ЖЭТФ, 2012, том 142, вып. 6 (12), стр. 1108–1126

ЭНТРОПИЙНЫЕ СООТНОШЕНИЯ НЕОПРЕДЕЛЕННОСТЕЙ И СТОЙКОСТЬ ФАЗОВО-ВРЕМЕННО́Й КВАНТОВОЙ КРИПТОГРАФИИ ПРИ КОНЕЧНЫХ ДЛИНАХ ПЕРЕДАВАЕМЫХ ПОСЛЕДОВАТЕЛЬНОСТЕЙ

С. Н. Молотков *

Академия криптографии Российской Федерации
121552, Москва, Россия

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

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

Поступила в редакцию 22 мая 2012 г.

Любой сеанс генерации ключей содержит конечное число посылок квантовых состояний, поэтому практически важно понимать принципиальные ограничения на минимальную длину последовательности, необходимую для получения секретного ключа заданной длины. Энтропийные соотношения неопределенностей для сглаженных min- и max-энтропий позволяют существенно упростить и сократить доказательство секретности. Приведено доказательство секретности для квантового распределения ключей с фазово-временны́м кодированием. Данный протокол обеспечивает максимальную, по сравнению с другими протоколами, критическую ошибку, до которой гарантируется секретное распределение ключей. Кроме того, в отличие от других базовых протоколов (типа BB84), которые уязвимы по отношению к атаке с «ослеплением» лавинных фотодетекторов, данный протокол устойчив по отношению к такой атаке и гарантирует секретность ключей.

1. ВВЕДЕНИЕ

Секретность ключей в квантовой криптографии гарантируется фундаментальными запретами квантовой механики на копирование [1] и на различимость квантовых состояний [2]. Некоммутативность пары наблюдаемых (эрмитовых операторов) R и L гарантирует невозможность существования общей системы собственных векторов этих операторов. Отсутствие общей системы собственных векторов приводит к фундаментальным соотношениям неопределенностей Гейзенберга [3]. Последние фактически означают невозможность выбора общего базиса измерений, при котором с достоверностью (вероятностью единица) можно различать некоммутирующие наблюдаемые.

В квантовой криптографии в качестве таких наблюдаемых выступают матрицы плотности — положительные эрмитовы операторы со следом единица, отвечающие, как правило, чистым информационным квантовым состояниям.

Основным параметром любого протокола квантовой криптографии является критическая ошибка Q_c, до которой гарантируется секретное распределение ключей. Критическая ошибка всех известных протоколов квантового распределения ключей не превышает 20 % [4]. Чем больше критическая ошибка, тем более устойчивым является протокол по отношению к шумам аппаратуры и действиям подслушивателя. Напомним, что ошибки на приемной стороне, возникающие от действий подслушивателя и шумов аппаратуры, принципиально невозможно различить. Поэтому все ошибки списываются на действия подслушивателя.

Протокол квантового распределения ключей BB84 [5] является базовым. Существует несколько

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

доказательств секретности протокола BB84. Первое полное и достаточно сложное доказательство стойкости BB84 представлено в работе [6].

Доказательство, приведенное в работе [7], является идейно достаточно простым, однако в нем предполагается использование квантовой памяти на приемной стороне, что неприемлемо в реальной ситуации. Простое доказательство стойкости протокола BB84 с использованием квантовых кодов и в асимптотическом пределе бесконечно длинных передаваемых последовательностей было дано в работе [8]. Важный шаг был сделан в работе [9], где было предложено использовать соотношения неопределенностей для доказательства секретности. Далее идея использования энтропийных соотношений неопределенности совместно со сглаженными квантовыми энтропиями Реньи была доведена до логического завершения в работах [10, 11]. Решающий вклад в развитие математического аппарата для квантовой теории информации с применением сглаженных квантовых энтропий был сделан в работах Реннера [12]. Совместное использование сглаженных энтропий и энтропийных соотношений неопределенности позволило упростить доказательство секретности протокола BB84 и сделать его более прозрачным [11].

Целью данной работы является доказательство секретности протокола квантового фазово-временно́го распределения ключей, предложенного в работе [12] (см. также [13, 14]) для конечных длин передаваемых последовательностей, основанное на фундаментальных энтропийных соотношениях неопределенностей [10]. В данном протоколе секретное распределение ключей возможно вплоть до критической ошибки $Q_c \to 50\,\%$. Данная величина критической ошибки является теоретическим пределом, который не может быть улучшен[1)].

Предельная допустимая ошибка для классического бинарного канала связи без памяти, до которой можно безошибочно передавать информацию в асимптотическом пределе длинных последовательностей, $Q \to 50\,\%$ [13, 14]. Неформально это означает, что при любой ошибке $Q < 50\,\%$, любых сколь угодно малых δ, ε ($\delta, \varepsilon \to 0$) и при $n > n(\delta, \varepsilon)$ найдется набор кодовых слов размером $N = 2^{n(C(Q)+\delta)}$, такой что максимальная ошибка декодирования (различения кодовых слов) не превысит $p_{err}(N, \delta) < \varepsilon$. Предельное количество информации в битах в пересчете на одну позицию, которое может быть передано через канал с шумом, ограничено пропускной способностью канала связи [17, 18]:

$$C(Q) = \lim_{\varepsilon \to 0} \lim_{n \to \infty} \frac{k}{n}, \tag{1}$$

где k — число позиций, несущих полезную информацию (соответственно доля контрольных символов в последовательности есть $n - k$). Пропускная способность (1) выражается через взаимную информацию

$$\begin{aligned} C(Q) &= \max_{\{p_X(x)\}} I(X;Y) = \\ &= \max_{\{p_X(x)\}} (H(X) - H(X|Y)) = 1 - h(Q). \end{aligned} \tag{2}$$

Максимум в (2) берется по распределениям вероятности на символах входного алфавита $X = \{0, 1\}$; $Y = \{0, 1\}$ — выходной алфавит,

$$\begin{aligned} H(X) &= -\sum_x p_X(x) \log_2 p_X(x), \\ H(X|Y) &= -\sum_x p_X(x) \times \\ &\times \sum_y p_{X|Y}(x|y) \log_2 p_{X|Y}(x|y), \end{aligned} \tag{3}$$

$$h(Q) = -Q \log_2 Q - (1 - Q) \log_2 (1 - Q).$$

Максимум в (2) достигается на равномерном распределении, при этом $H(X) = 1$. Условная энтропия $H(X|Y) = h(Q)$ — количество информации в битах, минимально необходимое для исправления ошибок. При $Q \to 50\,\%$ пропускная способность $C(Q) \to 0$, это означает, что вся переданная последовательность расходуется на исправление ошибок.

В квантовой криптографии после передачи квантовых состояний Алисой (передающая сторона) и измерений на приемной стороне Бобом легитимные пользователи имеют битовые последовательности X и Y. Последовательность Боба содержит ошибки с вероятностью Q. Для их исправления используется открытый аутентичный классический канал связи, через который для исправления ошибок требуется передать $h(Q)$ битов информации на одну позицию. Данная информация доступна подслушивателю — Еве. Кроме этого, Ева имеет еще информацию о ключе, которую она получила из квантового канала связи при передаче квантовых состояний от Алисы к Бобу. Собственно вторжение Евы в канал связи и приводит к ошибке Q на приемной стороне.

[1)] Протокол квантового распределения ключей с фазово-временны́м кодированием интересен также и тем, что в отличие от волоконных реализаций протокола BB84, которые уязвимы (не гарантируют секретность ключей) по отношению к атаке с «ослеплением» лавинных детекторов [15], является устойчивым по отношению к такой атаке и гарантирует секретность ключей [16].

Поскольку при $Q \to 50\,\%$ вся последовательность тратится на исправление ошибок, заведомо нельзя получить секретный ключ при вероятности ошибки, меньшей 50 %. Поэтому на первый взгляд кажется очевидным, что не может существовать протоколов квантового распределения ключей, которые бы гарантировали секретную передачу ключей при $Q \to 50\,\%$. Однако это не так. Ниже приведен такой протокол, дано простое доказательство его секретности на основе фундаментальных энтропийных соотношений неопределенностей, а также выявлена причина достижения теоретического предела по критической ошибке $Q_c \to 50\,\%$.

Для протокола BB84 [6–11] длина секретного ключа r в асимптотическом пределе бесконечно длинных последовательностей равна

$$r = 1 - 2h(Q). \tag{4}$$

Коррекция ошибок требует передачи по открытому каналу $h(Q)$ битов информации, которая доступна Еве. Кроме того, для протокола BB84 информация, которую получает Ева из квантового канала, равна $h(Q)$ битов. Информация на одну позицию после исправления ошибок составляет 1 бит, поэтому при $1 = 2h(Q_c)$ ($Q_c \approx 11\,\%$) длина секретного ключа обращается в нуль.

Для однопараметрических протоколов квантового распределения ключей, в которых длина секретного ключа зависит только от одного параметра — вероятности ошибки Q, достижение теоретического предела по ошибке $Q_c \to 50\,\%$ оказывается принципиально невозможным.

Для двухпараметрических протоколов, где длина секретного ключа зависит от двух параметров, достижение этого предела оказывается возможным. Для протокола квантового фазово-временно́го распределения ключей длина секретного ключа в асимптотическом пределе бесконечно длинных последовательностей равна [13, 14]

$$r = 1 - h(\delta) - (1 - \delta)h(Q), \tag{5}$$

где δ — вероятность отсчетов в контрольных временны́х окнах [13, 14]. При «движении» в плоскости параметров (Q, δ) (см. ниже) вдоль линии $\delta \approx 0$ критическая ошибка протокола $Q \to 50\,\%$, т. е. стремится к теоретическому пределу.

2. ЭНТРОПИЙНЫЕ СООТНОШЕНИЯ НЕОПРЕДЕЛЕННОСТЕЙ

Соотношения неопределенностей были введены Гейзенбергом [3] для канонически-сопряженных наблюдаемых x и p. Для произвольных наблюдаемых R и L они введены Робертсоном [19] и имеют вид

$$(\Delta R)_{|\psi\rangle}(\Delta L)_{|\psi\rangle} \geq \frac{1}{2}|\langle\psi|\ [R, L]|\psi\rangle|, \qquad [R, L] = R \cdot L - L \cdot R, \tag{6}$$

где $|\psi\rangle \in \mathcal{H}$ — вектор состояния квантовой системы, $\mathcal{H}$ — пространство состояний квантовой системы,

$$(\Delta R)^2_{|\psi\rangle} = \langle\psi|R^2|\psi\rangle - (\langle\psi|R|\psi\rangle)^2$$

и аналогично для $(\Delta L)^2_{|\psi\rangle}$. Эрмитовы операторы R и L имеют спектральные разложения:

$$R = \sum_i^{n_R} r_i |r_i\rangle\langle r_i|, \quad L = \sum_j^{n_L} l_j |l_j\rangle\langle l_j|. \tag{7}$$

Измерение наблюдаемых порождает распределение вероятностей на пространстве исходов, нумеруемых индексами i и j:

$$P_{R,\psi} = \{p_R(r_i)\}_{R,\psi} = \{|\langle r_i|\psi\rangle|^2\}_{R,\psi},$$
$$P_{L,\psi} = \{p_L(l_j)\}_{L,\psi} = \{|\langle l_j|\psi\rangle|^2\}_{L,\psi}.$$

Соотношения в форме (6) непригодны для использования в задачах квантовой криптографии, поскольку не имеют теоретико-информационной интерпретации. Кроме того, данные соотношения неоднократно подвергались вполне обоснованной критике [20]. Правая часть (6) зависит не только от наблюдаемых, но и от состояния квантовой системы $|\psi\rangle$, и поэтому не является нижней границей. Например, если в качестве $|\psi\rangle$ взять один из собственных векторов R (или L), то правая часть неравенства (6) будет равна нулю.

Энтропийные соотношения неопределенностей введены в работе [21] и в дальнейшем уточнены во многих работах [20–24]. Энтропийные соотношения неопределенностей не обладают отмеченными выше недостатками и имеют прозрачную теоретико-информационную интерпретацию.

2.1. Энтропийные соотношения неопределенностей для отдельной квантовой системы

Пусть квантовая система находится в состоянии $|\psi\rangle$ и пара наблюдаемых имеет вид (7). Энтропийные соотношения неопределенностей [21] выглядят следующим образом:

$$H(P_{R,\psi}) + H(P_{L,\psi}) \geq -2\log_2 c, \qquad c = \max_{i,j} |\langle r_i|l_j\rangle|, \tag{8}$$

где

$$H(x) = -x\log_2 x - (1-x)\log_2(1-x)$$

— энтропийная функция. Далее логарифмы берутся по основанию 2. Правая часть неравенства (8), определяющая нижнюю границу, не зависит теперь от квантового состояния, а определяется только самими наблюдаемыми R и L, точнее, максимальным перекрытием их собственных векторов.

В таком виде соотношения неопределенностей имеют простую теоретико-информационную интерпретацию и напрямую связаны с теоремой Шеннона для кодирования дискретного источника без памяти [17,18]. Собственные числа операторов можно рассматривать как алфавиты $\{r_1, r_2, \ldots, r_{n_R}\}$ и $\{l_1, l_2, \ldots, l_{n_L}\}$. При n-кратном измерении наблюдаемой R (или L) каждый раз над одинаково приготовленным состоянием $|\psi\rangle$ порождаются последовательности $\{r\}^n = \{r_{i_1}, r_{i_2}, \ldots, r_{i_n}\}$ ($\{l\}^n = \{l_{i_1}, l_{i_2}, \ldots, l_{i_n}\}$) с соответствующими вероятностями $P^n_{R\psi} = p_R(r_{i_1})p_R(r_{i_2})\ldots p_R(r_{i_n})$ ($P^n_{L\psi} = p_L(l_{i_1})p_L(l_{i_2})\ldots p_L(l_{i_n})$). Как известно [25], число типичных последовательностей, которые встречаются с вероятностью, стремящейся к единице, в асимптотическом пределе длинных последовательностей в случае измерения наблюдаемой R приблизительно равно $2^{nH(P_{R,\psi})}$. Соответственно, при измерении наблюдаемой L оно приблизительно равно $2^{nH(P_{L,\psi})}$. Минимальное количество битов информации, необходимое для нумерации всех типичных последовательностей, приблизительно равно соответственно $nH(P_{R,\psi})$ и $nH(P_{L,\psi})$. Энтропийные соотношения неопределенностей (8) гласят, что суммарное число битов информации при n-кратном измерении пары наблюдаемых на любом квантовом состоянии $|\psi\rangle$ не может быть меньше, чем правая часть неравенства (8), которая дает минимально необходимое количество битов информации для описания n исходов измерений наблюдаемых R и L.

2.2. Энтропийные соотношения неопределенностей для составных квантовых систем

Энтропийные соотношения неопределенностей в форме (8) для отдельной системы все еще непригодны для задач квантовой криптографии. В квантовой криптографии приходится иметь дело с составными квантовыми системами, состоящими из трех подсистем, относящихся к двум легитимным пользователям — Алисе и Бобу и подслушивателю — Еве. Состояние составной квантовой системы описывается матрицей плотности ρ_{ABE}, действующей в тензорном произведении пространств состояний $\mathcal{H}_A \otimes \mathcal{H}_B \otimes \mathcal{H}_E$.

Пусть над подсистемой A проводится одно из двух измерений. Любое измерение в квантовой механике описывается разложением единицы в $\mathcal{H}_A$. Для нашего случая имеем

$$I_A = \sum_x M_x, \quad I_A = \sum_x N_z, \tag{9}$$

каждому элементарному исходу x или z в каждом измерении сопоставляется положительная операторнозначная мера (positive operator valued measure, POVM) M_x или N_z. Вероятности исходов x или z соответственно равны

$$\begin{aligned} p_X(x) &= \mathrm{Tr}_{ABE}\{M_x\rho_{ABE}\},\\ p_Z(z) &= \mathrm{Tr}_{ABE}\{N_z\rho_{ABE}\}. \end{aligned} \tag{10}$$

Для дальнейшего будет удобно записывать результат измерений над подсистемой A в классический регистр, что эквивалентно записи результата в базис ортонормированных квантовых состояний $\{|x\rangle_A\}$ и $\{|z\rangle_A\}$, имеем

$$\begin{aligned} \rho_{XBE} &= \sum_x |x\rangle_{AA}\langle x| \otimes \rho^x_{BE},\\ \rho_{ZBE} &= \sum_z |z\rangle_{AA}\langle z| \otimes \rho^z_{BE}, \end{aligned} \tag{11}$$

$$\rho^x_{BE} = \mathrm{Tr}_A\{\sqrt{M_x}\rho_{ABE}\sqrt{M_x}\},$$

$$\rho^z_{BE} = \mathrm{Tr}_A\{\sqrt{N_z}\rho_{ABE}\sqrt{N_z}\}.$$

Энтропийные соотношения неопределенностей для трехсоставных систем принимают в этом случае вид [26]

$$\begin{aligned} H(X|B) + H(Z|E) &\geq -2\log c,\\ c = \max_{x,z} ||\sqrt{M_x}\sqrt{N_Z}||_\infty &= \\ = \max_{x,z} \mathrm{Tr}_A\{\sqrt{M_x}\sqrt{N_Z}\}&, \end{aligned} \tag{12}$$

где $H(\rho) = -\mathrm{Tr}\{\rho\log\rho\}$ — энтропия фон Неймана и условные энтропии равны

$$\begin{aligned} H(X|B) &= H(\rho_{XB}) - H(\rho_B),\\ H(Z|E) &= H(\rho_{ZE}) - H(\rho_E), \end{aligned} \tag{13}$$

$$\rho_{XB} = \mathrm{Tr}_E\{\rho_{XBE}\}, \quad \rho_B = \mathrm{Tr}_{XE}\{\rho_{XBE}\}. \tag{14}$$

Аналогично записываются выражения для ρ_{ZBE}.

2.3. Энтропийные соотношения неопределенностей для сглаженных квантовых min- и max-энтропий Реньи

Соотношения неопределенностей (8) и (12) неявно подразумевают, что матрица плотности системы известна точно. Однако в задачах квантовой криптографии такая ситуация имеет место только в асимптотическом пределе бесконечно длинных передаваемых последовательностей. В реальной ситуации, когда длина передаваемой последовательности конечна и матрица плотности оценивается путем раскрытия части конечной последовательности измерений, невозможно точно узнать матрицу плотности на приемной стороне. Можно лишь с конечной точностью, зависящей от длины последовательности, утверждать, что оценка матрицы плотности квантового состояния, полученная по конечной наблюдаемой статистике отсчетов, близка в определенном смысле (метрике) к истинной матрице плотности, которая дает данную наблюдаемую статистику измерений на приемной стороне. Поэтому соотношения неопределенностей (8) и (12) требуют обобщения на такой случай.

Оказывается, что удобными величинами являются квантовые аналоги энтропии Реньи для классических распределений вероятности нулевого (max) и бесконечного (min) порядков, которые по определению равны (см. подробности в работе [27])

$$H_{min}(A|B) = -\sup_{\sigma_B} \log \lambda, \tag{15}$$

где λ — минимальное число, при котором оператор $\lambda I_A \otimes \sigma_B - \rho_{AB} > 0$. Здесь σ_B и ρ_{AB} — матрицы плотности, действующие в $\mathcal{H}_B$ и $\mathcal{H}_A \otimes \mathcal{H}_B$, I_A — единичный оператор в $\mathcal{H}_A$. Соответственно, по определению [27] имеем

$$H_{max}(A|B) = \sup_{\sigma_B} \log(\mathrm{Tr}\{\rho^0_{AB}(I_A \otimes \sigma_B)\}), \tag{16}$$

где $\rho^0_{AB} = \mathrm{supp}(\rho_{AB})$ — носитель матрицы плотности ρ_{AB}.

Для определения сглаженных энтропий необходимо ввести меру близости матриц плотности. Удобной мерой близости между парой матриц плотности является следовое расстояние [27], которое по определению равно

$$d_1(\rho,\overline{\rho}) = \frac{1}{2}||\rho - \overline{\rho}||_1 = \frac{1}{2}\mathrm{Tr}\{|\rho - \overline{\rho}|\} = \\ = \frac{1}{2}\mathrm{Tr}\{\sqrt{(\rho - \overline{\rho})^2}\}. \tag{17}$$

Одной из главных причин выбора следового расстояния в задачах квантовой информатики является то, что квантовая операция (супероператор — линейное отображение, сохраняющее эрмитовость, след и являющееся вполне положительным (completely positive map, CPM)) не увеличивает расстояние между операторами. Любые допустимые законами квантовой механики преобразования матриц плотности описываются некоторым супероператором. Применительно к задачам квантовой криптографии это означает, что если исходное расстояние между точной матрицей плотности ρ и ее оценкой $\overline{\rho}$ не превосходило некоторой величины, то по мере выполнения шагов протокола можно гарантировать, что оно не будет увеличиваться (см. [27]). В квантовой криптографии исходное расстояние определяется на стадии оценки параметров (например, оценки величины ошибки на приемной стороне) путем раскрытия части переданной последовательности.

Для дальнейшего нам потребуется еще одна величина — соответствие (fidelity), — описывающая меру близости между матрицами плотности:

$$F(\rho,\overline{\rho}) = \mathrm{Tr}\{|\sqrt{\rho}\sqrt{\overline{\rho}}|\}, \tag{18}$$

причем имеют место соотношения (см., например, [28])

$$1 - F(\rho,\overline{\rho}) \le d_1(\rho,\overline{\rho}) \le \sqrt{1 - F^2(\rho,\overline{\rho})}. \tag{19}$$

По определению [27] сглаженные квантовые min- и max-энтропии равны

$$H^{\varepsilon}_{min}(A|B) = \sup_{\overline{\rho}_{AB} \in \mathcal{B}^{\varepsilon}(\rho_{AB})} H_{min}(A|B)_{\overline{\rho}_{AB}}, \\ H^{\varepsilon}_{max}(A|B) = \inf_{\overline{\rho}_{AB} \in \mathcal{B}^{\varepsilon}(\rho_{AB})} H_{max}(A|B)_{\overline{\rho}_{AB}}, \tag{20}$$

где точные верхняя и нижняя грани берутся по всем матрицам плотности $\overline{\rho}_{AB}$, находящимся в шаре $\mathcal{B}^{\varepsilon}(\rho_{AB})$ радиуса ε с центром в точке ρ_{AB},

$$\mathcal{B}^{\varepsilon}(\rho_{AB}) = \{\overline{\rho}_{AB} : ||\rho_{AB} - \overline{\rho}_{AB}||_1 \le \mathrm{Tr}\{\overline{\rho}_{AB}\}\varepsilon\}.$$

Согласно [29], энтропийные соотношения неопределенностей для сглаженных min- и max-энтропий имеют вид

$$H^{\varepsilon}_{max}(X|B) + H^{\varepsilon}_{min}(Z|E) \ge -2\log c. \tag{21}$$

Для конечномерных пространств состояний и компактных операторов можно в (20) заменить sup и inf на max и min. Матрица плотности $\overline{\rho}_{AB}$ является, вообще говоря, квазинормированной.

Сглаженные квантовые min- и max-энтропии имеют теоретико-информационную интерпретацию [30]. Пусть матрица плотности ρ_{XE} (типа (11), (14))

описывает корреляцию классической битовой строки X с квантовой системой E. Тогда $H^{\varepsilon}_{min}(X|E)$ дает максимальную длину битовой строки $l^{\varepsilon}_{extr}(X|E)$, которая ε-близка в следовой метрике к однородно распределенной битовой строке и не зависит от побочной информации, скрытой в квантовой системе,

$$l^{\varepsilon}_{extr}(X|E) = H^{\varepsilon}_{min}(X|E) + O\left(\log\frac{1}{\varepsilon}\right). \qquad (22)$$

Новая сжатая однородно распределенная битовая строка меньшей длины теперь не коррелирована с квантовой системой E. Сжатие происходит при помощи универсальных хэш-функций второго порядка, введенных в работах [31, 32]. Такое сжатие носит название усиления секретности (privacy amplification) [33].

Поскольку $H^{\varepsilon}_{min}(X|E)$ монотонно растущая функция ε, длина однородно распределенной и независимой от E битовой строки не менее [33] следующего значения:

$$l^{\varepsilon}_{extr}(X|E) \geq H_{min}(X|E) + O\left(\log\frac{1}{\varepsilon}\right), \qquad (23)$$

где $H(X|E)_{min}$ — сглаженная энтропия при $\varepsilon = 0$.

$H^{\varepsilon}_{max}(X|B)$ связана со сжатием классической случайной переменной X до размера $l^{\varepsilon}_{enc}(X|E)$ битов так, чтобы по ней (имея классическую информацию длиной $l^{\varepsilon}_{enc}(X|E)$ битов) можно было восстановить исходную битовую строку с вероятностью не хуже $1-\varepsilon$ при условии, что декодер имеет доступ к квантовой системе B.

Если система B является классической случайной переменной Y, то max-энтропия определяет количество битов информации, необходимое для восстановления величины X при доступе декодера к случайной величине Y. Величина сжатия не более [34] следующего значения:

$$l^{\varepsilon}_{enc}(X|B) \leq H^{\varepsilon}_{max}(X|B) + O\left(\log\frac{1}{\varepsilon}\right). \qquad (24)$$

Другими словами, в асимптотическом пределе бесконечно длинных последовательностей при $\varepsilon = 0$ минимально необходимое количество битов дополнительной информации для коррекции ошибок (восстановлении случайной величины X по случайной величине Y) с вероятностью положительного исхода не хуже $1-\varepsilon$ равно $l_{enc} = H_{max}(X|Y)$.

3. КРИТЕРИИ КОРРЕКТНОСТИ ПРОТОКОЛА И СЕКРЕТНОСТИ КЛЮЧЕЙ

К протоколу квантового распределения ключей предъявляются, по сути, два требования — корректности и секретности (см. детали в [27]). В конце протокола Алиса и Боб имеют битовые строки x и $\hat{x}$.

Протокол считается ε_{EC}-корректным, если вероятность того, что ключи на приемной и передающей сторонах различаются с вероятностью, не превышающей

$$\Pr[\hat{x} \neq x] \leq \varepsilon_{EC}. \qquad (25)$$

Протокол считается Δ-секретным, если

$$\min_{\sigma_E}\frac{1}{2}||\rho_{XE} - \rho_U \otimes \sigma_B||_1 \leq \Delta, \qquad (26)$$

где

$$\rho_U = \frac{1}{|X|}\sum_x |x\rangle\langle x|$$

— матрица плотности, описывающая однородное распределение ключей у легитимного пользователя. При $\Delta = 0$ корреляции между ключами легитимных пользователей и квантовой системой подслушивателя полностью отсутствуют — это является идеальной ситуацией.

Связь расстояния до идеальной ситуации (полное отсутствие корреляции между битовой строкой легитимных пользователей и строкой подслушивателя) и min-энтропией после сжатия очищенной битовой строки X (хэшировании универсальными хэш-функциями второго порядка [31, 32]) дается следующей замечательной теоремой (так называемая leftover hash теорема [34]).

Пусть $H^{\varepsilon'}_{max}(X|EC)$ — max-энтропия после коррекции ошибок. Индекс C учитывает дополнительную информацию подслушивателя, которую он получает из открытого классического канала при коррекции ошибок. Тогда после сжатия до длины l_{secr} (l_{secr} — длина секретного ключа) расстояние до идеальной ситуации равно (см. детали вывода в [27])

$$\Delta = \min_{\varepsilon'}\frac{1}{2}\sqrt{2^{l_{secr} - H^{\varepsilon'}_{min}(X|EC)}} + \varepsilon'. \qquad (27)$$

Учитывая, что

$$H^{\varepsilon'}_{min}(X|EC) \geq H^{\varepsilon'}_{min}(X|E) - \mathrm{leak}_{EC}, \qquad (28)$$

где leak_{EC} — утечка информации в битах при коррекции ошибок (см. ниже), находим, что

$$\Delta \leq \varepsilon' + \frac{1}{2}\sqrt{2^{l_{secr} - H^{\varepsilon'}_{min}(X|EC)}} \leq \varepsilon' + \overline{\varepsilon}. \qquad (29)$$

Протокол $\Delta = \varepsilon' + \overline{\varepsilon}$ секретен, если длина l_{secr} секретного ключа не превышает [11, 27] следующего значения:

$$l_{secr} \le H_{min}^{\varepsilon'}(X|E) - 2\log\frac{1}{2\overline{\varepsilon}} - \mathrm{leak}_{EC}. \qquad (30)$$

Выбирая параметры $\varepsilon', \overline{\varepsilon}$ сколь угодно малыми и соответственно длину сжатого финального секретного ключа, всегда можно приблизиться сколь угодно близко к идеальной ситуации — отсутствию полной корреляции между ключами Алисы, Боба и ключом Евы. Конечно, это возможно при условии, что ошибка на приемной стороне меньше некоторой критической для данного протокола. При ошибке, большей критической, длина секретного ключа будет равна нулю.

4. КОРРЕКЦИЯ ОШИБОК

После передачи квантовых состояний и измерений на приемной стороне происходит коррекция ошибок. Удобно рассматривать процедуру исправления ошибок как результат хэширования. Такой подход был предложен в работе [35], а применительно к задачам квантовой криптографии — в [27], последнему подходу будем следовать ниже.

Измерения, как и любые преобразования квантовых состояний, описываются супероператором. После измерений Бобом матрица плотности ρ_{XBE} переходит в матрицу

$$\rho_{XYE} = \sum_{x,y} |x\rangle\langle x| \otimes |y\rangle\langle y| \otimes \rho_E^{xy}, \qquad (31)$$

где $Y = \{0,1\}^N$ — алфавит Боба (отметим, что алфавит не обязательно бинарный, см. ниже). Данная матрица плотности порождает совместное распределение вероятностей результатов измерений Алисы и Боба

$$\begin{gathered} \mathrm{Tr}_E\{\rho_{XYE}\} \to \rho_{XY} = \\ = \sum_{x,y} P_{XY}(x,y)|x\rangle\langle x| \otimes |y\rangle\langle y|, \\ P_{XY}(x,y) = \mathrm{Tr}_E\{\rho_E^{xy}\}. \end{gathered} \qquad (32)$$

Цель процедуры коррекции ошибок сводится к тому, чтобы Боб, имея случайную переменную (в частности, например, битовую строку) y, а также получив дополнительную информацию от Алисы — хэш-значение $f(x)$, получил новую строку $\hat{x}$, такую что вероятность ошибки декодирования не превышала ε_{EC},

$$\Pr[\hat{x} \ne x] < \varepsilon_{EC}, \qquad (33)$$

строка $\hat{x}$ является очищенным ключом Боба. В этом случае процедура исправления ошибки называется ε_{EC}-корректной.

Процедура исправления ошибок также использует универсальные хэш-функции второго порядка и сводится к следующему (см. подробности в [27]). Алиса, имея битовую строку x, вычисляет хэш-значение $z = f(x)$. При этом хэш-функции выбираются открыто (Ева знает выбор хэш-функции), случайно и равновероятно из множества хэш-функций $f \in \mathcal{F} : X = \{0,1\}^N \to Z = \{0,1\}^k$. Алиса сообщает через открытый канал Бобу $(f, f(x))$. Поскольку выбор хэш-функции является открытым, число битов дополнительной информации, доступное Еве, есть число битов для сообщения хэш-значения $f(x)$, т. е. k битов.

Утечка информации leak_{EC} равна k битам дополнительной информации, которые становятся доступными Еве в процессе исправления ошибок. Оказывается, что утечка информации ограничена величиной (см. детали в [27])

$$k = \mathrm{leak}_{EC} \le H_{max}(P_{XY}|Y) + \log\frac{2}{\varepsilon_{EC}}, \qquad (34)$$

где под логарифмом множитель 2 добавляется из-за коэффициента $1/2$ в определении следового расстояния и расстояния в шаре. Max-энтропия вычисляется по распределению (32) и равна по определению (16) (см. детали в [27])

$$H_{max}(P_{XY}|Y) = \log\max_{y\in Y}|\mathrm{supp}(P_X^y)|, \qquad (35)$$

где $\hat{\mathcal{X}}_y = \mathrm{supp}(P_X^y)$ представляет множество значений y, в которые могут перейти различные x. Соответственно, $|\mathrm{supp}(P_X^y)|$ — это наибольшее число элементов по y при всех x. Другими словами, величина $|\mathrm{supp}(P_X^y)|$ определяет качество канала связи между Алисой и Бобом с учетом действий Евы. Чем больше $|\mathrm{supp}(P_X^y)|$, тем хуже канал, так как x может «размазаться» на бóльшее число элементов y. При идеальном канале каждое $x \to y = x$, $|\mathrm{supp}(P_X^y)| = 1$. При этом утечка равна нулю, ошибок нет и их не нужно исправлять.

Цель Боба при коррекции ошибок сводится к следующему: имея хэш-значение $z = f(x)$ от Алисы, найти такое $\hat{x}_y \in \hat{\mathcal{X}}_y = \mathrm{supp}(P_X^y)$, у которого $f(\hat{x}_y) = f(x)$. Хотя фактически такая процедура сводится к перебору и поэтому экспоненциально сложна, но пока это не важно. Зато такая процедура коррекции ошибок дает минимальную утечку информации (по существу, этот факт отражают неравенства (37) и (43) ниже).

Корректность протокола определяется вероятностью правильного декодирования $\Pr[x = \hat{x}] > 1 - \varepsilon_{EC}$. Ошибка при декодировании, соответственно, определяется вероятностью того, что такое $\hat{x}_y \in \hat{\mathcal{X}}_y = \mathrm{supp}(P_X^y)$, не равное x, существует, но при нем хэш-значения $f(\hat{x}) = f(x)$ совпадают. Имеем (см. также [27])

$$\begin{aligned}&\Pr\,[x \neq \hat{x}] \leq \Pr_f[\exists x \in \hat{\mathcal{X}}_y = \mathrm{supp}(P_X^y),\\ &\hat{x} \neq x \wedge f(\hat{x}) = f(x)] \leq |\mathrm{supp}(P_X^y)|2^{-k},\end{aligned} \tag{36}$$

поскольку вероятность совпадения хэш-значений универсальных хэш-функций второго порядка есть [31]

$$\Pr_f[f(\hat{x}) = f(x)] \leq \frac{1}{|Z|} = 2^{-k}, \quad \hat{x} \neq x. \tag{37}$$

Из (35) видно, что

$$\max_y |\mathrm{supp}(P_X^y)| = 2^{H_{max}(P_{XY}|Y)},$$

поэтому получаем

$$\begin{aligned}&\Pr[\hat{x} \neq x] \leq\\ &\quad \leq 2^{H_{max}(P_{XY}|Y) - [H_{max}(P_{XY}|Y) + \log(1/\varepsilon_{EC})]} \leq\\ &\qquad \leq \varepsilon_{EC}.\end{aligned} \tag{38}$$

Матрица плотности ρ_{XY} в (32) и, соответственно, распределение $P_{XY}(x,y)$ точно неизвестны, но известно, что ее оценка $\overline{\rho}_{XY}$ заключена в шаре (данный вывод следует после стадии оценки параметров, см. ниже):

$$||P_{XY}(x,y) - \overline{P}_{XY}(x,y)||_1 \leq \varepsilon'. \tag{39}$$

Здесь $\overline{P}_{XY}(x,y)$ — распределение вероятностей аналогично (32).

Поскольку

$$\begin{aligned}&H^{\varepsilon'}(P_{XY}|Y) =\\ &\qquad = \min_{\overline{P}_{XY}(x,i) \in \mathcal{B}^{\varepsilon'}(P_{XY}(x,y))} H(\overline{P}_{XY}|Y),\end{aligned} \tag{40}$$

утечка информации для любого распределения $\overline{P}_{XY}(x,y)$, ε'-близкого к $P_{XY}(x,y)$, также не превышает следующего значения:

$$\mathrm{leak}_{EC} \leq H(\overline{P}_{XY}|Y) + \log\frac{2}{\varepsilon_{EC}}. \tag{41}$$

Таким образом, утечка информации

$$\mathrm{leak}_{EC} \leq H^{\varepsilon'}(P_{XY}|Y) + \log\frac{2}{\varepsilon_{EC}}. \tag{42}$$

Пусть $P_{C|X=x}$ — условная вероятность выбрать одно из классических сообщений (фактически равновероятно выбрать одну из хэш-функций $f \in F$ и соответствующее хэш-значение). Размер множества классических сообщений $|C| = |\mathcal{F} \times Z|$. Для дальнейшего удобно выразить утечку следующим образом (см. детали в [27]):

$$\begin{aligned}\mathrm{leak}_{EC} &= \log|C| - \inf_{x \in X} H_{min}(P_{C|X=x}) =\\ &= \log|\mathcal{F} \times Z| - \log|Z| \leq \log|Z| = k.\end{aligned} \tag{43}$$

5. УСИЛЕНИЕ СЕКРЕТНОСТИ ОЧИЩЕННЫХ КЛЮЧЕЙ

Для дальнейшего важно отметить, что для вычисления длины секретного ключа (см. (30)) необходимо знать сглаженную min-энтропию от квантовых состояний (операторов), которая определяется максимизацией по всем матрицам плотности в шаре. Очевидно, что решение такой задачи напрямую практически невозможно.

Энтропийные соотношения неопределенностей (21) позволяют выразить min-энтропию от операторов через max-энтропию (42) для классического совместного распределения вероятностей Алисы и Боба $P_{XY}(x,y)$ (точнее говоря, оценку энтропии для эмпирического распределения $\overline{P}_{XY}(x,y)$ после стадии оценки параметров), что является существенно более простой задачей.

Другими, словами энтропийные соотношения неопределенностей выполняют такую максимизацию в неявном виде.

Цель процедуры усиления секретности [33] состоит в том, чтобы хэшированием при помощи универсальных хэш-функций второго порядка [31] получить из очищенного при коррекции ошибок ключа, о котором Ева имеет частичную информацию (после вторжения в квантовый канал и получения информации через открытый канал при коррекции ошибок), новый более короткий ключ, о котором Ева уже не имеет никакой информации. Более точно, пусть исходное расстояние до идеальной ситуации есть

$$\Delta(X|E)_\rho = \frac{1}{2}\min_{\sigma_B} ||\rho_{XE} - \rho_U \otimes \sigma_B||_1, \tag{44}$$

где ρ_{XE} — матрица плотности до процедуры усиления секретности,

$$\rho_U = \frac{1}{|X|}\sum_x |x\rangle\langle x|, \quad \sigma_B = \mathrm{Tr}_E\{\rho_{XE}\},$$

$$\rho_E^X = \mathrm{Tr}\{\rho_{XE}\}.$$

Хэш-функция сама является случайной величиной и выбирается равновероятно и открыто (через открытый классический канал связи сообщается Алисой Бобу) из множества хэш-функций F, $f : X = \{0,1\}^N \to Z = \{0,1\}^l$. Данные функции обладают свойством (37).

Матрица плотности после хэширования, которую «видит» подслушиватель, становится равной

$$\rho_{FZE} = \sum_f \sum_z p_f |f\rangle\langle f| \otimes |z\rangle\langle z| \otimes \rho_E^{fz},$$
$$\rho_E^{fz} = \sum_{x:f(x)=z} \rho_E^X, \quad p_f = \frac{1}{|F|}. \tag{45}$$

Расстояние до идеальной ситуации после сжатия теперь удовлетворяет соотношению (см. детали в [27])

$$\frac{1}{2}||\rho_{ZFE} - \rho_{UZ} \otimes \overline{\sigma}_{FE}||_1 \le$$
$$\le \frac{1}{2}||\rho_{ZFE} - \overline{\rho}_{ZFE}||_1 + \frac{1}{2}||\overline{\rho}_{ZFE} - \rho_{UZ} \otimes \overline{\sigma}_{FE}||_1 \le$$
$$\le \varepsilon + \Delta(Z|FE)_{\overline{\rho}}, \tag{46}$$

где

$$\Delta(Z|FE)_\rho = \varepsilon + \frac{1}{2}\sqrt{2^{(l - H_{min}^\varepsilon(X|E)_\rho)}}. \tag{47}$$

Выбором степени сжатия (длины l) расстояние до идеальной ситуации может быть сделано сколь угодно малым.

Таким образом,

— матрица плотности $\overline{\rho}_{XE}$ неизвестна, но заключена в шаре;

— поскольку преобразование хэширования есть квантовая операция (CPM), которая не увеличивает следовое расстояние, матрица плотности $\overline{\rho}_{ZFE}$ заключена в шаре радиуса 2ε:

$$||\rho_{ZFE} - \overline{\rho}_{ZFE}||_1 \le ||\rho_{XE} - \overline{\rho}_{XE}||_1 \le 2\varepsilon; \tag{48}$$

— расстояние до идеальной ситуации после хэширования выражается через старую матрицу плотности до хэширования, которая входит в выражение для $H^\varepsilon(X|E)_\rho$.

6. ПРОТОКОЛ КВАНТОВОГО ФАЗОВО-ВРЕМЕННО́ГО РАСПРЕДЕЛЕНИЯ КЛЮЧЕЙ

В протоколе квантового распределения ключей с фазово-временны́м кодированием биты 0 и 1 кодируются как в относительную фазу, так и во временны́е сдвиги квантовых состояний [12–14]. Из всех известных протоколов квантового распределения ключей данный протокол имеет наибольшую критическую ошибку. При этом протокол имеет стандартную оптоволоконную реализацию (см. детали в работе [12]).

В протоколе используются два временны́х базиса — левый (L) и правый (R), — в каждом из которых имеется еще по два базиса — прямой (+) и сопряженный (×). Информационные квантовые состояния в левом базисе обозначим как

$$|\overline{0_L^+}\rangle = \frac{1}{\sqrt{2}}(|1\rangle + |2\rangle), \quad |\overline{1_L^+}\rangle = \frac{1}{\sqrt{2}}(|1\rangle - |2\rangle). \tag{49}$$

Состояния в сопряженном базисе получаются из состояний (49) поворотом:

$$|\overline{0_L^\times}\rangle = \frac{1}{\sqrt{2}}(|1\rangle + i|2\rangle), \quad |\overline{1_L^\times}\rangle = \frac{1}{\sqrt{2}}(|1\rangle - i|2\rangle).$$

Соответственно в правом базисе имеем

$$|\overline{0_R^+}\rangle = \frac{1}{\sqrt{2}}(|2\rangle + |3\rangle), \quad |\overline{1_R^+}\rangle = \frac{1}{\sqrt{2}}(|2\rangle - |3\rangle) \tag{50}$$

и для состояний в сопряженном правом базисе —

$$|\overline{0_R^\times}\rangle = \frac{1}{\sqrt{2}}(|2\rangle + i|3\rangle), \quad |\overline{1_R^\times}\rangle = \frac{1}{\sqrt{2}}(|2\rangle - i|3\rangle).$$

Здесь $|1\rangle$, $|2\rangle$ и $|3\rangle$ — ортонормированные базисные векторы. Данные базисные векторы отвечают локализованным во времени однофотонным состояниям, попарно сдвинутым во времени на определенную величину. Формально пространство состояний $\mathcal{H}$ является трехмерным. Состояния внутри одного базиса ортогональны аналогично протоколу BB84, а из разных базисов — попарно неортогональны.

Формально протокол выглядит следующим образом.

1. Алиса на передающей станции равновероятно выбирает один из двух временны́х базисов L или R. Затем случайно и равновероятно в выбранном временно́м базисе выбирает подбазис L^+ или $L^\times$, если был выбран временно́й базис L, соответственно — подбазис R^+ или $R^\times$, если был выбран временно́й базис R. И, наконец, случайно и равновероятно выбирает значение информационного бита 0 или 1 и соответствующее биту квантовое состояние в базисе L^+ ($L^\times$), аналогично в базисе R^+ ($R^\times$) и направляет на приемную станцию Бобу.

2. Боб независимо от Алисы случайно и равновероятно выбирает один из четырех базисов для изме-

рений, которые описываются следующими разложениями единицы I в $\mathcal{H}$:

$$I = |\overline{0_L^+}\rangle\langle\overline{0_L^+}| + |\overline{1_L^+}\rangle\langle\overline{1_L^+}| + |3\rangle\langle 3|, \quad \text{измерение в базисе } L^+, \tag{51}$$

$$I = |\overline{0_L^\times}\rangle\langle\overline{0_L^\times}| + |\overline{1_L^\times}\rangle\langle\overline{1_L^\times}| + |3\rangle\langle 3|, \quad \text{измерение в базисе } L^\times, \tag{52}$$

$$I = |1\rangle\langle 1| + |\overline{1_R^+}\rangle\langle\overline{1_R^+}| + |\overline{2_R^+}\rangle\langle\overline{2_R^+}|, \quad \text{измерение в базисе } R^+, \tag{53}$$

$$I = |1\rangle\langle 1| + |\overline{1_R^\times}\rangle\langle\overline{1_R^\times}| + |\overline{2_R^\times}\rangle\langle\overline{2_R^\times}|, \quad \text{измерение в базисе } R^\times. \tag{54}$$

3. Боб сообщает только сам факт получения состояния.

4. После проведения серии посылок Алисой и измерений Бобом Алиса раскрывает базисы, но не раскрывает сами состояния.

5. Боб открыто сообщает номера посылок, где базисы не совпадали. Данные посылки отбрасываются. Результаты измерений в тех посылках, в которых базисы совпадали, сохраняются. В результате измерений Боб получает 0, 1 или отсчет в контрольном временном слоте 3 (в базисе $L^{+,\times}$) или слоте 1 (в базисе $R^{+,\times}$). Номера посылок, где был отсчет в контрольном временно́м слоте через открытый классический канал, сообщаются Алисе.

6. Боб подсчитывает δ — процент отсчетов в контрольных временны́х слотах.

7. Оценивается процент ошибок в той части посылок, где у Боба был результат 0 или 1 путем раскрытия части посылок и сравнения. Далее эта часть отбрасывается.

8. Если наблюдаемая ошибка при данном числе отсчетов в контрольных временны́х слотах $Q(\delta) < Q_c(\delta)$, то протокол продолжается. В противном случае протокол прерывается.

Дальнейшие действия аналогичны другим протоколам. Происходит распределенная коррекция ошибок в оставшейся части, если вероятность ошибки не превышает критической величины. Затем проводится усиление секретности очищенного ключа.

Для того чтобы напрямую воспользоваться энтропийными соотношениями неопределенностей (21) при доказательстве секретности будем использовать версию протокола на запутанных состояниях (entangled version). Данная версия полностью формально эквивалентна версии протокола приготовление–посылка состояний, изложенной выше.

Алиса готовит случайно и равновероятно одно из максимально запутанных состояний, в правом R_A

$$|\Phi_R\rangle_{AB} = \frac{|\overline{0_R^+}\rangle_A \otimes |\overline{0_R^+}\rangle_B + |\overline{0_R^+}\rangle_A \otimes |\overline{0_R^+}\rangle_B}{\sqrt{2}} = \frac{|\overline{0_R^\times}\rangle_A \otimes |\overline{0_R^\times}\rangle_B + |\overline{0_R^\times}\rangle_A \otimes |\overline{0_R^\times}\rangle_B}{\sqrt{2}}, \tag{55}$$

или в левом L_A

$$|\Phi_L\rangle_{AB} = \frac{|\overline{0_L^+}\rangle_A \otimes |\overline{0_L^+}\rangle_B + |\overline{0_L^+}\rangle_A \otimes |\overline{0_L^+}\rangle_B}{\sqrt{2}} = \frac{|\overline{0_L^\times}\rangle_A \otimes |\overline{0_L^\times}\rangle_B + |\overline{0_L^\times}\rangle_A \otimes |\overline{0_L^\times}\rangle_B}{\sqrt{2}}, \tag{56}$$

базисах, где

$$|\overline{0}, \overline{1_R^+}\rangle_{A,B} = \frac{|1\rangle_{A,B} \pm |2\rangle_{A,B}}{\sqrt{2}}, \qquad |\overline{0}, \overline{1_R^\times}\rangle_{A,B} = \frac{|1\rangle_{A,B} \pm i|2\rangle_{A,B}}{\sqrt{2}}, \tag{57}$$

$$|\overline{0}, \overline{1_L^+}\rangle_{A,B} = \frac{|2\rangle_{A,B} \pm |3\rangle_{A,B}}{\sqrt{2}}, \qquad |\overline{0}, \overline{1_L^\times}\rangle_{A,B} = \frac{|2\rangle_{A,B} \pm i|3\rangle_{A,B}}{\sqrt{2}}. \tag{58}$$

Здесь $|1\rangle_{A,B}, |2\rangle_{A,B}, |3\rangle_{A,B}$ — однофотонные состояния (пакеты), локализованные во временны́х окнах соответственно $1, 2, 3$. После вторжения Евы состояния (55), (56) переходят в некоторые новые состояния $|\psi\rangle_{ABE}$, которые зависят от исходных. Поскольку соотношения неопределенностей (8) справедливы для любого состояния, индексы R, L у состояния $|\psi\rangle_{ABE}$ опускаем.

Для получения бита ключа 0 или 1 Алиса случайно и равновероятно проводит измерения над своей подсистемой в базисе собственных векторов одного из операторов R_A^+: $\{|\overline{0_R^+}\rangle_A, |\overline{1_R^+}\rangle_A\}$ или $R_A^\times$: $\{|\overline{0_R^\times}|\rangle_A, |\overline{1_R^\times}\rangle_A\}$, если было приготовлено состояние (55). Аналогично, если было приготовлено состояние в базисе L_B (56), то Алиса проводит измерения над своей подсистемой в базисе собственных векторов одного из операторов L_A^+: $\{|\overline{0_L^+}\rangle_A, |\overline{1_L^+}\rangle_A\}$ или $L_A^\times$: $\{|\overline{0_L^\times}|\rangle_A, |\overline{1_L^\times}\rangle_A\}$. Через открытый аутентичный канал связи Алиса сообщает Бобу выбор своего базиса. Боб проводит измерения в том же базисе, что и Алиса, соответственно для R_B — R_B^+:

$\{|\overline{0}_R^+\rangle_B, |\overline{1}_R^+\rangle_B, |3\rangle_B\}$ или $R_B^\times$: $\{|\overline{0}_R^\times|\rangle_B, |\overline{1}_R^\times\rangle_B, |3\rangle_B\}$. Аналогично в базисах $L_B - L_B^+$: $\{|1\rangle_B, |\overline{0}_L^+\rangle_B, |\overline{1}_L^+\rangle_B\}$ или $L_B^\times$: $\{|1\rangle_B, |\overline{0}_L^\times|\rangle_B, |\overline{1}_L^\times\rangle_B\}$. В отсутствие Евы имеет место полная корреляция исходов измерений у Алисы и Боба. Поскольку Ева не может достоверно различать состояния из базисов L_B и R_B, из-за перекрытия во временно́м окне 2, неизбежно возникнут ошибочные отсчеты в контрольных временны́х окнах 1 или 3. При наличии Евы пространство исходов измерений у Боба должно быть дополнено событиями во временны́х окнах 1 и 3, соответственно, для базисов $L_{A,B}$ и $R_{A,B}$ у Алисы и Боба.

7. СТОЙКОСТЬ ПРОТОКОЛА КВАНТОВОГО ФАЗОВО-ВРЕМЕННО́ГО РАСПРЕДЕЛЕНИЯ КЛЮЧЕЙ В АСИМПТОТИЧЕСКОМ ПРЕДЕЛЕ БЕСКОНЕЧНО ДЛИННЫХ ПЕРЕДАВАЕМЫХ ПОСЛЕДОВАТЕЛЬНОСТЕЙ

Сначала для дальнейшего удобства получим длину секретного ключа в асимптотическом пределе бесконечно длинных передаваемых последовательностей $N \to \infty$.

В этом пределе после случайных перестановок позиций Алисы и Боба, проводимых согласованно через открытый канал связи, матрица плотности для N посылок, описывающая совместное состояние Алиса–Боб–Ева (X, Y, E), приобретает структуру тензорного произведения (см. подробности в [27])

$$\sigma_{X^N Y^N E^N} \to \sigma_{XYE}^{\otimes N}, \tag{59}$$

что фактически означает независимость отдельных посылок. Поэтому вычисление условных квантовых энтропий достаточно провести только для матрицы плотности σ_{XYE}. Кроме того, в асимптотическом пределе ($N \to \infty$) сглаженные квантовые min- и max-энтропии переходят в квантовые энтропии фон Неймана (см. детали в [27]), например, для $H^\varepsilon(X|E)$ имеем

$$\begin{aligned} H^\varepsilon(X^N|E^N) &\to NH(X|E), \\ H(X|E) &= H(\sigma_{XE}) - H(\sigma_E), \end{aligned} \tag{60}$$

$$\sigma_{XE} = \mathrm{Tr}_Y\{\sigma_{XYE}\}, \quad \sigma_E = \mathrm{Tr}_{XY}\{\sigma_{XYE}\},$$

где $H(\sigma_{XE}) = -\mathrm{Tr}\{\sigma_{XE}\log\sigma_{XE}\}$, $H(\sigma_E) = -\mathrm{Tr}\{\sigma_E\log\sigma_E\}$ — энтропии фон Неймана.

Соответственно, в асимптотическом пределе утечка информации leak_{EC} при коррекции ошибок (42) стремится к следующей величине:

$$\begin{aligned} \mathrm{leak}_{EC} &\to NH(X|Y), \\ H(X|Y) &= H(\sigma_{XY}) - H(\sigma_Y), \\ \sigma_{XY} = \mathrm{Tr}_E\{\sigma_{XYE}\}, &\quad \sigma_Y = \mathrm{Tr}_{XE}\{\sigma_{XYE}\}. \end{aligned} \tag{61}$$

С учетом сказанного и соотношения (30) длина секретного ключа в асимптотическом пределе бесконечно длинных последовательностей (точнее, доля секретных битов в пересчете на посылку) равна

$$r_{secr} = \frac{l_{secr}}{N} \le H(R_A|E) - H(R_A|R_B), \tag{62}$$

индексы «+», «×» опускаем. Формула (62) учитывает как коррекцию ошибок, так и сжатие очищенного ключа универсальными хэш-функциями второго порядка [31].

Измерения проводятся в ортогональном базисе, поэтому, учитывая симметрию по отношению к базисам R и L, находим, что

$$H(R_A^{+\times}|E) = H(L_A^{+\times}|E) = H(X_A|E),$$

где $X_A = \{0, 1\}$, соответственно,

$$H(R_A^{+\times}|R_B^{+\times}) = H(L_A^{+\times}|L_B^{+\times}) = H(X_A|Y_B),$$

где $Y_B = \{0, 1, ?\}$. Исход ? соответствует отсчетам в контрольных временны́х окнах 1 и 3.

Для вычисления условной энтропии необходимо вычислить условные вероятности $p_{X|Y}(x|y)$, например, для базиса R имеем

$$\begin{aligned} p_{X|Y}(x|y) = \mathrm{Tr}_E\{&{}_A\langle x| \otimes \\ &\otimes {}_B\langle y|\psi_R\rangle_{ABE}\ {}_{ABE}\langle\psi_R|y\rangle_B \otimes |x\rangle_A\}, \end{aligned} \tag{63}$$

где

$$|x\rangle_A = \{|\overline{0}_R^{+\times}\rangle_A, |\overline{1}_R^{+\times}\rangle_A\} \to \{0, 1\},$$

$$|y\rangle_B = \{|\overline{0}_R^{+\times}\rangle_B, |\overline{1}_R^{+\times}\rangle_B, |3\rangle_B\} \to \{0, 1, ?\}.$$

С учетом симметрии между 0 и 1, а также симметрии между базисами после измерений имеет место

$$\begin{aligned} H(R_A|E) &= H(L_A|E) = H(X_A|E), \\ H(R_A|R_B) &= H(L_A|L_B) = H(X_A|Y_B). \end{aligned}$$

Используя энтропийные соотношения неопределенностей (21)

$$H(X_A|E) + H(X_A|Y_B) \ge 2\log\frac{1}{c}, \tag{64}$$

для длины секретного ключа находим

$$l_{secr} \approx 2\log\frac{1}{c} - 2H(X_A|Y_B). \tag{65}$$

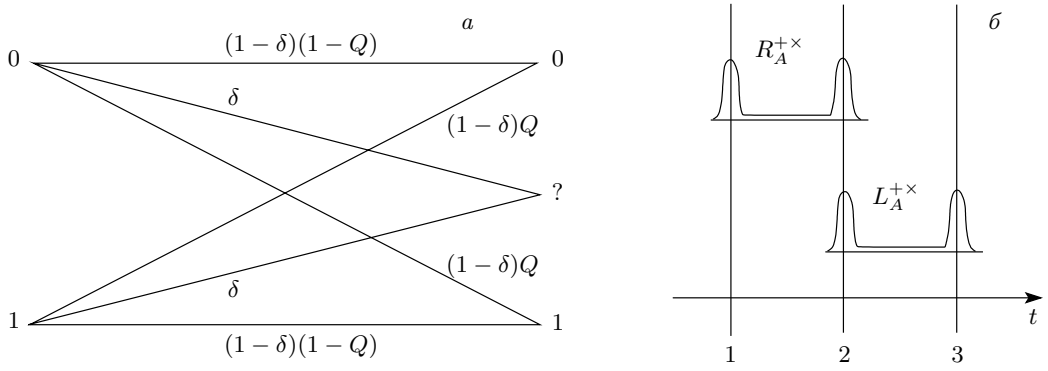

Рис. 1. *а*) Схематическое изображение классического канала связи Алиса–Боб. *б*) Информационные состояния в базисах R и L

Фактически это место, где выполняются соотношения неопределенностей (12), (21). Последние позволяют не вычислять непосредственно $H(X_A|E)$, а выразить ее через $H(X_A|Y_B)$ для классического распределения вероятностей. В этом случае $H(X_A|Y_B)$ совпадает с условной энтропией Шеннона. Данная величина легко вычисляется, поскольку ее вычисление совпадает с вычислением условной энтропии Шеннона для классического канала связи (рис. 1) с параметрами Q и δ. Наблюдаемые значения этих параметров в асимптотическом пределе бесконечно длинных последовательностей совпадают со своими точными значениями.

После измерений на приемной стороне ситуация между Алисой и Бобом описывается симметричным классическим каналом связи с двумя состояниями на входе и тремя — на выходе (рис. 1). С учетом симметрии и условий нормировки условных вероятностей параметризация осуществляется однозначно. Ее удобно выбрать в следующем виде:

$$\begin{gathered} p_{X|Y}(0|0) = p_{X|Y}(1|1) = (1-\delta)(1-Q), \\ p_{X|Y}(0|1) = p_{X|Y}(1|0) = (1-\delta)Q, \\ p_{X|Y}(0|?) = p_{X|Y}(1|?) = \delta. \end{gathered} \tag{66}$$

Подчеркнем, что в асимптотическом пределе величины δ и Q, параметризующие распределение вероятностей и имеющие смысл вероятности отсчетов в контрольных временны́х окнах и вероятности ошибки, являются точными значениями, а не их оценками, как это имеет место при конечных длинах последовательностей.

Поэтому стадия оценки параметров распределения формально отсутствует, так как они известны точно. Фактически это означает, что из бесконечной последовательности всегда можно выделить также бесконечную подпоследовательность, по которой можно сделать оценку эмпирических значений параметров $\overline{\delta}$ и $\overline{Q}$, которые при $N \to \infty$ стремятся к истинным значениям: $\overline{\delta} \to \delta$ и $\overline{Q} \to Q$ (детали см. ниже).

Теперь осталось вычислить константу c в выражении (64). С учетом (49), (50) имеем

$$\begin{aligned} c = |{}_A\langle\overline{0}_L^{+\times}|\overline{0}_R^{+\times}\rangle_A| = |{}_A\langle\overline{0}_L^{+\times}|\overline{1}_R^{+\times}\rangle_A| = \\ = |{}_A\langle\overline{1}_L^{+\times}|\overline{1}_R^{+\times}\rangle_A| = \frac{1}{2}. \end{aligned} \tag{67}$$

Окончательно для длины секретного ключа находим

$$\begin{aligned} l_{secr} \approx 2\,(1 - H(X_A|Y_B)) = \\ = 2\,(1 - (1-\delta)h(Q) - h(\delta))\,. \end{aligned} \tag{68}$$

Зависимости длины секретного ключа от величины ошибки Q при разных значениях параметра δ приведены на рис. 2.

В протоколе квантового распределения ключей с фазово-временны́м кодированием длина секретного ключа зависит от двух параметров δ и Q. Физический смысл параметров является прозрачным. Величина $1-\delta$ равна доле отсчетов в информационных временны́х окнах (напомним, что информационные состояния являются суперпозицией состояний во временны́х окнах 1 и 2 в базисе R и в окнах 2 и 3 в базисе L). Соответственно, δ — доля отсчетов в контрольных временны́х окнах 3 в базисе R и 1 в базисе L (рис. 1). В информационных окнах доля отсчетов $1-Q$ является правильной, а остальная доля Q — ошибочной.

Оба параметра зависят от действий подслушивателя. Однако Алиса и Боб перед передачей клю-

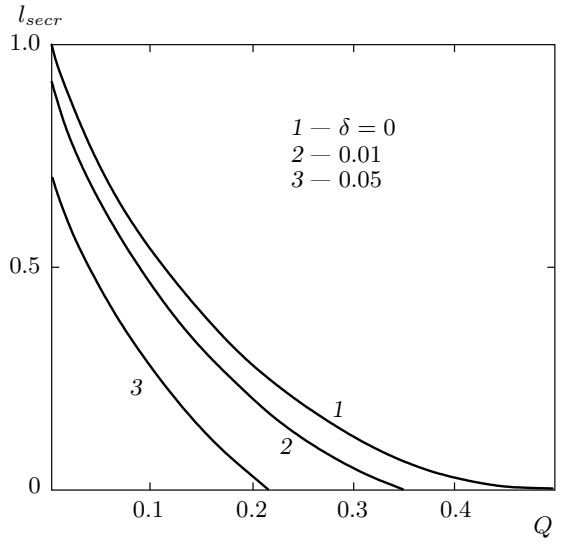

Рис. 2. Зависимости длины секретного ключа от параметров протокола Q, δ

чей могут декларировать, что протокол будет прерван, если величина δ превысит критическое значение $\delta > \delta_c \approx 0$. В этом случае у Евы не остается возможностей, кроме как регулировать ошибку Q, которая в этом случае может достигать $Q_c \to 50\,\%$. Это связано с тем, что Ева не может различить достоверно состояния в базисах R и L, что неизбежно будет приводить к отсчетам с вероятностью δ в тех контрольных временны́х окнах, где их не должно быть в случае совпадающих базисов у Алисы и Боба.

Отметим во избежании недоразумений, что в работе [13], где использовалось прямое доказательство секретности, для длины ключа было получено выражение $l_{secr} \approx 1 - h(Q) - h(\eta)$, $\eta = \delta/(1-\delta)$, поскольку использовалась постселекция отсчетов в контрольных временны́х окнах и величина ошибки пересчитывалась только на информационные временны́е окна. При этом предельная величина ошибки при $\delta \to 0$ также равна $Q_c \to 50\,\%$, критическое значение $\delta_c = 1/3$, вместо $\delta_c = 1/2$ в данном протоколе. Ограничение на величину $\delta \le 1/2$ возникает из условия унитарной реализуемости атаки Евы $(I_A \otimes U_{BE})|\Phi_{R,L}\rangle_{AB} \to |\Psi_{R,L}\rangle_{ABE}$.

Ошибка Q связана также с видностью интерференционной картины в интерферометре Маха–Цандера V, $Q = (1-V)/2$ [12, 13]. Случай $V \to 0$ отвечает почти полной потере видности интерференционной картины за счет разбалансировки интерферометра, при этом $Q \to 1/2$. Это означает, что протокол гарантирует секретность ключей (при $\delta \approx 0$) вплоть до полной потери видности. Разбалансировка интерферометра не приводит к сдвигам по времени, соответственно к отсчетам в контрольных временны́х окнах, которые регулируются параметром δ.

8. СТОЙКОСТЬ ПРОТОКОЛА КВАНТОВОГО ФАЗОВО-ВРЕМЕННО́ГО РАСПРЕДЕЛЕНИЯ КЛЮЧЕЙ ПРИ КОНЕЧНЫХ ДЛИНАХ ПЕРЕДАВАЕМЫХ ПОСЛЕДОВАТЕЛЬНОСТЕЙ

После передачи квантовых состояний в соответствии с протоколом (см. разд. 6) и процедурой согласования базисов происходит оценка значений параметров протокола (δ и Q) путем раскрытия части последовательности.

Алфавит на передающей стороне $X = \{0,1\}^N$, на приемной стороне — $Y = \{0,1,?\}^N$. Здесь N — длина зарегистрированных отсчетов при совпадающих базисах Алисы и Боба. Исходам ? отвечают отсчеты в контрольных временны́х окнах. Корреляция между случайными последовательностями Алисы X и Боба Y описывается функцией распределения $P(X,Y)_{\delta,Q}$. Пусть Q — истинные значения вероятности ошибки и δ — вероятности отсчетов в контрольных временны́х окнах для распределения вероятностей. Цель процедуры оценки параметров сводится к установлению близости эмпирического распределения вероятностей к истинному по наблюдаемым значениям параметров.

Пусть наблюдаемая доля отсчетов в контрольных окнах есть

$$\overline{\delta} = \frac{1}{N}|Y \neq 0,1|,$$

она может отличаться за счет флуктуаций при конечной длине последовательности от своего истинного значения δ при бесконечной длине последовательности. Соответственно, наблюдаемое число позиций, в которых были информационные отсчеты 0 или 1, равно $N_Q = N(1-\overline{\delta})$. Далее, наблюдаемая доля ошибочных отсчетов есть

$$\overline{Q} = \frac{1}{N_Q}|X \oplus Y \neq ?|.$$

Для оценки наблюдаемой доли ошибок $\overline{Q}$ в полной последовательности длины N легитимные пользователи раскрывают часть последовательности, где были только отсчеты $0,1$. Пусть раскрывается доля νN_Q случайно выбранных позиций, а оставшаяся

доля $(1-\nu)N_Q$ служит для выработки очищенного ключа.

Полное наблюдаемое число ошибок есть

$$\overline{Q}N_Q = \nu N_Q q + (1-\nu)N_Q Q_{key}, \tag{69}$$

где νN_Q, q — соответственно число раскрываемых позиций и доля ошибок в них, $(1-\nu)N_Q$ Q_{key} — число не раскрываемых позиций, которые входят в дальнейшем в ключ, Q_{key} — доля ошибочных отсчетов в этих позициях.

Далее нашей целью будет установить близость эмпирического распределения вероятностей $\overline{P}(X,Y)_{\overline{\delta},\overline{Q}}$ к истинному $P(X,Y)_{\delta,Q}$ по наблюдаемой доле отсчетов в контрольных временны́х окнах $\overline{\delta}$ и доле ошибок в раскрываемой части q. Фактически требуется установить, что распределение при заданном N является $\varepsilon(\overline{\delta},\overline{Q})$-близким к истинному, т. е. $\overline{P}(X,Y)_{\overline{\delta},\overline{Q}} \in \mathcal{B}^{\varepsilon(\overline{\delta},\overline{Q})}(P(X,Y)_{\delta,Q})$,

$$\frac{1}{2}||P(X,Y)_{\delta,Q} - \overline{P}(X,Y)_{\overline{\delta},\overline{Q}}||_1 \le \varepsilon(\overline{\delta},\overline{Q}). \tag{70}$$

Сделаем данную оценку в два этапа. Установим сначала близость распределений по числу отсчетов в контрольных временны́х окнах, а затем — по числу ошибок при заданном числе отсчетов в контрольных окнах.

Согласно неравенству для отклонений от математического ожидания (см. [36]), находим, что вероятность того, что наблюдаемое число отсчетов $(\overline{\delta})$ в контрольных временны́х окнах превышает математическое ожидание (точное значение δ) на величину ξ, не больше следующего значения:

$$\Pr[\overline{\delta} \ge \delta + \xi] \le \exp(-2N\xi^2) = \varepsilon^2(\overline{\delta}). \tag{71}$$

Введем распределение $\overline{P}(X,Y)_{\overline{\delta},Q}$, которое дает не более $\overline{\delta} < \delta + \xi$ отсчетов в контрольных временны́х окнах и является $\varepsilon(\overline{\delta})$-близким к истинному, т. е. лежит в шаре $\overline{P}(X,Y)_{\overline{\delta},Q} \in \mathcal{B}^{\varepsilon(\overline{\delta})}(P(X,Y)_{\delta,Q})$.

Распределение имеет вид

$$\overline{P}(X,Y)_{\overline{\delta},Q} = \begin{cases} \dfrac{P(X,Y)_{\overline{\delta},Q}}{\Pr[\overline{\delta} < \delta + \xi]}, & \overline{\delta} < \delta + \xi, \\ 0, & \overline{\delta} \ge \delta + \xi. \end{cases} \tag{72}$$

Следовое расстояние d_1 не превосходит расстояние, выражаемое через соответствие (18), поэтому с учетом (71) и того, что

$$\Pr[\overline{\delta} \ge \delta + \xi] + \Pr[\overline{\delta} < \delta + \xi] = 1, \tag{73}$$

получаем

$$d_1(P(X,Y)_{\delta,Q}, \overline{P}(X,Y)_{\delta,Q}) \le \le \sqrt{1 - F^2(P(X,Y)_{\delta,Q}, \overline{P}(X,Y)_{\overline{\delta},Q})}. \tag{74}$$

Учитывая (71)–(74), находим

$$F(P(X,Y)_{\delta,Q}, \overline{P}(X,Y)_{\overline{\delta},Q}) = = \sum_{Y=?,\overline{\delta}<\delta+\xi} \sqrt{P(X,Y)_{\delta,Q}\overline{P}(X,Y)_{\overline{\delta},Q}} = = \sqrt{\Pr[\overline{\delta} < \delta + \xi]} = \sqrt{1-\varepsilon^2(\overline{\delta})}. \tag{75}$$

Отсюда следует, что распределения $P(X,Y)_{\delta,Q}$ и $\overline{P}(X,Y)_{\overline{\delta},Q}$ являются $\varepsilon(\overline{\delta})$-близкими:

$$d_1(P(X,Y)_{\delta,Q}, \overline{P}(X,Y)_{\delta,Q}) = = \frac{1}{2}||P(X,Y)_{\delta,Q} - \overline{P}(X,Y)_{\overline{\delta},Q}||_1 \le \le \frac{1}{2}\varepsilon(\overline{\delta}) = \varepsilon_1. \tag{76}$$

Следующий шаг состоит в оценке величины истинной вероятности ошибки по наблюдаемой в раскрытой части для распределения $\overline{P}(X,Y)_{\overline{\delta},Q}$.

Согласно неравенству для вероятности уклонения наблюдаемого значения от истинного значения по выборке без возвращения (см. детали в [37]), получаем

$$\Pr[Q_{key} \ge \overline{Q} + \zeta] \le \exp\left(-2\frac{n_Q N_Q}{k_Q + 1}\zeta^2\right). \tag{77}$$

С учетом того, что

$$\overline{Q} = \nu Q_{obs} + (1-\nu)Q_{key}, \tag{78}$$

находим

$$\Pr[Q_{key} \ge \overline{Q} + \zeta] \le \exp\left(-2\frac{k_Q n_Q}{N_Q}\frac{k_Q}{k_Q+1}\zeta^2\right) = = \overline{\varepsilon}^2(\overline{Q}). \tag{79}$$

Протокол не прерывается, если величина ошибки $\overline{Q}$ не превосходит критической величины для протокола. Критическая величина ошибки, как видно из анализа стойкости в асимптотическом пределе (см. разд. 6), зависит от доли отсчетов в контрольных временны́х окнах δ. Вероятность пройти тест есть $\Pr[\text{test} = \text{OK}, \delta] = \Pr[Q_{obs} < \overline{Q}, \delta]$.

Введем новое распределение вероятностей

$$\overline{P}(X,Y)_{\overline{\delta},\overline{Q}}=\begin{cases}\dfrac{P(X,Y)_{\overline{\delta},Q}}{\Pr[Q_{key}<\overline{Q}+\zeta|\text{test}=\text{OK},\delta]}, & Q_{key}<\overline{Q}+\zeta,\\ 0, & Q_{key}\geq\overline{Q}+\zeta.\end{cases}\tag{80}$$

Данное распределение производит не более $Q_{key}<\overline{Q}+\zeta$ ошибок при заданном значении $\overline{\delta}$.

Далее, вводя обозначение

$$\varepsilon(\overline{Q})=\frac{\overline{\varepsilon}(\overline{Q})}{\sqrt{\Pr[\text{test}=\text{OK},\delta]}},\tag{81}$$

аналогично проведенному выше анализу (формулы (72)–(75)) получаем, что распределения $\overline{P}(X,Y)_{\overline{\delta},\overline{Q}}$ и $\overline{P}(X,Y)_{\overline{\delta},Q}$ являются $\varepsilon(\overline{Q})$-близкими:

$$d_1(\overline{P}(X,Y)_{\overline{\delta},\overline{Q}},\overline{P}(X,Y)_{\overline{\delta},Q})=$$
$$=\frac{1}{2}||\overline{P}(X,Y)_{\overline{\delta},Q}-\overline{P}(X,Y)_{\overline{\delta},\overline{Q}}||_1\leq\varepsilon(\overline{Q})=\varepsilon_2.\tag{82}$$

С учетом (82) расстояние между истинным распределением и эмпирическим равно

$$d_1(P(X,Y)_{\delta,Q},\overline{P}(X,Y)_{\overline{\delta},\overline{Q}})\leq$$
$$\leq\sqrt{1-F^2(P(X,Y)_{\delta,Q},\overline{P}(X,Y)_{\overline{\delta},\overline{Q}})}=\varepsilon(\overline{\delta},\overline{Q}).\tag{83}$$

Окончательно находим, что распределение $\overline{P}(X,Y)_{\overline{\delta},\overline{Q}}$ оказывается $\varepsilon(\overline{\delta},\overline{Q})$-близким к исходному, где $\varepsilon(\overline{\delta},\overline{Q})=\varepsilon(\overline{\delta})+\varepsilon(\overline{Q})$. Действительно, используя неравенство треугольника, получаем

$$\frac{1}{2}||P(X,Y)_{\delta,Q}-\overline{P}(X,Y)_{\overline{\delta},\overline{Q}}||_1\leq$$
$$\leq\frac{1}{2}||P(X,Y)_{\delta,Q}-\overline{P}(X,Y)_{\overline{\delta},Q}||_1+$$
$$+\frac{1}{2}||P(X,Y)_{\overline{\delta},Q}-\overline{P}(X,Y)_{\overline{\delta},\overline{Q}}||_1\leq$$
$$\leq\varepsilon(\overline{\delta},\overline{Q})=\varepsilon_1+\varepsilon_2.\tag{84}$$

Найдем теперь величину $H_{max}^{\varepsilon(\overline{\delta},\overline{Q})}(P(X,Y)_{\delta,Q}|Y)$, определяющую согласно (42) утечку информации в битах при коррекции ошибок.

Отметим, что оценка вероятности отсчетов в контрольных временны́х окнах проводится по всей последовательности длины N. Далее оценка вероятности ошибки проводится по случайной доле из $k_Q=\nu(1-\overline{\delta})N$ позиций, которая раскрывается и впоследствии отбрасывается. После отбрасывания к $n_Q=(1-\nu)(1-\overline{\delta})N$ позициям, где не было отсчетов в контрольных временны́х окнах, случайно добавляется $(1-\nu)\overline{\delta}N$ позиций. После этого полное число оставшихся позиций равно $n=(1-\nu)N$. Таким образом, отсчеты в контрольных временны́х окнах также считаются ошибками (вероятность ошибки в этих позициях известна точно и равна $1/2$).

Поскольку $H_{max}^{\varepsilon(\overline{\delta},\overline{Q})}(P(X,Y)_{\delta,Q})$ является точной нижней гранью (в нашем случае — минимумом) по всем распределениям в шаре $\overline{P}(X,Y)_{\overline{\delta},\overline{Q}}\in\mathcal{B}^{\varepsilon(\overline{\delta})}(P(X,Y)_{\delta,Q})$, имеем

$$H_{max}^{\varepsilon(\overline{\delta},\overline{Q})}(P(X,Y)_{\delta,Q}|Y)\leq H_{max}(\overline{P}_{\overline{\delta},\overline{Q}}(X,Y)|Y)\leq$$
$$\leq\log\left(\sum_{i=0}^{n(1-\overline{\delta})Q_{key}}\frac{n!}{[n\overline{\delta}]![n(1-\overline{\delta})-i]!i!}\right)=$$
$$=\log\left(\frac{n!}{[n\overline{\delta}]![n(1-\overline{\delta})]!}\times\right.$$
$$\left.\times\sum_{i=0}^{n(1-\overline{\delta})(Q_{key}}\frac{[n(1-\overline{\delta})]!}{[n(1-\overline{\delta})-i]!i!}\right).\tag{85}$$

Фактически $H_{max}(\overline{P}_{\overline{\delta},\overline{Q}}(X,Y)|Y)$ равна логарифму произведения числа способов раскидать $Q_{key}=\overline{Q}+\zeta$ ошибок по $n(1-\overline{\delta})$ позициям, не содержащим отсчетов в контрольных временны́х окнах, на число способов разместить $n\overline{\delta}$ отсчетов в контрольных временны́х окнах по n позициям.

Воспользовавшись неравенствами (см., например, [38])

$$\frac{n!}{(n-x)!x!}\leq 2^{nH(x)},$$
$$\sum_{k=0}^{x}\frac{n!}{(n-i)!i!}\leq\frac{n!}{(n-x)!x!}\leq 2^{nH(x)},\tag{86}$$

окончательно находим

$$H_{max}^{\varepsilon(\overline{\delta},\overline{Q})}(P(X,Y)_{\delta,Q}|Y)\leq$$
$$\leq n\left(H(\delta+\xi)+[1-(\delta+\xi)]H(\overline{Q}+\zeta)\right).\tag{87}$$

Таким образом, если наблюдаемые значения в последовательности длины n числа отсчетов в контрольных временны́х окнах $n\overline{\delta}$ и наблюдаемое число ошибок в оставшихся $n(1-\overline{\delta})$ позициях равно $n(1-\overline{\delta})\overline{Q}$, то это гарантирует, что любое распределение, дающее такие наблюдаемые значения $\overline{\delta}$ и $\overline{Q}$, заключено в шаре радиуса $\varepsilon(\overline{\delta},\overline{Q})$ с центром в истинном распределении вероятностей (см. (70)–(84)). Близость к истинному распределению гарантирует, что max-энтропия $H_{max}^{\varepsilon(\overline{\delta},\overline{Q})}(P(X,Y)_{\delta,Q}|Y)$, определяющая утечку информации в битах при коррекции ошибок, не превышает при данных значениях $N,\overline{\delta},\overline{Q}$ величину (84).

9. ДЛИНА СЕКРЕТНОГО КЛЮЧА

Задавая параметры корректности ε_{EC} и секретности Δ протокола, определим длину секретного ключа.

Собирая все результаты вместе, с учетом (70)–(84) имеем длину секретного ключа, которую можно получить при заданных параметрах $n, \overline{\delta}, \overline{Q}$:

$$l_{secr} \le n\left(2\log\frac{1}{c} - H_{max}^{\varepsilon(\overline{\delta},\overline{Q})}(P(X,Y)_{\delta,Q}|Y)\right) - \\ - 2\log\frac{1}{2\varepsilon} - \mathrm{leak}_{EC}. \quad (88)$$

С учетом того, что утечка информации при коррекции ошибок (см. (42), (87)) не более

$$\mathrm{leak}_{EC} \le H_{max}^{\varepsilon(\overline{\delta},\overline{Q})}(P(X,Y)_{\delta,Q}|Y) + \log\frac{2}{\varepsilon_{EC}} \le \\ \le n\left(H(\delta{+}\xi){+}[1{-}(\delta{+}\xi)]H(\overline{Q}{+}\zeta)\right) + \log\frac{2}{\varepsilon_{EC}}, \quad (89)$$

расстояние секретности до идеальной ситуации (26) не превосходит

$$\Delta \le \varepsilon + \frac{1}{2}\sqrt{2^{-(H_{min}^{\varepsilon}(X|EC)-l_{secr})}}. \quad (90)$$

Поскольку $\varepsilon = \varepsilon(\overline{\delta}, \overline{Q})$, с учетом соотношений неопределенности (21) имеем

$$H_{min}^{\varepsilon}(X|EC) \ge H_{min}^{\varepsilon}(X|E) - \mathrm{leak}_{EC} \ge \\ \ge 2n - H_{max}^{\varepsilon(\overline{\delta},\overline{Q})}(P(X,Y)_{\delta,Q}|Y) - \mathrm{leak}_{EC}. \quad (91)$$

Окончательно для длины финального секретного ключа находим

$$l_{secr} \le 2n\left(1{-}H(\delta{+}\xi){-}[1{-}(\delta{+}\xi)]H(\overline{Q}{+}\zeta)\right) - \\ - 2\log\frac{1}{2\overline{\varepsilon}} - \log\frac{2}{\varepsilon_{EC}}. \quad (92)$$

В этом случае ключи

$$\Delta \le \varepsilon(\overline{\delta}, \overline{Q}) + \overline{\varepsilon} \text{ секретен и } \varepsilon_{EC} \text{ корректен.} \quad (93)$$

10. ЧИСЛЕННЫЕ ОЦЕНКИ

Приведем некоторые численные результаты. Целью является получение определенной длины ключа при задаваемых легитимными пользователями параметрах — корректности и секретности протокола и передаваемой длине последовательности n. Задавая данные параметры и выражая из (71), (79) величины уклонений ξ и ζ для наблюдаемых параметров $\overline{\delta}$ и $\overline{Q}$ от их истинных значений δ и Q, находим

$$\xi(\varepsilon(\overline{\delta})) = \sqrt{\frac{1}{n}\ln\frac{1}{\varepsilon(\overline{\delta})}}, \\ \zeta(\overline{Q}) = \sqrt{\frac{1}{n\nu(1-\nu)[1-(\delta+\xi(\varepsilon(\overline{\delta})))]}\ln\frac{1}{\varepsilon(\overline{Q})}}, \quad (94) \\ n \gg 1.$$

На рис. 3 приведены зависимости длины секретного ключа от наблюдаемой ошибки $\overline{Q}$ при различных значениях доли отсчетов в контрольных временны́х окнах δ. Доля раскрываемой последовательности для всех рисунков $\nu = 1/2$.

Пусть длина передаваемой последовательности n фиксирована. Тогда, чем меньше параметры секретности, тем больше разброс оценок для величины уклонения параметров от их истинных значений. Как видно из (94), например, оценка уклонения для параметра δ пропорциональна логарифму от обратной величины параметра секретности ε. Фактически это означает, что чем меньше величины параметров секретности, тем более консервативной (завышенной) является оценка величины ошибки и доли отсчетов в контрольных временны́х окнах. Большие значения этих параметров означают завышение информации Евы, которую она получает при вторжении в квантовый канал связи. Отсюда автоматически следует, что длина секретного ключа обращается в нуль при меньших, по сравнению со значениями в асимптотическом пределе бесконечных последовательностей, значениях вероятности ошибки и доли отсчетов в контрольных окнах. Эта тенденция явно видна из сравнения на рис. 3 верхнего и нижнего рядов (при одинаковых значениях n).

Аналогичная тенденция имеет место при различных n и фиксированных параметрах секретности. При этом, как видно из (94), оценка величин уклонений наблюдаемых ошибки и доли отсчетов в контрольных окнах обратно пропорциональна корню из n, т. е. при меньших n точность оценки параметров хуже. Поэтому при малых n происходит завышение уклонений наблюдаемых параметров ошибки и доли отсчетов в контрольных окнах по сравнению с их истинными значениями, что дает меньшую допустимую длину секретного ключа, который можно получить из данной последовательности при наблюдаемой ошибке. При малых длинах $n = 10^5$–10^6 критическая ошибка, до которой возможно распределение секретных ключей, заметно отличается от ошибки в

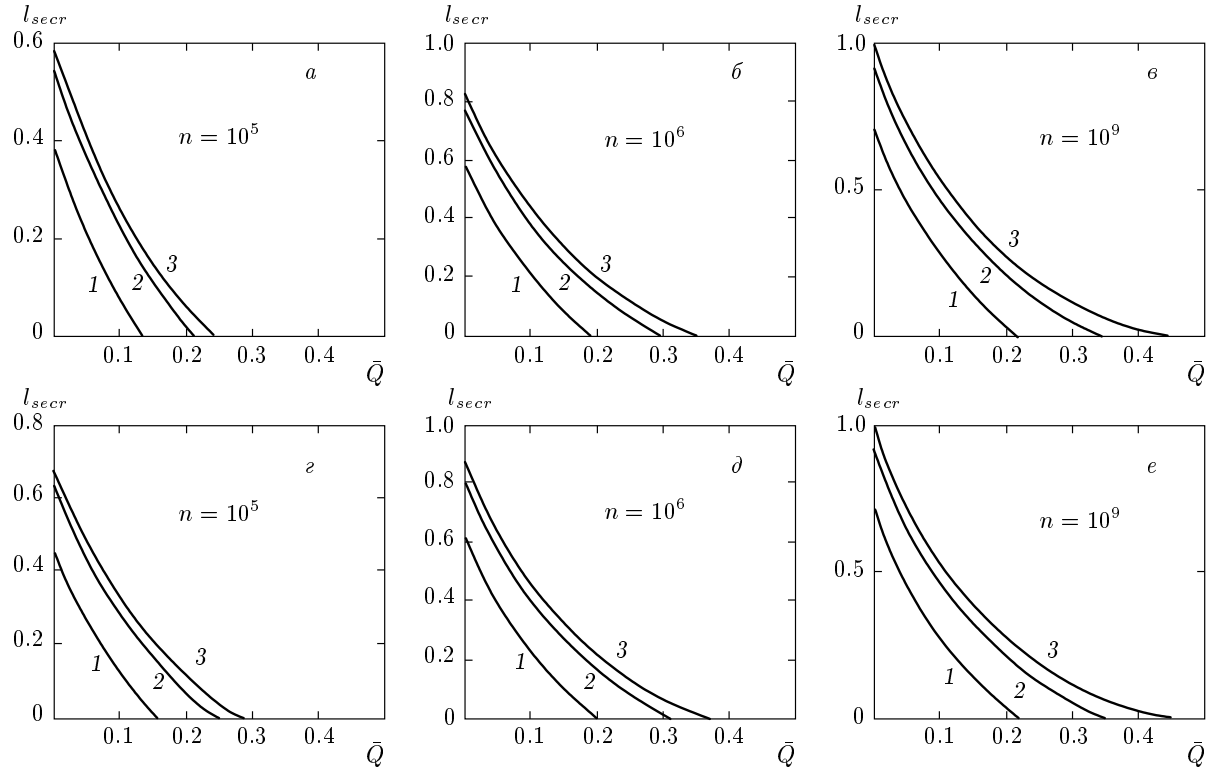

Рис. 3. Зависимости нормированной на длину последовательности длины секретного ключа при различной доле отсчетов в контрольных временны́х окнах. Длины n передаваемых последовательностей указаны на рис., $\delta = 0.001$ (*1*), 0.01 (*2*), 0.05 (*3*). Для рис. *а,б,в* параметры секретности $\varepsilon(\overline{\delta}) = \varepsilon(\overline{Q}) = \varepsilon = 10^{-20}$, $\varepsilon_{EC} = 10^{-20}$, для рис. *г,д,е* — $\varepsilon(\overline{\delta}) = \varepsilon(\overline{Q}) = \varepsilon = 10^{-10}$, $\varepsilon_{EC} = 10^{-10}$

асимптотическом пределе (разд. 6, рис. 2). При длинах передаваемых последовательностей $n = 10^9$ длина секретного ключа практически совпадает с длиной в асимптотическом пределе и слабо (логарифмически) зависит от параметров секретности протокола. Напомним, что зависимость от n степенная (94).

Этот факт интуитивно более-менее естествен, поскольку при больших n, а в пределе $n \to \infty$, оценки величины для уклонений параметров от их истинных значений стремятся к нулю, поэтому критическая ошибка и критическая доля отсчетов в контрольных окнах практически совпадают со своими значениями в асимптотическом пределе.

На рис. 4 приведены зависимости длины секретного ключа от длины передаваемой последовательности n при разных значениях вероятности ошибки и доли отсчетов в контрольных временны́х окнах.

Параметры секретности для рисунков в верхнем ряду имеют меньшие значения по сравнению с соответствующими значениями параметров в нижнем ряду. Общим свойством является то, что при фиксированных остальных параметрах протокола существует конечная критическая длина последовательности, начиная с которой можно вообще получить секретный ключ ненулевой длины. Данная ситуация радикально отличается от случая асимптотического предела, где зависимость от длины (поскольку она бесконечна) эффективно отсутствует. Как видно из рис. 4, чем больше величина ошибки и доля отсчетов в контрольных окнах (при фиксированных параметрах секретности и корректности), тем бóльшая требуется длина последовательности, начиная с которой можно получить секретный ключ ненулевой длины.

Далее, из сравнения верхнего и нижнего рядов рис. 4 видно, что уменьшение параметров секретности (при фиксированной вероятности ошибки и доли отсчетов в контрольных окнах) требует увеличения длины последовательности для извлечения секретного ключа ненулевой длины. Данный факт также интуитивно понятен, уменьшение параметров секретности и корректности неизбежно ведет к увеличению длины последовательности (см. формулы (92), (94)), чтобы получить оценку заданного укло-

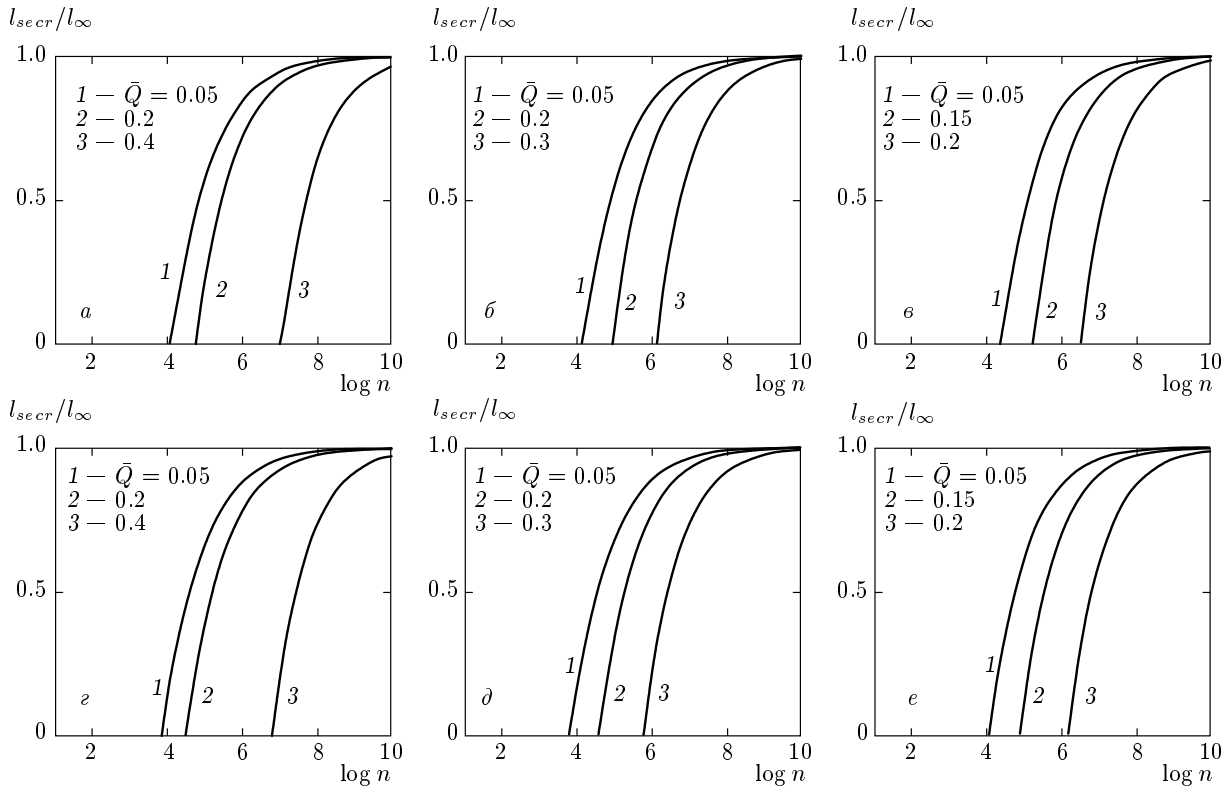

Рис. 4. Зависимости отношения длины секретного ключа для конечной последовательности и длины ключа в асимптотическом пределе от логарифма длины последовательности при различных значениях параметров. Для рис. *а,б,в* параметры секретности $\varepsilon(\overline{\delta}) = \varepsilon(\overline{Q}) = \varepsilon = 10^{-20}$, $\varepsilon_{EC} = 10^{-20}$, для рис. *г,д,е* — $\varepsilon(\overline{\delta}) = \varepsilon(\overline{Q}) = \varepsilon = 10^{-10}$, $\varepsilon_{EC} = 10^{-10}$. Параметр $\delta = 0.001$ (*а,б,г,д*), 0.05 (*в,е*)

нения от истинных значений. Поскольку уменьшение параметров секретности ведет (логарифмически) к увеличению уклонения (94), требуется соответствующим образом увеличить длину n, чтобы сохранить фиксированное значение уклонения.

11. ЗАКЛЮЧЕНИЕ

В заключение сделаем оценки времени генерации секретного ключа. Из рис. 4*а,г* видно, что для получения секретного ключа ненулевой длины при большой вероятности ошибки $Q = 40\,\%$, требуется длина последовательности не менее 10^6 бит, а для получения длины ключа[2)] 256 бит необходима длина последовательности гигабит.

Поскольку типичное значение среднего числа фотонов в ослабленном лазерном импульсе (когерентном состоянии), которое имеет место в системах квантовой криптографии, $\mu \approx 0.1$, квантовая эффективность InGaAs-лавинных фотодетекторов $\eta_{APD} \approx 0.1$. Далее, учитывая потери через волоконный оптический тракт (по два светоделителя на приемной и передающей стороне в интерферометрах Маха–Цандера) $\eta_{fiber} \approx (1/2)^4$, получаем, что полная эффективность $\eta_{eff} = \mu\eta_{APD}\eta_{fiber} \approx 10^{-3}$ (даже без учета потерь в самой линии). Для получения реальных 10^9 отсчетов требуется $10^9/\eta_{eff} \approx 10^{12}$ посылок. Типичные рабочие частоты повторения импульсов составляют $f \approx 100$ кГц, хотя известны успешные эксперименты на частотах $f \approx 1$ ГГц [39, 40]. При такой частоте и вероятности ошибки 40 % для генерации ключа требуется время $10^9/\eta_{eff} f \approx 10^3$ с ≈ 30 мин. При меньших тактовых частотах время генерации ключа при таком проценте ошибок оказывается неприемлемо большим.

При ошибке $Q \approx 10\,\%$ для генерации ключа требуется 10^4 реальных отсчетов, что на шесть порядков меньше, чем в предыдущем случае. Поэтому для генерации ключа необходимо время порядка нескольких минут при частоте генерации $f = 100$ кГц. При частоте $f \approx 1$ ГГц новый ключ можно генерировать несколько раз в секунду.

[2)] Такая длина ключа, например, используется в российском алгоритме шифрования ГОСТ 28147-89 Р.

Автор выражает благодарность коллегам по Академии криптографии Российской Федерации за постоянную поддержку. Работа выполнена при частичной финансовой поддержке РФФИ (грант № 11-02-00455).

ЛИТЕРАТУРА

1. W. K. Wootters and W. H. Zurek, Nature **299**, 802 (1982).
2. C. H. Bennett, Phys. Rev. Lett. **68**, 3121 (1992).
3. W. Heisenberg, Zeit. für Phys. **43**, 172 (1927).
4. V. Scarani, H. Bechmann-Pasquinucci, N. J. Cerf, M. Dusek, N. Lütkenhaus, and M. Peev, Rev. Mod. Phys. **81**, 1301 (2009).
5. C. H. Bennett and G. Brassard, Proc. of IEEE Int. Conf. on Comput. Sys. and Sign. Proces., Bangalore, India (1984), p. 175.
6. D. Mayers, J. ACM **48**, 351 (2001).
7. H.-K. Lo and H. F. Chau, Science **283**, 2050 (1999).
8. P. Shor and J. Preskill, Phys. Rev. Lett. **85**, 441 (2000).
9. M. Koashi, J. Phys. Conf. Ser. **36**, 98 (2006).
10. M. Tomamichel and R. Renner, arXiv/quant-ph: 10092015.
11. M. Tomamichel, C. Ci Wen Lim, N. Gisin, and R. Renner, arXiv/quant-ph:11034130.
12. С. П. Кулик, А. П. Маккавеев, С. Н. Молотков, Письма в ЖЭТФ **85**, 354 (2007).
13. С. Н. Молотков, ЖЭТФ **133**, 5 (2008).
14. Д. А. Кронберг, С. Н. Молотков, ЖЭТФ **136**, 650 (2009); **138**, 33 (2010).
15. L. Lydersen, C. Wiechers, C. Wittmann, D. Elser, J. Skaar, and V. Makarov, Nature Photonics **4**, 686 (2010).
16. С. Н. Молотков, ЖЭТФ **141**, 812 (2012).
17. C. E. Shannon, Bell Syst. Tech. J. **27**, 397; **27**, 623 (1948).
18. Р. Галлагер, *Теория информации и надежная связь*, Советское радио, Москва (1974). [R. G. Gallager, *Information Theory and Reliable Communication*, Wiley, New York (1968).]
19. H. P. Robertson, Phys. Rev. **34**, 163 (1929).
20. D. Deutsch, Phys. Rev. Lett. **50**, 631 (1983).
21. H. Maassen and J. B. M. Uffink, Phys. Rev. Lett. **60**, 1103 (1988).
22. K. Kraus, Phys. Rev. D **35**, 3070 (1987).
23. J. M. Renes and J.-C. Boileau, Phys. Rev. Lett. **103**, 020402-1 (2009).
24. M. Berta, M. Chritlandl, R. Colbeck, J. M. Renes, and R. Renner, arXiv/quant-ph:0909.0950.
25. T. M. Cover and J. A. Thomas, *Elements of Information Theory*, Wiley (1991).
26. M. Berta, M. Christandl, R. Colbeck, J. M. Renes, and R. Renner, Nature Phys. **6**, 659 (2010).
27. R. Renner, PhD Thesis, ETH Zürich, December, 2005; arXiv/quant-ph:0512258.
28. M. Nielsen and I. Chuang, *Quantum Computation and Quantum Information*, Cambridge Univ. Press, Cambridge (2000).
29. M. Tomamichel and R. Renner, arXiv/quant-ph: 10092015.
30. J. M. Renes and R. Renner, arXiv/quant-ph:10080452.
31. J. L. Carter and M. N. Wegman, J. Comp. Syst. Sci. **18**, 143 (1979).
32. M. N. Wegman and J. L. Carter, J. Comp. Syst. Sci. **22**, 265 (1991).
33. C. H. Bennett, G. Brassard, C. Crepeau, and U. M. Maurer, IEEE Trans. Inf. Theory **41**, 1915 (1995).
34. M. Tomamichel, C. Schaffner, A. Smith, and R. Renner, arXiv/quant-ph:10022436.
35. D. R. Stinson, ECCC TR95-052, Electronic Colloquium on Computational Complexity, Rep. Ser. (1995).
36. W. Hoeffding, J. Amer. Statistical Assoc. **58**, 13 (1963).
37. R. J. Serfling, Ann. Stat. **2**, 39 (1974).
38. В. К. Леонтьев, *Избранные задачи комбинаторного анализа*, Изд-во МГТУ, Москва (2001).
39. J. Zhang, P. Eraerds, N. Walenta, C. Barreiro, R. Thew, and H. Zbinden, arXiv/quant-ph:10023240.
40. D. Stucki, N. Walenta, F. Vannel, R. T. Thew, N. Gisin, H. Zbinden, S. Gray, C. R. Towery, and S. Ten, New J. Phys. **11**, 075003 (2009).