon^2})]\log(1+\sqrt{1-\varepsilon^2}) + \right.$$
$$\left. +(1-\sqrt{1-\varepsilon^2})]\log(1-\sqrt{1-\varepsilon^2})\right] , \quad (29)$$

и всегда $C_1(\varepsilon) < \overline{C}(\varepsilon)$. В этом случае в формуле (28) для степени сжатия ключа также будет фигурировать $C_1(\varepsilon)$ вместо $\overline{C}(\varepsilon)$.

Работа поддержана проектом Российского фонда фундаментальных исследований # 05-02-17837 и INTAS # 04-77-7284.

1. C. H. Bennett, 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.
2. C. H. Bennett, Phys. Rev. Lett. **68**, 3121 (1992); C. H. Bennett, G. Brassard, and N. D. Mermin, Phys. Rev. Lett. **68**, 557 (1992).
3. W. K. Wootters and W. H. Zurek, Nature **299**, 802 (1982).
4. D. Mayers, A. Yao, quant-ph/9802025.
5. E. Biham, M. Boyer, P. O. Boykin et al., quant-ph/9912053.
6. P. W. Shor and J. Preskill, quant-ph/0003004.
7. C. E. Shannon, Bell Syst. Tech. Jour. **27**, 397; **27**, 623 (1948).
8. Р. Галлагер, М.: Советское радио, 1974; J. Wolfowitz, Illinois J. of Math., **1**, 591 (1957).
9. А. С. Холево, Проблемы передачи информации **8**, 63 (1972); **15**, 3 (1979); Успехи математических наук **53**, 193 (1998); *Введение в квантовую теорию информации*, серия *Современная математическая физика, вып.5*, МЦНМО, Москва, 2002.
10. R. Jozsa and B. Schumacher, J. Mod. Optics. **41**, 2343 (1994); P. Hausladen, R. Jozsa, B. Schumacher et al., Phys. Rev. **A54**, 1869 (1996); B. Schumacher and M. D. Westmoreland, Phys. Rev. **A56**, 131 (1997).
11. T. Ogawa and H. Nagaoka, quant-ph/9808063.
12. C. H. Bennett, G. Brassard, C. Crépeau, and U. Maurer, IEEE Transaction on Information Theory **41**, 1915 (1995).
13. J. L. Carter and M. N. Wegman, J. of Computer and System Sciences **18**, 143 (1979).
14. C. H. Bennett, F. Bessette, G. Brassard et al., J. of Cryptology **5**, 3 (1992).
15. G. Brassard and L. Salvail, Lecture Notes in Computer Science **765**, 410 (1994).
16. А. П. Маккавеев, С. Н. Молотков, Д. И. Помозов, А. В. Тимофеев, *О практических методах "чистки" ключей в квантовой криптографии*, ЖЭТФ (в печати).