ЖЭТФ, 2006, том 130, вып. 2 (8), стр. 228–238

О НЕКОТОРЫХ КОНСЕРВАТИВНЫХ ОЦЕНКАХ В КВАНТОВОЙ КРИПТОГРАФИИ

С. Н. Молотков*

[a] *Институт физики твердого тела Российской академии наук*
142432, Черноголовка, Московская обл., Россия

[b] *Факультет вычислительной математики и кибернетики,*
Московский государственный университет им. М. В. Ломоносова
119992, Москва, Россия

Поступила в редакцию 14 марта 2006 г.

Установлена связь секретности квантового криптографического протокола распространения ключей *BB84* с прямой и обратной теоремами кодирования для квантовых каналов связи. Величина критической ошибки $Q_c \approx 11\,\%$, до которой гарантируется секретность распространения ключей, фактически определяется решением трансцендентного уравнения $H(Q_c) = \overline{C}(\rho)/2$, где ρ — матрица плотности ансамбля квантовых состояний, генерируемых на передающем конце, $\overline{C}(\rho)$ — классическая пропускная способность идеального квантового канала связи, $H(Q)$ — пропускная способность классического симметричного бинарного канала связи с вероятностью ошибки Q.

PACS: 03.67.Dd, 42.50.-p, 89.70.+c

1. ВВЕДЕНИЕ

Любая квантовая криптографическая система распределения ключей (квантовая криптография) гарантирует секретность ключей, если вероятность ошибки на приемном конце не превышает некоторой критической величины. Наиболее известным и широко используемым квантовым криптографическим протоколом распределения ключей является протокол *BB84*, предложенный в классической работе [1].

Доказательство секретности квантовой криптографии сводится к решению следующих задач. Первая задача при анализе любого квантового криптографического протокола состоит в выяснении величины критической ошибки, до которой возможно распространение секретного ключа. Вторая задача, если величина ошибки меньше критической величины, состоит в вычислении длины финального секретного ключа после исправления ошибок в первичном ключе.

Существует несколько доказательств секретности протокола *BB84*. Доказательство, предложенное в работе [2], является достаточно простым, но предполагает использование квантовой памяти легитимными пользователями (Alice и Bob). Строгое и достаточно формальное доказательство приведено в работе [3]. Это доказательство не требует использования квантовой памяти легитимными пользователями. Однако это доказательство является достаточно сложным для понимания и не имеет простой интуитивной интерпретации. То же самое можно сказать про доказательство, предложенное в работе [4]. Позднее в работе [5] было приведено относительно простое доказательство секретности протокола *BB84*, которое основано на «виртуальном» использовании квантовых кодов. Наконец, в недавней работе [6] с использованием обобщенной процедуры усиления секретности (privacy amplification) была показана секретность протокола *BB84* и ряда других квантовых криптографических протоколов (например, *E91* [6]).

Естественными и фундаментальными величинами, фигурирующими в любом квантовом криптографическом протоколе, являются следующие функции.

1. Энтропия Шеннона, которая описывает классический источник на передающем конце.

*E-mail: molotkov@issp.ac.ru

2. Энтропия фон Неймана для ансамбля квантовых состояний, ассоциированных с классическим источником. Энтропия фон Неймана совпадает в случае идеального канала связи с классической пропускной способностью квантового канала связи и является верхней границей для классической информации, которая может быть извлечена из ансамбля квантовых состояний посредством квантовомеханических измерений.

3. И, наконец, еще одна фундаментальная величина, — это пропускная способность бинарного симметричного классического канала связи, которая дает верхнюю границу классической информации, которая может быть получена легитимными пользователями при реально наблюдаемом потоке ошибок на приемном конце.

Исходно никаких других функций в задаче о распространении ключей нет, поэтому естественно думать, что их достаточно для доказательства секретности протокола, и не требуется привлекать другие, не фигурирующие исходно в задаче величины. Ниже будет приведен набросок доказательства секретности протокола *BB84*, который использует только данные фундаментальные функции классической и квантовой теории информации. Доказательство основано на строгих границах для классической пропускной способности квантового канала связи, точнее, на прямой теореме кодирования [7] и на так называемом сильном обращении, доказанном в работе [8].

2. КВАНТОВЫЙ ПРОТОКОЛ РАСПРОСТРАНЕНИЯ КЛЮЧА *BB*84

2.1. Энтропия Шеннона классического источника

Основная идея квантовой криптографии состоит в том, что вторжение в квантовый канал связи приводит к возмущению квантовых состояний и появлению ошибок на приемном конце. Любой квантовый криптографический протокол гарантирует секретность передаваемых ключей, если процент ошибок не превышает некоторой критической величины. К ошибкам на приемном конце приводят также неидеальность системы и собственные шумы в канале связи. Принципиально невозможно различить ошибки, вызванные подслушивателем, и ошибки, возникающие вследствие наличия шумов в канале связи, поэтому все наблюдаемые ошибки относят к действиям подслушивателя.

Первая задача состоит в выяснении величины критической ошибки на приемном конце, до которой возможно распространение секретного ключа.

Протокол *BB84* выглядит стандартным образом. Пользователь на передающем конце (Alice) имеет классический источник, который генерирует последовательность символов классического алфавита

$$X = \{x_i^j\}, \quad i,j = 0,1, \quad x_i^j = (ij).$$

Априорные вероятности появления символов классического алфавита $\pi_{ij} = 1/4$. Шенноновская классическая энтропия источника равна

$$H(X) = -\sum_{i,j=0,1} \pi_{ij} \log \pi_{ij} = 2 \tag{1}$$

и описывает количество информации в битах в пересчете на одну посылку, которое необходимо, для того чтобы полностью описать источник сообщений. Другими словами, прямая теорема кодирования для классического источника гласит, что минимальное количество бинарных строк $\{x_{i_1}^{j_1}, x_{i_2}^{j_2}, \dots x_{i_n}^{j_n}\}$ (кодовых слов) M_{class} длины n, необходимых, чтобы полностью характеризовать информацию, генерируемую источником без ее потери, не может быть меньше величины

$$M_{class} \geq 2^{nH(X)}, \quad n \to \infty. \tag{2}$$

Пусть теперь каждому символу классического алфавита Alice ставит в соответствие квантовые состояния по следующему правилу:

$$x_i^j \to |\varphi_i^j\rangle, \tag{3}$$

которые направляются через канал связи на приемную сторону (Bob). Здесь $i = 0$, $j = 0$ и $i = 0$, $j = 1$ отвечают, соответственно, 0 и 1 в базисе «+»:

$$|\varphi_0^0\rangle = |0\rangle, \quad |\varphi_0^1\rangle = |1\rangle, \tag{4}$$

где $|0\rangle$ и $|1\rangle$ — ортогональные базисные состояния двухуровневой системы. Далее, $i = 1$, $j = 0$ и $i = 1$, $j = 1$ отвечают, соответственно, 0 и 1 в базисе «×»:

$$|\varphi_1^0\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle), \quad |\varphi_1^1\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle). \tag{5}$$

Под ортогональными базисными состояниями $|0\rangle$ и $|1\rangle$ могут пониматься, например, состояния поляризации $|\updownarrow\rangle$ и $|\leftrightarrow\rangle$.

Кодовым словам классического источника ставятся в соответствие кодовые слова из квантовых состояний, которые последовательно посылаются через канал связи на приемную сторону к Bob:

$$\begin{gathered} w_{\vec{i}}^{\vec{j}} = \{x_{i_1}^{j_1}, x_{i_2}^{j_2}, \dots, x_{i_n}^{j_n}\} \to |w_{\vec{i}}^{\vec{j}}\rangle = \\ = |\varphi_{i_1}^{j_1}\rangle \otimes \dots \otimes |\varphi_{i_n}^{j_n}\rangle, \\ \vec{i} = (i_1, \dots, i_n), \quad \vec{j} = (j_1, \dots, j_n). \end{gathered} \tag{6}$$

Всего существует

$$M_{class} = 2^{nH(X)} = 2^{2n}$$

кодовых слов. При передаче ключа в квантовый канал связи с равной вероятностью $1/2^{2n}$ посылается одно из 2^{2n} квантовых кодовых слов, причем отдельные квантовые состояния из кодового слова $|\varphi_{i_k}^{j_k}\rangle$ $(k = 1, \ldots, n)$ посылаются последовательно друг за другом.

Квантовый канал связи (в реальной ситуации это либо оптоволокно, либо открытое пространство), через который посылаются квантовые состояния, является доступным для прослушивания. Постулаты квантовой механики гарантируют, что извлечение информации из квантовых состояний, принадлежащих неортогональным базисам, приводит к неизбежному возмущению состояний [9]. Данное обстоятельство является проявлением фундаментального соотношения неопределенностей Гейзенберга, которое фактически сводится к тому, что пара наблюдаемых, которым отвечают некоммутирующие эрмитовы операторы, не может иметь общих собственных векторов. В квантовой криптографии такими наблюдаемыми выступают некоммутирующие матрицы плотности состояний из разных базисов $\rho_i^j = |\varphi_i^j\rangle\langle\varphi_i^j|$.

2.2. Прямая и обратная теоремы кодирования. Энтропия фон Неймана и классическая пропускная способность идеального квантового канала связи

Основная задача при вычислении величины критической ошибки сводится к выяснению вопроса о связи потока ошибок и максимальной информации, которую может получить подслушиватель при наблюдаемом потоке ошибок на приемном конце. При этом цель подслушивателя — получить максимум информации о передаваемых состояниях при минимуме их возмущения (потоке ошибок на приемном конце).

Здесь при рассуждениях нам потребуется прямая теорема кодирования для квантовых каналов связи.

В каждом сеансе генерации ключа с равной вероятностью передается одна из 2^{2n} кодовых последовательностей (6). Если бы подслушиватель имел возможность безошибочно различать каждую кодовую последовательность, то при этом он мог бы не производить возмущений на приемном конце. В этом случае число бит классической информации в пересчете на одну посылку, извлекаемое из кодовой последовательности квантовых состояний, должно быть равно двум (один бит для базиса, второй — для состояния 0 или 1 в этом базисе). Другими словами, для полного восстановления передаваемых квантовых состояний число бит классической информации, которое может быть извлечено посредством квантовомеханических измерений, должно быть равно числу бит, генерируемых классическим источником, с алфавитом которого ассоциируются квантовые состояния (см. формулы (1) и (3)).

Однако число достоверно различимых последовательностей (точнее, последовательностей, различимых с вероятностью ошибки, стремящейся к нулю в асимптотическом пределе) принципиально ограничено некоторой величиной. Верхняя граница числа квантовых последовательностей, различимых с нулевой вероятностью ошибки, в пределе длинных последовательностей дается прямой теоремой кодирования [7].

Нам потребуются некоторые определения. Кодом размера M_{quant} называется набор кодовых слов

$$|w_{\vec{i}(k)}^{\vec{j}(k)}\rangle = |\varphi_{i_1(k)}^{j_1(k)}\rangle \otimes \ldots \otimes |\varphi_{i_n(k)}^{j_n(k)}\rangle \in \mathcal{H}^{\otimes n}, \quad k = 1, \ldots, M_{quant}, \tag{7}$$

при некоторых заранее фиксированных значениях индексов, полное число наборов которых равно M_{quant}. Набор решающих правил $\mathcal{X} = \{\mathcal{X}_k\}$ (измерение) описывается разложением единицы в $\mathcal{H}^{\otimes n}$:

$$I^{(n)} = \sum_{k=0}^{M_{quant}} \mathcal{X}_k. \tag{8}$$

Каждому k отвечают определенные значения $(i_1(k), \ldots, i_n(k)); (j_1(k), \ldots, j_n(k))$.

Прямая теорема кодирования Холево [7], имеющая фундаментальное значение для квантовых каналов связи, гласит, что средняя вероятность ошибки различения по всем кодам размера M_{quant}

$$\overline{P}_{error}(M_{quant}, \mathcal{X}) = \frac{1}{M_{quant}} \times \times \sum_{k=1}^{M_{quant}} [1 - p_{\mathcal{X}}(k|w_{\vec{i}(k)}^{\vec{j}(k)})] \to 0, \quad n \to \infty, \tag{9}$$

если число кодовых слов $M_{quant} < 2^{n\overline{C}(\rho)}$. Здесь

$$p_{\mathcal{X}}(k|w_{\vec{i}(k)}^{\vec{j}(k)}) = \mathrm{Tr}\{\mathcal{X}_k|w_{\vec{i}(k)}^{\vec{j}(k)}\rangle\langle w_{\vec{i}(k)}^{\vec{j}(k)}|\} \tag{10}$$

— вероятность правильного решения при измерении (послано слово $|w_{\vec{i}(k)}^{\vec{j}(k)}\rangle$ и в результате измерения был k-ый исход).

Величина $\overline{C}(\rho)$ определяется как

$$\overline{C}(\rho) = -\mathrm{Tr}\{\rho \log \rho\},$$
$$\rho = \sum_{i,j=0,1} \pi_{ij} |\varphi_i^j\rangle\langle\varphi_i^j| = \sum_{i,j=0,1} \pi_{ij}\rho_i^j = \frac{1}{2}\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \quad (11)$$

где ρ — матрица плотности ансамбля квантовых состояний, генерируемых на передающей стороне, записанная в базисе $|0\rangle$, $|1\rangle$. Величина $\overline{C}(\rho)$ имеет двоякую роль. С одной стороны, $\overline{C}(\rho)$ имеет смысл классической пропускной способности идеального квантового канала связи, т. е. верхней границы числа классических бит информации в пересчете на одну посылку, которое может быть извлечено из квантового ансамбля с нулевой вероятностью ошибки в асимптотическом пределе длинных последовательностей. Точнее говоря, из общего числа 2^{2n} последовательностей безошибочно различимо не более $M_{quant} < 2^{n\overline{C}(\rho)}$ последовательностей $|w_{\vec{i}(k)}^{\vec{j}(k)}\rangle$. Для такого числа последовательностей может быть известен и базис, и состояние в базисе для каждой посылки.

Соответственно, на языке числа бит на посылку это означает, что из двух бит классической информации (см. формулу (1), один бит для базиса, другой для состояния в этом базисе), генерируемых классическим источником, из квантовых состояний (6) может быть извлечено безошибочно не более одного бита классической информации,

$$\overline{C}(\rho) = 1.$$

Одного бита классической информации на посылку (или n бит на последовательность) достаточно, чтобы занумеровать $2^{n\overline{C}(\rho)} = 2^n$ последовательностей, если набор кодовых последовательностей заранее фиксирован.

Действительно, если $2^{n\overline{C}(\rho)} = 2^n$ кодовых слов фиксированы заранее (т. е. заранее известно, что будет послано одно из этих слов, но не известно какое именно), то это означает, что имеется соответствие между номером кодового слова k и набором индексов $(i_1(k), \ldots i_n(k))$; $(j_1(k), \ldots j_n(k))$:

$$\begin{aligned} k = 1 &\to \quad |w_{\vec{i}(1)}^{\vec{j}(1)}\rangle, \\ k = 2 &\to \quad |w_{\vec{i}(2)}^{\vec{j}(2)}\rangle, \\ &\ldots \\ k = 2^n &\to \quad |w_{\vec{i}(2^n)}^{\vec{j}(2^n)}\rangle, \end{aligned} \quad (12)$$

поэтому достаточно перенумеровать 2^n значений k (номеров кодовых слов), для такой нумерации достаточно n бит (на все 2^n последовательностей, или 1 бит в пересчете на посылку).

С другой стороны, как следует из формулы (11), $\overline{C}(\rho)$ совпадает с энтропией фон Неймана ансамбля квантовых состояний. Поэтому величина

$$\dim \mathcal{H}_c = 2^{n\overline{C}(\rho)} = 2^n \quad (13)$$

определяет минимальную размерность пространства состояний $\mathcal{H}_c$, в которое с вероятностью единица попадают носители всех 2^{2n} последовательностей длины n,

$$\mathrm{supp}|w_{\vec{i}}^{\vec{j}}\rangle \in \mathcal{H}_c.$$

В пространстве размерности (13) существует ортогональный базис из 2^n векторов, которые достоверно различимы, поскольку они ортогональны. Поэтому число достоверно различимых последовательностей не может быть больше, чем размерность пространства (13).

Для дальнейшего нам потребуется также сильное обращение теоремы кодирования для квантовых каналов связи, доказанное в работе [8]. Данная теорема дает величину ошибки для случая, когда число кодовых слов выбрано большим, чем

$$M_{quant} > 2^{n\overline{C}(\rho)} = 2^n.$$

В этом случае ошибка стремится к единице:

$$\overline{P}_{error}(M_{quant}, \mathcal{X}) > 1 - 2^{-\mathrm{const}\cdot n}, \quad (14)$$

где const — некоторая константа, зависящая от ρ, но не зависящая от n.

Неформально это означает, что даже если кодовые слова известны заранее, но их число превышает 2^n, то вероятность ошибки при различении стремится к единице в асимптотическом пределе длинных последовательностей.

2.3. Консервативные оценки для протокола *BB84*

Применительно к протоколу распространения ключей *BB84* прямая теорема кодирования утверждает следующее. Если бы из общего числа классических кодовых слов $M_{class} = 2^{nH(X)}$ Alice случайным образом выбирала бы не более

$$M_{quant} < 2^{n\overline{C}(\rho)} \quad (15)$$

кодовых слов, которым ставятся в соответствие квантовые состояния по правилу (6), и затем помещала их в открытый справочник и посылала одно из квантовых кодовых слов в канал связи, но

не сообщала, какое именно, то в этом случае вероятность правильного различения подслушивателем (Eve) в асимптотическом пределе длинных кодовых слов стремилась бы к единице. То есть посредством квантовомеханических оптимальных измерений (коллективных измерений над целыми кодовыми словами) каждое кодовое слово может быть с нулевой вероятностью ошибки идентифицировано. Для измерения над целыми кодовыми словами требуется квантовая память, чтобы перед измерением можно было «накопить» квантовые состояния из всех n посылок. В этом случае Eve знала бы все передаваемые состояния и не производила бы ошибок на приемном конце.

Если заранее кодовые слова не фиксируются (именно такая ситуация имеет место в протоколе распространения ключей) и любое из $M_{class} = 2^{nH(X)}$ слов может быть кодовым, то консервативная оценка дает, что безошибочно различимо не более M_{quant} (формула (13)) слов из $M_{class} = 2^{nH(X)}$ возможных.

Применительно к задачам квантовой криптографии последнее означает, что если Alice посылает с равной вероятностью одно из $M_{class} = 2^{nH(X)}$ слов, то Eve достоверно может различить не более $M_{quant} = 2^{n\overline{C}(\rho)}$ слов, остальные с вероятностью единица она не знает. Данное обстоятельство гарантируется сильным обращением теоремы кодирования для квантовых каналов связи [8].

Таким образом, поскольку для нумерации всех 2^{2n} квантовых состояний в каждой посылке требуется два классических бита (один бит для нумерации базиса, второй — для состояния 0 или 1 в этом базисе), то из случайно посланной последовательности длины n Eve достоверно может знать не более половины состояний в каждой посылке, поскольку

$$\overline{C}(\rho) = \frac{1}{2}H(X) = 1$$

— количество бит информации, достоверно извлекаемой из квантового ансамбля, в пересчете на одну посылку.

Найдем теперь величину критической ошибки на приемном конце, до которой возможно распространение секретного ключа.

Пусть Alice генерирует одну из множества $2^{nH(X)} = 2^{2n}$ случайных строк. На каждую позицию приходится два бита классической информации, один бит для базиса, второй — для состояния 0 или 1 в базисе. Далее Alice ассоциирует с каждой позицией квантовое состояние по правилу (6) и посылает в канал связи к Bob. Bob делает последовательно индивидуальные измерения в случайном и независимом от Alice базисе «+» или «×» и сообщает факт регистрации. После передачи всей последовательности Bob сообщает открыто для каждой позиции свой базис измерений, но не раскрывает результат (0 или 1). Позиции, в которых базисы Alice и Bob не совпадали, отбрасываются.

Поскольку Bob выбирает базис независимо и случайно от Alice и Eve, то половина позиций, которые отбрасываются при согласовании базисов, приводит к тому, что Eve по-прежнему может знать состояния не более, чем в $2^{n_1\overline{C}(\rho)}$ последовательностях из возможных 2^{2n_1} оставшихся ($n_1 \approx n/2$ — длина последовательности после согласования базисов). Bob после согласования и раскрытия базисов имеет по одному биту информации на каждую позицию, т. е. всего n_1 бит (возможно, часть бит при этом с ошибкой), а Eve знает не более $n_1/2$ бит. Иначе говоря, после раскрытия базисов Eve может знать не более $2^{n_1\overline{C}(\rho)/2}$ последовательностей из оставшихся 2^{n_1} возможных. Если бы не было процедуры согласования базисов (постселекции), то секретное распространение ключа было бы невозможно, поскольку Bob также не мог бы извлечь из квантового ансамбля информации больше, чем Eve, что диктуется прямой и обратной теоремами кодирования. Таким образом, после процедуры согласования базисов Eve (консервативно) знает не более половины бит в оставшейся последовательности длины $n_1 \approx n/2$. Информация Eve составляет не более $n_1\overline{C}(\rho)/2$ бит. Напомним, что $\overline{C}(\rho)/2$ возникает из-за отбрасывания бита информации при согласовании базисов.

Далее легитимные пользователи раскрывают часть последовательности (обычно половину) и оценивают вероятность ошибки на приемном конце. Раскрытая часть затем отбрасывается. Поскольку позиции выбираются случайно и равновероятно, после этой процедуры Eve остается в той же ситуации, что и до раскрытия, т. е. знает в оставшейся последовательности не более половины бит. Пусть длина оставшейся строки $n_r \approx n/4$.

2.4. Критическая величина ошибки

Поскольку число посылаемых последовательностей превышает число достоверно различимых $M_{quant} = 2^n$, действия Eve неизбежно будут приводить к ошибке на приемном конце.

Пусть наблюдаемая вероятность ошибки у Bob равна Q. Далее Alice случайно выбирает $2^{n_r H(Q)}$ битовых строк длины n_r (классических кодовых слов) и открыто сообщает их. В множество кодовых слов

Alice также включает битовую последовательность, которую она реально посылала к Bob. Bob последовательно сравнивает свою битовую строку, которая содержит ошибки, со всеми кодовыми словами и выбирает ближайшее в смысле расстояния Хэмминга (выбирает кодовое слово, которое отличается от его последовательности в минимальном числе позиций). Согласно прямой теореме кодирования Шеннона [10,11] для бинарных классических каналов с шумом, с вероятностью единица Bob выберет правильную строку, которую посылала Alice, и сможет исправить ошибки. Eve с вероятностью единица сможет выбрать правильную битовую строку лишь при условии

$$2^{n_r\overline{C}(\rho)/2} \geq 2^{n_r H(Q)}.$$

Критическая величина ошибки находится как корень уравнения

$$H(Q_c) = \frac{\overline{C}(\rho)}{2}, \quad Q_c \approx 11\,\%, \tag{16}$$

$$H(Q) = 1 + Q\log Q + (1-Q)\log(1-Q).$$

Здесь $H(Q)$ — пропускная способность классического симметричного бинарного канала связи. При

$$2^{n_r\overline{C}(\rho)/2} < 2^{n_r H(Q)},$$

согласно сильному обращению [11, 12] теоремы кодирования для классического симметричного бинарного канала связи, Eve с вероятностью единица не сможет различить правильную битовую строку, т. е. легитимные пользователи в этом случае могут использовать всю битовую строку как секретный ключ. Отметим, однако, что эта граница не является конструктивно достижимой, поскольку требует экспоненциально большой таблицы случайных кодовых слов.

Полученная величина критической ошибки на приемном конце совпадает с найденной в работе [5] с привлечением совершенно других рассуждений, основанных на «виртуальном» использовании квантовых кодов.

Фактически до согласования базисов для строки длиной n Eve принципиально не может знать более чем $n\overline{C}(\rho) = n$ бит информации, что гарантируется фундаментальными (прямой [7] и обратной [8]) теоремами кодирования. Грубо говоря, этой информации хватает Eve лишь на половину позиций, чтобы знать и базис, и состояние (по два бита на $n/2$ позиций). После согласования базисов по одному биту из двух в $n/2$ позициях отбрасывается, при этом у Eve остается $n/2$ бит, а у Bob по одному биту в n позициях (результат измерения в каждом базисе 0 или 1).

2.5. Связь секретности ключа с соотношением неопределенностей и классической пропускной способностью квантового канала связи

В данном разделе приводятся рассуждения, которые проясняют связь секретности ключа в квантовой криптографии с фундаментальным соотношением неопределенностей [13–15] в квантовой механике, а также с классической пропускной способностью квантового канала связи (напомним, что для идеального канала и чистых входных состояний классическая пропускная способность совпадает с энтропией фон Неймана).

В квантовой механике наблюдаемым A и B ставятся в соответствие эрмитовы операторы. Пусть $\mathcal{A}$ и $\mathcal{B}$ — два эрмитовых оператора, $|\psi\rangle$ — квантовое состояние (с соответствующей матрицей плотности $\rho_\psi = |\psi\rangle\langle\psi|$), для которого измеряются наблюдаемые A и B.

Операторы $\mathcal{A}$ и $\mathcal{B}$ имеют спектральное представление вида

$$\mathcal{A} = \sum_j a_j |a_j\rangle\langle a_j|, \quad \mathcal{B} = \sum_j b_j |b_j\rangle\langle b_j|, \tag{17}$$

где a_j, b_j — собственные числа, а $|a_j\rangle, |b_j\rangle$ — соответствующие им собственные векторы.

Измерение наблюдаемых генерирует распределение вероятностей $\{p_j\}$ и $\{q_j\}$:

$$p_j = |\langle a_j|\psi\rangle|^2, \quad q_j = |\langle b_j|\psi\rangle|^2. \tag{18}$$

Соотношение неопределенностей гласит, что

$$\Delta_\psi\mathcal{A}\Delta_\psi\mathcal{B} \geq \frac{1}{2}|(\langle[\mathcal{A},\mathcal{B}]\rangle_\psi|. \tag{19}$$

Здесь $\Delta_\psi\mathcal{A}$ и $\Delta_\psi\mathcal{B}$ — среднеквадратичные отклонения для распределения вероятностей $\{p_j\}$ и $\{q_j\}$:

$$(\Delta_\psi\mathcal{A})^2 = \langle\mathcal{A}^2\rangle_\psi - (\langle\mathcal{A}\rangle_\psi)^2, \tag{20}$$

$$(\Delta_\psi\mathcal{B})^2 = \langle\mathcal{B}^2\rangle_\psi - (\langle\mathcal{B}\rangle_\psi)^2, \tag{21}$$

где

$$\langle\mathcal{A}^2\rangle_\psi = \mathrm{Tr}\{\mathcal{A}^2\rho_\psi\}, \quad (\langle\mathcal{A}\rangle_\psi)^2 = (\mathrm{Tr}\{\mathcal{A}\rho_\psi\})^2, \tag{22}$$

$$\langle\mathcal{B}^2\rangle_\psi = \mathrm{Tr}\{\mathcal{B}^2\rho_\psi\}, \quad (\langle\mathcal{B}\rangle_\psi)^2 = (\mathrm{Tr}\{\mathcal{B}\rho_\psi\})^2. \tag{23}$$

Статистическая интерпретация соотношений (19)–(23) сводится к следующему. Если многократно готовится состояние $|\psi\rangle$ и проводится измерение наблюдаемой $\mathcal{A}$, то исходом в каждом измерении будет одно из собственных чисел a_j, которое возникает с вероятностью p_j. Аналогично для наблюдаемой $\mathcal{B}$, если проводятся измерения на том же входном состоянии $|\psi\rangle$, то исходом измерения с вероятностью q_j будет собственное число b_j.

Измерения наблюдаемых на одном и том же входном состоянии $|\psi\rangle$ генерируют распределение вероятностей на множестве собственных значений этих наблюдаемых. По данным распределениям вероятностей могут быть вычислены средние значения наблюдаемых (их собственных значений) и среднеквадратичных отклонений (20), (21). Если операторы наблюдаемых не коммутируют, то произведение дисперсий наблюдаемых (19), вообще говоря, отлично от нуля. Соотношения неопределенностей в форме (19) неоднократно подвергались критике, поскольку правая часть явно зависит от измеряемого состояния $|\psi\rangle$ и не фиксирует нижнюю границу произведения дисперсий. Правая часть (19) равна нулю, если состояние квантовой системы $|\psi\rangle$ является собственным состоянием оператора наблюдаемой $\mathcal{A}$. В этом случае $(\Delta_\psi \mathcal{A})^2 = 0$ и $|([\mathcal{A},\mathcal{B}])_\psi| = 0$, поэтому неравенство (19) не дает нижнюю границу для значения дисперсии $(\Delta_\psi \mathcal{B})^2$, т. е. из неравенства не следует, что даже для некоммутирующих наблюдаемых дисперсия $(\Delta_\psi \mathcal{B})^2$ должна быть отлична от нуля.

Применительно к задачам квантовой криптографии более удобными оказываются соотношения неопределенностей в энтропийной форме [16–20]

$$\begin{aligned} &h(p)+h(q)\ge -2\log c, \quad c=\max_{i,k}|\langle a_i|b_k\rangle|,\\ &h(p)=-\sum_i p_i\log p_i, \quad h(q)=-\sum_i q_i\log q_i \end{aligned} \tag{24}$$

(h — энтропийная функция Шеннона).

Получим энтропийное неравенство применительно к квантовой криптографии. При этом необходимо учесть процедуру согласования базисов. Это означает, что Bob выбирает наблюдаемую (базис измерения) согласованную с Alice. Точнее говоря, те посылки, в которых базис измерения Bob и базис, в котором состояния посылала Alice не совпадали, отбрасываются. Формально это означает, измерение Bob после отбрасывания позиций, где базисы не совпадали, описывается разложением единицы:

$$\begin{aligned} &I^{(n)}=\sum_{\vec{i}}|w_{\vec{i}}^{\vec{j}}\rangle\langle w_{\vec{i}}^{\vec{j}}|,\\ &|w_{\vec{i}}^{\vec{j}}\rangle=|\varphi_{i_1}^{j_1}\rangle\otimes\ldots\otimes|\varphi_{i_n}^{j_n}\rangle. \end{aligned} \tag{25}$$

Индекс, относящийся к базису $\vec{j}=(j_1,\ldots,j_n)$ фиксирован. Соответственно, матрица плотности, над которой проводятся измерения, после согласования базисов имеет вид

$$\rho^{\vec{j}}=\sum_{\vec{i}} p_{\vec{i}}\rho_{\vec{i}}^{\vec{j}}, \quad \rho_{\vec{i}}^{\vec{j}}=|w_{\vec{i}}^{\vec{j}}\rangle\langle w_{\vec{i}}^{\vec{j}}|, \quad p_{\vec{i}}=\frac{1}{2^n}. \tag{26}$$

С разложением единицы (25) может быть ассоциирована наблюдаемая вида

$$\mathcal{B}=\sum_{\vec{i}} b(\vec{i})|w_{\vec{i}}^{\vec{j}}\rangle\langle w_{\vec{i}}^{\vec{j}}|, \tag{27}$$

где $b(\vec{i})$ — есть число, которому отвечает двоичное представление $(i_1,i_2,\ldots,i_n)$, нумерующее исход измерения. Фактически после измерения Bob получает битовую строку $(i_1,i_2,\ldots,i_n)$.

Подслушивателю (Eve) заранее не известен выбор базиса, поэтому лучшее, что может сделать Eve, — выбрать обобщенную наблюдаемую и измерение, которое дается, в общем случае, неортогональным разложением единицы (8):

$$I^{(n)}=\sum_k^{2^{\overline{C}n}}\mathcal{X}_k=\sum_k^{2^{\overline{C}n}}|\mathcal{X}_k\rangle\langle\mathcal{X}_k|, \tag{28}$$

где векторы $|\mathcal{X}_k\rangle$ неортогональны и строятся из случайно выбранных кодовых слов. Соответствующая обобщенная наблюдаемая имеет вид

$$\mathcal{E}=\sum_k^{2^{\overline{C}n}} e(k)|\mathcal{X}_k\rangle\langle\mathcal{X}_k|. \tag{29}$$

Здесь $e(k)$ — число, нумерующее исход измерения.

Взаимная информация между битовой строкой Alice и битовыми строками Eve и Bob имеет смысл степени корреляции между ними и дает количество информации в битах, которое может быть извлечено посредством измерений с нулевой вероятностью ошибки при достаточно длинной последовательности. Энтропийные соотношения неопределенностей для взаимной информации [20] (см. также [21]) могут быть записаны в виде

$$I(\mathcal{B}|\rho^{\vec{j}})=S(\mathcal{B}|\rho^{\vec{j}})-\sum_{\vec{i}} p_{\vec{i}}S(\mathcal{B}|\rho_{\vec{i}}^{\vec{j}}), \tag{30}$$

где энтропия фон Неймана

$$S(\mathcal{B}|\rho^{\vec{j}}) = -\sum_{\vec{i}} p(\vec{i}|\rho^{\vec{j}}) \log p(\vec{i}|\rho^{\vec{j}}),$$
$$p(\vec{i}|\rho^{\vec{j}}) = \mathrm{Tr}\{\rho_{\vec{i}}^{\vec{j}} |w_{\vec{i}}^{\vec{j}}\rangle\langle w_{\vec{i}}^{\vec{j}}|\}. \quad (31)$$

Аналогичное выражение можно записать для $S(\mathcal{B}|\rho_{\vec{i}}^{\vec{j}})$.

Соответственно, для Eve получаем

$$I(\mathcal{E}|\rho^{\vec{j}}) = S(\mathcal{E}|\rho^{\vec{j}}) - \sum_{\vec{i}} p_{\vec{i}} S(\mathcal{E}|\rho_{\vec{i}}^{\vec{j}}), \quad (32)$$

$$S(\mathcal{E}|\rho^{\vec{j}}) = -\sum_{k} p(k|\rho^{\vec{j}}) \log p(k|\rho^{\vec{j}}),$$
$$p(k|\rho^{\vec{j}}) = \mathrm{Tr}\{\rho_{\vec{i}}^{\vec{j}} |\mathcal{X}_k\rangle\langle\mathcal{X}_k|\}. \quad (33)$$

Аналогичное выражение можно записать для $S(\mathcal{E}|\rho_{\vec{i}}^{\vec{j}})$.

Согласно неравенству для взаимной информации, имеем

$$I(\mathcal{E}|\rho^{\vec{j}}) + I(\mathcal{B}|\rho^{\vec{j}}) \le 2\log(2^n c), \quad (34)$$

где c — перекрытие состояний:

$$c = \max_{k,\vec{i}} |\langle w_{\vec{i}}^{\vec{j}} | \mathcal{X}_k\rangle|. \quad (35)$$

Поскольку базис измерения (индекс $\vec{j}$), в отличие от Bob, заранее Eve не известен, число возможных векторов, из которых будут выбраны векторы $|w_{\vec{i}}^{\vec{j}}\rangle$, составляет

$$2^{H(x)n} = 2^{2n}.$$

В то же время векторы $|\mathcal{X}_k\rangle$ имеют носители в пространстве размерности не более чем

$$\dim \mathcal{H}_c = 2^{n\overline{C}} = 2^n,$$

поэтому в силу условия нормировки перекрытие не может превышать корня из отношения размерностей данных пространств состояний

$$c = \max_{k,\vec{i}} |\langle w_{\vec{i}}^{\vec{j}} | \mathcal{X}_k\rangle| \le \sqrt{\frac{\dim \mathcal{H}_c}{2^{H(x)n}}} = 2^{-n/2}. \quad (36)$$

Согласно работе [22], извлечение секретного ключа возможно, если взаимная информация легитимного пользователя Bob о строке Alice больше, чем взаимная информация подслушивателя,

$$I(\mathcal{E}|\rho^{\vec{j}}) < I(\mathcal{B}|\rho^{\vec{j}}). \quad (37)$$

С учетом выражений (34) и (37) приходим к неравенству

$$I(\mathcal{E}|\rho^{\vec{j}}) \le \log(2^n c) < \frac{n}{2}. \quad (38)$$

Отметим, что после согласования базисов реализуется ситуация, когда состояния $|w_{\vec{i}}^{\vec{j}}\rangle$, посылаемые Alice, являются собственными состояниями оператора наблюдаемой у Bob. Подслушиватель заранее не знает, в каких позициях у легитимных пользователей базисы совпадут, поскольку они выбирают их случайно и независимо друг от друга и согласовывают только после передачи всех состояний. Поэтому лучшее, что может сделать Eve, — это выбрать обобщенную наблюдаемую (28), которая позволяет различать максимально возможное число случайно выбранных кодовых последовательностей, равное $2^{n\overline{C}}$.

2.6. Сжатие ключа

После согласования базисов Alice и Bob имеют частично коррелированные бинарные строки X и Y длиной n (здесь и ниже n — длина строки после согласования базисов). Взаимная информация между строками Alice и Bob в шенноновском пределе есть пропускная способность бинарного классического канала связи $I(X;Y) = nH(Q)$, соответственно взаимная информация Eve о строке Alice не превышает $n\overline{C}(\rho)/2$. Длина секретного ключа в шенноновском пределе равна

$$nr = n\left(H(Q) - \frac{\overline{C}(\rho)}{2}\right) =$$
$$= n\left(\frac{1}{2} + Q\log Q + (1-Q)\log(1-Q)\right). \quad (39)$$

Длина секретного ключа в шенноновском пределе не является конструктивно достижимой, поскольку требует экспоненциально большого по длине последовательности блокнота из кодовых слов при коррекции ошибок.

После коррекции ошибок проводится усиление секретности ключа, введенное в работе [23]. Процедура усиления секретности сводится к сжатию промежуточного ключа (хэшированию при помощи универсальных однородных хэш-функций второго рода [24]) до финального ключа, о котором Eve будет иметь экспоненциально малую информацию по заданному параметру секретности. Степень сжатия зависит от конкретных деталей процедуры коррекции ошибок через открытый канал связи. В общем виде невозможно определить степень сжатия клю-

ча в отрыве от процедуры коррекции ошибок, поскольку исправление ошибок, вообще говоря, изменяет условные вероятности о промежуточном ключе у Eve.

Если процедура коррекции ошибок сохраняет конфиденциальность, не изменяет переходные вероятности об «очищенном» ключе у Eve, то сжатие ключа сводится к случаю $Q = 0$. Для определения степени сжатия ключа в этом случае необходимо иметь оценку для условной вероятности того, что Eve будет иметь информацию об «очищенном» ключе. Границы для переходных вероятностей можно получить на основании консервативных оценок. Такие оценки заведомо не занижают информацию Eve об «очищенном» ключе[1)].

Воспользуемся следствием из фундаментальной теоремы об усилении секретности [23]. Пусть

$$E : \{0,1\}^n \to \{0,1\}^t$$

— произвольная функция, описывающая стратегию подслушивателя в том смысле, что для произвольной строки бит длиной n Eve известно не более t бит ($t < n$). Пусть s — параметр секретности ($s < n - t$), выбираемый легитимными пользователями. Далее пусть

$$G : \{0,1\}^n \to \{0,1\}^r$$

— универсальная однородная функция хэширования второго рода (см. детали в [23, 24]), которая сама является случайной величиной. Тогда взаимная информация Eve о секретном ключе $K = G(X)$ не превосходит величину

$$I(K;GZ) \le \frac{2^{-s}}{\ln 2}. \tag{40}$$

Пусть

$$Z : \{0,1\}^t$$

— строка Eve, согласованная со строкой легитимных пользователей X в том смысле, что эта строка могла произойти из строк X как $Z = E(X)$. Наша цель состоит в вычислении длины финального ключа r, о котором Eve имеет экспоненциально малую по s информацию. Для этого потребуется знание энтропии Реньи второго рода, которая в свою очередь выражается через вероятность коллизий.

После согласования базисов Eve может различить не более $2^{n\overline{C}(\rho)/2}$ строк из общего множества 2^n (2^n число возможных строк у Alice и Bob после согласования базисов). Условная вероятность определяется отношением общего числа строк к числу областей декодирования у Eve, поэтому имеем

$$P_{X|Z=z} = \frac{2^{n\overline{C}(\rho)/2}}{2^n} = 2^{-n(1-\overline{C}(\rho)/2)} = a_z. \tag{41}$$

Фактически $1/a_z$ — доля строк длины n таких, что $z = E(X)$, т. е. с каждой частичной строкой Eve согласовано множество строк, определяемое формулой (13). Для вероятности коллизий получаем

$$P_c(X|Z=z) = \sum_{X:\{z=E(X)\}} P^2_{X|Z=z} = 2^{-n(1-\overline{C}(\rho)/2)} = \frac{1}{a_z} a_z^2. \tag{42}$$

Доля строк X, удовлетворяющих условию $z = E(X)$, равна $1/a_z$. Соответственно, энтропия Реньи второго рода равна

$$R(X|Z=z) = -\log P_c(X|Z=z) = n\left(1 - \frac{\overline{C}(\rho)}{2}\right). \tag{43}$$

Согласно теореме об усилении секретности [23], находим

$$H(K|G,Z=z) \ge r - \frac{2^{r-R(X|Z=z)}}{\ln 2} > r - \frac{2^r}{a_z \ln 2}. \tag{44}$$

Для взаимной информации между строками Eve и секретным ключом у легитимных пользователей с учетом того, что

$$P_Z(z) = \frac{1}{2^{n\overline{C}(\rho)/2}} = \frac{2^{-n}}{a_z},$$

имеем

$$I(K;GZ) = H(K) - H(K|GZ) \le r - \sum_{z\in\{0,1\}^t} P_Z(z) H(K|G,Z=z) \le \sum_{z\in\{0,1\}^t} a_z 2^{-n} \frac{2^r}{a_z \ln 2} = \frac{2^{-n+t+r}}{\ln 2} = \frac{2^{-s}}{\ln 2}. \tag{45}$$

Секретный ключ определяется как

$$K = G(X) \in \{0,1\}^r,$$

а для длины финального секретного ключа имеем формулу

$$r = n\left(1 - \frac{\overline{C}(\rho)}{2}\right) - s = \frac{n}{2} - s. \tag{46}$$

[1)] Например, оценки длины ключа в шенноновском пределе [6] дают вместо выражения (39) выражение $nr = n[1 + 2(Q\log Q + (1-Q)\log(1-Q))]$, т. е. консервативные оценки являются более жесткими.

Консервативная оценка (46) гласит, что ключ должен быть сжат наполовину даже при нулевой наблюдаемой вероятности ошибки.

Случай $Q \neq 0$ требует отдельного рассмотрения, поскольку длина финального ключа сильно зависит от конкретной конструктивной процедуры исправления ошибок. Наиболее простой для анализа является процедура коррекции ошибок на основе бисективного поиска с выбрасыванием ошибок и битов четности подстрок [25]. Однако эта процедура с практической точки зрения не самая эффективная в смысле длины финального ключа. Наиболее эффективной из известных на сегодняшний день является процедура *Cascade* [26], однако она не сохраняет секретности, поскольку в ней не отбрасываются раскрытые биты четности при коррекции ошибок, что изменяет условные вероятности наличия информации о ключе у Eve. То же самое относится к процедурам коррекции на основе классических кодов [27, 28]. Детали исправления ошибок каскадной процедурой с сохранением конфиденциальности можно найти в работе [29].

3. ЗАКЛЮЧЕНИЕ

Из консервативной оценки следует, что Eve, зная и базис, и состояние для половины позиций, не будет производить ошибок на приемном конце у Bob для этих позиций. Для второй половины информация Eve равна нулю. Eve могла бы «размазать» всю доступную ей информацию о передаваемых состояниях на все позиции. В этом случае на каждую позицию приходился бы один бит информации, что недостаточно для того, чтобы полностью знать состояние в каждой позиции (базис и само состояние). Это приводило бы к ошибкам на приемном конце. В этом случае пришлось бы явно связывать поток ошибок у Bob с конкретной стратегией Eve, т. е. явно связывать поток ошибок с информацией у Eve при данном потоке. Никаких явных формул на этом пути, по-видимому, получить нельзя, поэтому лучше исходить из консервативных оценок.

Прямой подход состоит в вычислении условных вероятностей о ключе для наиболее эффективной стратегии подслушивания Eve. При таком подходе необходимо явно найти максимальную информацию Eve о ключе при наблюдаемой вероятности ошибки Q у легитимных пользователей. Такой подход технически вряд ли осуществим, поскольку невозможно перебрать все стратегии и быть уверенным, что найдена самая эффективная, поэтому надежнее пользоваться консервативными оценками, которые возможно завышают информацию Eve о ключе, но, по крайней мере, гарантируют верхнюю границу этой информации (не занижая информацию Eve о ключе).

Работа выполнена при финансовой поддержке Академии криптографии РФ, РФФИ (грант № 05-02-17387) и ИНТАС (грант № 04-77-7284).

ЛИТЕРАТУРА

1. C. H. Bennett and G. Brassard, Proc. of IEEE Int. Conf. on Comput. Sys. and Sign. Proces., Bangalore, India (1984), p. 175.
2. H.-K. Lo and H. F. Chau, Science **283**, 2050 (1999).
3. D. Mayers and A. Yao, E-print archives quant-ph/9802025.
4. E. Biham, M. Boyer, P. O. Boykin, T. Mor, and V. Roychowdhury, E-print archives quant-ph/9912053.
5. P. W. Shor and J. Preskill, E-print archives quant-ph/0003004.
6. M. Christandl, A. Ekert, and R. Renner, E-print archives quant-ph/040231; A. K. Ekert, Phys. Rev. Lett. **67**, 661 (1991).
7. А. С. Холево, Проблемы передачи информации **8**, 63 (1972); **15**, 3 (1979); УМН **53**, 193 (1998); А. С. Холево, *Введение в квантовую теорию информации*, сер. *Современная математическая физика, вып. 5*, МЦНМО, Москва (2002).
8. T. Ogawa and H. Nagaoka, E-print archives quant-ph/9808063.
9. C. H. Bennett, Phys. Rev. Lett. **68**, 3121 (1992); C. H. Bennett, G. Brassard, and N. D. Mermin, Phys. Rev. Lett. **68**, 557 (1992).
10. C. E. Shannon, Bell Syst. Tech. J. **27**, 397; **27**, 623 (1948).
11. Р. Галлагер, *Теория информации и надежная связь*, Сов. радио, Москва (1974).
12. J. Wolfowitz, Illinois J. of Math. **1**, 591 (1957).
13. W. Heisenberg, Z. Phys. **43**, 172 (1927); В. Гейзенберг, УФН **122**, 657 (1977).
14. N. Bohr, Nature **121**, 580 (1928).
15. H. P. Robertson, Phys. Rev. **34**, 163 (1929); Phys. Rev. **35**, 667 (1930).

16. D. Deutsch, Phys. Rev. Lett. **50**, 631 (1983).

17. M. H. Partovi, Phys. Rev. Lett. **50**, 1883 (1983).

18. K. Kraus, Phys. Rev. D **35**, 3070 (1987).

19. H. Maasen and J. B. M. Uffink, Phys. Rev. Lett. **60**, 1103 (1988).

20. M. J. W. Hall, Phys. Rev. Lett. **74**, 3307 (1995).

21. N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, E-print archives quant-ph/0101098; Rev. Mod. Phys. **74**, 145 (2002).

22. I. Csiszár and J. Körner, IEEE Trans. Inf. Theory **IT-24**, 339 (1978).

23. C. H. Bennett, G. Brassard, C. Crépeau, and U. Maurer, IEEE Trans. Inf. Theory **41**, 1915 (1995).

24. J. L. Carter and M. N. Wegman, J. Comp. Syst. Sci. **18**, 143 (1979).

25. C. H. Bennett, F. Bessette, G. Brassard, L. Salvail, and J. Smolin, J. Cryptology **5**, 3 (1992).

26. G. Brassard and L. Salvail, Lect. Notes in Comp. Sci. **765**, 410 (1994).

27. W. T. Buttler, S. K. Lamoreaux, J. R. Torgerson, G. H. Nickel, C. H. Donahue, and C. G. Peterson, E-print archives quant-ph/0203096.

28. А. П. Маккавеев, С. Н. Молотков, Д. И. Помозов, А. В. Тимофеев, ЖЭТФ **128**, 263 (2005).

29. А. В. Тимофеев, С. Н. Молотков, Письма в ЖЭТФ **82**, 868 (2005).