ЖЭТФ, 2005, том 128, вып. 2 (8), стр. 263–291

О ПРАКТИЧЕСКИХ МЕТОДАХ «ЧИСТКИ» КЛЮЧЕЙ В КВАНТОВОЙ КРИПТОГРАФИИ

А. П. Маккавеев [b,c], ***С. Н. Молотков*** [a,b*], ***Д. И. Помозов*** [b,c], ***А. В. Тимофеев*** [b]

[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

[c] *Физико-технологический институт Российской академии наук*
117428, Москва, Россия

Поступила в редакцию 25 февраля 2005 г.

Система квантовой криптографии — распространение секретных ключей — должна включать в себя методы коррекции ошибок в первичном ключе, переданном по квантовому каналу связи. В работе рассмотрены различные методы «чистки» первичного ключа и проведено сравнение их эффективности.

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

1. ВВЕДЕНИЕ

Квантовая криптография [1, 2], или распространение секретных ключей, в принципе позволяет реализовать абсолютно стойкие (не дешифруемые подслушивателем даже теоретически) системы шифрования с одноразовыми ключами [3–5]. Секретность ключей в квантовой криптографии основана на фундаментальных запретах квантовой механики [6], а именно, на том обстоятельстве, что пара наблюдаемых, которым отвечают некоммутирующие операторы, не может быть достоверно одновременно различима, что является следствием соотношений неопределенности Гейзенберга. В квантовой криптографии в качестве таких наблюдаемых выступают матрицы плотности информационных состояний, соответствующих классическим битам 0 и 1. Для чистых состояний одновременная ненаблюдаемость (достоверная неразличимость) матриц плотности эквивалентна неортогональности информационных квантовых состояний [7]. Сказанное означает, что не существует измерений, которые с вероятностью единица позволяют различать одно из пары неортогональных состояний, так чтобы после измерения система оказалась в исходном состоянии, в котором она была до измерения. Таким образом, любое измерение, если оно дает информацию о передаваемых состояниях, неизбежно приводит к их возмущению, что позволяет детектировать любые попытки подслушивания в канале связи. Другими словами, подслушивание (соответственно, возмущение состояний) передаваемых состояний должно неизбежно приводить к изменению статистики результатов измерений на приемном конце по сравнению со статистикой результатов измерений на невозмущенных состояниях. Искажение квантовых состояний возникает в неидеальном квантовом канале, что также приводит к изменению статистики результатов измерений. В квантовой криптографии принципиально невозможно отличить изменение статистики результатов по сравнению с идеальным случаем, возникающих за счет шума в канале или от действий подслушивателя, поэтому любые изменения статистики приходится относить на действия подслушивателя.

Если бы законы квантовой механики позволяли обнаруживать только сам факт возмущения передаваемых состояний, то это было бы бесполезно для це-

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

лей криптографии, точнее, передачи ключей. Квантовая механика позволяет не только обнаруживать возмущение состояний, но и связать изменение статистики результатов измерений с количеством информации, которое может быть получено подслушивателем при наблюдаемом изменении статистики отсчетов по сравнению с идеальным случаем.

В квантовой криптографии кроме квантового канала связи (в реальных условиях это либо оптоволокно, либо открытое пространство), по которому передаются квантовые состояния, необходим также открытый классический канал связи. Классический открытый канал связи необходим для выяснения легитимными пользователями изменений статистики отсчетов и коррекции ошибок в первичном ключе, переданном по квантовому каналу связи. Единственное требование, которое предъявляется к классическому каналу связи, состоит в том, что передаваемая открыто и доступная всем, включая подслушивателя, классическая информация не могла бы быть изменена подслушивателем, т. е. сохраняла бы целостность (так называемый unjamable channel). Такой открытый классический канал является математической идеализацией, поскольку подобных каналов в природе не существует. Для сохранения целостности открыто передаваемых классических данных в реальных условиях необходимо использовать процедуры аутентификации и контроля целостности данных. Для подобных процедур в свою очередь требуется секретный ключ. Если в качестве открытого классического канала используется, например, интернет, то для целей аутентификации возможна генерация ключей по схеме Хеллмана–Диффи [8]. Если же для открытого классического канала используется та же самая оптоволоконная линия, что и для квантового канала связи, то генерация ключей для аутентификации по схеме Хеллмана–Диффи оказывается принципиально неприемлемой из-за очевидной атаки, так называемой атаки «man in the middle». В такой ситуации требуется небольшой стартовый ключ один раз при первом сеансе. При последующих сеансах этот ключ выбрасывается, и для аутентификации и сохранения целостности данных, передаваемых по классическому каналу, используется часть ключа, сгенерированного по квантовому каналу в предыдущем сеансе обмена. Остальная бóльшая часть ключа, полученного по квантовому каналу, используется собственно для шифрования данных. Если для аутентификации и сохранения целостности данных используются процедуры на основе ГОСТа, то длина стартового ключа составляет 256 бит. При этом в течение нескольких секунд обмена может быть получен новый секретный ключ по квантовому каналу гораздо более длинный, чем исходный.

Разумеется, стартовый ключ мог бы быть использован для шифрования нового ключа и передаче его второму легитимному пользователю. Однако при этом абсолютная секретность нового ключа гарантируется, лишь если его длина не более длины ключа, на котором он шифруется. То есть более длинного ключа получить нельзя. В квантовой криптографии стартовый ключ не используется напрямую для передачи нового ключа, который генерируется по квантовому каналу связи. Как будет видно ниже, число бит открытой информации, переданной по открытому классическому каналу на один бит нового секретного ключа, меньше единицы, поэтому возможно расширение ключа.

Подход с небольшим стартовым ключом является более предпочтительным, поскольку при этом возможно свести к минимуму число раундов обмена по открытому каналу связи в процессе «чистки» и усиления секретности ключа (privacy amplification).

Основная задача теории сводится к выяснению длины секретного ключа, который может быть получен при наблюдаемых изменениях статистики результатов измерений на приемном конце по сравнению со статистикой на невозмущенных состояниях. Как правило, величиной, которая характеризует отклонение статистики измерений от идеальной, является величина вероятности ошибки. Точнее, вероятности того, что переданный бит был 0, а зарегистрирован как 1, и наоборот. Хотя возможны и другие критерии для изменения статистики. Оценка вероятности ошибки получается путем сравнения через открытый канал части переданной последовательности по квантовому каналу, в дальнейшем раскрытая часть отбрасывается.

Следующий этап состоит в коррекции ошибок в нераскрытой части последовательности у легитимных пользователей посредством обмена информацией через открытый канал связи. Обычно легитимные пользователи называются Alice и Bob, а подслушиватель — Eve. В результате коррекции ошибок остается последовательность бит меньшей длины и одинаковая у Alice и Bob. Одинаковая означает, что последовательности совпадают с вероятностью сколь угодно близкой к единице (например, $1-2^{-200}\approx 1-10^{-70}$. Напомним, что число атомов в видимой части Вселенной оценивается как 10^{77}).

После «чистки» первичного ключа у подслушивателя имеется строка бит или регистр квантовой памяти с состояниями, или и то, и другое вместе. По-

следний шаг при получении финального секретного ключа состоит в сжатии (фактически в применении случайной функции хэширования) уже одинаковой последовательности у Alice и Bob. Сжатая последовательность бит является общим секретным ключом для легитимных пользователей, для которых гарантируется, что подслушиватель имеет о ключе сколь угодно малую информацию по некоторому, заданному Alice и Bob параметру секретности.

Естественным требованием к процедурам коррекции ошибок и усиления секретности ключа является сохранение как можно большего числа бит в финальном ключе. Еще одно требование состоит в минимизации числа обменов по открытому каналу связи в пересчете на один бит в финальном секретном ключе.

При коррекции ошибок в первичном ключе задача легитимных пользователей состоит не только в исправлении ошибок, но также в оценке верхней границы информации, которую может получить об оставшемся ключе подслушиватель из обменов по открытому каналу связи. Для коррекции ошибок возможно использование различных процедур, включая хорошо разработанные классические коды, исправляющие ошибки. Причем заранее отнюдь не очевидно, какой из методов окажется более эффективным по упомянутым выше критериям.

Ниже будут рассмотрены методы коррекции ошибок, основанные на процедуре бисективного поиска, комбинированном каскадном методе, а также на классических кодах Боуза–Чоудхури–Хоквингема и Хэмминга. Важно отметить, что эффективность различных методов не может быть выяснена в отрыве от квантовой части протокола генерации ключа.

Из анализа будет видно, что независимо от используемых конструктивных методов коррекции ошибок, окончательный ответ о величине верхней границы информации, которую может получить подслушиватель о финальном ключе после исправления ошибок, определяется тем, что подслушиватель может делать коллективные измерения над целыми блоками квантовых состояний с использованием квантовой памяти. Хотя на сегодняшний день такие измерения над большим числом запутанных состояний находятся за пределами технологических возможностей, законы квантовой механики не запрещают делать такие измерения. Данная проблема отсутствует, если подслушиватель ограничен индивидуальными измерениями.

2. КВАНТОВАЯ ЧАСТЬ ПРОТОКОЛА ГЕНЕРАЦИИ ПЕРВИЧНОГО КЛЮЧА

Концептуально наиболее простым квантовым протоколом распространения ключа является квантовая криптография на двух неортогональных состояниях (протокол B92). Хотя для практических целей данный протокол ограничен затуханием в оптоволокне, длина квантового канала связи для этого протокола не превышает 20 км. Для наших целей данный протокол удобен в силу простоты анализа, и он содержит все основные моменты, которые являются общими для других, более практически важных протоколов распространения ключа.

Квантовая часть протокола выглядит стандартным образом [9, 10]. В качестве информационных состояний на передающем конце выбирается пара неортогональных состояний, отвечающих классическим битам 0 и 1, $0 \leftrightarrow |u_0\rangle$, $1 \leftrightarrow |u_1\rangle$. Угол перекрытия (степень неортогональности) удобно параметризовать углом (рис. 1)

$$\langle u_0|u_1\rangle = \sin 2\alpha. \tag{1}$$

Базисные ортогональные векторы в подпространстве, натянутом на векторы $|u_{0,1}\rangle$, обозначим как $|0\rangle$, $|1\rangle$.

На приемном конце Bob использует индивидуальные измерения, которые описываются следующим разложением единицы:

$$\begin{aligned} &I = A_0 + A_1 + A_?, \quad A_0 = \frac{(I - |u_1\rangle\langle u_1|)}{1 + \langle u_1|u_0\rangle}, \\ &A_1 = \frac{(I - |u_0\rangle\langle u_0|)}{1 + \langle u_1|u_0\rangle}, \quad A_? = I - A_0 - A_1. \end{aligned} \tag{2}$$

Пространство результатов Ω состоит из трех событий $\Omega = \{0, 1, ?\}$. Отсчет в канале A_0 интерпрети-

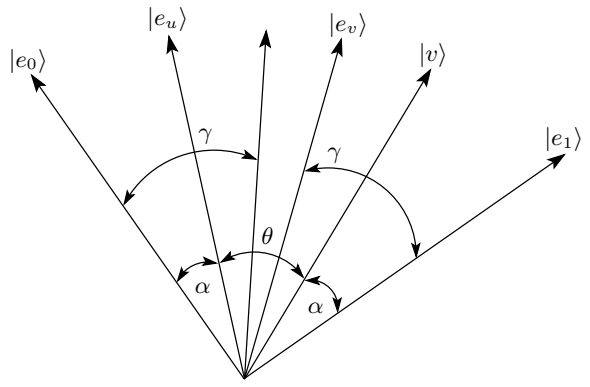

Рис. 1.

руется как 0 и имеет место на невозмущенных состояниях, лишь если было послано состояние $|u_0\rangle$, и никогда на $|u_1\rangle$. Отсчет в канале A_1 на состоянии $|u_1\rangle$ никогда не может произойти. Аналогично, наоборот, если было послано состояние $|u_1\rangle$, то отсчет будет иметь место в канале A_1 и интерпретируется как 1 и никогда не будет иметь место в канале A_0. Отсчет в канале $A_?$ является результатом с неопределенным исходом и может иметь место как на состоянии $|u_0\rangle$, так и на состоянии $|u_1\rangle$.

Для условных вероятностей $\Pr(i|j)$ того, что было послано состояние $|u_j\rangle$ $(j = 0, 1)$, а зарегистрирован исход i $(i = 0, 1, ?)$, имеют место соотношения

$$\Pr(0|0) = \Pr(1|1) = \mathrm{Tr}\{|u_0\rangle\langle u_0|A_0\} = \\ = \mathrm{Tr}\{|u_1\rangle\langle u_1|A_1\} = 1 - \cos\theta, \quad (3)$$

$$\Pr(1|0) = \Pr(0|1) = \mathrm{Tr}\{|u_0\rangle\langle u_0|A_1\} = \\ = \mathrm{Tr}\{|u_1\rangle\langle u_1|A_0\} = 0.$$

Вероятность inconclusive исходов

$$\Pr(?|0) = \Pr(?|1) = \mathrm{Tr}\{|u_0\rangle\langle u_0|A_?\} = \\ = \mathrm{Tr}\{|u_1\rangle\langle u_1|A_?\} = \cos\theta. \quad (4)$$

Различные стратегии подслушивания условно можно разделить на следующие типы.

1) Стратегия «непрозрачного» (opaque) подслушивания часто также называемая прием–переposылка, сводится к измерению непосредственно передаваемого состояния, а затем перепосылке нового состояния в зависимости от результата измерения.

2) При стратегии индивидуального «прозрачного» (translucent) подслушивания подслушиватель в каждой посылке использует свое вспомогательное состояние, которое на время приводится во взаимодействие с передаваемым состоянием. После взаимодействия передаваемое и вспомогательное состояния оказываются в общем запутанном состоянии. Далее подслушиватель проводит измерение в каждой посылке над своим вспомогательным состоянием, а информационное состояние направляется на приемный конец к легитимному пользователю.

3) При «коллективной» атаке подслушиватель действует аналогично предыдущему случаю, но с той разницей, что сохраняет свои вспомогательные состояния в квантовой памяти и не проводит измерения до тех пор, пока не будут переданы все состояния легитимным пользователем и не закончится обмен по открытому каналу с целью исправления ошибок и усиления секретности. Только после этого подслушиватель проводит измерения коллективно сразу над всеми своими состояниями. Такая коллективная атака на ключ является для подслушивателя более эффективной, чем индивидуальные измерения.

4) И наконец, самая общая и, по-видимому, самая эффективная атака (joint attack) аналогична предыдущей с той лишь разницей, что подслушиватель использует единое вспомогательное состояние из гильбертова пространства состояний большой размерности, с которым взаимодействуют передаваемые состояния и все измерения над которым также производятся в самом конце.

Будем рассматривать стратегию прозрачного подслушивания. В каждой посылке Eve готовит свое вспомогательное состояние $|e\rangle$, которое некоторое время взаимодействует с передаваемым состоянием. Формально стратегия Eve формализуется выбором унитарного преобразования, описывающего совместную эволюцию ее состояния и состояния Alice. Имеем

$$|u_0\rangle \otimes |e\rangle \to U(|u_0\rangle \otimes |e\rangle) = \\ = a|u_0\rangle \otimes |e_0\rangle + b|u_1\rangle \otimes |e_1\rangle = |\phi_0\rangle, \quad (5)$$

$$|u_1\rangle \otimes |e\rangle \to U(|u_1\rangle \otimes |e\rangle) = \\ = b|u_0\rangle \otimes |e_0\rangle + a|u_1\rangle \otimes |e_1\rangle = |\phi_1\rangle. \quad (6)$$

Здесь $|e_0\rangle$, $|e_1\rangle$ — состояния (неортогональные) в двумерном подпространстве Eve, a и b — вещественные коэффициенты, которые могут выбираться подслушивателем (фактически определяются оператором совместной унитарной эволюции).

Состояние после совместной эволюции является запутанным (entangled state) — общим для Eve и Bob, Eve и Bob имеют доступ каждый к своему состоянию.

При коллективной атаке на ключ Eve не проводит измерений над своими состояниями до самого конца, пока не закончится обмен информацией по открытому каналу связи.

Состояние, к которому Bob имеет доступ, при условии, что Eve не проводит пока никаких действий над своей частью, дается взятием частичного следа по подпространству Eve:

$$\begin{aligned}
&\rho(|u_0\rangle) = \mathrm{Tr}_E\{|\phi_0\rangle\langle\phi_0|\} = \\
&= a^2|u_0\rangle\langle u_0| + ab\sin 2\gamma(|u_0\rangle\langle u_1| + \\
&+ |u_1\rangle\langle u_0|) + b^2|u_1\rangle\langle u_1|, \\
&\rho(|u_1\rangle) = \mathrm{Tr}_E\{|\phi_1\rangle\langle\phi_1|\} = \\
&= b^2|u_0\rangle\langle u_0| + ab\sin 2\gamma(|u_1\rangle\langle u_0| + \\
&+ |u_0\rangle\langle u_1|) + a^2|u_1\rangle\langle u_1|.
\end{aligned} \tag{7}$$

Bob совершает индивидуальные измерения (2) над состояниями (7). Условные вероятности (3), (4) на возмущенных состояниях теперь имеют вид

$$\begin{aligned}
&\Pr(0|0) = Pr(1|1) = \mathrm{Tr}\{\rho(|u_0\rangle)A_0\} = \\
&= \mathrm{Tr}\{\rho(|u_1\rangle)A_1\} = a^2(1-\sin 2\gamma), \\
&\Pr(1|0) = Pr(0|1) = \mathrm{Tr}\{\rho(|u_0\rangle)A_1\} = \\
&= \mathrm{Tr}\{\rho(|u_1\rangle)A_0\} = b^2(1-\sin 2\gamma).
\end{aligned} \tag{8}$$

Вероятность inconclusive исходов равна

$$\begin{aligned}
&\Pr(?|0) = Pr(?|1) = \mathrm{Tr}\{\rho(|u_0\rangle)A_?\} = \\
&= \mathrm{Tr}\{\rho(|u_1\rangle)A_?\} = 1-(a^2+b^2)(1-\sin 2\gamma).
\end{aligned} \tag{9}$$

Параметром, который описывает отклонение статистики результатов по отношению к статистике на невозмущенных состояниях, является вероятность ошибки. Вероятность того, что послан 0, а зарегистрирована 1, и наоборот, равна

$$Q = \frac{\Pr(1|0)+\Pr(0|1)}{\Pr(0|0)+\Pr(1|1)} = \frac{b^2}{a^2+b^2}. \tag{10}$$

Результаты с неопределенным исходом отбрасываются посредством сообщений через открытый канал. Величина ошибки Q оценивается через открытый канал путем случайной выборки примерно половины переданной последовательности. Раскрытая часть последовательности затем отбрасывается.

Имеется взаимно однозначное соответствие между состояниями Eve и битами, зарегистрированными Bob. Если Alice было послано $|u_0\rangle$ и Bob зарегистрировал 0, то состояние (ненормированное) у Eve будет

$$\begin{aligned}
&\rho^{Eve}_{0\to 0}(|u_0\rangle) = \mathrm{Tr}\{\sqrt{A_0}|\phi_0\rangle\langle\phi_0|\sqrt{A_0}\} = \\
&= (1-Q)|e_0\rangle\langle e_0|.
\end{aligned} \tag{11}$$

Соответственно, если Alice посылала состояние $|u_1\rangle$, и Bob также зарегистрировал 1, то состояние Eve будет

$$\begin{aligned}
&\rho^{Eve}_{1\to 1}(|u_1\rangle) = \mathrm{Tr}\{\sqrt{A_1}|\phi_1\rangle\langle\phi_1|\sqrt{A_1}\} = \\
&= (1-Q)|e_1\rangle\langle e_1|.
\end{aligned} \tag{12}$$

Таблица 1. Соответствие между битовыми строками Alice, Bob и квантовыми состояниями Eve

Alice	0	1	...	0	0	1
Bob	0	1	...	1	0	0
Eve	$\|e_0\rangle$	$\|e_1\rangle$	...	$\|e_1\rangle$	$\|e_0\rangle$	$\|e_0\rangle$
Error position	...	...	...	x	...	x

Аналогично, если Alice посылала состояние $|u_0\rangle$, а Bob зарегистрировал состояние с ошибкой, т. е. 1, то состояние Eve тоже будет отвечать неправильному состоянию

$$\begin{aligned}
&\rho^{Eve}_{0\to 1}(|u_0\rangle) = \mathrm{Tr}\{\sqrt{A_1}|\phi_1\rangle\langle\phi_1|\sqrt{A_1}\} = \\
&= Q|e_1\rangle\langle e_1|.
\end{aligned} \tag{13}$$

Соответственно, наоборот

$$\begin{aligned}
&\rho^{Eve}_{1\to 0}(|u_0\rangle) = \mathrm{Tr}\{\sqrt{A_0}|\phi_1\rangle\langle\phi_1|\sqrt{A_1}\} = \\
&= Q|e_0\rangle\langle e_0|.
\end{aligned} \tag{14}$$

Таким образом, после завершения обмена по квантовому каналу, и отбрасывания через открытый канал inconclusive исходов, Alice, Eve и Bob оказываются в ситуации, отраженной в табл. 1.

Таким образом, Alice и Bob имеют битовые строки. Доля ошибочных позиций у Bob по отношению к Alice есть Q. Eve имеет регистр квантовой памяти. Между состояниями Eve и классическими битами у Bob имеется взаимно однозначное соответствие $0 \leftrightarrow |e_0\rangle$ и $1 \leftrightarrow |e_1\rangle$.

3. ДЛИНА СЕКРЕТНОГО КЛЮЧА В ШЕННОНОВСКОМ ПРЕДЕЛЕ

Формально ситуация между Alice и Bob после отбрасывания inconclusive исходов описывается классическим бинарным симметричным каналом связи с переходными вероятностями

$$\begin{aligned}
&\Pr(0|0) = \Pr(1|1) = 1-Q, \\
&\Pr(1|0) = \Pr(0|1) = Q.
\end{aligned} \tag{15}$$

С равными априорными вероятности на входе

$$\Pr(0) = \Pr(1) = \frac{1}{2}.$$

Из-за взаимно однозначного соответствия между битами у Bob и состояниями Eve ситуация между Alice

и Eve описывается квантовым бинарным симметричным каналом связи со входными состояниями

$$\rho_0 = |u_0\rangle\langle u_0|, \quad \rho_1 = |u_1\rangle\langle u_1|$$

и выходными состояниями у Eve

$$|e_0\rangle\langle e_0|, \quad |e_1\rangle\langle e_1|.$$

Формально квантовый канал описывается как преобразование входных матриц плотности в выходные матрицы плотности. Такое преобразование задается супероператором $\mathcal{T}_{AE}[\dots]$ линейным вполне положительным отображением, сохраняющим (или уменьшающим) след; унитарное представление супероператора есть

$$\mathcal{T}_{AE}[\dots] = \mathrm{Tr}_B\{\sqrt{A_0}U([\dots]\otimes|e\rangle\langle e|)U^{-1}\sqrt{A_0}\} + \\ + \mathrm{Tr}_B\{\sqrt{A_1}U([\dots]\otimes|e\rangle\langle e|)U^{-1}\sqrt{A_1}\}. \quad (16)$$

Далее имеем

$$\mathcal{T}_{AE}[|u_0\rangle\langle u_0|] = (1-Q)|e_0\rangle\langle e_0| + Q|e_1\rangle\langle e_1|, \\ \mathcal{T}_{AE}[|u_1\rangle\langle u_1|] = (1-Q)|e_1\rangle\langle e_1| + Q|e_0\rangle\langle e_0|. \quad (17)$$

Найдем теперь критическую величину ошибки между Alice и Bob, до которой возможно распространение секретного ключа, а также его длину в пределе длинной последовательности, $n\to\infty$. При этом удобно воспользоваться методом случайного кодирования в духе Шеннона. Конечно, на практике такой метод кодирования неприемлем, поскольку требует перебора по экспоненциально большому числу кодовых слов, но удобен для установления верхней границы ошибки, до которой возможна передача секретного ключа. Пусть кодовые слова длины n выбираются Alice случайно. Первым кодовым словом выбирается битовая строка, переданная Alice. Далее генерируется случайно еще $M-1$ кодовое слово. Все M кодовых слов через открытый классический канал сообщаются Bob. Естественно, считается, что все они доступны также и Eve.

Обозначим кодовые слова как

$$w^{(1)}, w^{(2)}, \dots, w^{(M)},$$

где

$$w^{(j)} = (j_1, j_2, \dots, j_n), \quad j_k = 0, 1.$$

Избыточность кода (фактически число кодовых слов) должна быть такой, чтобы Bob с вероятностью единица смог отличить правильное кодовое слово, первую битовую строку, посланную Alice по квантовому каналу связи. Прямая терема кодирования Шеннона гласит [11, 12], что если число кодовых слов

$$M < 2^{n[C_{AB}(Q)-\delta]}, \quad \delta\to 0, \\ C_{AB}(Q) = 1 + Q\log Q + (1-Q)\log(1-Q), \quad (18)$$

где $C_{AB}(Q)$ — классическая пропускная способность классического бинарного симметричного канала связи, то вероятность правильного декодирования в среднем по всем кодовым словам стремится к единице [11, 12]. Другими словами, Bob сравнивает свою битовую строку со всеми кодовыми словами и выбирает ближайшее в смысле расстояния по Хэммингу, которое отличается от его строки в минимальном числе позиций. С вероятностью единица Bob попадает на правильное кодовое слово (переданную строку Alice). Это позволяет ему исправить ошибки в его строке и получить одинаковую с Alice строку, которая является первичным ключом. Вероятность ошибки декодирования в среднем по всем кодовым словам при условии (18) есть

$$P_e(n,M) = \frac{1}{M}\sum_{j=1}^{M}[1-\Pr(w_B^j|w^j)] \le \\ \le \varepsilon + (M-1)2^{-n[C_{AB}(Q)-\delta]} < \varepsilon(n,M)\to 0, \quad (19)$$

где $\Pr(w_B^j|w^j)$ — условная вероятность того, что посланное кодовое слово w^j правильно декодировано. Иначе говоря, для любого наперед заданного $\varepsilon(n,M)$ найдется сколь угодно малое δ и $n > N$, начиная с которого выполняется соотношение (19).

По сути случайный выбор M кодовых слов в пространстве битовых строк длиной n и размерностью 2^n означает, что расстояние по Хэммингу между ближайшими кодовыми словами слегка превышает Qn (число ошибочных позиций), что позволяет Bob декодировать свою строку в правильное кодовое слово с вероятностью единица.

Подслушиватель имеет регистр квантовой памяти с неортогональными состояния (табл. 1), над которыми Eve может делать индивидуальные измерения над состоянием в каждой ячейке, либо коллективные сразу над всем регистром. Рассмотрим сначала индивидуальные измерения. К коллективным измерениям вернемся несколько позже. Оптимальное измерение, минимизирующее ошибку различения пары неортогональных состояний, дается разложением единицы [13]

$$I = \mathcal{M}_0 + \mathcal{M}_1, \quad \mathcal{M}_{0,1} = |m_{0,1}\rangle\langle m_{0,1}|, \quad (20)$$

где $|m_{0,1}\rangle$ — собственные векторы оператора

$|e_0\rangle\langle e_0| - |e_1\rangle\langle e_1|$. Вероятность ошибки различения при этом есть

$$\varepsilon(Q) = \frac{1}{2}[1 - \sqrt{1 - |\langle e_0|e_1\rangle|^2}] = \frac{1}{2}(1 - \cos 2\gamma), \quad (21)$$

и

$$\sin 2\gamma = \frac{\sqrt{1-(1-2Q)^2} - \sin 2\alpha}{\sin 2\alpha[\sqrt{1-(1-2Q)^2}\sin 2\alpha - 1]}.$$

Здесь были использованы условия унитарности и нормировки состояний $|\phi_{0,1}\rangle$ (см. формулы (5), (6)), которые приводят к условиям

$$\begin{aligned} &\sin 2\alpha = 2ab + (a^2+b^2)\sin 2\alpha \sin 2\gamma, \\ &a^2 + b^2 + 2ab \sin 2\alpha \sin 2\gamma = 1. \end{aligned} \quad (22)$$

Отметим, что несложно увидеть, что такая же ошибка при различении будет иметь место, если Eve сразу делает измерение (20) в каждой посылке и не использует квантовую память. Однако использование квантовой памяти при индивидуальных измерениях делает дальнейший анализ более прозрачным.

До исправления ошибок у Bob и после проведение индивидуальных измерений у Eve для вероятности ошибок между Alice–Bob имеет место

$$\Pr\{b_A(i) = b_B(i)\} = 1 - Q, \quad (23)$$

между Bob–Eve

$$\Pr\{b_B(i) = b_E(i)\} = 1 - \varepsilon(Q), \quad (24)$$

между Alice–Eve

$$\Pr\{b_A(i) = b_E(i)\} = (1-Q)(1-\varepsilon) + Q\varepsilon, \quad (25)$$

т. е. ошибка Eve равна

$$E(Q) = 1 - (1-Q)(1-\varepsilon(Q)) + Q\varepsilon(Q). \quad (26)$$

С учетом (21) соотношение (26) может быть переписано в виде

$$E(Q) = Q\cos^2\gamma + (1-Q)\sin^2\gamma.$$

Eve сможет с вероятностью единица декодировать кодовое слово Alice, если $E \le Q$. Равенство

$$Q = E(Q)$$

дает критическую величину ошибки, до которой возможна передача секретного ключа между Alice и Bob.

Если ошибка Alice–Eve больше, чем ошибка Alice–Bob, и, соответственно, пропускная способность бинарного симметричного канала

$$C_{AB}(Q) > C_{AE}(E(Q)),$$

то в пределе, когда длина строки $n \to \infty$, длина секретного ключа, который может быть получен между Alice–Bob, стремится к величине

$$n_{secret} \to n. \quad (27)$$

Для средней вероятности ошибки Eve относительно ключа по всем кодовым словам имеет место соотношение

$$\begin{aligned} &P_e(n,M) = \frac{1}{M}\sum_{j=1}^{M}[1 - \Pr(w_E^j|w^j)] \ge \\ &\ge 1 - O(1)2^{-n[C_{AB}(Q) - C_{AE}(E(Q))]} \to 1, \\ &\qquad n \to \infty, \\ &C_{AE}(E(Q)) = 1 + E(Q)\log E(Q) + \\ &+ (1-E(Q))\log(1-E(Q)). \end{aligned} \quad (28)$$

Это фактически является следствием теоремы для величины ошибки при передаче со скоростью, превышающей пропускную способность классического канала связи без памяти [11, 12, 14]. Другими словами, соотношение (28) является следствием «сильного обращения» теоремы кодирования Шеннона. Слова «сильное обращение» означают стремление ошибки декодирования к единице при превышении пропускной способности. Если имеет место оценка, при которой ошибка декодирования лишь отлична от нуля, но, вообще говоря, не гарантируется ее стремление к единице с ростом n, то говорят о слабом обращении прямой теоремы кодирования. Именно такая ситуация имеет место при коллективных измерениях.

Для идентификации переданных состояний Eve может выполнять коллективные измерения. Формально ситуация между Alice и Eve описывается квантовым каналом связи, который сам по себе описывается супероператором, преобразующим матрицы плотности на стороне Alice в выходные матрицы плотности, доступные для измерений Eve. Супероператор $\mathcal{T}_{AE}[\dots]$ дается соотношениями (16), (17). Квантово-механические измерения Eve задаются решающими операторами, которые образуют разложение единицы в пространстве состояний Eve:

$$I = \sum_{k=1}^{M} \mathcal{X}_{w^k}, \quad (29)$$

где решающие (измеряющие) операторы имеют вид (детали см. в работах [15–18])

$$\mathcal{X}_{w^k} = \left(\sum_{l=1}^{M} \mathcal{P}\mathcal{P}_{w^l}\right)^{-1/2} \times \times \mathcal{P}\mathcal{P}_{w^k}\mathcal{P}\left(\sum_{l=1}^{M} \mathcal{P}\mathcal{P}_{w^l}\mathcal{P}\right)^{-1/2}. \quad (30)$$

Здесь $\mathcal{P}$ — проектор на типичное подпространство матрицы плотности

$$\left(\frac{1}{2}\mathcal{T}_{AE}[|u_0\rangle\langle u_0|] + \frac{1}{2}\mathcal{T}_{AE}[|u_1\rangle\langle u_1|]\right)^{\otimes n} = = \left(\frac{1}{2}\left(|e_0\rangle\langle e_0| + |e_1\rangle\langle e_1|\right)\right)^{\otimes n}, \quad (31)$$

а $\mathcal{P}_{w^k}$ — проектор на типичное подпространство матрицы плотности, отвечающей некоторому кодовому слову w^k:

$$\rho_{w^k} = \rho_{i_1} \otimes \rho_{i_2} \otimes \cdots \cdot \rho_{i_n}, \quad i_k = 0,1, \quad k = 1,2,\ldots,M, \quad (32)$$

$$\rho_{i_k} = \begin{cases} (1-Q)|e_0\rangle\langle e_0| + Q|e_1\rangle\langle e_1|, & i_k = 0, \\ (1-Q)|e_1\rangle\langle e_1| + Q|e_0\rangle\langle e_0|, & i_k = 1. \end{cases} \quad (33)$$

$\mathcal{P}_{w^k}$ выбирается как спектральный проектор ρ_{w^k}, отвечающий произведению собственных чисел $\Lambda_I = \lambda_{i_1} \cdot \lambda_{i_2} \cdots \lambda_{i_n}$, лежащих в интервале

$$e^{-n\ [\overline{H}(\rho)+\delta]} < \Lambda_I < e^{-n[\overline{H}(\rho)-\delta]}, \quad (34)$$

где

$$\overline{H}(\rho) = \frac{1}{2}\left[S((1-Q)|e_0\rangle\langle e_0| + Q|e_1\rangle\langle e_1|) + + S((1-Q)|e_1\rangle\langle e_1| + Q|e_0\rangle\langle e_0|)\right], \quad (35)$$

$$S(\rho) = -\mathrm{Tr}\{\rho\log(\rho)\} \quad (36)$$

— энтропия фон Неймана.

Проекторы обладают следующими важными свойствами [15]:

$$\mathcal{P}_{w^k} \le \rho_{w^k} e^{n[\overline{H}(\rho)+\delta]}, \quad \mathbf{E}\left\{\mathrm{Tr}\{\rho_{w^k}(I - \mathcal{P}_{w^k})\}\right\} \le \varepsilon. \quad (37)$$

Символ $\mathbf{E}$ означает усреднение по всем последовательностям случайных кодовых слов. Вероятность различения кодовых последовательностей при помощи измеряющих операторов (30) у Eve равна

$$P_e(n,M) = \frac{1}{M}\sum_{k=1}^{M}[1 - \Pr(w^k = w_E^k)], \quad \Pr(w^k = w_E^k) = \mathrm{Tr}\{\rho_{w^k}\mathcal{X}_{w^k}\}. \quad (38)$$

Как показано в работах [15,18], ошибка стремится к нулю, если число кодовых слов M не превосходит величины

$$M \le 2^{n[\overline{C}_{\mathcal{T}_{AE}} - \delta]}, \quad (39)$$

и ошибка

$$P_e(n,M) < 8\varepsilon + (M-1)2^{-n[\overline{C}_{\mathcal{T}_{AE}} - 3\delta]} \to 0 \quad (40)$$

стремится к нулю при условии (39). Величина в показателе в соотношении (39) представляет собой классическую пропускную способность неидеального квантового канала связи [15,18], который описывается супероператором (16), (17):

$$\overline{C}_{\mathcal{T}_{AE}} = S\left(\frac{1}{2}\mathcal{T}_{AE}[|u_0\rangle\langle u_0|] + \frac{1}{2}\mathcal{T}_{AE}[|u_1\rangle\langle u_1|]\right) - - \frac{1}{2}S\left(\mathcal{T}_{AE}[|u_0\rangle\langle u_0|]\right) - \frac{1}{2}S\left(\mathcal{T}_{AE}[|u_1\rangle\langle u_1|]\right) = = -\frac{1-\sin 2\gamma}{2}\log\frac{1-\sin 2\gamma}{2} - \frac{1+\sin 2\gamma}{2} \times \times \log\frac{1+\sin 2\gamma}{2} + \Lambda_-\log\Lambda_- + \Lambda_+\log\Lambda_+, \quad (41)$$

где

$$\Lambda_\pm = \frac{1}{2}\left(1 \pm \sqrt{1-4\mathcal{Z}}\right), \quad (42)$$

$$\mathcal{Z} = \left[(1-Q)\cos^2\gamma + Q\sin^2\gamma\right] \times \times \left[(1-Q)\sin^2\gamma + Q\cos^2\gamma\right] - \cos^2\gamma\sin^2\gamma. \quad (43)$$

Передача секретного ключа возможна лишь при условии, что Eve не сможет распознать правильное слово. Если выбранное число кодовых слов M в канале Alice–Bob меньше, чем в канале Alice–Eve, то передача ключа заведомо невозможна. Eve различает правильную строку с вероятностью единица. Если Eve ограничена лишь индивидуальными измерениями, а Alice и Bob корректируют ошибки на приемном конце при помощи случайного кодирования, то критерий секретности (возможности передачи ключа) выглядит как (28) (см. также [19])

$$C_{AB}(Q) > C_{AE}(E(Q)). \quad (44)$$

При этом в пределе больших n Bob сможет исправить все ошибки в своей строке с вероятностью единица. Ошибка Eve при этом будет стремится к единице (т. е. имеет место сильное обращение прямой теоремы кодирования). Alice и Bob могут использовать всю строку длины n как секретный ключ.

Если же Eve имеет возможность делать коллективные квантово-механические измерения (29), (30),

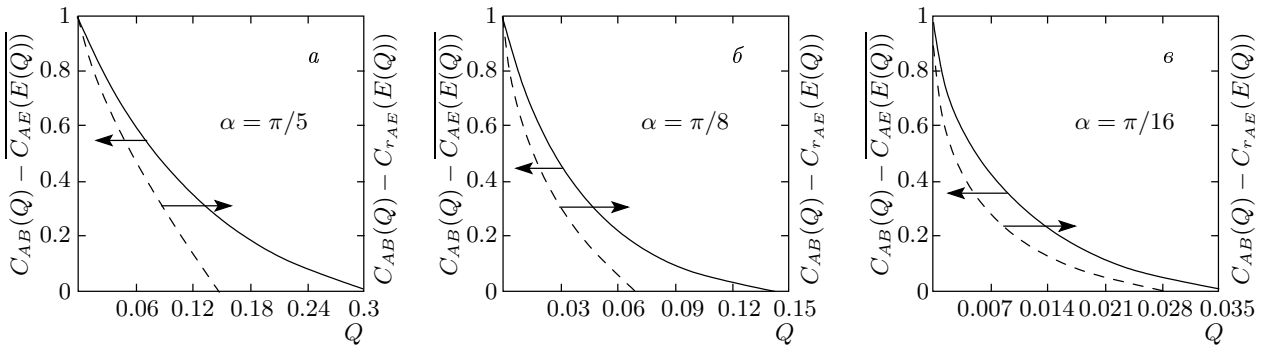

Рис. 2.

то она сможет различить с вероятностью единица правильную строку, если выбранное число кодовых слов легитимными пользователями

$$M < 2^{n[\overline{C}_{\tau_{AE}} - \delta]}.$$

Поэтому заведомо с момента, когда

$$C_{AB}(Q) = \overline{C}_{\tau_{AE}}, \tag{45}$$

передача секретного ключа невозможна, если Eve может выполнять коллективные измерения.

В том случае, если выбранное Alice число кодовых слов $M > 2^{n\overline{C}_{\tau_{AE}}}$, то даже с использованием коллективных измерений Eve не сможет декодировать свою строку в правильное кодовое слово, в отличие от Bob, который при числе кодовых слов

$$M < 2^{n[C_{AB}(Q) - \delta]}$$

сможет исправить с вероятностью единица все ошибки в своей строке длины n. Ошибка Eve при декодировании в среднем по всем кодовым словам при этом не менее

$$P_e(n, M = 2^{nC_{AB}(Q)}) > C_{AB}(Q) - \overline{C}_{\tau_{AE}}. \tag{46}$$

То есть имеет место так называемое слабое обращение прямой теоремы кодирования. Ошибка отлична от нуля, но стремится к единице, однако, в отличие от классического случая или индивидуальных измерений Eve, не экспоненциально по параметру

$$n[C_{AB}(Q) - C_{AE}(E(Q))],$$

а существенно медленнее.

При индивидуальных измерениях (фактически в классическом случае) Eve при условии

$$C_{AB}(Q) > C_{AE}(E(Q))$$

с вероятностью единица при больших n не знает битовую строку у Alice и Bob, поэтому вся строка может быть использована как секретный ключ.

В случае коллективных измерений (истинно квантовый случай) вероятность ошибки Eve в среднем при различении кодового слова не лучше, чем $C_{AB}(Q) - \overline{C}_{\tau_{AE}}$, соответственно, вероятность правильной интерпретации не более чем

$$1 - [C_{AB}(Q) - \overline{C}_{\tau_{AE}}].$$

При консервативной оценке, возможно завышенной в пользу Eve, Eve из всего числа кодовых слов M знает $2^{n\overline{C}_{\tau_{AE}}}$. Поскольку при

$$M < 2^{nC_{AB}(Q)}$$

Bob исправляет все ошибки в своей строке длины n, то, завышая оценку по числу кодовых слов до полной размерности пространства 2^n, можно считать, что Eve знает долю бит из всего пространства, равную $2^{n\overline{C}_{\tau_{AE}}}/2^n$. Поскольку кодовые слова выбираются случайно и равномерно, доля бит в каждой конкретной строке, которые Eve знает, не более $n\overline{C}_{\tau_{AE}}$. В каждой строке $n[1 - \overline{C}_{\tau_{AE}}]$ бит могут считаться легитимными пользователями секретными.

Границы критической величины ошибки Q на приемном конце у Bob показаны на рис. 2 для различных значений углов перекрытия α информационных состояний, посылаемых Alice $|u_0\rangle$ и $|u_1\rangle$.

Вообще говоря, того факта, что средняя ошибка Eve стремится к единице, еще недостаточно для гарантии секретности ключа. Дело в том, что соотношения (27), (28) являются асимптотическими результатами, справедливыми при $n \to \infty$. В реальной ситуации длина битовой строки может быть хотя и большой, но все же конечной. Требование секретности ключа сводится к тому, что взаимная информация данной битовой строки Eve w_E длины n из мно-

жества всевозможных строк W_E относительно множества битовых строк Alice и Bob W, которые уже равны, должна быть экспоненциально мала по заданному параметру секретности s

$$I(W;W_E=w_E)<\frac{2^{-s}}{\ln 2} \tag{47}$$

или в терминах условной энтропии

$$H(W|W_E=w_e)>n-\frac{2^{-s}}{\ln 2}. \tag{48}$$

Таким образом, n бит «очищенного» и одинакового ключа у Alice и Bob еще не могут быть использованы как секретный ключ, поскольку при конечном n соотношение (28) еще не гарантирует, что взаимная информация Eve будет экспоненциально мала по параметру секретности s. Напомним, что величина

$$I(W;W_E=w_E)=0$$

отвечает вероятности простого угадывания.

Конечным этапом получения финального секретного ключа из одинаковой n-битовой строки у Alice и Bob является сжатие (хэширование) до строки размером r, для которой будет гарантироваться выполнение соотношений (47), (48) по параметру секретности s. Сжатие ключа называется усилением секретности (privacy amplification) и основано на замечательной теореме [20], использующей свойства энтропии Реньи второго порядка и универсальных функций хэширования [21].

Введем необходимые определения. Универсальной функцией хэширования второго порядка называется функция

$$g(x):\{0,1\}^n\to\{0,1\}^r(X\to Y),$$

такая что для любых

$$x_1,x_2\in X,\quad x_1\neq x_2$$

вероятность того, что $y_1=y_2$ ($y_1=g(x_1)$ и $y_2=g(x_2)$) не более чем

$$\frac{1}{|Y|}=\frac{1}{2^r}$$

($|Y|$ — объем пространства r-битовых строк). Множество случайный функций $g\in G$ есть множество универсальных функций второго порядка, если при случайном выборе с равномерным распределением на G найдется не более $|G|/|Y|$ функций, для которых возможна коллизия значений функций при разных аргументах. Другими словами, если функции выбираются случайно в соответствии с равномерным распределением, то для данной выбранной функции вероятность для двух различных n-битовых строк иметь одно и то же хэш-значение функции не превышает 2^{-r}.

Применительно к задачам криптографии (в том числе и квантовой) это означает, что если подслушиватель имеет n-битовую строку, отличную от n-битовых строк легитимных пользователей, то после хэширования (сжатия) случайно выбранной и известной всем хэш-функцией, вероятность того, что r-битовая строка совпадает со строками легитимных пользователей, не превышает 2^{-r}.

Теорема об усилении секретности позволяет связать параметры n,r,s и свойства универсальных функций хэширования через энтропию Реньи второго рода, которая определяется через условные вероятности $\Pr(W|w_E)$. Для этого потребуются следующие определения. Пусть $x\in X$ — случайная величина с распределением $P_X(x)$ на X. Вероятностью коллизий по определению называется величина

$$P_c(X)=\sum_{x\in X}P_X^2(x), \tag{49}$$

которая представляет собой вероятность того, что в двух независимых испытаниях случайная величина x примет одно и то же значение. Энтропия Реньи второго порядка по определению есть

$$R(X)=-\log P_c(X). \tag{50}$$

Аналогичные соотношения имеют место для условных распределений вероятности

$$P_c(X|Y=y)=\sum_{y\in Y}P^2_{X|Y=y}(y), \tag{51}$$

$$R(X|Y=y)=-\log P_c(X|Y=y). \tag{52}$$

Среднее значение энтропии Реньи есть

$$R(X|Y)=\sum_{y\in Y}P_Y(y)R(X|Y=y). \tag{53}$$

Для дальнейшего при вычислении взаимной информации подслушивателя о ключе важны следующие соотношения между энтропией Реньи и энтропией Шеннона:

$$R(X)\le H(X), \tag{54}$$

$$H(X)=-\sum_{x\in X}P_X(x)\log P_X(x).$$

Имеет место соотношение для любого совместного распределения

$$R(X|Y) \le H(X|Y). \tag{55}$$

Следующая теорема играет фундаментальную роль в криптографии.

Теорема об усилении секретности (privacy amplification theorem) [20]. Пусть $x \in X$ — случайная величина с распределением $P_X(x)$ и $R(X)$ — энтропия Реньи второго порядка. Пусть $g \in G$ — случайная величина с равномерным распределением на множестве универсальных хэш-функций второго порядка G, $g : X \to \{0,1\}^r$, и $K = G(X)$. Тогда имеет место неравенство

$$H(K|G) \ge R(K|G) \ge r - \log(1 + 2^{r-R(X)}) \ge \\ \ge r - \frac{2^{r-R(X)}}{\ln 2}, \tag{56}$$

где $H(K|G) = H(G(X)|G)$ — средняя условная энтропия Шеннона. Хэш-функция здесь сама является случайной величиной.

Применительно к задачам квантовой криптографии важно следующее следствие теоремы. Пусть имеется совместное распределение вероятностей P_{WW_E}, вообще говоря, неизвестное. Если энтропия Реньи

$$R(W|W_E = w_E) = c$$

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 неравенство

$$H(K|G, W_E = w_E) \ge r - \log(1 + 2^{r-c}) \ge \\ \ge z - \frac{2^{r-c}}{\ln 2}. \tag{57}$$

Для индивидуальных измерений условная вероятность $P_{W|W_E=w_E}(w_E)$ есть

$$P_{W|W_E=w_E}(w_E) = (1-\varepsilon)^{n-d(w_E,W)}\varepsilon^{d(w_E,W)}, \tag{58}$$

где $d(w_E, W)$ — расстояние по Хэммингу между строками W и $W_E = w_E$. Энтропия Реньи при этом равна

$$R(W|W_E = w_E) = -n\log[\varepsilon^2 + (1-\varepsilon)^2], \\ \varepsilon = \frac{1}{2}(1 - \cos 2\gamma). \tag{59}$$

Для взаимной информации Eve относительно ключа имеем

$$I(K; GW_E) = H(K) - H(K|GW_E) \le \frac{2^{-s}}{\ln 2}, \tag{60}$$

где

$$r = c - s = -n\log[\varepsilon^2 + (1-\varepsilon)^2] - s, \tag{61}$$

s — параметр секретности.

Для дальнейшего принципиально важно, что степень сжатия ключа зависит от конкретной процедуры коррекции ошибок в первичном ключе, которую используют легитимные пользователи. Выше под величиной $P_{W|W_E=w_E}(w_E)$ нужно понимать условную вероятность уже после очистки ключа легитимными пользователями. Исходно Alice и Bob имеют несовпадающие строки,

$$P_{W_A|W_B=w_B}(w_B) \ne 1,$$

соответственно, для Eve

$$P_{W_A|W_E=w_E}(w_E) \ne 1.$$

После коррекции ошибок в ключе посредством обмена через открытый канал $w = w_A = w_B$, а $w_E \ne w$. Поскольку все обмены при «чистке» первичного ключа идут через открытый канал, Eve также может частично исправлять ошибки в своей битовой строке, т. е. после коррекции ошибок

$$P_{W|W_E=w_E}(w_E) \ne P_{W_A|W_E=w_E}(w_E).$$

Иными словами, процедура «чистки» ключа, вообще говоря, изменяет переходную вероятность у Eve.

Поэтому задача легитимных пользователей состоит не только в исправлении ошибок, но и установлении того, как изменяется условная вероятность для Eve об их строке.

Ниже будут рассмотрены несколько методов коррекции ошибок в первичном ключе. В зависимости от используемого метода условная информация Eve может изменяться, а может оставаться прежней. Отметим, что эффективность того или иного метода определяется длиной финального ключа (при одинаковых параметрах секретности), а не только длиной очищенного ключа. Возможна ситуация, когда при одном методе после «чистки» остается строка большей длины, чем при использовании другого метода, но при этом увеличивается условная вероятность для Eve, так что требуется более сильное сжатие (при заданном параметре секретности), которое приводит к более короткому финальному ключу. Как будет видно ниже, именно такая ситуация имеет место при чистке первичного ключа при помощи классических кодов.

4. «ЧИСТКА» ПЕРВИЧНОГО КЛЮЧА БИСЕКТИВНЫМ ПОИСКОМ (BINARY)

Рассмотрим метод бисективного поиска с последующим выбрасыванием ошибок [22]. Выбрасывание ошибок позволяет достаточно прозрачно проследить изменение условных вероятностей.

После завершения квантовой части протокола Alice и Bob имеют, вообще говоря, разные битовые строки длины N. Eve имеет регистр квантовой памяти со своими состояниями, между которыми и классическими битами у Bob существует взаимно однозначное соответствие. Точное число ошибочных бит в строке Bob заранее неизвестно. Alice (или Bob) делает случайную выборку длины $N/2$ и открыто сообщает биты в выбранных позициях. После сравнения этих бит Alice и Bob получают оценку вероятности ошибки, равную Q. Далее процедура локализации ошибок выглядит следующим образом.

1. Bob вычисляет размер блока L, исходя из оценки вероятности ошибки, так чтобы в блоке длины L в среднем была одна ошибка.

2. Alice разбивает свою строку на блоки длины L, вычисляет биты четности и посылает их Bob.

3. Bob сравнивает биты четности для каждого блока. Если биты четности не совпадают (в блоке есть нечетное число ошибок), то происходит бисективный поиск (см. ниже).

4. Раскрытие битов четности для каждого блока через открытый канал приводит к утечке информации ровно в один бит. Alice и Bob согласованно выбрасывают по одному биту из каждого блока, тем самым компенсируя утечку информации при раскрытии битов четности.

5. Alice производит случайное перемешивание оставшейся строки и сообщает Bob о сделанной перестановке. Данная процедура не меняет информацию Eve о битовых строках Alice и Bob. Далее процесс повторяется с п. 1.

6. Если ошибки не обнаруживаются после 20–30 проходов, то ключ вероятно одинаков у Alice и Bob.

7. После этого Alice генерирует случайную строку, сообщает ее Bob. Alice и Bob сравнивают биты четности строк и сообщают их друг другу. Затем происходит согласованное отбрасывание по одному биту. Если биты четности совпадают после M проходов, то с вероятностью $1-2^{-M}$ Alice и Bob имеют идентичные строки — очищенный ключ. Параметр M выбирается из технических требований.

Вычисление размера блока проводится, исходя из условия, чтобы в блоке в среднем было не более одной ошибки. Если исходная строка бит длины

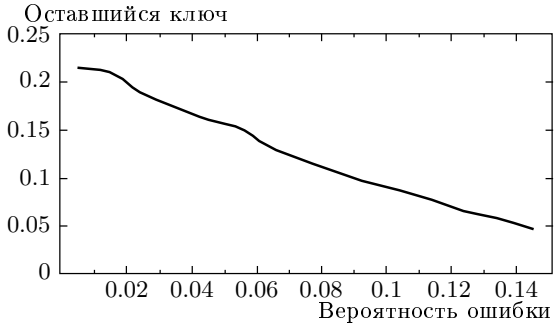

Рис. 3.

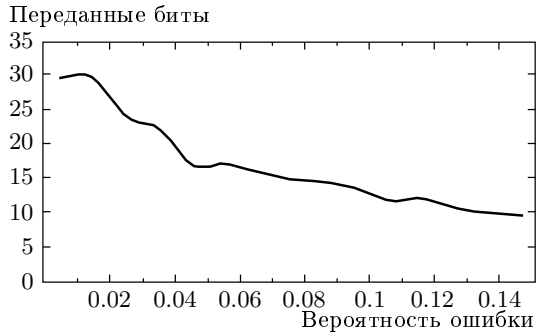

Рис. 4.

$N/2$ имела вероятность ошибки Q, то среднее число ошибок $N_{err} \approx QN/2$, размер блока выбирался как $L = p(N/N_{err})$. Параметр p лежит в пределах $0 < p < 1$, и, как показывает численный эксперимент, хорошим значением является $p = 0.5$. Грубо говоря, в среднем ошибка присутствует лишь в каждом втором блоке.

Бисективный поиск используется для локализации ошибок в тех блоках, в которых биты четности у Alice и Bob не совпадают, и сводится к следующим шагам.

1. Bob разбивает каждый блок, в котором осуществляется поиск, пополам (с округлением в большую сторону) и посылает Alice биты четности для первой половины.

2. Если биты четности не совпадают, то происходит переход к п. 1.

3. Если биты четности первого блока совпадают, то Bob переходит ко второму блоку, как описано в п. 1. Все раскрытые биты четности отбрасываются.

4. Если размер блока меньше 4 бит, то блок целиком выбрасывается и поиск останавливается. Найденные ошибочные биты также отбрасываются.

Результаты расчетов приведены на рис. 3, 4, 5.

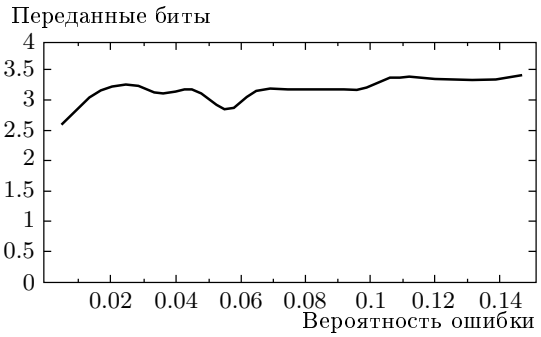

Рис. 5.

5. СВЯЗЬ ДЛИНЫ ФИНАЛЬНОГО КЛЮЧА С КВАНТОВОЙ ЧАСТЬЮ ПРОТОКОЛА

После коррекции ошибок Alice и Bob имеют одинаковые строки. Рассмотрим, в какой ситуации находится Eve. Следуя обмену по открытому каналу, Eve удаляет из квантовой памяти те позиции, которые отбрасываются Alice и Bob, не делая пока никаких измерений над своими состояниями. Поскольку до коррекции ошибок было взаимно однозначное соответствие между битами Bob и состояниями Eve, то после исправления ошибок имеет место ситуация, отраженная в табл. 2.

Таблица 2. Соответствие между битовыми строками Alice, Bob и квантовыми состояниями Eve после коррекции ошибок

Alice	0	1	...	0
Bob	0	1	...	0
Eve	$\|e_0\rangle$	$\|e_1\rangle$	...	$\|e_0\rangle$

Соответствие сохраняется, только теперь у Bob неправильные биты отсутствуют, соответственно, у Eve отсутствуют неправильные квантовые состояния, т. е. условная вероятность между любым битом i у Alice и Bob и состоянием Eve равна

$$\Pr(i||e_i\rangle) = 1 \quad (i = 0, 1).$$

После выполнения оптимального измерения (20), (21) над состояниями Eve и получения некоторой конкретной битовой строки условная вероятность становится равной (58), где под величиной n следует понимать длину оставшейся строки после коррекции ошибок Alice и Bob. Степень сжатия строки при получении окончательного секретного ключа дается соотношением (61), при этом информация Eve о секретном ключе не превышает (60).

Законы квантовой механики не запрещают Eve делать коллективные измерения сразу над всеми состояниями регистра, в этом случае Eve может получить больше информации о ключе, чем это позволяют сделать индивидуальные измерения.

После «чистки» ключа легитимные пользователи имеют уже одинаковые классические битовые строки, а Eve — регистр квантовой памяти с состояниями. Формально Eve может рассматривать такую ситуацию между Alice(Bob) – Eve как передачу классической информации по бинарному квантовому каналу связи. Точнее, из-за того что имеется взаимно однозначное соответствие между классическими битами у Alice (Bob)и квантовыми состояниями у Eve,

$$0 \leftrightarrow |e_0\rangle, \quad 1 \leftrightarrow |e_1\rangle,$$

Eve считает, что Alice (Bob) случайно с равной вероятностью $1/2$ выбирают 0 или 1, сопоставляют (кодируют) им квантовые состояния $|e_0\rangle$ или $|e_1\rangle$ и посылают их по идеальному квантовому каналу к Eve. Это как раз и есть передача классической информации при помощи квантовых состояний. Цель Eve — определить с наименьшей ошибкой посредством квантово-механических измерений, какую строку бит передали ей Alice (Bob). Саму исходную классическую строку бит Eve, естественно, не знает.

Пусть набор строк, которые Alice (Bob) кодируют квантовыми состояниями (набор кодовых слов) есть $w^1, w^2, \ldots, w^M$, каждое кодовое слово представляет собой бинарную строку длины n (n — длина «очищенного» ключа у Alice (Bob)), $w^i = \{i_1, i_2, \ldots, i_n\}$, $i_k = 0, 1$. Полное число строк длины n есть $M = 2^n$, но пока будем считать M произвольным.

Цель Eve «привязаться» к классическим кодовым словам. Если бы состояния были ортогональны, то Eve могла бы их достоверно различить, т. е. вписать в соответствующие позиции 0 или 1 и иметь такую же битовую строку, как и Bob. Однако из-за неортогональности состояний они достоверно неразличимы, и при измерении Eve будет иметь дополнительную ошибку по сравнению с Bob. Eve может осуществлять индивидуальные измерения состояний в каждой позиции и интерпретировать результат как 0 или 1, однако ошибка будет меньше, если Eve будет делать коллективные измерения [15], используя описанные ниже измеряющие операторы.

Поскольку кодовые слова выбираются случайно и независимо друг от друга, вероятность появления

отдельного кодового слова (детали см. в [15, 18]) равна

$$\Pr\{w=(i_1,i_2,\ldots,i_n)\}= \\ =p_{i_1}p_{i_2}\cdots p_{i_n}=\frac{1}{2^n},\quad p_{i_k}=\frac{1}{2}, \tag{62}$$

тогда математическое ожидание $\rho_{w^i}=|\psi_{w^i}\rangle\langle\psi_{w^i}|$ есть

$$\mathbf{E}(\rho_{w^i})=\sum_{i_1,i_2,\ldots,i_n} p_{i_1}p_{i_2}\cdots p_{i_n}|e_{i_1}\rangle\langle e_{i_1}|\otimes\cdots \\ \cdots\otimes|e_{i_n}\rangle\langle e_{i_n}|=\rho_E^{\otimes n}, \tag{63}$$

где

$$\rho_E=\frac{1}{2}|e_0\rangle\langle e_0|+\frac{1}{2}|e_1\rangle\langle e_1| \tag{64}$$

— матрица плотности, описывающая состояния квантовой памяти.

Далее Eve использует декодирование квантовых кодовых слов (по сути осуществляет их перевод в классические битовые строки), используя решающее правило, которое задается измеряющими операторами

$$\mathcal{X}_k=|\tilde{\psi}_{w^k}\rangle\langle\tilde{\psi}_{w^k}|,\quad |\tilde{\psi}_{w^k}\rangle=\mathcal{P}|\psi_{w^k}\rangle, \tag{65}$$

где $\mathcal{P}$ — проектор на типичное подпространство матрицы плотности $\rho_E^{\otimes n}$:

$$\mathcal{P}=\sum_{J\in B}|\lambda_J\rangle\langle\lambda_J|, \\ |\lambda_J\rangle=|\lambda_{j_1}\rangle\otimes|\lambda_{j_2}\rangle\otimes\cdots\otimes|\lambda_{j_n}\rangle, \tag{66}$$

$|\lambda_{j_k}\rangle$ — собственные векторы матрицы ρ_E, а $\lambda_J=\lambda_{j_1}\lambda_{j_2}\cdots\lambda_{j_n}$ — ее собственные числа. Типичное подпространство матрицы плотности определено как

$$B=\{J: 2^{-n[H(\rho_E)+\delta]}<\lambda_J<2^{-n[H(\rho_E)-\delta]}\}, \tag{67}$$

при этом выполнены условия (см. [15])

$$\|\rho_E^{\otimes n}\mathcal{P}\|<2^{-n[H(\rho_E)-\delta]},\quad \mathrm{Tr}\{\rho_E^{\otimes n}(1-\mathcal{P}\}<\varepsilon. \tag{68}$$

Величина $H(\rho_E)$ является энтропией фон Неймана и в нашем случае по сути совпадает с классической пропускной способностью бинарного квантового канала связи [15]:

$$\overline{C}(\varepsilon(Q))=H(\rho_E)= \\ =-\mathrm{Tr}\{\rho_E\log\rho_E\}=-\lambda_1\log\lambda_1-\lambda_2\log\lambda_2= \\ =-\frac{1-\sin 2\gamma}{2}\log\frac{1-\sin 2\gamma}{2}-\frac{1+\sin 2\gamma}{2}\times \\ \times\log\frac{1+\sin 2\gamma}{2}, \tag{69}$$

где

$$\lambda_{1,2}=\frac{1\pm\sin 2\gamma}{2}$$

— собственные числа ρ_E.

Подчеркнем, что Eve производит коллективные измерения, т. е. осуществляет измерения, которые являются проектированием на запутанные (сцепленные по терминологии [15]) состояния матрицы плотности (63).

Ошибка Eve при декодировании M кодовых слов, сгенерированных Alice, есть [15]

$$p_E(n,M)=\frac{1}{M}\sum_{k=1}^{M}[1-\Pr(w^k=w_E^k)], \\ \Pr(w^k=w_E^k)=\langle\psi_{w^k}|\mathcal{X}_k|\psi_{w^k}\rangle, \tag{70}$$

что приводит к (детали см. в работе [15]) неравенству

$$p_E(n,M)\le 2\mathrm{Tr}\{\rho^{\otimes n}(1-\mathcal{P})\}+ \\ +(M-1)\mathrm{Tr}\{(\rho^{\otimes n}\mathcal{P})^2\}\le \\ \le 2\varepsilon+(M-1)2^{-n[H(\rho_E)-\delta]}. \tag{71}$$

Величина $\overline{C}(\varepsilon(Q))$ является классической пропускной способностью бинарного квантового канала связи [15]. Если бы Eve делала оптимальные (в смысле минимальности ошибки различения пары неортогональных состояний) индивидуальные измерения, то вместо $\overline{C}(\varepsilon(Q))$ фигурировала бы классическая пропускная способность бинарного квантового канала связи за один шаг (one shot) [15], равная

$$C(\varepsilon(Q))=\frac{1}{2}\left[\left(1+\sqrt{1-\sin^2 2\gamma}\right)\times\right. \\ \times\log\left(1+\sqrt{1-\sin^2 2\gamma}\right)+ \\ \left.+\left(1-\sqrt{1-\sin^2 2\gamma}\right)\log\left(1-\sqrt{1-\sin^2 2\gamma}\right)\right], \tag{72}$$

которая никогда не превосходит $C(\varepsilon(Q))<\overline{C}(\varepsilon(Q))$. Фактически $C(\varepsilon(Q))$ совпадает с величиной $C_{AE}(E(Q))$ из соотношений (28).

Эти результаты требуют аккуратной интерпретации. По сути они означают следующее. Если из числа случайных строк длины n случайным образом выбрано

$$M<2^{n[\overline{C}(\varepsilon(Q))-\delta]},\quad \delta\to 0,$$

строк, одна из которых является истинной строкой Alice (Bob), которая закодирована (сопоставлена) квантовым состояниям $|e_{0,1}\rangle$ (вся таблица, включая

M строк, публично известна), то Eve сможет построить решающие правила для коллективных квантово-механических измерений и с вероятностью единица определить истинную строку среди множества из

$$M < 2^{n[\overline{C}(\varepsilon(Q))-\delta]}$$

строк длины n.

Если же число строк

$$M = 2^{nR} > 2^{n[\overline{C}(\varepsilon(Q))-\delta]}, \quad 0 < R < 1,$$

то Eve не сможет определить правильную строку, имеющуюся у Alice (Bob). Реально после чистки ключа $M = 2^n$ — все множество строк длины n. Поэтому можно считать, что Eve имеет таблицу всех $M = 2^n$ случайных кодовых слов. Eve сможет определить строку (ключ) лишь с некоторой вероятностью ошибки. В квантовом случае известно лишь, что вероятность ошибки при этом отлична от нуля и ведет себя как

$$P_e(n, M) > R - \overline{C}(\varepsilon(Q)), \quad M > 2^{n[\overline{C}(\varepsilon(Q))-\delta]}. \quad (73)$$

Это так называемое слабое обращение прямой теоремы кодирования в квантовом случае. В классическом случае (аналогично и в квантовом, если Eve ограничена лишь индивидуальными измерениями) величина ошибки стремится к единице экспоненциально по параметру $n[C_{AB}(Q) - C_{AE}(E(Q))]$ (см. (28)), т. е. имеет место сильное обращение.

Другими словами, при индивидуальных измерениях Eve и при условии

$$C_{AB}(Q) > C_{AE}(E(Q))$$

Alice может выбрать таблицу кодовых слов

$$M < 2^{n[C_{AB}(Q)-\delta]}$$

и открыто анонсировать ее, Bob сможет с вероятностью единица определить истинную строку Alice из этой таблицы и исправить все ошибки в своей строке длины n, а Eve с вероятностью единица не сможет найти правильную строку при достаточно большом n (см. (26), (27)). То есть Alice и Bob могут использовать всю строку бит длиной n как секретный ключ.

В случае коллективных измерений, если бы таблица кодовых слов составляла

$$M < 2^{n[\overline{C}(\varepsilon(Q))-\delta]},$$

то Eve смогла бы определить всю строку у Alice (Bob). Если же таблица кодовых слов

$$M = 2^n > 2^{n[\overline{C}(\varepsilon(Q))-\delta]},$$

то средняя вероятность правильного определения кодового слова целиком была бы не более чем

$$1 - P_e(n, M) < 1 - [R - \overline{C}(\varepsilon(Q))].$$

Иными слова, при консервативной оценке, завышенной в пользу Eve, при $R = 1$ это означает, что Eve знает достоверно не более

$$n\overline{C}(\varepsilon(Q)) \quad (74)$$

бит в ключе и, соответственно, не знает

$$n[1 - \overline{C}(\varepsilon(Q))] \quad (75)$$

бит из ключа. Иными словами, Alice и Bob могут сделать секретными

$$r = n[1 - \overline{C}(\varepsilon(Q))] - s \quad (76)$$

бит, используя универсальную хэш-функцию

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

Здесь s — параметр секретности, назначаемый Alice и Bob. После этого информация Eve о финальном секретном ключе не превышает величину, определяемую соотношением (60).

Напомним, что здесь n — число бит, которые остаются уже после «чистки» первичного ключа конструктивным алгоритмом Binary. Коллективные измерения также являются конструктивными, но на сегодняшний день еще технологически недостижимыми. Тем не менее при вычислении длины финального секретного ключа следует исходить из наиболее консервативных требований, завышенных в пользу подслушивателя. Если Eve ограничена лишь индивидуальными измерениями, то длина секретного ключа, которая может быть получена после его «чистки», равна

$$r = nR(\varepsilon(Q)) - s, \quad R(\varepsilon(Q)) = \\ = -\log[\varepsilon^2(Q) + (1 - \varepsilon(Q))^2], \quad (77)$$

где $R(\varepsilon(Q))$ — энтропия Реньи (см. (59)).

На рис. 6 для различных значений углов перекрытия α показана доля секретных бит, которые могут быть извлечены из n-битной строки «очищенного» ключа для случаев, когда Eve делает только индивидуальные или коллективные измерения. Степень неортогональности (угол перекрытия α) информационных состояний Alice показан на рис. 1. Параметр s положен равным нулю.

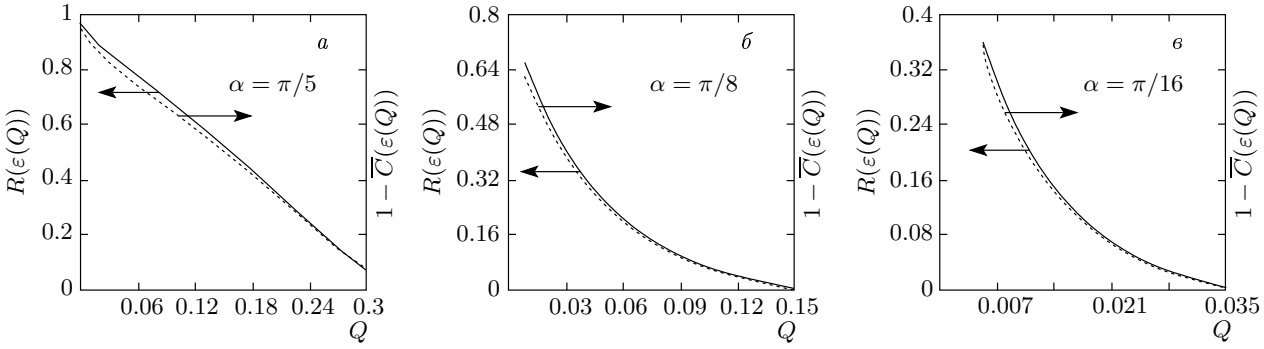

Рис. 6.

Следует отметить, на наш взгляд, удивительный факт, который, по-видимому, не является случайным. Энтропия Реньи и классическая пропускная способность квантового канала связи практически совпадают. Этот факт скорее отражает скрытую глубокую связь между классической пропускной способностью квантового канала связи (которая достигается на коллективных измерениях) и энтропией Реньи, вычисленной для оптимальных индивидуальных измерений.

Например, для генерации финального секретного ключа в 256 бит при заданном параметре секретности s, например, $s = 200$ бит, при наблюдаемой ошибке в 6 % требуется примерно 17812 бит первичного ключа. Из них примерно половина (8900 бит) отбрасывается сразу после оценки вероятности ошибки. После «чистки» ключа остается 16 % от первичного ключа (примерно 2850 бит, см. рис. 3). Дальнейшее сжатие (хэширование универсальной функцией) зависит от угла перекрытия (степени неортогональности) информационных состояний Alice. Например, при угле $\alpha = \pi/8$ (рис. 6*б*) от «очищенного» ключа остается 16 % (при наблюдаемой ошибке у Bob в 6 %). То есть 2850 бит «очищенного» ключа сжимаются хэшированием до 256 бит (при параметре секретности $s = 200$ бит). Это и есть финальный секретный ключ, про который информация Eve составляет не более 2^{-200} (см. формулу (60)).

Другим важным параметром процедуры коррекции ошибок является число бит, пересылаемых через открытый канал, на один бит секретного ключа. Поскольку в реальных условиях, как об этом упоминалось во Введении, требуется обеспечить целостность и аутентичность открытой информации.

Возможны два подхода. В первом случае аппаратный генератор случайных чисел имеется только на стороне Alice, поэтому случайный выбор позиций для оценки вероятности ошибки, вычисление битов четности со случайными строками и т. д. требуют пересылки всей этой информации через открытый классический канал связи от Alice к Bob. Зависимость числа передаваемых бит на один бит финального секретного ключа от наблюдаемой легитимными пользователями вероятности ошибки Q приведен на рис. 4. Характерный масштаб переданных бит зависит от вероятности ошибки и, например, при $Q = 6\,\%$ составляет примерно 20 на один бит финального секретного ключа.

Во втором подходе, когда у Alice и Bob имеется небольшой стартовый ключ, который используется только при первом запуске системы, возможно уменьшить количество передаваемой информации через открытый классический канал связи. В этом случае можно использовать согласованные генераторы псевдослучайных чисел у Alice и Bob. Конкретно нами использовался генератор псевдослучайных чисел на основе стандарта шифрования ГОСТ 28147-89. В этом случае число переданных бит примерно на порядок меньше и составляет 2–3 бита на один бит ключа (см. рис. 5).

6. КОМБИНИРОВАННАЯ ПРОЦЕДУРА «ЧИСТКИ» ПЕРВИЧНОГО КЛЮЧА (CASCADE)

Каскадный метод представляет собой комбинированный итерационный метод, включающий в себя Binary как подпрограмму и использующий на каждом новом шаге информацию о предыдущих проходах [23].

Аналогично предыдущему, Alice и Bob раскрывают часть последовательности для получения оценки вероятности ошибки Q, исходя из которой вычисля-

ется размер блока на первом проходе. Далее метод состоит из следующих шагов.

1. Для каждого прохода генерируется случайная хэш-функция. Пусть номер очередного прохода i, а длина первичной строки после оценки вероятности ошибки и отбрасывания этих битов есть N, текущий размер блока k_i. Тогда

$$F_i(m) : \{1, 2, \dots N\} \to \left\{1, 2, \dots \left[\frac{N}{k_i}\right]\right\} \qquad (78)$$

Вся строка разбивается на блоки. В блок с номером j попадают биты, которые в исходной строке имели позиции

$$K_j^i = \{m | F_i(m) = j\}.$$

Другими словами, в блок с номером j попадают те биты, для которых номера их позиций имеют коллизию на хэш-функции. По сути, отдельные блоки получаются случайным «выдергиванием» бит по k_i штук. Хэш-функция дает просто однородный способ формирования блоков.

2. Alice вычисляет биты четности,

$$b_j^{parity} = \bigoplus_{l \in K_j^i} b_l,$$

для каждого блока и посылает их значения через открытый канал Bob. Bob сравнивает биты четности, если они не совпадают, то проводится бисективный поиск. Ошибка локализуется и помечается, но пока не выбрасывается. Подсчитывается также раскрытое число битов четности во время работы Binary. Пусть j — номер ошибочного бита.

3. Составляется множество блоков $\mathcal{K}$, в которое входят все блоки из предыдущих проходов (по одному блоку из каждого прохода), содержащие ошибочный бит j. Поскольку раньше биты четности этих блоков совпадали (блоки содержали четное число ошибок), теперь после маркирования ошибочного бита j они содержат нечетное число ошибок.

4. Далее выбирается один блок наименьшего размера из этого множества и в нем ищется ошибка при помощи Binary. Пусть найденная ошибка имеет номер l, она исправляется и отмечается, но пока не отбрасывается. Множество блоков, которые ранее содержали ошибку l, обозначим $\mathcal{B}$.

5. Формируется новое множество блоков

$$\mathcal{K}' = (\mathcal{B} \cup \mathcal{K})/(\mathcal{B} \cap \mathcal{K}).$$

Это множество содержит теперь нечетное число ошибок (или не содержит вовсе). Если оно не пусто, то происходит переход к шагу 1.

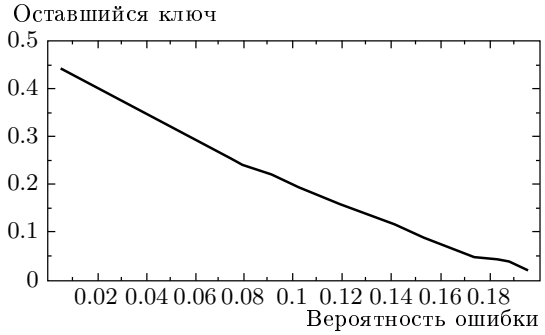

Рис. 7.

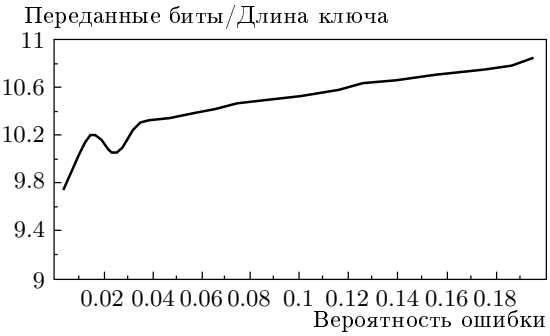

Рис. 8.

Проход заканчивается, когда биты четности всех блоков совпадают. После исправления ошибок и отбрасывания всех найденных ошибочных позиций и раскрытых битов четности Eve оказывается в той же ситуации, что и после завершения процедуры Binary. Поэтому величина сжатия посредством случайного хэширования определяется аналогично. Разница состоит в том, что после «чистки» процедурой Cascade остается более длинный ключ. Возможно также сохранение всех исправленных битов и битов четности. Однако при этом анализ изменения условных вероятностей очень сильно усложняется.

Зависимость доли оставшихся битов «очищенного» ключа для процедуры Cascade примерно вдвое больше, чем для процедуры Binary. Например, при ошибке в 6 %, для того чтобы в финальном секретном ключе оставалось 256 бит (при параметре секретности $s = 200$ бит), требуется примерно 9500 бит первичного ключа, что вдовое меньше, чем для Binary (см. рис. 7).

Число переданных битов по открытому каналу на бит секретного ключа, когда генератор случайных чисел находится только на передающей стороне, также вдвое меньше, чем в случае Binary (рис. 8). А в случае, когда имеются согласованные

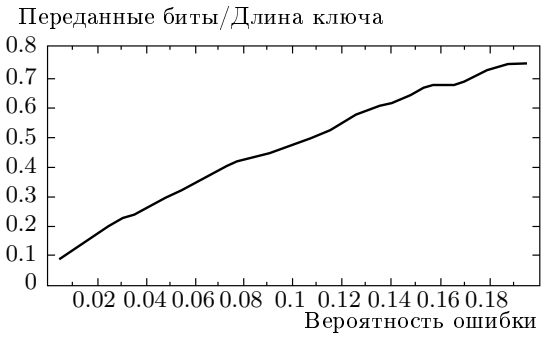

Рис. 9.

генераторы псевдослучайных чисел у Alice и Bob, это число меньше на порядок, чем для процедуры Binary, и составляет доли битов на бит секретного ключа (рис. 9).

7. «ЧИСТКА» ПЕРВИЧНОГО КЛЮЧА ПРИ ПОМОЩИ БЧХ-КОДОВ

Один из естественных способов «чистки» первичного ключа состоит в использовании классических кодов, исправляющих ошибки. Еще раз отметим, что эффективность кода не может быть установлена в отрыве от квантово-механической части протокола. Эффективность классического кода самого по себе еще не означает его эффективности применительно к задачам квантовой криптографии, поскольку эффективность кода определяется не только тем, сколь хорошо он исправляет, но и тем, сколь сильно он изменяет исходные условные вероятности относительно первичного ключа у Eve.

Ниже будет рассмотрена «чистка» первичного ключа при помощи БЧХ-кодов (Bose-Chaudhuri-Hocquenghem) [24, 25], представляющих собой широкий класс достаточно хороших кодов, которые позволяют исправлять по несколько ошибок в блоке (кодовом слове), что дает возможность в зависимости от оценки вероятности ошибки Q выбирать код динамически.

Сначала введем минимально необходимые определения для БЧХ-кодов, исправляющих t ошибок.

Поле Галуа $GF(2^n)$ — векторное пространство двоичных слов длины n, где все арифметические действия происходят по модулю 2. Линейный код $\mathcal{E}$ образует линейное подпространство в $GF(2^n)$. Код называется циклическим в следующем случае: если $\mathbf{c} = (c_0, c_1, \ldots, c_{n-1})$ $(c_i = 0, 1)$ является кодовым словом, то $\mathbf{c}' = (c_1, \ldots, c_{n-1}, c_0)$ также есть кодовое слово. Удобно представлять векторы из $GF(2^n)$ многочленами от x степени не выше $n-1$, коэффициентами которых являются координаты векторов

$$c(x) = c_0 + c_1 x + c_2 x^2 + \ldots + c_{n-1} x^{n-1}. \qquad (79)$$

Циклический код задается своим порождающим многочленом $g(x)$ степени $n-k$ (k — число информационных символов, n — длина кодового слова). Порождающий многочлен $g(x)$ является делителем многочлена $x^{n-1}-1$. Для любого циклического кода выполнено равенство

$$x^{n-1} - 1 = g(x)h(x),$$

$h(x)$ — проверочный многочлен.

Код БЧХ, исправляющий t ошибок, строится следующим образом. Выбирается примитивный элемент α расширенного поля $GF(2^n)$ (любой элемент поля получается как некоторая степень примитивного элемента, кроме того, имеет место в $GF(2)$ $\alpha = \alpha^2$). Определяется множество элементов

$$[\alpha, \alpha^2, \alpha^3, \ldots, \alpha^{2t}]. \qquad (80)$$

По этим элементам строится порождающий многочлен $g(x)$, корнями которого является множество (80). Считается, что t задано, затем берется некоторое m, которое определяет длину кодового слова $n = 2^m - 1$. Далее находятся минимальные многочлены $f_j(x)$ (многочлены минимальной степени), корнями которых являются степени примитивного элемента α^j $(j = 1, 2, \ldots, 2t)$ в расширении поля $GF(2)$–$GF(2^n)$. Порождающий многочлен $g(x)$ кода длиной n находится как наименьшее общее кратное:

$$g(x) = \text{НОК}[f_1(x), f_2(x), \ldots, f_{2t}(x)]. \qquad (81)$$

При декодировании был использован метод Питерсона–Горенштейна–Цирлера [24, 25]. Пусть было передано кодовое слово $\mathbf{c} = (c_0, c_1, \ldots, c_{n-1})$, которое на приемном конце содержит ошибку

$$\mathbf{y} = \mathbf{c} + \mathbf{e}, \qquad (82)$$

где $\mathbf{e} = (e_{i_1}, \ldots, e_{i_\nu})$ (аналогично, в виде многочлена $e(x) = e_{i_1} x^{i_1} + \ldots + e_{i_\nu} x^{i_\nu}$, $e_{i_l} = 0, 1$) — вектор ошибок, ν — число ошибок, которое, вообще говоря, неизвестно.

Декодирование с исправлением ошибок осуществляется в три этапа. Во-первых, вычисление синдрома ошибок. Во-вторых, определение многочлена локаторов ошибок $S(x)$. В-третьих, вычисление корней многочлена локаторов ошибок $S(x)$, исправление ошибок. То есть определение e_j и исправление.

При разных α^j значение кодового вектора $C(\alpha^j) = 0$, поэтому

$$y(\alpha^j) = e(\alpha^j). \tag{83}$$

Удобно ввести обозначения

$$Y_l = e_{i_l}, \quad X_l = \alpha^{i_l}.$$

В этих обозначениях компоненты синдрома представляются как

$$\begin{gathered} S_1 = Y_1 X_1 + \ldots + Y_\nu X_\nu, \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ S_{2t} = Y_1 X_1^{2t} + \ldots Y_\nu X_\nu^{2t}. \end{gathered} \tag{84}$$

По определению синдрома эта система уравнений, вообще говоря, нелинейная, должна иметь единственное решение. Вводится многочлен локаторов ошибок

$$\Lambda(x) = \Lambda_\nu x^\nu + \ldots + \Lambda_x x + 1, \tag{85}$$

корнями которого являются X_l^{-1} $(l = 1, 2, \ldots, \nu)$:

$$\Lambda(x) = (1 - xX_1) \cdots (1 - xX_\nu). \tag{86}$$

Требуется найти корни этого многочлена. Если коэффициенты Λ_l известны, то можно найти и сами корни. По известным локаторам ошибок S_l можно найти Λ_l, решая уже линейную систему уравнений. Далее имеем

$$Y_l(X_l^{j+\nu} + \Lambda_l X_l^{j+\nu-1} + \ldots + \Lambda_\nu X_l^j) = 0. \tag{87}$$

Суммируя при всех индексах l (87), получим

$$\sum_{l=1}^{\nu} Y_l(X_l^{j+\nu} + \Lambda_l X_l^{j+\nu-1} + \ldots + \Lambda_\nu X_l^j) = 0. \tag{88}$$

С учетом (84) при $j = 1, \ldots, \nu$ получаем линейную систему уравнений для коэффициентов Λ_l многочлена $\Lambda(x)$:

$$\Lambda_1 S_{j-\nu-1} + \Lambda_2 S_{j+\nu-2} + \ldots \Lambda_\nu S_j = -S_{j+\nu}, \tag{89}$$

$$\begin{pmatrix} S_1 & . & . & . & . & S_\nu \\ . & . & . & . & . & . \\ . & . & . & . & . & . \\ S_\nu & . & . & . & . & S_{2\nu-1} \end{pmatrix} \begin{pmatrix} -S_{\nu+1} \\ . \\ . \\ -S_{2\nu} \end{pmatrix} = \begin{pmatrix} \Lambda_\nu \\ . \\ . \\ \Lambda_1 \end{pmatrix} \tag{90}$$

Имеет место следующее утверждение. Если ν равно истинному числу ошибок (пока оно неизвестно), то система уравнений (90) невырождена, в противном случае система вырождена. Поэтому фиксируется $\nu = t$ и вычисляется детерминант. Если он равен нулю, то ν уменьшается на единицу, и так далее до тех пор, пока детерминант становится не равным нулю. Данное ν дает истинное число ошибок. Решается система уравнений (90), однозначно находятся коэффициенты Λ_l, а затем корни многочлена (85), (86). Корни многочлена локаторов ошибки находятся с помощью последовательного вычисления значения многочлена для каждого элемента поля. Корни равны

$$X_l^{-1} = \alpha^{-i_l}.$$

Далее находится степень примитивного элемента поля i_l

$$X_l \cdot \alpha^{i_l} = 1,$$

такая что дает позицию ошибки e_{i_l} (индекс i_l), которая исправляется.

Процедура «чистки» БЧХ-кодами ключа состоит из следующих шагов.

1. Проводится оценка вероятности ошибки Q путем раскрытия и сравнения через открытый канал примерно половины переданной последовательности. В зависимости от вероятности ошибки Q при заданной длине кодового слова $n = 2^m - 1$ выбирается t — среднее число ошибок в кодовом слове $t = [Q \cdot n]$. Вся последовательность разбивается на блоки, длина которых равна длине кодового слова n. Были рассмотрены несколько кодов БЧХ с разной длиной кодового слова $n = 2^m - 1$ $(n = 15, 31, 63, 127, 255)$. По заданным n, m, t строится порождающий многочлен кода $g(x)$.

2. Alice формирует кодовые слова, осуществляет кодирование. Первые k бит в каждом блоке длины n считаются информационными, остальные $n - k$ — контрольными, для этого необходимые биты инвертируются, что сообщается Bob через открытый канал. Инверсия битов не изменяет информацию Eve о строке бит Alice и Bob. То есть Alice создает кодовые слова путем вычисления контрольных символов при известных информационных. При этом для кода (n, k) с порождающим многочленом $g(x)$ в поле $GF(2^m)$ $(n - 2^m - 1)$ кодовых символов в представлении многочленов равны остатку от деления $i(x) \cdot x^{n-k}$ по модулю

$$g(x) - c(x) = -R_{g(x)}[x^{n-k} i(x)],$$

где

$$i(x) = i_0 + i_1 x + \ldots + i_{k-1} x^{k-1}, \quad i_l = 0, 1,$$

— информационный многочлен. Биты i_l ($l = 0, \ldots, k-1$) берутся как первые биты из каждого блока переданной Alice последовательности.

3. Bob декодирует свои кодовые слова, после этого контрольные символы в каждом кодовом слове Alice и Bob отбрасывают.

Для удобства в табл. 3 приведены используемые БЧХ-коды. Указаны только те коды, для которых t попадает в интервал при вычислении ошибки с шагом $\Delta Q = 0.01$ до $Q = 0.15$. В самой правой колонке указана вероятность ошибки Q_t, до которой данный код использовался.

Ниже приведены порождающие ($g(x)$) и проверочные ($h(x)$) многочлены для кодов БЧХ с длиной слова, соответственно, 15, 31, 63, 127 и 255 бит при начальной вероятности ошибки порядка 10 %. Соответственно, код с длиной слова 15 бит правит 2 ошибки, 31 бит — 4 ошибки, 63 бита — 7 ошибок, 127 — 13 ошибок и 255 бит — 26 ошибок. Код БЧХ $[15, 7]$, исправляющий 2 ошибки, имеет вид

$$g(x) = x^8 + x^7 + x^6 + x^4 + 1,$$
$$h(x) = x^7 + x^6 + x^4 + 1.$$

Код БЧХ $[31, 11]$, исправляющий 4 ошибки имеет вид

$$g(x) = x^{20} + x^{18} + x^{17} + x^{13} + x^{10} + x^9 + x^7 + x^6 + x^4 + x^2 + 1,$$
$$h(x) = x^{11} + x^9 + x^8 + x^7 + x^2 + 1.$$

Код БЧХ $[63, 24]$, исправляющий 7 ошибок имеет вид

$$g(x) = x^{39} + x^{38} + x^{37} + x^{36} + x^{34} + x^{33} + x^{31} + x^{28} + x^{27} + x^{25} + x^{23} + x^{22} + x^{17} + x^{11} + x^8 + x^5 + 1,$$
$$h(x) = x^{24} + x^{23} + x^{20} + x^{18} + x^{17} + x^{16} + x^{15} + x^{11} + x^{10} + x^8 + x^5 + 1.$$

Код БЧХ $[127, 50]$, исправляющий 13 ошибок имеет вид

$$g(x) = x^{77} + x^{75} + x^{74} + x^{71} + x^{68} + x^{65} + x^{64} + x^{62} + x^{60} + x^{57} + x^{55} + x^{53} + x^{51} + x^{49} + x^{46} + x^{45} + x^{43} + x^{42} + x^{39} + x^{38} + x^{30} + x^{28} + x^{26} + x^{22} + x^{18} + x^{17} + x^{15} + x^9 + x^8 + x^4 + 1,$$
$$h(x) = x^{50} + x^{48} + x^{47} + x^{46} + x^{44} + x^{43} + x^{39} + x^{38} + x^{36} + x^{35} + x^{30} + x^{27} + x^{26} + x^{25} + x^{24} + x^{23} + x^{16} + x^{15} + x^{12} + x^9 + x^4 + 1.$$

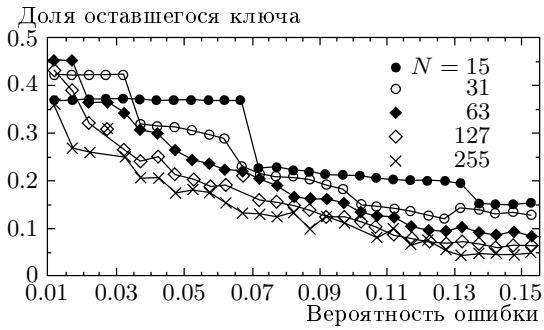

Рис. 10.

Код БЧХ $[255, 87]$, исправляющий 26 ошибок имеет вид

$$g(x) = x^{168} + x^{165} + x^{159} + x^{157} + x^{156} + x^{155} + x^{154} + x^{152} + x^{151} + x^{150} + x^{149} + x^{148} + x^{145} + x^{144} + x^{143} + x^{138} + x^{137} + x^{134} + x^{133} + x^{132} + x^{131} + x^{127} + x^{126} + x^{124} + x^{121} + x^{120} + x^{119} + x^{118} + x^{116} + x^{112} + x^{111} + x^{110} + x^{108} + x^{106} + x^{103} + x^{102} + x^{99} + x^{98} + x^{97} + x^{94} + x^{93} + x^{92} + x^{88} + x^{87} + x^{83} + x^{82} + x^{81} + x^{78} + x^{77} + x^{76} + x^{75} + x^{73} + x^{68} + x^{65} + x^{64} + x^{61} + x^{56} + x^{55} + x^{53} + x^{52} + x^{51} + x^{49} + x^{46} + x^{44} + x^{42} + x^{41} + x^{38} + x^{36} + x^{34} + x^{32} + x^{31} + x^{30} + x^{28} + x^{27} + x^{25} + x^{24} + x^{21} + x^{18} + x^{17} + x^{16} + x^{15} + x^{13} + x^9 + x^7 + x^6 + x^3 + x^2 + x + 1,$$

$$h(x) = x^{87} + x^{84} + x^{81} + x^{76} + x^{74} + x^{73} + x^{71} + x^{66} + x^{64} + x^{63} + x^{61} + x^{58} + x^{57} + x^{56} + x^{54} + x^{52} + x^{50} + x^{48} + x^{46} + x^{45} + x^{42} + x^{40} + x^{38} + x^{36} + x^{35} + x^{34} + x^{33} + x^{32} + x^{31} + x^{29} + x^{27} + x^{23} + x^{22} + x^{21} + x^{20} + x^{17} + x^{16} + x^{15} + x^{14} + x^{13} + x^{11} + x^9 + x^7 + x^6 + x^5 + x^4 + x + 1.$$

Была рассмотрена коррекция ошибок в первичном ключе при помощи БЧХ-кодов с различной длиной кодового слова. Осуществлялся один проход. Доля оставшихся бит в ключе в зависимости от вероятности наблюдаемой ошибки Q приведена на рис. 10. При одном проходе остается определенный процент ошибок. Дело состоит в том, что если в кодовом слове встречается больше ошибок, чем код с данной длиной позволяет исправить, то возникают новые ошибки (слово декодируется в неправильное кодовое слово). Второй проход уже невыгоден по той при-

Таблица 3. Параметры используемых БЧХ-кодов при разной величине ошибки у легитимных пользователей

n — длина кодового слова	k — число информационных символов	t — число ошибок в слове	Q_t — критическая ошибка
$15 = 2^4–1$	11	1	0.066
	7	2	0.132
$31 = 2^5–1$	26	1	0.032
	21	2	0.065
	16	3	0.097
	11	5	0.161
$63 = 2^6–1$	57	1	0.016
	51	2	0.032
	45	3	0.048
	39	4	0.063
	36	5	0.079
	30	6	0.095
	24	7	0.111
	18	10	0.159
$127 = 2^7–1$	120	1	0.008
	113	2	0.016
	106	3	0.024
	99	4	0.031
	92	5	0.039
	85	6	0.047
	78	7	0.055
	71	9	0.070
	64	10	0.079
	57	11	0.087
	50	13	0.102
	43	14	0.110
	36	15	0.118
	29	21	0.165
$255 = 2^8–1$	239	2	0.011
	231	3	0.012
	223	4	0.016
	215	5	0.023
	207	6	0.024
	199	7	0.027
	191	8	0.031
	187	9	0.035
	179	10	0.039
	171	11	0.043

Таблица 3. Продолжение

n — длина кодового слова	k — число информационных символов	t — число ошибок в слове	Q_t — критическая ошибка
	163	12	0.047
	155	13	0.051
	147	14	0.055
	139	15	0.059
	131	18	0.071
	123	19	0.075
	115	21	0.082
	107	22	0.086
	99	23	0.090
	91	25	0.098
	87	26	0.102
	79	27	0.106
	71	29	0.114
	63	30	0.118
	55	31	0.122
	47	42	0.165

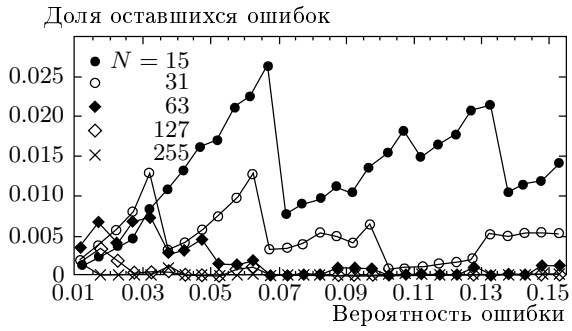

Рис. 11.

чине, что остается слишком маленькая длина ключа. Фактически, каждый проход оставляет долю k/n (скорость кода) от исходной последовательности.

При длине кодового слова 127 и 255 бит при исходной вероятности ошибки $Q = 6\,\%$ ошибок не остается уже после одного прохода «чистки» (рис. 11). Оставшийся процент бит в ключе составляет приблизительно 20 %, что примерно совпадает с долей оставшихся бит для процедуры Cascade (естественно, при том же проценте ошибок $Q = 6\%$). При меньших длинах кодового слова (15, 31, 63 бит) остается заметный процент ошибок. Хотя доля бит в ключе при этом сама по себе и больше (до 35 %), эти оставшиеся биты содержат ошибки. Второй проход уже неэффективен по сравнению с ранее рассмотренными процедурами.

При длине кодового слова в 127 и 255 бит «чистка» первичного ключа происходит за один проход, что по эффективности сравнимо с процедурой Cascade. Однако здесь нужно сделать важное замечание. Если в процедуре Cascade с выбрасыванием условная вероятность для Eve при определении битовых строк Alice и Bob остается неизменной после завершения «чистки» первичного ключа в том смысле, что определяется вероятностью ошибки $\varepsilon(Q)$ (см. формулы (20), (21)) оптимального различения неортогональных состояний $|e_0\rangle$ и $|e_1\rangle$, то после исправления ошибок при помощи БЧХ-кодов (как, впрочем, и любых других кодов) она существенно меняется. Эта измененная условная вероятность для Eve при определении информации об «очищенном» ключе обусловливает величину сжатия посредством хэширования битовой строки для получения финального секретного ключа. Поэтому тот факт, что длина «очищенного» ключа такая же, как после процедуры Cascade, еще не означает, что длина финального

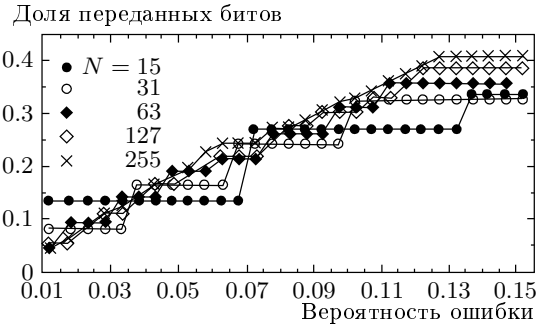

Рис. 12.

ключа будет той же самой.

На рис. 12 приведена зависимость переданных бит через открытый канал связи на один бит «очищенного» ключа в зависимости от вероятности ошибки на приемном конце Q. Как видно, эта величина составляет доли бит, и она примерно такая же, как для процедуры Cascade.

8. ВЫЧИСЛЕНИЕ ОШИБКИ ПОДСЛУШИВАТЕЛЯ ПОСЛЕ «ЧИСТКИ» КЛЮЧА БЧХ-КОДАМИ

Теперь выясним, как изменяется условная вероятность для Eve после «чистки» ключа. Рассмотрим сначала индивидуальные измерения Eve. До «чистки» ключа Eve знает каждый бит в строке Alice с ошибкой

$$E(Q) = 1 - (1 - Q)(1 - \varepsilon(Q)) + Q\varepsilon(Q)$$

(см. (26)), а Bob знает каждый бит Alice с ошибкой Q. Если после «чистки» ключа у Bob ошибки фактически отсутствуют, то вероятность ошибки у Eve определяется из следующих соображений.

Поскольку, как обычно считается, вся информация о параметрах выбранных кодов коррекции ошибок известна (длина кодового слова, число информационных и проверочных символов, а также разбиение на кодовые слова и т. д.), то Eve также может пытаться исправить свои ошибки, используя известные правила декодирования. Как известно, вероятность неправильного декодирования равна [24, 25]

$$P_e = \frac{1}{M}\sum_{i=1}^{M} \Pr(w_E^i \neq w^i), \tag{91}$$

где w_E^i — кодовое слово, в которое Eve декодирует посланное Alice кодовое слово w^i. Для $[n, k]$ кода вероятность ошибки равна

$$P_e(p) = 1 - \sum_{j=0}^{n} \alpha_j p^j (1 - p)^{n-j}, \tag{92}$$

где α_j — число лидеров смежного класса веса j, p — исходная ошибка на символ. Нас на самом деле интересует ошибка на символ $P_{symb}(p)$, как известно, последняя ограничена снизу (занижена в пользу Eve)

$$P_{symb}(p) \geq \frac{P_e(p)}{k}. \tag{93}$$

Прямой подсчет $P_{symb}(p)$ представляет собой достаточно сложную переборную задачу, особенно для кодов с большой длиной кодового слова, поэтому удобнее пользоваться оценками снизу. Для любого $[n, k]$ кода справедлива оценка

$$P_e(p) \geq [C_n^{t+1} - \alpha_{t+1}]p^{t+1}(1 - p)^{n-t-1} + \sum_{i=t+2}^{n} C_n^i p^i (1 - p)^{n-i}, \tag{94}$$

где α_{t+1} и t определяются как

$$\alpha_{t+1} = 2^{n-k} - 1 - \sum_{i=1}^{t} C_n^i \geq 0, \tag{95}$$

t — наибольшее целое число, при котором удовлетворяется (95).

Ошибка Eve на символ уже одинакового ключа у Alice и Bob определяется соотношениями (93), (94), где заменено

$$p \to E(Q) = 1 - (1 - Q)(1 - \varepsilon(Q)) + Q\varepsilon(Q).$$

Ошибка на символ у Bob после одного прохода рассчитывается по формулам (93), (94), где вместо p нужно подставить наблюдаемую ошибку Q.

Зависимости вероятности ошибки у Eve и Bob после одного прохода коррекции ошибок БЧХ-кодом с параметрами $\{63; 39\}$, «настроенным» на начальный процент ошибки у Bob $Q = 6\,\%$, показаны на рис. 13 для разных углов перекрытия информационных состояний Alice.

На рис. 13*а′*, *б′*, *в′* приведена энтропия Eve после одного прохода. Величина $R(P_e(E(Q)))$ определяет долю бит, которая может быть оставлена в секретном ключе. Как видно на рис. 13, после хэширования остается не более 8 % от «очищенного» ключа. При малых углах $\alpha = \pi/16$ (исходные информационные состояния почти ортогональны) энтропия

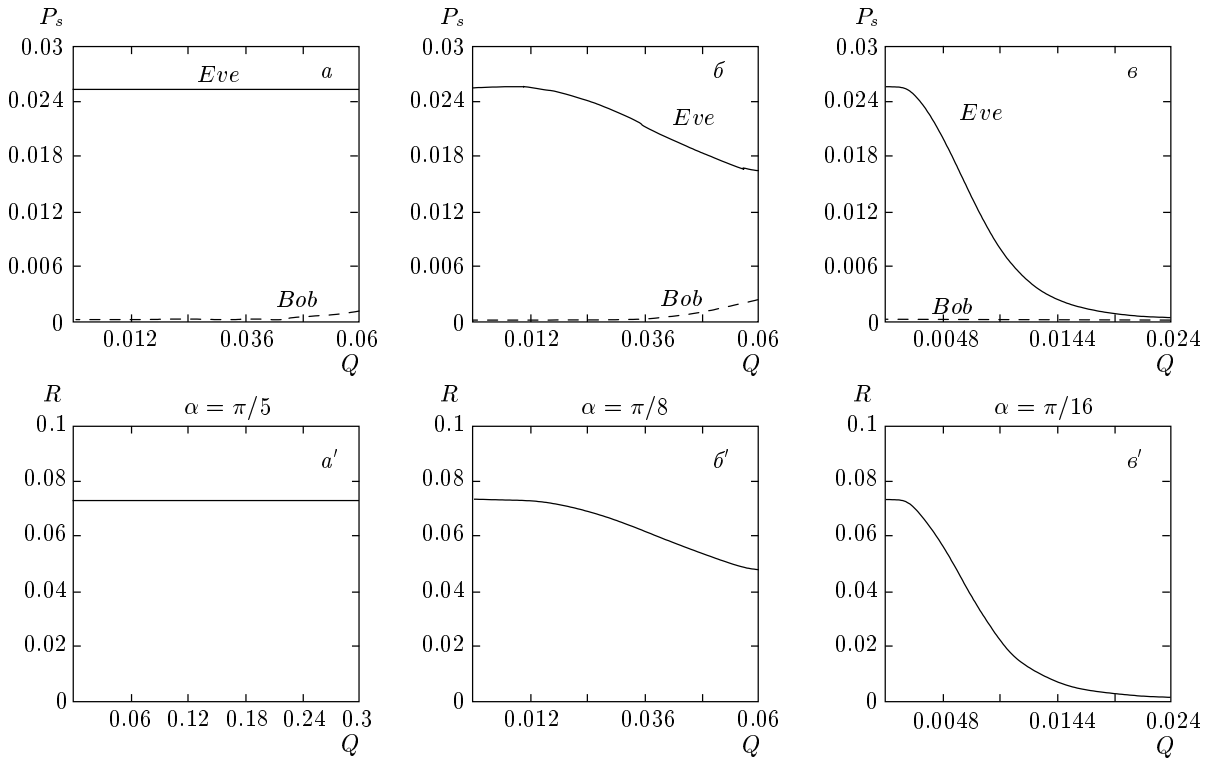
P_s
Eve
Bob
а
б
в
Q
R
$\alpha = \pi/5$
$\alpha = \pi/8$
$\alpha = \pi/16$
а′
б′
в′

Рис. 13.

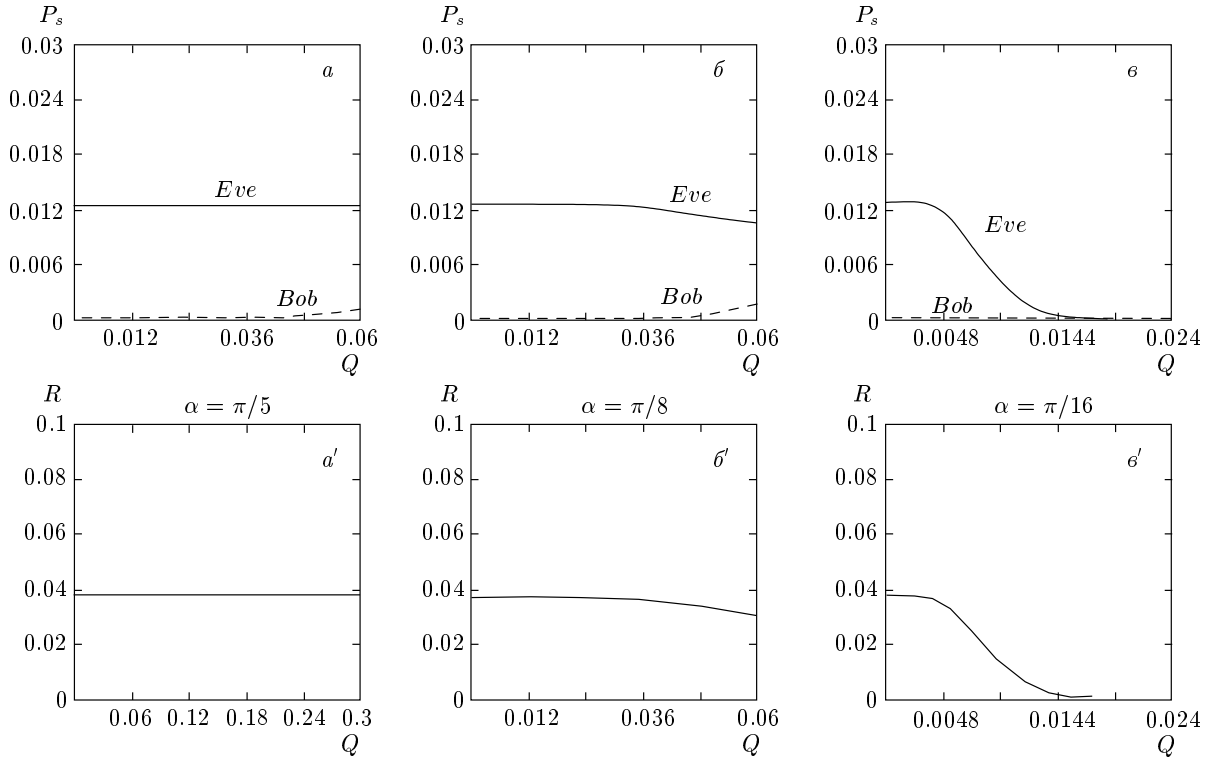
P_s
Eve
Bob
а
б
в
Q
R
$\alpha = \pi/5$
$\alpha = \pi/8$
$\alpha = \pi/16$
а′
б′
в′

Рис. 14.

Реньи стремится к нулю уже при ошибке $Q \approx 1\,\%$ ($R(P_e(E(Q))) \approx 0.02$, см. рис. 13*в*′). Это означает, что длина «очищенного» ключа должна быть уменьшена как минимум до 2 %.

На рис. 14 приведены аналогичные зависимости ошибки у Eve и Bob после одного прохода с использованием БЧХ-кода $\{127; 78\}$ для разных углов перекрытия информационных состояний. При сильном перекрытии состояний ($\alpha = \pi/5$) после коррекции ошибок вероятность ошибки относительно оставшихся бит в ключе практически постоянна. При почти ортогональных исходных состояниях величина ошибки Eve резко уменьшается с увеличением первичной ошибки Q у Bob. На рис. 14*а*′, *б*′, *в*′ приведена энтропия Реньи для Eve, которая определяет долю оставшихся бит в финальном секретном ключе. В лучшем случае остается лишь 4 % бит от «очищенного» ключа. Отметим, что при использовании кода $\{63; 39\}$ доля оставшихся бит составляет 8 %, хотя в «очищенном» ключе остается больший процент.

Данный факт демонстрирует как раз то обстоятельство, что эффективность кода в смысле исправления ошибок используют не только легитимные пользователи, но и подслушиватель. Чем эффективнее код исправляет ошибки, тем он сильнее увеличивает условную вероятность для Eve при определении информации об «очищенном» ключе, так что в финальном секретном ключе остается в итоге меньший процент бит от первичного ключа.

Поэтому сама по себе эффективность кода при исправлении ошибок без привязки ее к квантовой части протокола еще ничего не говорит о его эффективности в смысле длины остающегося секретного ключа.

9. «ЧИСТКА» ПЕРВИЧНОГО КЛЮЧА ПРИ ПОМОЩИ КОДОВ ХЭММИНГА

Ниже для сравнения будет проведена коррекция ошибок в первичном ключе при помощи кодов Хэмминга (Hamming). Коды Хэмминга, как известно, исправляют одну ошибку в кодовом слове и являются наиболее просто декодируемыми кодами [24, 25]. (По поводу применения этих кодов к задачам квантовой криптографии см. работу [26].)

Код Хэмминга с примитивной длиной $n = 2^m - 1$ может быть задан проверочной матрицей вида

$$\mathbf{H} = [\alpha^0, \alpha^1, \ldots, \alpha^{n-1}], \tag{96}$$

где α — как обычно, примитивный элемент поля $GF(2^m)$. Кодовые векторы $\mathbf{c} = (c_0, c_1, \ldots, c_{n-1})$ удовлетворяют соотношениям

$$\mathbf{c} \cdot \mathbf{H}^T = 0, \quad \sum_{i=0}^{n-1} c_i \alpha^i = 0, \tag{97}$$

или в записи многочлена

$$c(x) = \sum_{i=0}^{n-1} c_i x^i, \tag{98}$$

где элемент α является корнем многочлена $c(\alpha) = 0$. Поскольку $\alpha^{2^m-1} = 1$, α есть корень многочлена $x^{2^m-1} - 1$, поэтому минимальный многочлен элемента α в поле $GF(2^m)$ является делителем многочлена $x^{2^m-1} - 1$ и может быть взят в качестве порождающего многочлена кода. Код имеет параметр $n = 2^m - 1$ — длина кодового слова, из них $2^m - 1 - m$ информационных символов и m проверочных символов.

Если послано кодовое слово $c(x)$ и получено кодовое слово с одной ошибкой

$$y(x) = c(x) + e(x),$$

то

$$y(\alpha) = c(\alpha) + e(\alpha) = e(\alpha) = \alpha^i,$$

где i — позиция, в которой произошла ошибка. Многочлен ошибок (точнее одной ошибки) имеет вид

$$e(x) = \sum_{i=0}^{n-1} e_i x^i,$$

в котором лишь один символ $e_i = 1$, остальные равны нулю.

«Чистка» первичного ключа реализуется по следующей схеме.

1. Боб вычисляет количество контрольных бит m на основе информации о вероятности ошибки и посылает его Alice. Поскольку код Хэмминга исправляет одну ошибку в кодовом слове, размер слова выбирается из тех соображений, чтобы вероятность более одной ошибки была мала. Количество контрольных бит m вычисляется как

$$m = \max\left(3, \log\frac{1}{Q}\right).$$

2. Alice разбивает свой ключ на блоки (нумерация ячеек в блоке начинается с нуля) размером 2^m бит и посылает Bob биты четности для каждого блока.

3. Если в некотором блоке бит четности Bob отличается от посланного ему Alice, то в этом блоке проводится кодирование блока (за исключением нулевого бита) кодом Хемминга. Кодирование заключается в том, что все контрольные биты располагаются в ячейках блока с номерами $1, 2, \ldots, 2^i, \ldots, 2^{m-1}$ и представляют собой m-битовое двоичное слово (здесь удобнее, чтобы нумерация ячеек в блоке начиналась с единицы). Над индексами всех остальных ненулевых битов проводится операция «исключающее или» (XOR) и получившееся число записывается в контрольные биты.

4. Bob проводит декодирование. При декодировании опять проводится операция «исключающее или» над индексами всех ненулевых битов (включая контрольные). Получившееся число называется синдромом и является индексом ошибочного бита, если оно равно единице, или является признаком отсутствия ошибок, если оно нулевое. После декодирования контрольные символы в слове выбрасываются, для того чтобы не дать Eve дополнительной информации о ключе. Если ошибок в блоке больше одной, то декодирование может добавить ошибку или исправить ее.

5. Alice и Bob удаляют из ключа нулевой бит из каждого блока. Это проводится, для того чтобы Eve (в случае, если она есть) не получала бы никакой информации от известного ей бита четности, который передавался легитимными пользователями по открытому каналу.

6. Alice и Bob вычисляют новую теоретическую вероятность ошибки на основе старой вероятности (см. детали, например, в [26]).

7. Alice перемешивает случайным образом свой ключ и посылает новый порядок последовательности Bob. После чего процесс повторяется с первого пункта.

Алгоритм продолжает свою работу до некоторого количества пустых циклов (в которых все биты четности блоков совпадают).

Результаты расчетов длины оставшегося ключа после коррекции ошибок кодами Хэмминга приведены на рис. 15. Как следует из рис. 15, например, при вероятности ошибки в первичном ключе при исходной вероятности ошибки $Q = 6\,\%$ остается примерно $30\,\%$ от длины первичного неочищенного ключа, что приблизительно совпадает с тем, что дает процедура Cascade, и вдвое лучше, чем дает процедура бисективного поиска Binary. Кроме того, сама по себе «чистка» кодами Хэмминга несколько более эффективна, чем коррекция ошибок при помощи кодов

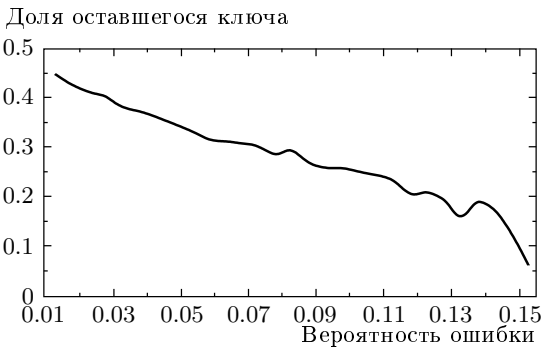

Рис. 15.

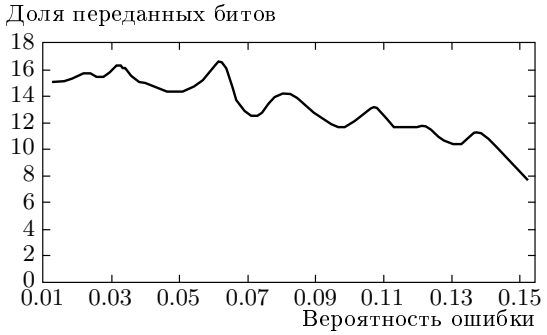

Рис. 16.

БЧХ. Это связано с тем, что используется предварительная проверка на четность каждого блока, перед тем как Alice будет использовать кодирование. Если четность блока равна нулю (блок содержит четное число ошибок), то кодирование не применяется. Нулевой бит четности означает, что в блоке либо нет ошибок, либо их четное число, т. е. ошибок более одной. В этом случае кодирование данного блока не только бесполезно, но и вредно, поскольку при наличии более одной ошибки он будет декодирован неверно. Более того, могут быть внесены дополнительные ошибки. Поэтому с этими блоками Alice никаких действий не проводит. В тех блоках, где биты четности не совпадают, имеется нечетное число ошибок. Поскольку размер блока выбирается так, чтобы вероятность появления трех ошибок была мала, в нем с вероятностью, близкой к единице, имеется одна ошибка, которую код Хэмминга исправляет с гарантией. После проводится перемешивание и процедура повторяется.

По числу переданных бит через открытый канал связи на один бит «очищенного» ключа коды Хэмминга имеют примерно такие же показатели, как у процедуры Cascade и кодов БЧХ, но вдвое лучше,

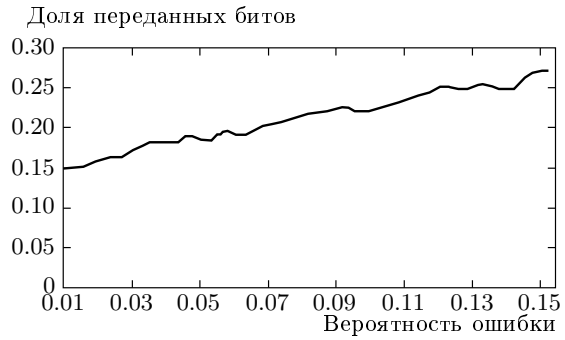

Рис. 17.

чем у процедуры Binary. На рис. 16 и 17 приведено число переданных через открытый канала бит на один бит ключа для случаев, когда генератор случайных чисел имеется соответственно только на стороне Alice и на стороне Alice и Bob.

Напомним, что длина «очищенного» ключа является лишь промежуточной величиной. Для оценки полной эффективности необходимо сравнивать длину финального секретного ключа после сжатия посредством хэширования. Для этого необходимо знать новые условные вероятности для Eve о ключе после коррекции ошибок. Окончательного ответа на сегодняшний день у авторов нет. Дело связано с тем, что процедура с предварительной проверкой на четность кодовых блоков делает задачу «неоднородной» в том смысле, что после каждого прохода «чистки» кодами Хэмминга условные вероятности становятся разными для отдельных групп бит. В тех блоках, где кодирование не применялось, условная вероятность не меняется, а в блоках, где происходила коррекция ошибок, условная вероятность для бит в «очищенных» позициях становится другой. После перемешивания биты с разными условными вероятностями для Eve также случайно распределяются по новым блокам на следующем проходе. Поэтому вряд ли можно найти аналитическое выражение для новой условной вероятности для Eve (соответственно, энтропии Реньи), которая определяет длину финального ключа. По нашим предварительным оценкам выигрыш на промежуточном этапе кодов Хэмминга аннигилируется по сравнению с процедурой Cascade для финального ключа.

Задача с неоднородными условными вероятностями по ключу представляет самостоятельный интерес.

10. ОТКРЫТЫЕ ВОПРОСЫ, СВЯЗАННЫЕ С КОЛЛЕКТИВНЫМИ ИЗМЕРЕНИЯМИ В КВАНТОВОЙ КРИПТОГРАФИИ

Выше рассматривался протокол B92 на двух неортогональных состояниях. Этот протокол является в значительной степени модельным, но содержит все основные моменты, которые имеют место и для других практически важных протоколов квантовой криптографии, таких как BB84.

При прозрачном подслушивании эти моменты сводятся к следующему. После проведения измерений на приемном конце для любого протокола возникает соответствие между битами Bob i_k и состояниями Eve, $i_k \leftrightarrow \rho_{i_k}$, где ρ_{i_k} — квантовое состояние в регистре квантовой памяти у Eve, которое может быть как чистым, так и смешанным. Причем соответствие между квантовыми состояниями Eve и битами Bob имеет место для всех позиций, независимо от того, правильные или неправильные биты, по сравнению с посланными Alice, находятся в этих позициях. Сами состояния Eve определяются вероятностью Q неправильных позиций на стороне Bob.

Дальнейшее положение определяется используемой процедурой коррекции ошибок легитимными пользователями. Если используется процедура с таблицей (вообще говоря, экспоненциально большой) случайных кодов в духе Шеннона, то при индивидуальных измерениях Eve секретный ключ может быть извлечен, если классическая пропускная способность канала Alice–Bob больше, чем канала Alice–Eve. При этом длина ключа при больших n (формально при $n \to \infty$) равна длине переданной строки n. В силу того что имеет место сильное обращение прямой теоремы кодирования для классических каналов связи, информация Eve о ключе стремится к нулю с ростом n (см. формулу (28)). Если же Eve (формальных запретов на это нет) может делать коллективные измерения над целым регистром своих квантовых состояний, то после коррекции ошибок легитимными пользователями на стороне Bob строка длиной n еще не может быть использована в качестве секретного ключа. Для получения секретного ключа «очищенная» строка бит длиной n должна быть сжата при помощи универсальной хэш-функции. Степень сжатия (длина секретного ключа) определяется переходными вероятностями при коллективных измерениях Eve:

$$P_{W|W_E=w_E^k}(w_E^k) = \mathrm{Tr}\{\mathcal{X}_{w_E^k}\hat{\rho}_W\},$$
$$\hat{\rho}_W = \rho_{i_1} \otimes \cdots \otimes \rho_{i_n}. \qquad (99)$$

Здесь $\mathcal{X}_{w_E^k}$ — измеряющий оператор, аналогичный (30), (65). Отсчет в канале измерений $\mathcal{X}_{w_E^k}$ интерпретируется Eve как бинарная строка $w_E^k = (i_1^E, i_2^E, \ldots, i_n^E)$ при условии, что истинная строка есть W. Степень сжатия ключа определяется величиной энтропии Реньи (52), вычисленной с условными вероятностями (99). На сегодняшний день точные неравенства для энтропии Реньи в случае коллективных измерений нам неизвестны.

Исправление ошибок легитимными пользователями при помощи экспоненциально большой таблицы случайных кодовых слов является неконструктивной и может быть использовано лишь для выяснения теоретического предела вероятности ошибок Q, до которой возможна генерация секретного ключа. Однако вопрос о коллективных измерениях имеет место и для конструктивных практических процедур коррекции ошибок.

После процедур Binary и Cascade с выбрасыванием ситуация аналогична описанной выше, с той лишь разницей, что теперь у Bob нет неправильных бит, соответственно, у Eve нет квантовых состояний, отвечающих неправильным битам. «Очищенный» первичный ключ еще не может быть использован как секретный, требуется хэширование (сжатие), которое определяется переходными вероятностями Eve (99), но уже после коррекции ошибок.

При коррекции ошибок при помощи классических кодов также возможны коллективные измерения Eve. После того как легитимными пользователями установлена вероятность ошибки Q, выбран соответствующий классический код и проведено разбиение всей строки на кодовые слова, Eve может также делать коллективные квантово-механические измерения не над каждой ячейкой памяти, а над целыми кодовыми словами. В этом случае решающие операторы (30), (65), (99) дают разложение единицы в подпространстве, натянутом на все векторы кодовых слов. В такой ситуации анализ величины сжатия «очищенного» ключа еще более усложняется.

Хотя на сегодняшний день коллективные измерения являются скорее теоретической угрозой, но имеющиеся эксперименты по квантовой памяти (см., например, [27]) могут сделать их технологически реализуемыми в ближайшее время.

Таким образом, способ исправления ошибок в первичном ключе радикально влияет на длину финального секретного ключа. Кроме того, длина ключа определяется не только процедурой коррекции, но и квантовой частью протокола, поэтому эффективность процедуры исправления ошибок сама по себе еще ничего не говорит об эффективности в целом при учете квантовой части протокола.

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

ЛИТЕРАТУРА

1. S. Wiesner, SIGACT News **15**, 78 (1983).
2. C. H. Bennett and G. Brassard, Proc. of IEEE Int. Conf. on Comput. Sys. and Sign. Proces., Bangalore, India (1984), p. 175.
3. G. S. Vernam, J. Amer. Inst. Elect. Eng. **55**, 109 (1926).
4. В. А. Котельников, Отчет (1941).
5. C. E. Shannon, Bell Syst. Tech. J. **28**, 658 (1949).
6. W. K. Wootters and W. H. Zurek, Nature **299**, 802 (1982).
7. C. H. Bennett, Phys. Rev. Lett. **68**, 3121 (1992); C. H. Bennett, G. Brassard, and N. D. Mermin, Phys. Rev. Lett. **68**, 557 (1992).
8. W. Diffi and M. E. Hellman, IEEE Trans. on Inf. Theory **IT-22**, 644 (1976).
9. A. K. Ekert, B. Huttner, G. M. Palma, and A. Peres, Phys. Rev. A **50**, 1047 (1994).
10. H. E. Brandt, J. M. Myer, and S. J. Lomonaco Jr., Phys. Rev. A **56**, 4456 (1997).
11. C. E. Shannon, Bell Syst. Tech. J. **27**, 397; 623 (1948).
12. Р. Галлагер, *Теория информации и надежная связь*, Советское радио, Москва (1974).
13. C. W. Helstrom, *Quantum Detection and Estimation Theory*, Academic Press, New York, San Francisco, London (1976).
14. J. Wolfowitz, Illinois J. of Math. **1**, 591 (1957).
15. А. С. Холево, *Введение в квантовую теорию информации*, сер. Соврем. мат. физ., вып. 5, МЦНМО, Москва (2002); А. С. Холево, Проблемы передачи информации **8**, 63 (1972); **15**, 3 (1979); УМН **53**, 193 (1998).
16. R. Jozsa and B. Schumacher, J. Mod. Optics **41**, 2343 (1994).
17. P. Hausladen, R. Jozsa, B. Schumacher, M. Westmoreland, and W. K. Wootters, Phys. Rev. A **54**, 1869 (1996).

18. B. Schumacher and M. D. Westmoreland, Phys. Rev. A **56**, 131 (1997).

19. D. Maurer, IEEE Trns. Inf. Theory **39**, 733 (1993).

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

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

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

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

24. E. J. Mac Williams and N. J. A. Sloane, *The Theory of Error-Correcting Codes*, North-Holland Publ. Company, Amsterdam, New York, Oxord (1977).

25. W. W. Peterson and E. J. Weldon, *Error-Correcting Codes*, The MIT Press, Cambridge, Massachusetts, London, England (1972).

26. 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.

27. B. Julsgaard, J. Sherson, J. I. Cirac, J. Fiurášek, and E. S. Polzik, Nature **432**, 482 (2004).