ЖЭТФ, 2019, том 155, вып. 5, стр. 824–831

КВАНТОВОЕ РАСПРЕДЕЛЕНИЕ КЛЮЧЕЙ С НЕБИНАРНЫМ ФАЗОВО-ВРЕМЕННЫМ КОДИРОВАНИЕМ, ДОПУСКАЮЩЕЕ ТОЧНОЕ ДОКАЗАТЕЛЬСТВО СЕКРЕТНОСТИ

С. Н. Молотков*

Институт физики твердого тела Российской академии наук
142432, Черноголовка, Московская обл., Россия

Академия криптографии Российской Федерации
121552, Москва, Россия

Факультет вычислительной математики и кибернетики,
Московский государственный университет им. М. В. Ломоносова
119899, Москва, Россия

Центр квантовых технологий,
Московский государственный университет им. М. В. Ломоносова
119899, Москва, Россия

Поступила в редакцию 21 декабря 2018 г.,
после переработки 21 декабря 2018 г.
Принята к публикации 25 декабря 2018 г.

Предложен протокол квантового распределения ключей с небинарным кодированием, который допускает точное доказательство секретности. Протокол обеспечивает бóльшую скорость генерации ключей по сравнению с протоколом BB84, кроме того, имеет простую экспериментальную реализацию без активных элементов на приемной стороне, не требующую подстройки поляризации на выходе из линии связи.

DOI: 10.1134/S0044451019050055

1. ВВЕДЕНИЕ

Цель квантовой криптографии — распределение криптографических ключей, секретность которых гарантируется фундаментальными ограничениями квантовой механики на различимость квантовых состояний. Главное требование к протоколам квантового распределения ключей (КРК) — это доказуемая секретность протокола. Под доказуемой секретностью понимается то обстоятельство, что протокол должен обеспечивать секретность ключей относительно всевозможных атак, а также то, что доказательство должно быть основано только на фундаментальных принципах квантовой теории и не содержать каких-то предположений о конкретных типах атак.

Главная проблема любого доказательства секретности состоит в установлении верхней границы утечки информации к подслушивателю по наблюдаемым параметрам на приемной стороне, обычно по наблюдаемому числу ошибок. Если известна верхняя граница утечки информации к подслушивателю по всем атакам как функция наблюдаемых параметров на приемной стороне, то после коррекции ошибок и усиления секретности можно утверждать, что система обеспечивает безусловную секретность ключей при любых атаках.

Если гарантируется секретность ключей относительно одной атаки, то, вообще говоря, нельзя гарантировать секретность ключей относительно других атак. Принципиально невозможно перебрать все мыслимые атаки. Однако существуют случаи, когда не нужно перебирать все атаки и при этом можно гарантировать секретность ключей. Этот выделенный случай относится к системам, использующим строго однофотонный источник информационных квантовых состояний и протокол квантового распределения ключей с двумя базисами. Классическим примером такого протокола является протокол

* E-mail: sergei.molotkov@gmail.com

BB84 [1]. Для этого выделенного случая не требуется перебирать все атаки и явно их предъявлять, но при этом можно установить фундаментальную верхнюю границу утечки информации к подслушивателю по наблюдаемым параметрам на приемной стороне [2]. При доказательстве секретности принципиально важны два момента. Первый момент — это возможность свести описание протокола распределения ключей к так называемой ЭПР-версии протокола (ЭПР — эффект Эйнштейна – Подольского – Розена, см. ниже). Второй момент — это возможность использовать энтропийные соотношения неопределенностей, связывающие утечку информации к подслушивателю с классической условной энтропией между Алисой и Бобом. Энтропийными соотношениями неопределенностей для трехчастичных систем, описывающих общее квантовое состояние Алиса – Боб – Ева, удается воспользоваться только благодаря редукции протокола к ЭПР-версии. Данный инструментарий работает только для протоколов с двумя базисами (см. ниже). Протокол BB84, по-видимому, на сегодняшний день является единственным и уникальным примером, который обладает упомянутыми свойствами.

Хотя на сегодняшний день строго однофотонный источник отсутствует, исследование подобных протоколов является принципиально важным для понимания фундаментальных принципов секретности ключей в квантовой криптографии.

Одна из задач при реализации систем квантовой криптографии состоит в увеличении скорости распределения ключей. Часто при реализации систем квантовой криптографии доказуемая секретность приносится в жертву скорости генерации ключей.

В протоколе BB84 в каждом базисе только два состояния, поэтому на каждую посылку можно распределить не более одного бита секретного ключа. Существуют технические способы увеличения скорости, один из способов — увеличение тактовой частоты. Эти способы в данной работе не обсуждаются. Еще один способ увеличения скорости состоит в разработке новых протоколов квантовой криптографии. Наиболее естественный способ увеличения скорости состоит в увеличении размерности пространства квантовых информационных состояний.

На теоретическом уровне был предложен ряд протоколов, использующих квантовые состояния в пространстве размерностью больше двух. Однако реализовать подобные протоколы бывает практически невозможно, поскольку экспериментальный арсенал технически реализуемых квантовых состояний достаточно ограничен. Кроме того, часто не удается доказать на уровне фундаментальных принципов секретность протокола.

Ниже предлагается протокол КРК, который допускает точное решение — доказательство секретности на основе энтропийных соотношений неопределенностей, и имеет в $\log_2(3) = 1.585$ бóльшую, по сравнению с BB84, скорость распределения ключей. Данный протокол в однопроходном варианте имеет простую экспериментальную реализацию, при которой не требуется подстройка поляризации информационных состояний на выходе из линии связи. Реализация, аналогичная [3], не использует активных поляризационно-чувствительных элементов на приемной стороне — фазовых модуляторов, контроллеров поляризации (см. детали в [3]). Кроме того, отсутствие активных элементов делает систему устойчивой к атакам на техническую реализацию — к атакам активного зондирования аппаратуры, в частности фазовых модуляторов, которые несут информацию о ключе. Важно отметить, что протокол BB84 не допускает подобной экспериментальной реализации без фазовых модуляторов и модуляторов поляризации.

2. ИНФОРМАЦИОННЫЕ СОСТОЯНИЯ И ИЗМЕРЕНИЯ

В этом разделе приведем описание информационных состояний и покажем, как данный протокол редуцируется к ЭПР-версии, которая позволит воспользоваться в дальнейшем энтропийными соотношениями неопределенностей. В протоколе используются два базиса L и R. В каждом базисе имеется три взаимно ортогональных информационных состояния, которые равновероятно внутри базиса посылаются Алисой в канал связи к Бобу. Информационные состояния Алисы в базисе L имеют вид

$$|0_L\rangle_A = \frac{|1\rangle_A + |2\rangle_A}{\sqrt{2}}, \qquad |1_L\rangle_A = \frac{|1\rangle_A - |2\rangle_A}{\sqrt{2}}, \quad |3\rangle_A, \tag{1}$$

соответственно, информационные состояния в базисе R —

$$|0_R\rangle_A = \frac{|2\rangle_A + |3\rangle_A}{\sqrt{2}}, \qquad |1_R\rangle_A = \frac{|2\rangle_A - |3\rangle_A}{\sqrt{2}}, \quad |1\rangle_A. \tag{2}$$

В формулах (1), (2) $|i\rangle_A$ $(i = 1, 2, 2)$ — однофотонные фоковские состояния, локализованные во вре-

менны́х окнах 1, 2 и 3. Пространство состояний является трехмерным. При известном базисе из-за ортогональности внутри базиса состояния достоверно различимы. Технически данные состояния реализуются, например, как в работе [3]. На приемной стороне используются два разных измерения в базисах L и R, которые позволяют достоверно различить состояния при известном базисе. Измерения Боба даются разложениями единицы: в базисе L

$$I_B(L) = |0_L\rangle_{BB}\langle 0_L| + |1_L\rangle_{BB}\langle 1_L| + |3\rangle_{BB}\langle 3|, \quad (3)$$

в базисе R

$$I_B(R) = |1\rangle_{BB}\langle 1| + |0_R\rangle_{BB}\langle 0_R| + |1_R\rangle_{BB}\langle 1_R|. \quad (4)$$

В ЭПР-версии Алиса готовит максимально запутанное состояние. Важно, что ЭПР-пара Алиса–Боб $|\Psi\rangle_{AB}$ неформально является общей «заготовкой» Алисы и Боба для приготовления равновероятно информационных состояний в двух разных базисах из одного запутанного состояния. Одно и то же квантовое состояние — ЭПР-пара Алиса–Боб $|\Psi\rangle_{AB}$ — имеет разные представления в разных базисах:

$$\begin{aligned}|\Psi\rangle_{AB} = \\ = \frac{1}{\sqrt{3}}\left(|1\rangle_A\otimes|1\rangle_B + |2\rangle_A\otimes|2\rangle_B + |3\rangle_A\otimes|3\rangle_B\right) = \\ = \frac{1}{\sqrt{3}}\left(|0_L\rangle_A\otimes|0_L\rangle_B + |1_L\rangle_A\otimes|1_L\rangle_B + \right. \\ \left. + |3\rangle_A\otimes|3\rangle_B\right) = \frac{1}{\sqrt{3}}\left(|1\rangle_A\otimes|1\rangle_B + |0_R\rangle_A\otimes|0_R\rangle_B + \right. \\ \left. + |1_R\rangle_A\otimes|1_R\rangle_B\right). \quad (5)\end{aligned}$$

Далее, свою подсистему A из ЭПР-пары Алиса оставляет у себя, данная подсистема никому кроме Алисы недоступна. Подсистему B Алиса направляет через квантовый канал связи к Бобу, данная подсистема доступна для подслушивания Еве. После достижения подсистемой B (возможно, уже в искаженном виде из-за действий Евы) приемной стороны Боба Алиса случайно и равновероятно выбирает один из базисов измерений для своей подсистемы A. Два измерения на передающей стороне Алисы даются разложениями единицы в пространстве состояний Алисы. В базисе L имеем

$$\begin{aligned}I_A(L) = |0_L\rangle_{AA}\langle 0_L| + |1_L\rangle_{AA}\langle 1_L| + |3\rangle_{AA}\langle 3| = \\ = \mathcal{P}_A(0_L) + \mathcal{P}_A(1_L) + \mathcal{P}_A(3), \quad (6)\end{aligned}$$

соответственно в базисе R —

$$\begin{aligned}I_A(R) = |1\rangle_{AA}\langle 1| + |0_R\rangle_{AA}\langle 0_R| + |1_L\rangle_{AA}\langle 1_L| = \\ = \mathcal{P}_A(1) + \mathcal{P}_A(0_R) + \mathcal{P}_A(1_R). \quad (7)\end{aligned}$$

При этом случайно и равновероятно Алиса получит один из исходов измерений, например, в базисе L ($x_L \in X_L = \{0_L, 1_L, 3\}$). Если бы не было возмущения состояния в линии связи, то Боб получил бы в том же базисе полностью коррелированный с Алисой исход измерений. Напомним, что посылки, когда базисы Алисы и Боба не совпадают, отбрасываются. Действия Евы искажают состояния Боба и в самом общем случае описываются действием унитарного оператора U_{BE} на подсистему B и вспомогательное квантовое состояния Евы $|E\rangle_E$. В итоге возникает трехчастичное состояние, имеем

$$|\Psi\rangle_{ABE} = U_{BE}\left(|\Psi\rangle_{AB}\otimes|E\rangle_E\right). \quad (8)$$

Еве доступна только квантовая подсистема B. Любое допустимое квантовой теорией преобразование квантового состояния в квантовое состояние дается действием супероператора — вполне положительное отображение матриц плотности в матрицы плотности. Любой супероператор унитарно представи́м, т. е. может быть представлен как действие унитарного оператора на квантовое состояние и вспомогательную подсистему (окружение, среду), что и имеет место в (8). Явный вид супероператора, соответственно U_{BE}, для оценки верхней границы утечки информации к Еве не требуется, данную работу делают энтропийные соотношения неопределенностей. Далее, матрица плотности после измерений Алисы, например, в базисе L имеет вид

$$\begin{aligned}\rho_{X_L BE} = \sum_{x_L=0_L,1_L,3}\mathcal{P}_A(x_L)\times \\ \times \mathrm{Tr}_A\left\{\mathcal{P}_A(x_L)|\Psi\rangle_{ABEABE}\langle\Psi|\mathcal{P}_A(x_L)\right\}\mathcal{P}_A(x_L). \quad (9)\end{aligned}$$

Измерения Боба в том же базисе L приводят к матрице плотности (ниже исходы измерений Боба $y_L \in$ $\in Y_L = \{0_l, 1_L, 3\}$)

$$\begin{aligned}\rho_{X_L Y_L E} = \sum_{y_L=0_L,1_L,3}\mathcal{P}_B(x_L)\times \\ \times \mathrm{Tr}_B\{\mathcal{P}_B(x_L)\rho_{X_L BE}\mathcal{P}_B(x_L)\}\mathcal{P}_B(x_L). \quad (10)\end{aligned}$$

Аналогично измерения Алисы в базисе R приводят к матрице плотности

$$\begin{aligned}\rho_{X_R BE} = \sum_{x_L=0_R,1_R,1}\mathcal{P}_A(x_R)\times \\ \times \mathrm{Tr}_A\left\{\mathcal{P}_A(x_R)|\Psi\rangle_{ABEABE}\langle\Psi|\mathcal{P}_A(x_R)\right\}\mathcal{P}_A(x_R). \quad (11)\end{aligned}$$

Измерения Боба в том же базисе R приводят к матрице плотности ($y_R \in Y_R = \{0_R, 1_R, 1\}$)

$$\rho_{X_R Y_R E} = \sum_{y_R=0_R,1_R,1} \mathcal{P}_B(x_R) \times \\ \times \mathrm{Tr}_B\{\mathcal{P}_B(x_R)\rho_{X_R BE}\mathcal{P}_B(x_R)\}\mathcal{P}_B(x_R). \quad (12)$$

Матрица плотности Алисы–Боба после их измерений является чисто классической:

$$\begin{aligned} \rho_{X_L Y_L} &= \mathrm{Tr}_E\{\rho_{X_L Y_L E}\}, \\ \rho_{X_R Y_R} &= \mathrm{Tr}_E\{\rho_{X_R Y_R E}\}. \end{aligned} \quad (13)$$

Алиса и Боб имеют коррелированные (без Евы полностью коррелированные) классические случайные величины в базисе L: $x_L \in X_L = \{0_L, 1_L, 3\}$ и $y_L \in Y_L = \{0_L, 1_L, 3\}$. Ева имеет в своем распоряжении квантовую систему E, коррелированную с классической случайной переменной Алисы.

Из описания ЭПР-версии видно, что протокол эквивалентен протоколу, когда Алиса случайно и равновероятно выбирает базис, затем внутри базиса случайно и равновероятно выбирает одно из трех состояний и посылает их к Бобу.

На данном этапе Алиса и Боб находятся в ситуации классического канала связи с тремя состояниями на входе и тремя состояниями на выходе (рис. 1*а*). Алиса случайно и равновероятно посылала Бобу, например, в базисе L величину $x_L \in X_L = \{0_L, 1_L, 3\}$, Боб получал $y_L \in Y_L = \{0_L, 1_L, 3\}$. Классический канал без памяти (рис. 1) описывается в самом общем виде переходными (условными) вероятностями. Данные переходные вероятности выражаются через частичную матрицу плотности Алисы–Боба (8) с учетом (9)–(12).

К переходным вероятностям предъявляется требование сохранения нормировки — сумма переходных вероятностей для каждого входного символа по всем выходным символам должна быть равна единице:

$$\sum_{y_L \in Y_L} P_{Y_L|X_L}(y_L|X_L = x_L) = 1, \quad (14)$$

где величина x_L фиксирована. Неформально говоря, каждый входной символ обязательно перейдет в какие-то выходные символы. Выражения для условных вероятностей при переходе $x \to y$ непосредственно получаются из рис. 1. В самом общем случае (рис. 1*а*) с учетом условия нормировки (14) в каждом базисе атака Евы описывается шестью независимыми параметрами: три входных состояния, каждое из которых может перейти в любое из трех выходных. Данный канал связи описывается тремя переходными (условными) вероятностями, сумма которых равна единице, в итоге остается два независимых параметра на каждое входное состояние. В базисе L имеем $(q_0^L, q_1^L, Q_0^L, Q_1^L, \delta_0^L, \delta_1^L)$, аналогично в базисе R. При этом все три входных и три выходных состояния являются информационными.

Во избежание путаницы отметим, что канал, изображенный на рис. 1*б*, относится к принципиально другому протоколу с фазово-временны́м кодированием [4, 5], где два входных и три выходных состояния — два информационных и одно контрольное. В симметричном случае атака Евы параметризуется двумя параметрами Q и q [4, 5]. Рисунок 1*в* относится к протоколу BB84, который параметризуется в симметричном случае одним параметром Q. Для протоколов [4, 5] и BB84 можно построить явные атаки. Отметим, что для протокола BB84 можно привести явную атаку [6], причем нижняя граница энтропийных соотношений неопределенностей достигается на симметричной атаке (рис. 1*в*).

Чтобы не загромождать выкладки, рассмотрим симметричный случай (об особой выделенности симметричного случая см. ниже): $q_0^L = q_1^L = q$, $Q_0^L = Q_1^L = Q$, $\delta_0^L = \delta_1^L = \delta$, аналогично в базисе R. Общий случай (рис. 1*а*) рассматривается полностью аналогично, переходные вероятности выписываются непосредственно по рис. 1*а*. Совместная матрица плотности Алисы–Боба имеет вид

$$\begin{aligned} \rho_{X_L Y_L} = \frac{1}{3}|0_L\rangle_{XX}\langle 0_L| \otimes \{(1-q)(1-Q)|0_L\rangle_{YY}\langle 0_L| + \\ + (1-q)Q|1_L\rangle_{yY}\langle 1_L| + q|3\rangle_{YY}\langle 3|\} + \\ + \frac{1}{3}|1_L\rangle_{XX}\langle 1_L| \otimes \{(1-q)(1-Q)|1_L\rangle_{YY}\langle 1_L| + \\ + (1-q)Q|0_L\rangle_{YY}\langle 0_L| + q|3\rangle_{YY}\langle 3|\} + \\ + \frac{1}{3}|3\rangle_{XX}\langle 3| \otimes \left\{\delta|3\rangle_{YY}\langle 3| + \left(\frac{1-\delta}{2}\right)|0_L\rangle_{YY}\langle 0_L| + \right. \\ \left. + \left(\frac{1-\delta}{2}\right)|1_L\rangle_{YY}\langle 1_L|\right\}, \end{aligned} \quad (15)$$

соответственно, частичная матрица плотности Боба имеет вид

$$\begin{aligned} \rho_{Y_L} = \mathrm{Tr}_A\{\rho_{X_L Y_L}\} = \\ = \frac{1}{3}|0_L\rangle_{YY}\langle 0_L|\left\{(1-q) + \frac{1-\delta}{2}\right\} + \\ + \frac{1}{3}|1_L\rangle_{YY}\langle 1_L|\left\{(1-q) + \frac{1-\delta}{2}\right\} + \\ + \frac{1}{3}|3\rangle_{YY}\langle 3|\{2q + \delta\}. \end{aligned} \quad (16)$$

3. УСЛОВНЫЕ ЭНТРОПИИ

В асимптотическом пределе длинных последовательностей утечка информации к Еве выражается

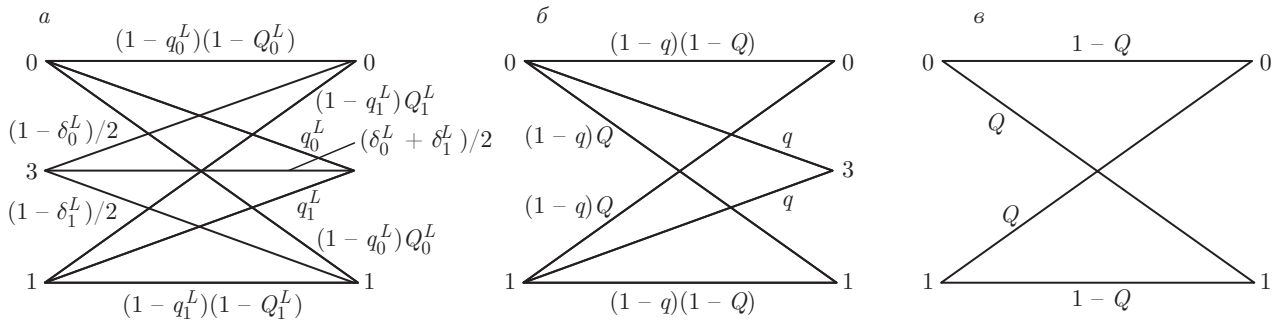

Рис. 1. Схемы классических каналов. *а*) Канал с небинарным кодированием — три входных информационных, три выходных информационных состояния. Переходные вероятности приведены для общего случая. *б*) Канал, отвечающий фазово-временно́му кодированию — два входных информационных состояния, два выходных информационных состояния и одно контрольное. Переходные вероятности приведены для симметричного случая. *в*) Канал, отвечающий протоколу BB84, переходные вероятности приведены для симметричного случая

через условную энтропию фон Неймана, которая, в свою очередь, выражается через частичную матрицу плотности Алисы–Евы и матрицу плотности Евы:

$$\rho_{X_L E}=\mathrm{Tr}_B\{\rho_{X_L Y_L E}\},\quad \rho_E=\mathrm{Tr}_{AB}\{\rho_{X_L Y_L E}\}. \quad (17)$$

Энтропийные соотношения неопределенностей позволяют выразить верхнюю границу утечки информации к подслушивателю через условную энтропию Алисы–Боба, которая является классической и для вычисления которой достаточно знать наблюдаемые значения параметров на приемной стороне. В рассматриваемом случае это (q,Q,δ). Напомним, что рассматриваем предел асимптотически длинных последовательностей, в этом пределе частоты случайных событий совпадают с вероятностями. Параметры определяются путем раскрытия части переданной последовательности, которая затем, естественно, отбрасывается. Параметр q определяется следующим образом. Алиса раскрывает часть посылок, когда было послано 0 и 1 в данном базисе, подсчитывается доля отсчетов, когда $y_L=3$, что дает параметр q. Затем для определения параметра Q подсчитывается число правильных (или ошибочных) отсчетов в раскрытой последовательности 0 и 1, которые дали отсчеты в информационных окнах $y_L=0,1$. Далее, для определения параметра δ Алиса раскрывает часть последовательности, когда она посылала состояние $|3\rangle_E$. Боб подсчитывает долю посылок, которые дали отсчеты $y_L=3$, что определяет параметр δ. Отметим, что для произвольного несимметричного случая определение параметров происходит аналогично. Алиса раскрывает, например, когда посылался 0 в данном базисе. Боб подсчитывает, какая доля будет зарегистрирована как $y_L=0$, какая доля даст $y_L=1$ и какая доля отсчетов дает $y_L=3$. Аналогично для других состояний. В общем случае подсчет происходит в каждом базисе отдельно.

Вычислим условные энтропии Алисы–Боба по определению и с учетом (15)–(17):

$$H(X_L|Y_L)=H(X_L,Y_L)-H(Y_L)=\\ =H(\rho_{X_L Y_L}|\rho_{Y_L})=H(\rho_{X_L Y_L})-H(\rho_{Y_L}), \quad (18)$$

$$H(X_L,Y_L)=H(\rho_{X_L Y_L})=\log(3)+\frac{2}{3}h(q)+\\ +\frac{2}{3}(1-q)h(Q)+\frac{1}{3}h(\delta)+\frac{1}{3}(1-\delta), \quad (19)$$

$$H(Y_L)=H(\rho_{Y_L})=\log(3)-\frac{2}{3}\left[1-q+\frac{1-\delta}{2}\right]\times\\ \times\log\left[1-q+\frac{1-\delta}{2}\right]-\frac{1}{3}[2q+\delta]\log[2q+\delta], \quad (20)$$

где $h(x)=-x\log(x)-(1-x)\log(1-x)$. Здесь и везде ниже $\log\equiv\log_2$. Энтропийные соотношения неопределенностей позволяют не вычислять явно условную энтропию Алисы–Евы

$$H(X_L|E)=H(\rho_{X_L E}|\rho_E)=H(\rho_{X_L E})-H(\rho_E), \quad (21)$$

которая связана с утечкой информации к Еве, а определить нижнюю границу данной энтропии через классическую энтропию Алисы–Боба, которая, в свою очередь, выражается через наблюдаемые параметры на приемной стороне.

4. ЭНТРОПИЙНЫЕ СООТНОШЕНИЯ НЕОПРЕДЕЛЕННОСТЕЙ

Энтропийные соотношения неопределенностей выражают верхнюю границу условной энтропии Алисы–Евы в одном базисе через условную классическую энтропию Алисы–Боба в другом базисе. Условная энтропия Алисы–Евы в асимптотическом пределе имеет простую интерпретацию. Условная энтропия Алисы–Евы дает информацию в битах, которой Еве не хватает, чтобы полностью знать битовую строку Алисы. Согласно [7, 8], энтропийные соотношения неопределенностей применительно к нашему случаю в базисах L и R имеют вид

$$\begin{aligned} H(X_R|E) + H(X_L|Y_L) &\geq \log\left(\frac{1}{c}\right), \\ H(X_L|E) + H(X_R|Y_R) &\geq \log\left(\frac{1}{c}\right), \end{aligned} \tag{22}$$

$$\begin{aligned} c = \max_{\{x_L \in X_L, x_R \in X_R\}} \mathrm{Tr}_A\{\mathcal{P}_A(x_L)\cdot\mathcal{P}_A(x_R)\} = \\ = |{}_A\langle 0_L, 1_L|1\rangle_A|^2 = |{}_A\langle 0_R, 1_R|3\rangle_A|^2 = \frac{1}{2}. \end{aligned} \tag{23}$$

Подчеркнем, что c — максимальная величина перекрытия между состояниями из разных базисов при измерениях Алисы. Знание условной энтропии Алисы–Евы позволяет определить длину секретного ключа (точнее, долю секретных битов в пересчете на посылку, деленную на $\log(3)$) в каждом базисе. Для длины секретного ключа в базисе L с учетом (22), (23) находим (см. детали в [9])

$$\begin{aligned} \ell_L = H(X_L|E) - H(X_L|Y_L) \geq \\ \geq 1 - (H(X_R|Y_R) + H(X_L|Y_L)), \end{aligned} \tag{24}$$

соответственно, в базисе R находим

$$\begin{aligned} \ell_R = H(X_R|E) - H(X_R|Y_R) \geq \\ \geq 1 - (H(X_L|Y_L) + H(X_R|Y_R)). \end{aligned} \tag{25}$$

Как видно из (24), (25), длина секретного ключа одинакова в разных базисах независимо от симметричности или асимметричности атаки как по отношению к входным и выходным состояниям, так и по отношению к базису. Поэтому часто, исходя из консервативных соображений, для длины ключа используют средние значения наблюдаемых параметров по всем базисам (см. ниже). Формулы (24), (25) имеют наглядную интерпретацию. Длина секретного ключа есть разность между нехваткой информации Евы о битовой строке Алисы и нехваткой информации Боба о строке Алисы. Нехватка информации Боба о строке Алисы дается условной энтропией Алисы–Боба (21).

5. СРАВНЕНИЕ С ПРОТОКОЛОМ BB84

Энтропия источника при совпадающих базисах на передающей и приемной сторонах в протоколе BB84 составляет $H(X) = \log(2) = 1$ бит, поскольку внутри базиса имеется два состояния. В нашем протоколе внутри базиса имеется три ортогональных, достоверно различимых состояния, поэтому энтропия источника равна $H(X) = \log(3) = 1.585$ бит, поэтому данный протокол обеспечивает бóльшую скорость распределения ключей при прочих равных параметрах системы — тактовой частоте, квантовой эффективности лавинных детекторов и вероятности темновых шумов. При этом условная классическая энтропия Алисы–Боба определяется для бинарного классического канала связи (рис. 1*в*). В симметричном случае находим

$$H(X_L|Y_L) = H(X_R|Y_R) = h(Q). \tag{26}$$

Соответственно для длины ключа получается знаменитая формула (см., например, [10])

$$\begin{aligned} \ell_L = H(X_L|E) - H(X_L|Y_L) \geq \\ \geq 1 - 2H(X_L|Y_L) = 1 - 2h(Q). \end{aligned} \tag{27}$$

Максимальное перекрытие (величина c в формуле (23)) для измеряющих операторов в разных базисах Алисы для протокола BB84 также равна $c = 1/2$.

Определим, до какой длины линии связи оба протокола гарантируют секретное распределение ключей. В отсутствие подслушивателя ошибки Q в информационных окнах ($1 - q$ — доля отсчетов в этих окнах), а также отсчеты в контрольных временны́х окнах для 0 и 1 возникают только из-за темновых шумов детекторов. Доля ошибочных отсчетов, когда посылалось состояние 3, равна $(1 - \delta)/2$, доля правильных отсчетов равна δ. Пусть пропускание канала связи есть

$$T(\mathrm{Len}) = 10^{-\kappa\,\mathrm{Len}/10}, \tag{28}$$

где Len — длина линии связи, κ — коэффициент удельных потерь в линии. Типичное значение для одномодового волокна $\kappa = 0.2$ дБ/км. Для параметров канала связи находим

$$\begin{gathered} q = \frac{p_d}{\eta T(\mathrm{Len}) + 2p_d}, \quad Q = \frac{1}{2}\,\frac{p_d}{\eta T(\mathrm{Len}) + p_d}, \\ 1 - \delta = \frac{p_d}{\eta T(\mathrm{Len}) + 3p_d}, \end{gathered} \tag{29}$$

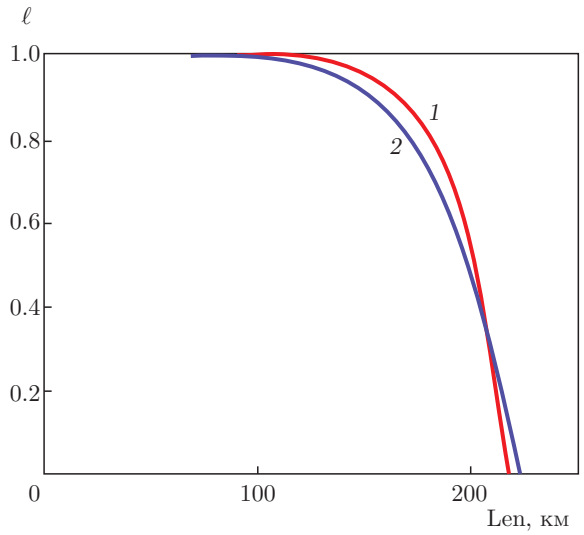

Рис. 2. Длина секретного ключа в пересчете на один зарегистрированный символ как функция длины линии связи. Кривая *1* относится к новому протоколу, кривая *2* — к протоколу BB84. Параметры $\eta = 0.1$, $p_d = 10^{-6}$ отсч./строб.

где параметры без подслушивателя: p_d — вероятность темновых шумов во временно́м окне, η — квантовая эффективность детектора.

Как следует из рис. 2, новый протокол несколько проигрывает протоколу BB84 по дальности. Однако, вплоть до длины канала связи приблизительно 170 км, новый протокол обеспечивает большую скорость генерации ключей из-за большего числа ортогональных состояний внутри каждого базиса. Напомним, что протокол с фазово-временны́м кодированием (два состояния внутри базиса, рис. 1*б*), [4,5]), обеспечивает бо́льшую по сравнению с BB84 дальность при той же скорости распределения ключей.

В протоколе BB84 в симметричном случае фигурирует только один параметр — ошибка Q. Обычно рассматривают симметричный случай, что связано с выпуклостью вверх шенноновской энтропии [11], хотя часто это не оговаривается, а неявно подразумевается. Рассуждения выглядят следующим образом. Пусть атака Евы несимметрична. Это означает, что с вероятностью $0 \le p \le 1$ Ева выбирает в (8) разные унитарные операторы. Поскольку базисы выбираются равновероятно, в доле посылок p условная энтропия Алисы–Боба оказывается равной $h(Q_+)$, а в доле посылок $1-p$ — равной $h(Q_\times)$, где Q_+ и $Q_\times$ — ошибки в базисах $+$ и $\times$ для протокола BB84. Боб видит на приемной стороне полную наблюдаемую ошибку $Q_{total} = pQ_+ + (1-p)Q_\times$. Тогда условная энтропия Алисы–Боба равна $h(Q_{total})$. Из выпуклости энтропии следует, что

$$h(Q_{total}) \ge ph(Q_+) + (1-p)h(Q_\times), \qquad (30)$$

равенство имеет место при $Q_+ = Q_\times$, $p = 1-p = 1/2$. Если для длины ключа Алисы–Боба используют оценку, исходя только из полной по обоим базисам, наблюдаемой ошибки (обычно ошибка внутри каждого базиса отдельно не выделяется), то длина ключа

$$\ell = 1-2h(Q_{total}) \le 1-[ph(Q_+)+(1-p)h(Q_\times)], \quad (31)$$

что эквивалентно длине ключа при симметричной атаке Евы (рис. 1*в*) с ошибкой $Q = Q_{total}$. Кроме того, в [6] показано путем построения явной атаки для протокола BB884, что нижняя граница энтропийных соотношений неопределенностей достигается при симметричной атаке. С точки зрения подслушивателя выгоднее использовать симметричную атаку, т. е. один и тот же унитарный оператор — атаковать все посылки одинаково, поскольку это дает максимум информации для Евы при заданной наблюдаемой ошибке. Аналогичные соображения, основанные на выпуклости шенноновской энтропии, только с более длинными выкладками, справедливы и для нового протокола. Для нового протокола при необходимости можно использовать и общие выражения для энтропий (см. рис. 1*а*).

6. ЗАКЛЮЧЕНИЕ

Основная причина для разработки нового протокола связана с его уникальной технической реализацией, аналогичной [3]. А именно, реализация протокола в однопроходном варианте не требует подстройки состояния поляризации на выходе из линии связи. Кроме того, на приемной стороне не используются активные поляризационно-чувствительные элементы — фазовые модуляторы, что фактически исключает активное зондирование активных элементов в отличие от других реализаций. Подчеркнем, что уникальная реализация [3] возможна только для протоколов с фазово-временны́м кодированием. Например, для протокола BB84 невозможна реализация без активных поляризационно-чувствительных элементов (фазовых модуляторов, модуляторов поляризации). Это связано с тем, что пространство состояний является трехмерным, а не двумерным, как для BB84. Неортогональность состояний в разных базисах, которая нужна для детектирования подслушивания, достигается за счет частичного перекрытия информационных состояний, сдвинутых по времени. На сегодняшний день это единственное

семейство протоколов, которое в однопроходном варианте не использует активных элементов на приемной стороне. Кроме того, протокол имеет точное доказательство секретности, основанное на фундаментальных энтропийных соотношениях неопределенностей. Доказательство секретности протокола допускает обобщение на случай конечных последовательностей. Это требует большего места для изложения.

Благодарности. Выражаем благодарность коллегам из Академии криптографии Российской Федерации за обсуждения. Автор благодарит И. М. Арбекова, К. А. Балыгина, А. Н. Климова, К. С. Кравцова, С. П. Кулика за многочисленные и интенсивные обсуждения.

Финансирование. Работа поддержана Российским научным фондом (проект № П-П (2019)).

ЛИТЕРАТУРА

1. C. H. Bennett and G. Brassard, Proc. IEEE Int. Conf. on Comp., Sys. and Signal Process., pp. 175–179, Bangalore, India (1984).

2. M. Tomamichel, Ch. Ci Wen Lim, N. Gisin, and R. Renner, Nature Commun. **3**, 1 (2012).

3. A. N. Klimov, K. A. Balygin, and S. N. Molotkov, Laser Phys. Lett. **15**, 075207 (2018).

4. S. N. Molotkov, JETP **106**, 1 (2008).

5. S. N. Molotkov, JETP Lett. **102**, 473 (2015).

6. С. Н. Молотков, ЖЭТФ **153**, 895 (2018).

7. M. Tomamichel and R. Renner, Phys. Rev. Lett. **106**, 110506 (2011).

8. M. Tomamichel, PhD thesis, ETH Zürich, arXiv/quant-ph:1203.2142 (2012).

9. R. Renner, PhD thesis, ETH Zürich, arXiv/quant-ph: 0512258 (2005).

10. P. Shor and J. Preskill, Phys. Rev. Lett. **85**, 441 (2000).

11. T. M. Cover and J. A. Thomas, *Elements of Information Theory*, Wiley (1991).