ЖЭТФ, 2018, том 153, вып. 6, стр. 895–907

КВАНТОВОЕ РАСПРЕДЕЛЕНИЕ КЛЮЧЕЙ КАК СХЕМА С БЕРНУЛЛИЕВСКИМИ ИСПЫТАНИЯМИ

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

Поступила в редакцию 20 февраля 2018 г.

Явно построено семейство атак на протокол квантового распределения ключей BB84, при которых в асимптотическом пределе длинных последовательностей достигается нижняя граница фундаментальных энтропийных соотношений неопределенностей. Все атаки параметризуются одним параметром Q, который имеет смысл вероятности ошибки на приемной стороне и находится у подслушивателя, но достоверно неизвестен легитимным пользователям. Ситуация на приемной стороне выглядит как схема с бернуллиевскими классическими испытаниями с неизвестным параметром Q. Для подслушивателя ситуация также выглядит как бернуллиевская схема — «подбрасывание монетки» с квантовыми состояниями, где в каждой посылке у подслушивателя выпадает одно из квантовых состояний, которое однозначно определяется исходом измерений на приемной стороне. Дается также статистическая интерпретация оценки вероятности ошибки Q и параметра секретности ключей $\varepsilon_{\delta,n}$. Показано, что фактически ширина доверительного интервала δ при заданной длине серии испытаний n определяет точность оценки параметра Q и, соответственно, степень секретности ключей — величину параметра секретности $\varepsilon_{\delta,n} = 2e^{-2\delta^2 n}$.

DOI: 10.7868/S0044451018060056

1. ВВЕДЕНИЕ

Квантовое распределение ключей, по сути, представляет собой статистический эксперимент по передаче и регистрации квантовых состояний с последующей обработкой результатов измерений. Финальным продуктом является общий секретный ключ между передающей (Алиса) и приемной (Боб) сторонами, который представляет собой случайную строку битов длиной ℓ и который неизвестен третьей стороне — подслушивателю (Ева). Протокол квантового распределения ключей BB84 [1] является одним из основных протоколов, секретность которого наиболее детально исследована [2–7]. Данный протокол как составная часть входит в ряд протоколов, например, decoy state (протокол с состояниями-ловушками) и др. [8,9]. Уникальность протокола в случае строго однофотонного источника состоит в том, что возможно доказательство секретности протокола с использованием фундаментальных энтропийных соотношений неопределенностей [10]. Данные соотношения позволяют не перебирать всевозможные атаки подслушивателя на передаваемый ключ и не предъявлять явно оптимальную атаку. Оптимальность понимается в смысле максимума информации Евы о ключе при данной наблюдаемой ошибке на приемной стороне Боба.

Любой протокол состоит из следующих стадий: приготовление, передача, измерение квантовых состояний, согласование базисов и интерпретация результатов измерений. После этих стадий Алиса и Боб имеют битовые строки — сырой ключ. Строка Боба содержит ошибки. Если аппаратура не имеет собственных шумов, то процент ошибок определяется вторжением Евы в канал связи. В общем случае невозможно отличить ошибки, вносимые подслушивателем, от ошибок из-за неидеальности аппаратуры, поэтому все ошибки списываются на действия подслушивателя.

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

Энтропийные соотношения неопределенностей позволяют определить верхнюю границу утечки информации к Еве при наблюдаемом проценте ошибок на приемной стороне. Оценку вероятности ошибок можно сделать двумя способами.

В первом способе раскрывается часть последовательности, определяется наблюдаемое число ошибок в раскрытой части, по которому оценивается число ошибок в нераскрытой части. Точнее оценивается условная вероятность того, что при наблюдаемом числе ошибок в раскрытой части, число ошибок в нераскрытой части не будет превышать некоторой пороговой величины. После этого происходит коррекция ошибок в нераскрытой части. Оценка количества ошибок на приемной стороне позволяет выбрать соответствующий корректирующий код для их исправления. После этой стадии Алиса и Боб имеют одинаковые битовые строки — очищенный ключ. Идентичность битовых строк Алисы и Боба — очищенного ключа — проверяется случайным хешированием.

Во втором способе коррекция ошибок происходит сразу после интерпретации результатов измерений на стороне Боба и без раскрытия части последовательности. Оценка вероятности ошибки происходит из контрольных параметров системы — темновых шумов, квантовой эффективности однофотонных детекторов, среднего числа фотонов в информационных состояниях, длины линии связи и пр. После процедуры коррекции ошибок известно наблюдаемое число ошибок на приемной стороне $\overline{k}$. Уточним, что имеется в виду.

Корректирующий код может исправить все ошибки, в этом случае их число известно точно. После процедуры коррекции ошибок и проверки идентичности очищенных ключей может оказаться с какой-то маленькой вероятностью, что не все ошибки исправлены. Далее из этого очищенного ключа будет получен секретный ключ. Если ошибки были исправлены не полностью, то секретные ключи Алисы и Боба не будут совпадать. Это обнаружится сразу же при шифровании на этом ключе, и он будет отбракован.

В анализе ниже будем использовать второй способ и будем считать, что количество ошибок $\overline{k}$ на приемной стороне известно точно. Это упростит и сократит выкладки[1)].

[1)] Как будет видно ниже (см. комментарии в Заключении), данное рассмотрение с минимальными изменениями переносится и на первый способ.

Зная количество ошибок, можно оценить информацию подслушивателя через энтропийные соотношения неопределенностей [10]. На финальной стадии протокола происходит усиление секретности [11] — сжатие очищенного ключа длины n до длины ℓ при помощи случайных хеш-функций второго порядка [12]. Степень сжатия определяется требованием к финальным ключам.

На стадии сжатия очищенных ключей необходимо знать верхнюю границу информации Евы об очищенном ключе. Даже если известно точное количество ошибок в сыром ключе, это не значит, что известна точная граница информации Евы, поскольку одно и то же наблюдаемое число ошибок $\overline{Q} = \overline{k}/n$ в конкретной серии длины n может возникнуть из разных квантовых состояний. Иначе говоря, точное знание частоты ошибок $\overline{Q}$ может дать знание об истинной вероятности ошибки Q лишь с определенной вероятностью.

Это обстоятельство приводит к тому, что квантовые состояния, которые привели к данной наблюдаемой ошибке, соответственно, информация Евы о ключе, могут быть определены лишь с некоторой точностью. Для оценки точности информации Евы о ключе наиболее удобным оказывается аппарат сглаженных квантовых энтропий Реньи [4].

1.1. Сглаженные минимальная, максимальная энтропии и длина секретного ключа

После процедуры усиления секретности Алиса и Боб имеют одинаковый секретный ключ $x \in X = \{0,1\}^\ell$ длины ℓ, а Ева — квантовую систему E. Данная ситуация описывается матрицей плотности $\rho_{XE}^{(\ell)}$. Под словами секретный ключ понимается секретность по определенному критерию. Одним из принятых критериев секретности является критерий, основанный на следовом расстоянии. По определению ключ является ε-секретным [4, 6, 7], если

$$||\rho_{XE}^{(\ell)} - \rho_U^{(\ell)} \otimes \rho_E^{(\ell)}||_1 \le \varepsilon, \tag{1}$$

$$\rho_U^{(\ell)} = \frac{1}{2^\ell} \sum_{x_1,x_2,\ldots,x_\ell=0,1} |x_1\rangle\langle x_1| \otimes |x_2\rangle\langle x_2| \ldots |x_\ell\rangle\langle x_\ell|,$$

$$\rho_E^{(\ell)} = \mathrm{Tr}_X\{\rho_{XE}^{(\ell)}\},$$

где $||\rho||_1 = (1/2)\mathrm{Tr}\{|\rho|\}$, $\rho_E^{(\ell)}$ — матрица плотности квантовой системы Евы после сжатия очищенных ключей.

Степень сжатия очищенного ключа определяется информацией Евы, которую она получила из

квантового канала связи при передаче квантовых состояний, и информацией из открытого классического канала при коррекции ошибок. Ранее было показано [4], что следовое расстояние (1) ограничено сверху [13]:

$$||\rho_{XE}^{(\ell)} - \rho_U^{(\ell)} \otimes \rho_E^{(\ell)}||_1 \le 2^{-\frac{1}{2}\left(H_2(\rho_{XE}^{(n)}|\rho_E^{(n)}C)-\ell\right)}, \quad (2)$$

где C — вся совокупность классической информации, используемой при коррекции ошибок, $H_2(\rho_{XE}^{(n)}|\rho_E^{(n)}C)$ — энтропия Реньи второго порядка [4], $\rho_E^{(n)}$ — матрица плотности квантовой системы Евы до коррекции ошибок.

Формула (2) предполагает, что матрица плотности $\rho_{XE}^{(n)}$ известна точно. Однако это не так. Во-первых, нужно знать, каким образом Ева проводит подслушивание передаваемых квантовых состояний. Говоря точнее, нужно знать оптимальную атаку Евы. Но даже зная оптимальную атаку, можно оценить матрицу плотности лишь с некоторой точностью. Для легитимных пользователей единственной величиной, из которой можно оценить матрицу плотности, является наблюдаемое число ошибок $\overline{k}$. Исходя из наблюдаемого числа ошибок можно оценить матрицу плотности лишь с некоторым разбросом. Под этими словами фактически понимается то, что точность определения матриц плотности фиксирует их некоторое множество. Можно гарантировать только то, что наблюдаемое число ошибок произошло от измерения матриц плотности из заданного множества с вероятностью не менее $1-\varepsilon_1$. Требуемая вероятность (точность) $1-\varepsilon_1$ задается легитимными пользователями.

Сглаженная минимальная энтропия содержит всю информацию об атаках Евы по определению [4], имеем

$$H_{min}^{\varepsilon_1}(\rho_{XE}^{(n)}|\rho_E^{(n)}) = \\ = \sup_{\{\overline{\rho}_{XE}^{(n)} \in \mathcal{B}^{\varepsilon_1}(\rho_{XE}^{(n)})\}} H_{min}(\overline{\rho}_{XE}^{(n)}|\overline{\rho}_E^{(n)}). \quad (3)$$

Здесь $\overline{\rho}_{XE}^{(n)}$ — множество матриц плотности, которые гарантируют, что при их измерении возникнет наблюдаемое число ошибок с вероятностью не менее $1-\varepsilon_1$.

Сглаженная максимальная энтропия напрямую связана с количеством ошибок на приемной стороне и дает минимальное число битов, которые требуются для исправления ошибок с вероятностью успеха не менее $1-\varepsilon_1$. По определению [4]

$$H_{max}^{\varepsilon_1}(\rho_{XE}^{(n)}|\rho_E^{(n)}) = \\ = \inf_{\{\overline{\rho}_{XE}^{(n)} \in \mathcal{B}^{\varepsilon_1}(\rho_{XE}^{(n)})\}} H_{max}(\overline{\rho}_{XE}^{(n)}|\overline{\rho}_E^{(n)}), \quad (4)$$

где верхняя и нижняя грани берутся по матрицам плотности ε_1, близким в смысле следового расстояния, а $\overline{\rho}_{XE}^{(n)} \in \mathcal{B}^{\varepsilon_1}(\rho_{XE}^{(n)})$ означает, что $||\rho_{XE}^{(n)} - \overline{\rho}_{XE}^{(n)}||_1 < \varepsilon_1$.

Далее, с учетом (3), используя цепочку неравенств [4], имеем

$$H_2(\rho_{XE}^{(n)}|\rho_E^{(n)}C) \ge H_{min}^{\varepsilon_1}(\rho_{XE}^{(n)}|\rho_E^{(n)}C) \ge \\ \ge H_{min}^{\varepsilon_1}(\rho_{XE}^{(n)}|\rho_E^{(n)}) - \mathrm{leak}_n. \quad (5)$$

Фактически это означает, что на матрице плотности $\rho_{XE}^{(n)}$ достигается максимум, а так как пространство конечномерное и компактное, то $H_{min}^{\varepsilon_1}(\rho_{XE}^{(n)}|\rho_E^{(n)}) = H_{min}(\rho_{XE}^{(n)}|\rho_E^{(n)})$. Далее, C — вся совокупность классической информации, используемой при коррекции ошибок, где $\mathrm{leak}_n = \log|C|$ — информация в битах, выдаваемая через открытый канал при коррекции ошибок; здесь и везде ниже $\log \equiv \log_2$. Если включить в утечку информацию для проверки идентичности очищенных ключей Алисы и Боба, то выражение для leak_n заменяется на

$$\mathrm{leak}_n = \log|C| + \log(2^M) = \log|C| + M.$$

Такое выражение для leak_n имеет место, если идентичность ключей проверяется следующим образом. Алиса и Боб умножают по модулю 2 очищенный ключ со случайной битовой строкой, которая оглашается через открытый канал связи. Вычисляют и сравнивают биты четности своих результирующих строк. Если бит четности совпадает, то процедура повторяется M раз. Если биты четности на каждом шаге совпадают, то с вероятностью $1-2^{-M}$ исходные очищенные ключи Алисы и Боба совпадают. В противном случае ключ отбрасывается. Такая процедура выдает подслушивателю M дополнительных битов информации, которые необходимо учесть при сжатии очищенного ключа.

Далее, с учетом (2), (5) несложно перейти от энтропии Реньи второго рода к минимальной энтропии (см. подробности [4], разд. 5.6). Имеем

$$||\rho_{XE}^{(\ell)} - \rho_U^{(\ell)} \otimes \rho_E^{(\ell)}||_1 \le \varepsilon = \\ = \varepsilon_1 + 2^{-\frac{1}{2}\left(H_{min}^{\varepsilon_1}(\rho_{XE}^{(n)}|\rho_E^{(n)})-\mathrm{leak}_n-\ell\right)}. \quad (6)$$

Если длина секретного ключа ℓ выбрана равной

$$\ell \le H_{min}^{\varepsilon_1}(\rho_{XE}^{(n)}|\rho_E^{(n)}) - \mathrm{leak}_n - \log\left(\frac{1}{\varepsilon_1}\right), \\ \varepsilon_1 = \frac{\varepsilon}{2}, \quad (7)$$

то выполнен критерий (1), ключ является ε-секретным. Однако приведенные выше соотношения не избавляют от необходимости знать $\rho_{XE}^{(n)}$, т. е. требуется знание оптимальной атаки.

Энтропийные соотношения неопределенностей избавляют от явного нахождения оптимальной атаки, но не избавляют от необходимости знать саму матрицу плотности $\rho_{XE}^{(n)}$. Вместо этого требуется знание другой матрицы плотности, которую нужно оценить из наблюдаемого числа ошибок.

Нижнюю границу для $H_{min}^{\varepsilon_1}(\rho_{XE}^{(n)}|\rho_E^{(n)})$ можно получить, исходя только из числа ошибок на приемной стороне, используя энтропийные соотношения неопределенностей [10]:

$$\begin{aligned} &H_{min}^{\varepsilon_1}(\rho_{XE}^{(n)}|\rho_E^{(n)}) + H_{max}^{\varepsilon_1}(\rho_{XY}^{(n)}|\rho_Y^{(n)}) \geq 1 \cdot n, \\ &\rho_{XY}^{(n)} = \mathrm{Tr}_E\{\rho_{XYE}^{(n)}\}, \quad \rho_Y^{(n)} = \mathrm{Tr}_{XE}\{\rho_{XYE}^{(n)}\}, \end{aligned} \tag{8}$$

где $\rho_{XYE}^{(n)}$ — совместная матрица плотности Алиса–Боб–Ева до коррекции ошибок, $\rho_{XY}^{(n)}$ — матрица плотности Алиса–Боб. Битовая строка Боба содержит ошибки $y \in Y = \{0,1\}^n$. Данные соотношения применимы только для протокола BB84 в однофотонном случае и, к сожалению, не переносятся на другие протоколы.

Оценка $H_{min}^{\varepsilon_1}(\rho_{XE}^{(n)}|\rho_E^{(n)})$ может быть получена через $H_{max}^{\varepsilon_1}(\rho_{XY}^{(n)}|\rho_Y^{(n)})$ с использованием (8). Для вычисления $H_{max}^{\varepsilon_1}(\rho_{XY}^{(n)}|\rho_Y^{(n)})$ требуется знать матрицу плотности $\rho_{XY}^{(n)}$. Если известна матрица плотности, то можно вычислить вероятность появления $\overline{k}$ ошибок на приемной стороне. Однако матрица $\rho_{XY}^{(n)}$ неизвестна и оценку матрицы плотности можно сделать только через наблюдаемое число ошибок $\overline{k}$.

Даже точное знание числа ошибок в конкретной серии не дает точного вида $\rho_{XY}^{(n)}$. Задача напоминает замкнутый круг. Чтобы оценить вероятность того, что произойдет случайное событие с $\overline{k}$ ошибками на приемной стороне, нужно знать матрицу плотности $\rho_{XY}^{(n)}$. С другой стороны, данную матрицу плотности неоткуда взять, кроме как оценить ее через наблюдаемое число ошибок $\overline{k}$.

Тем не менее, данные оценки можно сделать, используя сглаженные минимальную и максимальную энтропии. Методы математической статистики позволяют сделать однородные оценки, а именно, предсказать вероятность того, что данное число ошибок произошло из матриц плотности из определенного класса.

Как увидим ниже, матрицы плотности полностью определяются одним параметром Q, который имеет смысл истинной вероятности ошибки на приемной стороне и неизвестен Алисе и Бобу. Имея наблюдаемое число ошибок $\overline{k}$ на приемной стороне, Алиса и Боб могут выбрать параметр Q, который определяет матрицу плотности $\rho_{XY}^{(n)}$. Сам параметр Q определяется наблюдаемой ошибкой $\overline{k}$ ($Q = \overline{k}/n + \delta$, δ — ширина доверительного интервала) и гарантирует, что матрицы плотности с таким параметром приведут к наблюдаемой ошибке с вероятностью не менее $1-\varepsilon_{\delta,n}$. Вероятность уже не зависит от наблюдаемой ошибки $\overline{k}$, а зависит только от расстояния между параметром Q и наблюдаемой ошибкой $\overline{k}$.

По этой причине удобнее будет воспользоваться другим определением минимальной и максимальной энтропий (см., например, [14]), которое, по сути, эквивалентно (3) и (4), но имеет боле прозрачную интерпретацию и более удобно при вычислениях. А именно, sup и inf в (3), (4) вычисляются по матрицам плотности, которые дают наблюдаемое число ошибок с вероятностью не менее $1 - \varepsilon_1$.

Далее, для прямого вычисления сглаженной минимальной энтропии в (3) требуется тем не менее знать структуру матрицы плотности $\rho_{XE}^{(n)}$. Ниже будет показано, что граница энтропийных соотношений неопределенностей достигается на матрицах плотности, имеющих структуру тензорного произведения, т. е. $\rho_{XE}^{(n)} = \rho_{XE}^{\otimes n}(Q)$, причем $\rho_{XE}^{\otimes n}(Q)$ параметризуется только одним параметром Q, имеющим смысл истинной вероятности ошибки на приемной стороне. Достижение нижней границы энтропийных соотношений неопределенностей будет гарантировать оптимальность атаки Евы.

1.2. Классическая бернуллиевская схема

Удобно рассмотреть следующую бернуллиевскую схему — подбрасывание несимметричной монеты. В дальнейшем увидим, что ситуация на приемной стороне выглядит как схема с бернуллиевскими испытаниями. Боб может получить правильный отсчет или ошибочный. По наблюдаемому числу ошибок требуется оценить истинную вероятность ошибки Q, а затем получить по ней оценку для минимальной и максимальной сглаженных энтропий. Рассмотрим две ситуации.

1. Истинный параметр Q неизвестен, требуется оценить Q, имея наблюдаемое число ошибок $\overline{k}$.

2. Параметр Q известен, требуется оценить вероятность появления $\overline{k}$ ошибок, точнее, что $\overline{k}$ лежит в определенном диапазоне.

Эти две ситуации являются в некотором смысле дуальными.

Применительно к квантовой криптографии возникают обе ситуации. Первая ситуация: получен сырой ключ с наблюдаемым числом ошибок $\overline{k}$, требуется оценка параметра истинной вероятности ошибки Q. Вторая ситуация: оценка параметра Q должна гарантировать, что любая матрица плотности с параметром Q из доверительного интервала будет приводить к появлению $\overline{k}/n \in [Q-\delta, Q+\delta]$ ошибок с вероятностью не менее $1-\varepsilon_{\delta,n}$. Именно по этим матрицам плотности будет проводиться сглаживание в минимуме энтропии.

Математическая статистика позволяет получить однородные оценки для истинной вероятности ошибки Q, а именно, известная оценка [15] дает

$$\Pr\{|Q-\overline{Q}| \le \delta\} > 1-\varepsilon_{\delta,n} = 1-2e^{-2\delta^2 n}, \quad (9)$$

где $\varepsilon_{\delta,n}$ не зависит от наблюдаемой частоты ошибок $\overline{Q}=\overline{k}/n$, а зависит только от точности δ — ширины доверительного интервала и длины последовательности n [15].

Пусть параметр Q известен, требуется оценить вероятность появления $\overline{k}/n \in [Q-\delta, Q+\delta]$ ошибочных исходов. Зная истинный параметр бернуллиевского распределения Q, можно получить довольно точные оценки, но при этом вероятность числа ошибочных исходов $\overline{k}$ будет зависеть от самого параметра Q (см., например, [16, 17]). Нам же потребуются однородные оценки, когда вероятность не зависит от Q.

Однородность оценки обеспечивает следующее.

Пусть наблюдаемое число ошибок $\overline{k}$. Если в качестве оценки параметра Q взято значение из отрезка $Q \in [\overline{Q}-\delta, \overline{Q}+\delta]$, то это будет гарантировать, что измерения над матрицами плотности с таким параметром приведут к появлению числа ошибок из интервала $[Q-\delta, Q+\delta]$ с вероятностью не менее $1-\varepsilon_{\delta,n}$. Соответственно, вероятность появления числа ошибок вне интервала $[Q-\delta, Q+\delta]$ будет иметь место с вероятностью не более $\varepsilon_{\delta,n}$.

2. ПРЕДЛАГАЕМЫЙ ПОДХОД

Наш подход будет состоять в следующем.

1. Сначала покажем, что граница энтропийных соотношений достигается на определенном классе оптимальных в асимптотическом пределе атак подслушивателя на передаваемые квантовые состояния. Все атаки параметризуются одним параметром Q, который имеет смысл истинной вероятности ошибки на приемной стороне. Подслушиватель атакует унитарно каждое передаваемое состояние с использованием вспомогательного квантового состояния ancilla, которое запутывается с передаваемым состоянием. Искаженное состояние ancilla сохраняется в квантовой памяти подслушивателя до самой последней стадии протокола. Легитимные пользователи проводят коррекцию ошибок, затем усиление секретности очищенных ключей. После этого Ева проводит коллективные измерения над всей квантовой памятью. Соотношения неопределенностей минимизируются при любом значении параметра Q, что гарантирует оптимальность атаки, т. е. максимум информации подслушивателя при данной наблюдаемой ошибке на приемной стороне. Данный параметр находится у Евы и неизвестен Алисе и Бобу.

2. Данная оптимальная атака приводит к бернуллиевской схеме испытаний (измерений) на приемной стороне. Вероятность наблюдаемого числа ошибок $\overline{k}$ на приемной стороне в серии измерений длины n определяется вероятностью истинной ошибки Q.

3. Зная наблюдаемое число ошибок $\overline{k}$ на приемной стороне и тот факт, что ошибки произошли из биномиального распределения — бернуллиевских испытаний, Алиса и Боб могут получить оценку параметра Q. После этой стадии Алиса и Боб имеют оценку вероятности ошибки Q с точностью до ширины доверительного интервала $Q \in [\overline{k}/n-\delta, \overline{k}/n+\delta]$. Ширина доверительного интервала δ выбирается Алисой и Бобом. Фиксация ширины доверительного интервала δ гарантирует, что вероятность события с $\overline{k}/n \in [Q-\delta, Q+\delta]$ ошибками не менее $1-\varepsilon_{\delta,n}$. Соответственно, вероятность появления большего (или меньшего) числа ошибок будет не более $\varepsilon_{\delta,n}$. Имеем [15]

$$\Pr\left\{\left|\frac{\overline{k}}{n}-Q\right| \le \delta\right\} > 1-\varepsilon_{\delta,n}. \quad (10)$$

4. Знание оценки вероятности ошибки позволяет в явном виде вычислить сглаженную минимальную энтропию $H_{min}^{\varepsilon_{\delta,n}}\left(\rho_{XE}^{\otimes n}(Q)|\rho_E^{\otimes n}(Q)\right)$ и, соответственно, длину ключа, который будет $\varepsilon_{\delta,n}$-секретным.

Минимальная энтропия вычисляется по тем матрицам плотности, которые с вероятностью не менее $1-\varepsilon_{\delta,n}$ гарантируют появление $\overline{k}/n \in [Q-\delta, Q+\delta]$ ошибок, имеем

$$H_{min}^{\varepsilon_{\delta,n}}\left(\rho_{XE}^{\otimes n}(Q)|\rho_E^{\otimes n}(Q)\right) = \\ = \sup_{\left\{\overline{\rho}_{XE}(Q):\left|Q-\frac{\overline{k}}{n}\right|\le\delta\right\}} H_{min}(\overline{\rho}_{XE}^{\otimes n}(Q)|\overline{\rho}_E^{\otimes n}(Q)). \quad (11)$$

При этом матрицы плотности $\overline{\rho}_{XE}(Q)$ могут быть вычислены явно (см. ниже), и sup в (11) вычисляется по матрицам плотности с бернуллиевским распре-

делением, параметр Q которых при заданном наблюдаемом числе ошибок $\overline{k}$ удовлетворяет неравенству $|Q-\overline{k}/n|\le\delta$.

Аналогично может быть явно вычислена сглаженная максимальная энтропия:

$$H_{max}^{\varepsilon_{\delta,n}}\left(\rho_{XE}^{\otimes n}(Q)|\rho_E^{\otimes n}(Q)\right)= \\ =\inf_{\left\{\overline{\rho}_{XE}(Q):\left|Q-\frac{\overline{k}}{n}\right|\le\delta\right\}} H_{max}(\overline{\rho}_{XE}^{\otimes n}(Q)|\overline{\rho}_E^{\otimes n}(Q)). \quad (12)$$

Использование выражений (11), (12) для минимальной и максимальной энтропий позволяет получить $\varepsilon_{\delta,n}$-секретные ключи, а не $\sqrt{\varepsilon_{\delta,n}}$-секретные ключи, которые получаются, если пользоваться выражениями (3), (4) (см. также [6,7]). Это позволяет достичь нужного уровня секретности ключей при меньших длинах сырых ключей и, соответственно, увеличить скорость генерации секретных ключей.

3. УНИТАРНАЯ ИНДИВИДУАЛЬНАЯ АТАКА НА КВАНТОВЫЕ СОСТОЯНИЯ С ПОСЛЕДУЮЩИМИ КОЛЛЕКТИВНЫМИ ИЗМЕРЕНИЯМИ

Оптимальная атака сводится к атаке Евой каждого передаваемого состояния с использованием вспомогательного состояния, которое сохраняется в квантовой памяти до конца протокола, а затем проводятся коллективные измерения над всеми квантовыми состояниями в квантовой памяти. Параметр Q имеет смысл истинной вероятности ошибки на приемной стороне. При этом нижняя граница соотношений неопределенностей достигается не для одной атаки, а для каждой из бесконечного числа однотипных атак, которые параметризуются разными параметрами Q. Данный параметр однозначно определяет матрицы плотности $\rho_{XYE}^{(n)}$, для которых получаются явные аналитические выражения.

Будет показано, что результаты измерений Боба выглядят как бернуллиевские испытания с неизвестным параметром Q (см. формулу (20) ниже). Для подслушивателя задача также выглядит как бернуллиевская схема — «подбрасывание монетки» с квантовыми состояниями, где в каждой посылке у Евы «выпадает» одно из квантовых состояний, которое однозначно определяется исходом измерений у Боба. Информационные состояния Алисы в прямом (символ +) и сопряженном (символ ×) базисах имеют вид

$$|0^+\rangle=\frac{|0\rangle+|1\rangle}{\sqrt{2}},\quad |1^+\rangle=\frac{|0\rangle-|1\rangle}{\sqrt{2}},\quad \text{базис } +; \\ |0^\times\rangle=\frac{|0\rangle+i|1\rangle}{\sqrt{2}},\quad |1^\times\rangle=\frac{|0\rangle-i|1\rangle}{\sqrt{2}},\quad \text{базис } \times. \quad (13)$$

Алиса в каждой посылке i из n посылок посылает состояние $|x_i\rangle_B$ ($x_i=0,1$) к Бобу, себе оставляет копию $|x_i\rangle_A$. Подслушиватель унитарно атакует каждую посылку:

$$U_{BE}(Q)\left(|0^+\rangle_A\otimes|0^+\rangle_B\otimes|E\rangle_E\right)= \\ =|0^+\rangle_A\otimes|\Psi_Q^{0^+}\rangle_{BE}= \\ =|0^+\rangle_A\otimes\left(\sqrt{1-Q}|0^+\rangle_B\otimes|\Phi_Q^{0^+}\rangle_E+\right. \\ \left.+\sqrt{Q}|1^+\rangle_B\otimes|\Theta_Q^{0^+}\rangle_E\right). \quad (14)$$

Аналогично для состояния $|1^+\rangle_A$:

$$U_{BE}(Q)\left(|1^+\rangle_A\otimes|1^+\rangle_B\otimes|E\rangle_E\right)= \\ =|1^+\rangle_A\otimes|\Psi_Q^{1^+}\rangle_{BE}= \\ =|1^+\rangle_A\otimes\left(\sqrt{1-Q}|1^+\rangle_B\otimes|\Phi_Q^{1^+}\rangle_E+\right. \\ \left.+\sqrt{Q}|0^+\rangle_B\otimes|\Theta_Q^{1^+}\rangle_E\right). \quad (15)$$

Аналогичные выражения можно записать для состояний в базисе ×. Вся информация об атаке Евы заключена в унитарном операторе $U_{BE}(Q)$, который регулируется Евой. Требования унитарности для оператора $U(Q)_{BE}$, которые фактически сводятся к сохранению скалярного произведения между разными информационными состояниями до и после атаки Евы, приводят к следующим соотношениям для искаженных состояний ancilla:

$${}_E\langle\Phi_Q^{(0,1)^{+,\times}}|\Theta_Q^{(0,1)^{+,\times}}\rangle_E=0,\quad {}_E\langle\Phi_Q^{0^+}|\Psi_Q^{1^\times}\rangle_E= \\ ={}_E\langle\Theta_Q^{0^+}|\Theta_Q^{1^\times}\rangle_E=\cos\phi=1-2Q. \quad (16)$$

Матрица плотности для одной посылки в базисе + (аналогично в базисе ×) имеет вид

$$\rho_{XBE}(Q)=\frac{1}{2}|0^+\rangle_A\langle 0^+|\otimes|\Psi_Q^{0^+}\rangle_{BE}\langle\Psi_Q^{0^+}|+ \\ +\frac{1}{2}|1^+\rangle_A\langle 1^+|\otimes|\Psi_Q^{1^+}\rangle_{BE}\langle\Psi_Q^{1^+}|. \quad (17)$$

4. КВАНТОВОЕ РАСПРЕДЕЛЕНИЕ КЛЮЧЕЙ КАК БЕРНУЛЛИЕВСКАЯ СХЕМА ИСПЫТАНИЙ

Покажем, что оптимальная атака приводит к биномиальному распределению ошибок на приемной

стороне, что отвечает бернуллиевской схеме испытаний (см. формулы (20), (23) ниже). Действительно, из (17) с учетом (14), (15) получаем частичные матрицы плотности:

$$\rho_{XB}(Q) = \frac{1}{2}(1-Q)|0^+\rangle_X\langle 0^+| \otimes |0^+\rangle_B\langle 0^+| + \\ + \frac{1}{2}Q|0^+\rangle_X\langle 0^+| \otimes |1^+\rangle_B\langle 1^+| + \\ + \frac{1}{2}(1-Q)|1^+\rangle_X\langle 1^+| \otimes |1^+\rangle_B\langle 1^+| + \\ + \frac{1}{2}Q|1^+\rangle_X\langle 1^+| \otimes |0^+\rangle_B\langle 0^+|. \quad (18)$$

Поскольку матрица плотности (18) имеет диагональный вид, при измерениях в прямом и сопряженном базисах сразу обозначим $\rho_{XB}(Q) \to \rho_{XY}(Q)$. Интерпретация (18) достаточно проста. Пусть измерения Боба происходят в согласованном базисе, например, в базисе +. В этом случае, если Алиса посылала 0, то Боб с вероятностью $1-Q$ получит правильный исход 0, а с вероятностью Q — неправильный исход 1. Аналогично, если Алиса посылала 1. В сопряженном базисе ситуация аналогичная.

Аналогично для Боба получаем

$$\rho_Y(Q) = (1-Q)\rho_{OK}(Q)_Y + Q\rho_{\overline{OK}}(Q)_Y = \\ = \frac{1}{2}(1-Q)\left(\rho^{0^+}(y_B=0|x_A=0) + \right. \\ \left. + \rho^{1^+}(y_B=1|x_A=1)\right) + \\ + \frac{1}{2}Q\left(\rho^{0^+}(y_B=0|x_A=1) + \right. \\ \left. + \rho^{1^+}(y_B=1|x_A=0)\right), \quad (19)$$

$$\rho_Y(Q)^{\otimes n} = \sum_{m=0}^{n} C_n^m (1-Q)^{n-m} Q^m \rho_{OK}(Q)_Y^{\otimes(n-m)} \times \\ \times \rho_{\overline{OK}}(Q)_Y^{\otimes m}, \quad C_n^m = \frac{n!}{m!(n-m)!}, \quad (20)$$

где

$$\rho_{OK}(Q)_Y = \\ = \frac{1}{2}\left(\rho^{0^+}(y_B=0|x_A=0) + \rho^{1^+}(y_B=1|x_A=1)\right),$$

$$\rho_{\overline{OK}}(Q)_Y = \\ = \frac{1}{2}\left(\rho^{0^+}(y_B=0|x_A=1) + \rho^{1^+}(y_B=1|x_A=0)\right).$$

Матрица плотности (17) отвечает бернуллиевским испытаниям. Неформально это означает, что в сыром ключе Боба в каждой конкретной серии могут произойти $0 \le \overline{k} \le n$ ошибок, но с разной вероятностью, которая определяется биномиальными коэффициентами и неизвестным для Боба параметром Q.

Если выделить те посылки, где Алиса посылала 0, то ситуация на приемной стороне будет выглядеть как подбрасывание несимметричной монеты: с вероятностью $1-Q$ выпадает 0 — правильный отсчет, а с вероятностью Q выпадает 1 — ошибочный отсчет. Аналогично для посылок, когда Алиса посылала 1.

Биномиальные коэффициенты в сумме (20) дают явные выражения для вероятности m ошибочных отсчетов в последовательности длины n, где $0 \le m \le n$, (на приемной стороне этим отсчетам отвечает матрица плотности $\rho_{\overline{OK}}(Q)_B$) и $n-m$ правильных отсчетов (на приемной стороне этой ситуации отвечает матрица плотности $\rho_{OK}(Q)_B$).

Параметр Q Бобу неизвестен и подлежит оценке по наблюдаемому числу ошибок в данной последовательности.

Ошибочные или правильные отсчеты на приемной стороне однозначно связаны с квантовыми состояниями, которые возникают у подслушивателя после измерений Боба. Действительно, матрица плотности Алиса–Ева с учетом (17) имеет вид

$$\rho_{XE}(Q) = \frac{1}{2}|0^+\rangle_X\langle 0^+| \otimes \\ \otimes \left((1-Q)\rho_E^{0^+}(x_B=0) + Q\rho_E^{0^+}(x_B=1)\right) + \\ + \frac{1}{2}|1^+\rangle_X\langle 1^+| \otimes \left((1-Q)\rho_E^{1^+}(x_B=1) + \right. \\ \left. + Q\rho_E^{1^+}(x_B=0)\right). \quad (21)$$

Частичная матрица плотности Евы имеет вид

$$\rho_E(Q) = (1-Q)\rho_{OK}(Q)_E + Q\rho_{\overline{OK}}(Q)_E = \\ = \frac{1}{2}(1-Q)\left(\rho_E^{0^+}(x_B=0) + \rho_E^{1^+}(x_B=1)\right) + \\ + \frac{1}{2}Q\left(\rho_E^{0^+}(x_B=1) + \rho_E^{1^+}(x_B=0)\right). \quad (22)$$

Матрица плотности Евы, по сути, отвечает бернуллиевской схеме испытаний с квантовыми состояниями:

$$\rho_E(Q)^{\otimes n} = \sum_{m=0}^{n} C_n^m (1-Q)^{n-m} Q^m \times \\ \times \rho_{OK}(Q)_E^{\otimes(n-m)} \rho_{\overline{OK}}(Q)_E^{\otimes m}. \quad (23)$$

Если Боб получил правильный отсчет, то у Евы возникает квантовое состояние $\rho_{OK}(Q)_E$ (22). Если Боб получил ошибочный отсчет, то у Евы возникает квантовое состояние $\rho_{\overline{OK}}(Q)_E$ (22). При этом число

квантовых состояний $\rho_{OK}(Q)_E$ и $\rho_{\overline{OK}}(Q)_E$ в последовательности из n позиций, а также их размещение по позициям однозначно связаны с результатами измерений Боба. Если Боб получил правильный результат 0 с вероятностью $1-Q$, то Ева получит состояние $\rho_E^{0^+}(x_B=0)$. Соответственно, если Боб получил правильный отсчет 1 с вероятностью $1-Q$, то состояние Евы будет $\rho_E^{1^+}(x_B=1)$.

Далее, если у Боба возник с вероятностью Q неправильный результат (1 вместо 0), то в распоряжении Евы оказывается состояние $\rho_E^{0^+}(x_B=1)$. Аналогично, если у Боба неверный отсчет с вероятностью Q (0 вместо 1), то у Евы будет состояние $\rho_E^{1^+}(x_B=0)$.

Таким образом, описанная выше атака имеет прозрачную интерпретацию. Согласно (20) и (23) в каждой конкретной серии испытаний длины n у Боба на приемной стороне имеется $\overline{k}$ $(0\le\overline{k}\le n)$ ошибок, которые возникают из бернуллиевской схемы испытаний с некоторым параметром Q.

У Евы имеется последовательность длины n квантовых состояний: $n-\overline{k}$ состояний $\rho_{OK}(Q)_E$, отвечающих правильным отсчетам у Боба, и $\overline{k}$ состояний $\overline{\rho}_{OK}(Q)_E$, отвечающих ошибочным отсчетам у Боба. При этом имеется точное соответствие в каждой позиции правильных и неправильных отсчетов у Боба и квантовых состояний у Евы.

Ниже будет видно, что такое семейство атак при любом Q минимизирует энтропийные соотношения неопределенностей, что гарантирует оптимальность такой атаки.

5. ЭНТРОПИЙНЫЕ СООТНОШЕНИЯ НЕОПРЕДЕЛЕННОСТЕЙ

Энтропийные соотношения неопределенностей имеют фундаментальный характер для квантовой криптографии, поскольку позволяют связать верхнюю границу информации подслушивателя о ключе с количеством ошибок на приемной стороне, не прибегая к перебору всевозможных атак. При этом соотношения неопределенностей не дают ответа на вопрос, существует ли конструктивная атака подслушивателя, на которой достигается минимум соотношений неопределенностей, или энтропийные соотношения неопределенностей играют роль теоремы существования для оптимальной атаки.

Явное построение такой атаки позволяет глубже понять природу секретности ключей в квантовой криптографии и получить более простые, наглядные и точные оценки. Как было показано в предыдущем разделе, за энтропийными соотношениями неопределенности стоит схема с бернуллиевскими испытаниями.

При любом параметре Q, который параметризует атаку подслушивателя, имеет место соотношение

$$H^{\varepsilon}_{min}(\rho^{(n)}_{X^+E}|\rho^{(n)}_E)+H^{\varepsilon}_{max}(\rho^{(n)}_{X^+B^+}|\rho^{(n)}_{B^+})\ge n\cdot q,\quad q=-\log(|\langle i^+|j^\times\rangle|^2)=1,\quad i,j=0,1, \tag{24}$$

где учтено, что

$$H^{\varepsilon}_{max}(\rho^{(n)}_{X^+B^+}|\rho^{(n)}_{B^+})=H^{\varepsilon}_{max}(\rho^{(n)}_{X^\times B^\times}|\rho^{(n)}_{B^\times}).$$

Далее индексы «+» и «×» в (24) опускаем. Используя выражения для минимальной и максимальной сглаженных энтропий в случае тензорного произведения (см. [4]), с учетом (18), (20) и (21), (23) получаем

$$H^{\varepsilon}_{min}(\rho_{XE}(Q)^{\otimes n}|\rho_E(Q)^{\otimes n})\ge n\,(H(\rho_{XE}(Q)|\rho_E(Q))-\delta_{\varepsilon,n})=n\,(1-h(Q)-\delta_{\varepsilon,n}), \tag{25}$$

$$H^{\varepsilon}_{max}(\rho_{XB}(Q)^{\otimes n}|\rho_B(Q)^{\otimes n})\le n\,(H(\rho_{XE}(Q)|\rho_E(Q))+\delta_{\varepsilon,n})=n\,(h(Q)+\delta_{\varepsilon,n}), \tag{26}$$

где $\delta_{\varepsilon,n}=\text{const}\cdot\sqrt{\log(1/\varepsilon)/n}$, $\text{const}=\sqrt{5}$ [4]. Из соотношений следует, что матрицы плотности (20), (21) и (26) в асимптотическом пределе минимизируют энтропийные соотношения неопределенностей. Напомним, что параметр Q имеет смысл истинной вероятности ошибки на приемной стороне.

В асимптотическом пределе длинных последовательностей $n\to\infty$, $\varepsilon\to 0$ параметр Q известен точно. С учетом (19), (20) и (21)–(23) получаем известный классический результат (см., например, [2]):

$$\ell\to n(1-2h(Q)).$$

В асимптотическом пределе длинных последовательностей длина секретного ключа обращается в нуль при критической ошибке (истинном значении параметра Q), определяемой равенством $1=2h(Q_c)$ и равной $Q_c\approx 11\,\%$.

6. ДОВЕРИТЕЛЬНЫЙ ИНТЕРВАЛ ДЛЯ ОЦЕНКИ ВЕРОЯТНОСТИ ОШИБКИ

Единственной случайной наблюдаемой величиной является число ошибок $\overline{k}$ на приемной стороне,

которые произошли из бернуллиевского распределения (21) с некоторым точно неизвестным Q. Цель — определить Q.

Данному вопросу посвящена обширная литература (см., например, [17], компактный обзор по различным неравенствам для вероятностей «хвостов» распределений содержится в [16, 17]). Удобно, следуя [18], ввести верхнюю и нижнюю границы доверительного интервала:

$$L = L_{\overline{k},n,\varepsilon} = \begin{cases} 0, & \overline{k} = 0, \\ \underline{Q}, & \overline{k} \geq 0, \end{cases}$$
$$U = U_{\overline{k},n,\varepsilon} = \begin{cases} 1, & \overline{k} = n, \\ \overline{Q}, & \overline{k} \leq n. \end{cases} \tag{27}$$

Единственной случайной величиной является наблюдаемое число ошибок $\overline{k}$, поэтому и доверительный интервал, привязанный к своей центральной точке $\overline{k}$, также имеет случайное положение. Оценка истинного значения параметра Q бернуллиевского распределения не является случайной величиной. Вероятность $1-\varepsilon$ того, что доверительный интервал $L \leq Q \leq U$ накроет значение параметра Q, определяется как решение пары трансцендентных уравнений [18]

$$\sum_{m=0}^{\overline{k}-1} C_n^m (1-\underline{Q})^{n-m} \underline{Q}^m = 1 - \frac{\varepsilon}{2},$$
$$\sum_{m=0}^{\overline{k}} C_n^m (1-\overline{Q})^{n-m} \overline{Q}^m = \frac{\varepsilon}{2}, \tag{28}$$

которые практически невозможно вычислить.

Параметр Q не является случайной величиной, но неизвестен легитимным пользователям[2)]. Вероятность накрытия истинного значения параметра доверительным интервалом $[L, U]$ есть

$$\Pr\{L \leq Q \leq U\} > 1 - \varepsilon. \tag{29}$$

Точное аналитическое решение данной задачи до конца неизвестно. Хотя решение может быть получено численно, удобнее воспользоваться приближенными методами.

[2)] Отметим, что вероятность накрытия относится к интервалу, а не к параметру Q, который не является случайной величиной. Существует несколько интерпретаций доверительного интервала. Нам данные интерпретации не слишком важны, поскольку для дальнейшего требуется лишь следующее: вероятность того, что наблюдаемое число ошибок $\overline{k}/n \in \in [Q-\delta, Q+\delta]$ будет иметь место с вероятностью не менее $\varepsilon_{\delta,n}$, см. (10) и комментарии.

Аналитические выражения для более точных оценок вероятностей «хвостов» бернуллиевского распределения можно найти в работе [16]. Однако в случае более точных и плотных оценок вероятность накрытия доверительным интервалом параметра распределения зависит от самого параметра, что в нашем случае неприемлемо, поскольку требуются однородные оценки, когда вероятность не зависит от неизвестного параметра распределения.

Часто для практических оценок пользуются нормальным приближением [17], но при этом оценка вероятности также зависит от Q,

$$\Pr\left\{\left|\frac{\overline{k}}{n} - Q\right| \leq \delta\right\} > 2\Phi\left(\delta\sqrt{\frac{n}{\overline{Q}(1-\overline{Q})}}\right) - 1 = 1 - \varepsilon_{\delta,n}, \quad \overline{Q} = \frac{\overline{k}}{n}, \tag{30}$$

где функция ошибок

$$\Phi(z) = \frac{1}{\sqrt{2\pi}} \int_{-\infty}^{z} e^{-t^2/2}\, dt.$$

Правая часть (30) (параметр секретности $\varepsilon_{\delta,n}$) зависит от величины наблюдаемой ошибки $\overline{Q} = \overline{k}/n$. Наиболее подходящей является оценка [15], имеем

$$\Pr\left\{\left|\frac{\overline{k}}{n} - Q\right| \leq \delta\right\} > 1 - \varepsilon_{\delta,n}, \quad \varepsilon_{\delta,n} = 2e^{-2\delta^2 n}. \tag{31}$$

7. ВЫЧИСЛЕНИЕ МИНИМАЛЬНОЙ ЭНТРОПИИ И СТАТИСТИЧЕСКАЯ ИНТЕРПРЕТАЦИЯ ДОВЕРИТЕЛЬНОГО ИНТЕРВАЛА ДЛЯ ОЦЕНКИ ВЕРОЯТНОСТИ ОШИБКИ

Воспользуемся статистической интерпретацией (31) применительно к матрицам плотности. Вычисление минимальной энтропии $H_{min}^{\varepsilon_{\delta,n}}(\rho_{XE}^{\otimes n}(Q)|\rho_E^{\otimes n}(Q))$ согласно (11), (12) подразумевает минимизацию по матрицам плотности, которые дают наблюдаемое число ошибок на приемной стороне $\overline{k}/n \in \in [Q-\delta, Q+\delta]$ с вероятностью не менее $1-\varepsilon_{\delta,n}$. Соответственно, вероятность того, что наблюдаемое число ошибок выйдет из $\overline{k}/n \overline{\in} [Q-\delta, Q+\delta]$, будет не более $\varepsilon_{\delta,n}$.

Между матрицей плотности на приемной стороне у Боба (20) и матрицей плотности у Евы (23) имеется точное соответствие, они параметризуются одним параметром Q и отвечают бернуллиевским испытаниям, поэтому вероятность появления $\overline{k}/n \in \in [Q-\delta, Q+\delta]$ ошибок однозначно определяется параметром Q. Вычисление минимальной энтропии в

(11) проводится по тем матрицам плотности, для которых параметр Q накрывается доверительным интервалом в (31). С учетом сказанного имеем

$$H_{min}^{\varepsilon_{\delta,n}}(\rho_{XE}^{\otimes n}(Q)|\rho_E^{\otimes n}(Q)) = \\ = \sup_{\{\overline{\rho}_{XE}(Q):Q\in[\overline{Q}-\delta,\overline{Q}+\delta]\}} \times \\ \times H_{min}(\overline{\rho}_{XE}^{\otimes n}(Q)|\overline{\rho}_E^{\otimes n}(Q)). \quad (32)$$

Фактически это означает, что любая матрица плотности с параметром Q из доверительного интервала даст наблюдаемое число ошибок $\overline{k}/n \in [Q-\delta, Q+\delta]$ с вероятностью не менее $1-\varepsilon_{\delta,n}$. В этом месте принципиально важна однородная оценка параметра Q — независимость вероятности от наблюдаемого числа ошибок $\overline{k}$. Соответственно в обратную сторону однородность оценки обеспечивает то, что вероятность появления $\overline{k}$ ошибок из интервала $\overline{k}/n \in [Q-\delta, Q+\delta]$ зависит только от его ширины. Аналогичная ситуация имеет место для максимальной энтропии.

Для бернуллиевской схемы испытаний любая матрица плотности $\rho_{XE}^{\otimes n}(Q)$ с параметром $Q \in \in [\overline{k}/n-\delta, \overline{k}/n+\delta]$ даст наблюдаемое число ошибок из интервала $[Q-\delta, Q+\delta]$ с вероятностью не менее $1-\varepsilon_{\delta,n}$. Поэтому при вычислении минимальной энтропии в (11) можно воспользоваться сразу оценкой для сглаженной минимальной энтропии. Консервативно считаем, что параметр Q лежит на верхней границе доверительного интервала $Q = \overline{k}/n + \delta$.

Поскольку матрицы плотности из этого множества имеют структуру тензорного произведения, в этом случае для сглаженной минимальной энтропии от тензорного произведения имеет место неравенство (см. детали в [4])

$$H_{min}^{\varepsilon_{\delta,n}}(\rho_{XE}^{\otimes n}(Q)|\rho_E^{\otimes n}(Q)) \geq \\ \geq n\left(H(\rho_{XE}(Q)|\rho_E(Q)) - \text{const}\sqrt{\frac{\log(1/\varepsilon_{\delta,n})}{n}}\right) = \\ = n\left(H(\rho_{XE}(Q)) - H(\rho_E(Q)) - \right. \\ \left. - \text{const}\sqrt{\frac{\log(1/\varepsilon_{\delta,n})}{n}}\right). \quad (33)$$

С учетом явных выражений для матриц плотности (17) и (23) находим

$$H_{min}^{\varepsilon_{\delta,n}}(\rho_{XE}^{\otimes n}(Q)|\rho_E^{\otimes n}(Q)) \geq \\ \geq n\left(1 - h(Q) - \text{const}\sqrt{\frac{\log(1/\varepsilon_{\delta,n})}{n}}\right), \quad (34)$$

где оценка вероятности ошибки $Q = \overline{k}/n + \delta$. Все функции в (33), (34) выражаются через наблюдаемое число ошибок $\overline{k}$ и величину доверительного интервала δ, которая выбирается легитимными пользователями.

8. ДЛИНА СЕКРЕТНОГО КЛЮЧА И НЕКОТОРЫЕ ЧИСЛЕННЫЕ ОЦЕНКИ

Реальная ситуация в эксперименте выглядит следующим образом. После посылки серии квантовых состояний, проведения измерений на приемной стороне и согласования базисов остается число зарегистрированных посылок n, которое в каждой серии разное. Пусть обнаружено $\overline{k}$ ошибок. Требуется получить $\varepsilon_{\delta,n}$-секретный ключ. Данный параметр задается требованием к ключам извне. Если данный параметр фиксирован, то через него и n выражается ширина доверительного интервала δ (см. формулу (31)). Этот набор параметров определяет количество секретных битов ℓ, которое можно получить в серии. В каждой серии это число разное. Данное число битов можно использовать для ключа. Может оказаться, что при данном уровне ошибок $\overline{k}$ ключ получить нельзя, формально это будет приводить к тому, что $\ell < 0$. Финальная формула для длины секретного ключа автоматически «следит» за такими ситуациями.

Получим формулу для длины секретного ключа. С учетом (34), а также выражения $Q = \overline{k}/n + \delta$, для длины ключа ℓ получаем

$$\ell = n\,(1 - h(Q)) - \text{leak}_n - M - \\ - \text{const}\sqrt{n\log\left(\frac{1}{\varepsilon_{\delta,n}}\right)}. \quad (35)$$

Здесь, в отличие от формулы (6), число проверок на идентичность очищенных ключей M вынесено из leak_n.

Если ℓ удовлетворяет (35) и параметр секретности $\varepsilon_{\delta,n}$ выбран как $\varepsilon = \varepsilon_{\delta,n}/2$, то выполнен критерий (1) и ключ является ε-секретным.

Ниже в численных примерах для leak_n использовалось выражение $\text{leak}_n = nh(\overline{k}/n)$, что отвечает шенноновскому пределу по «расходу» информации на коррекцию $\overline{k}$ ошибок. Для реальных кодов величина leak_n изменяется в пределах $\text{leak}_n = \\ = n(1.2 \div 1.6)h(\overline{k}/n)$.

Явное построение оптимальной атаки подслушивателя позволяет непосредственно вычислить сглаженные как минимальную, так и максимальную энтропии, не прибегая к энтропийным соотношениям

неопределенностей, и получить более точные оценки для длины сырого ключа n, который требуется для достижения заданного уровня секретности, $\varepsilon_{\delta,n}$.

Все величины выражаются только через единственный наблюдаемый в каждой серии испытаний параметр $\overline{k}$ — наблюдаемое на приемной стороне число ошибок в последовательности длины n (сыром ключе), которое становится известным после коррекции ошибок (см. пояснения во Введении). Никакие последовательности ни при каком наблюдаемом числе ошибок $\overline{k}$ исходно не отбрасываются.

Выше ширина доверительного интервала выводилась через параметр секретности и длину серии. Возможно задание ширины доверительного интервала δ заранее. То есть *a priori* Алиса и Боб задают точность оценки истинной вероятности ошибки δ, также заранее задается финальный параметр секретности $\varepsilon_{\delta,n}$, который вычисляется при данных δ и n через вероятность того, что оценка Q накрывается доверительным интервалом, при этом имеет место неравенство

$$\Pr\left\{\frac{\overline{k}}{n}-\delta\le Q\le\frac{\overline{k}}{n}+\delta\right\}>1-\varepsilon_{\delta,n}.$$

Если не удается достичь при данных δ и n требуемой величины параметра секретности $\varepsilon_{\delta,n}$, то процесс прерывается. Если параметр секретности достижим, то вычисляется длина секретного ключа по формуле (35). Длина секретного ключа будет такой, какой окажется. Если секретный ключ не удается получить (формально это означает отрицательную длину), то процесс прерывается.

Таким образом, длина ключа выражается только через наблюдаемые величины.

1. $\overline{k}=n\cdot\overline{Q}$ — наблюдаемое число ошибок.

2. n — длина последовательности до очистки в совпадающих базисах.

3. Задается точность δ для оценки вероятности ошибки — величина доверительного интервала.

4. Параметр секретности ключей $\varepsilon_{\delta,n}$ задается заранее и функционально зависит от δ и n. При заданных δ и n требуемый параметр секретности $\varepsilon_{\delta,n}$ может оказаться недостижимым. Это означает, что из последовательности длины n при доверительном интервале, определяемом δ, нельзя получить $\varepsilon_{\delta,n}$-секретный ключ.

5. leak_n — число битов, израсходованных на чистку $\overline{k}$ ошибок в последовательности длины n, которое зависит от эффективности процедуры коррекции ошибок.

6. В формулу для длины финального ключа входит также параметр M — число итераций для проверки идентичности очищенных ключей Алисы и Боба.

Приведем для примера некоторые численные оценки. Пусть наблюдаемая частота ошибок $\overline{k}/n=\overline{Q}=0.05$, пусть параметр $\delta=0.025$, что составляет 50 % от $\overline{Q}$. Пусть требуемый параметр секретности $\varepsilon=10^{-10}$. Зависимости длины секретного ключа и параметра секретности от длины сырого ключа приведены на рис. *а,б* соответственно.

Как видно из рис. *б*, минимальная длина сырого ключа, при которой достижим заданный уровень секретности ключей равна, $n\approx1.84\cdot10^4$. При этом длина секретного ключа при минимальной длине сырого ключа, на которой достигается требуемый уровень секретности, равна $\ell\approx2.118\cdot10^3$. Если частота ошибок $\overline{k}/n=\overline{Q}=0.05$ оценивается с точностью 20 %, $\delta=0.01$ (рис. *в,г*), то для достижения уровня секретности $\varepsilon=10^{-10}$ требуется существенно бóльшая длина сырого ключа $n\approx1.15\cdot10^5$ бит. Длина секретного ключа при такой длине сырого ключа оказывается равной $\ell\approx3.46\cdot10^4$ бит.

9. ЗАКЛЮЧЕНИЕ

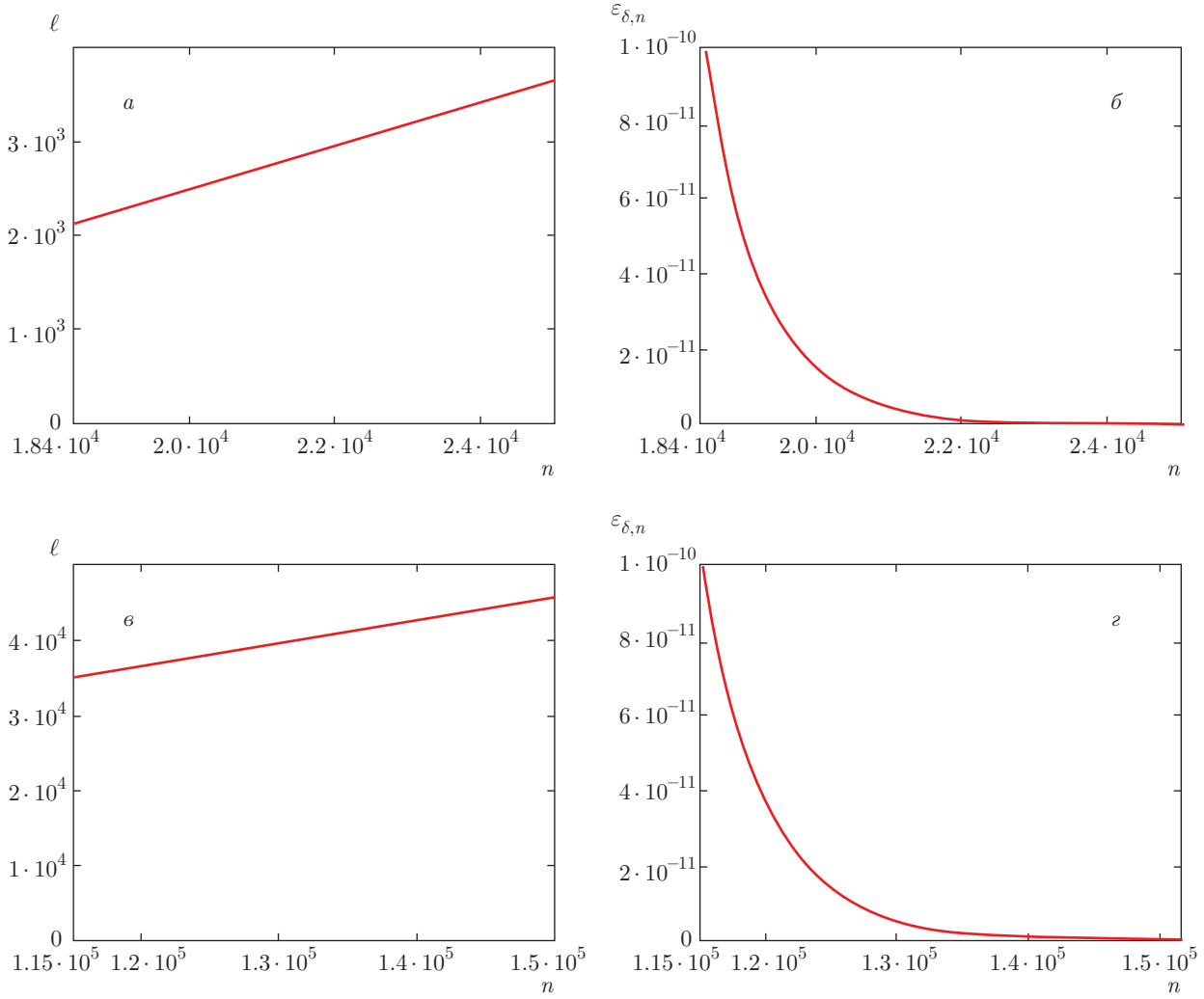
Одна из интерпретаций [4, 19] критерия секретности, основанного на следовом расстоянии (1), сводится к тому, что величина $\varepsilon_{\delta,n}$ дает превышение вероятности простого угадывания при различении двух ситуаций — идеальной и реальной [19] — над вероятностью простого угадывания. Точнее говоря, это вероятность различения двух квантовых состояний:

$$\Pr\left\{\rho_{XE}^{(\ell)},\rho_U^{(\ell)}\otimes\rho_E^{(\ell)}\right\}\le\frac{1}{2}(1+\varepsilon_{\delta,n}).$$

Состояние $\rho_{XE}^{(\ell)}$ отвечает реальной ситуации, когда квантовое состояние подслушивателя $\rho_E^{(\ell)}$ коррелировано с ключами легитимных пользователей. Идеальной ситуации отвечает квантовое состояние $\rho_U^{(\ell)}\otimes\otimes\rho_E^{(\ell)}$, когда квантовое состояние подслушивателя некоррелировано с секретными ключами. Величина $\varepsilon_{\delta,n}$ есть превышение вероятности над вероятностью простого угадывания при различении двух квантовых состояний — ситуаций.

Интерпретация, близкая к [4, 19], сводится к тому, что с вероятностью не менее $1-\varepsilon_{\delta,n}$ ключи, полученные в результате квантового распределения, неотличимы от идеальных ключей, которые полностью некоррелированы с состоянием подслушивателя.

В работах [20, 21] была показана прямая связь параметра секретности $\varepsilon_{\delta,n}$ со сложностью перебо-



Зависимости длины секретного ключа ℓ (формула (35)) ($а$,$в$) и параметра секретности $\varepsilon_{\delta,n}$ ($б$,$г$) от длины сырого ключа. Наблюдаемая ошибка $\overline{Q}$ и ширина доверительного интервала δ следующие: $а$,$б$ — $\overline{Q} = 0.05$, $\delta = 0.025$; $в$,$г$ — $\overline{Q} = 0.05$, $\delta = 0.01$

ра по ключевому пространству как полному, так и частичному. В частности, обратная величина параметра секретности $1/\varepsilon_{\delta,n}$ определяет среднее число шифр-сообщений $N_{dec} \approx 1/\varepsilon_{\delta,n}$ до их дешифрования при тотальном переборе ключей.

Один и тот же параметр $\varepsilon_{\delta,n}$ входит в сглаженную минимальную энтропию в (34) и в критерий секретности — следовое расстояние (1), (6). Упомянутые выше интерпретации возникают исключительно из того факта, что следовое расстояние не превосходит $\varepsilon_{\delta,n}$,

$$||\rho_{XE}^{(\ell)} - \rho_U^{(\ell)} \otimes \rho_E^{(\ell)}||_1 \leq \varepsilon_{\delta,n},$$

и никак не апеллируют к «истории происхождения» $\varepsilon_{\delta,n}$.

Выше было показано, что данный параметр определяет вероятность накрытия оценки вероятности ошибки Q доверительным интервалом шириной δ с центром в наблюдаемом числе ошибок $\overline{Q} = \overline{k}/n$. Приведенное выше рассмотрение позволяет дать простую интерпретацию параметра секретности. По сути, параметр $1 - \varepsilon_{\delta,n}$ есть точность определения истинной ошибки Q. Точнее, $1 - \varepsilon_{\delta,n}$ есть вероятность того, что при Q из интервала $Q \in [\overline{Q} - \delta, \overline{Q} + \delta]$ произойдет наблюдаемое число ошибок $\overline{k}/n \in [Q - \delta, Q + \delta]$.

Чем меньше доверительный интервал (маленькая δ), тем бóльшая длина n сырого ключа требуется для достижения заданного уровня секретности. При бóльших δ (грубая оценка истинного зна-

чения Q) бóльшая вероятность $1-\varepsilon_{\delta,n}$ (высокий уровень секретности) достигается при более коротких длинах сырого ключа. Однако грубая оценка Q при большом доверительном интервале приводит к сильному завышению информации подслушивателя (слагаемое $1-h(Q)$ в (35)), что в итоге снижает длину финального секретного ключа.

Фактически ширина доверительного интервала δ при заданной длине серии испытаний n определяет точность оценки параметра Q и, соответственно, секретность ключей — величину параметра секретности $\varepsilon_{\delta,n}=2e^{-2\delta^2 n}$.

До сих пор считалось, что число ошибок в последовательности известно. Все сказанное выше переносится и на тот случай, когда часть последовательности раскрывается и в ней определяется реальное число ошибок. Число ошибок в раскрытой части используется для оценки вероятности ошибки в той части последовательности, которая не раскрывается и будет использована для выработки ключа.

Пусть полная длина последовательности $n+n_1$. Пусть раскрытая часть последовательности для оценки вероятности ошибок n_1, а нераскрытая часть n, которая затем используется для получения ключа. Пусть число ошибок в раскрытой части последовательности $\overline{k}$, тогда однородная оценка, основанная на теоремах о выборках без возвращения [22], при ширине доверительного интервала δ дает

$$\Pr\left\{\left|\frac{\overline{k}}{n_1}-Q\right|\le\delta\right\}>$$
$$>1-2\exp\left(-2\frac{n_1 n}{n+n_1}\,\frac{n}{n+1}\delta^2\right)=1-\varepsilon_{\delta,n,n_1}. \quad (36)$$

Из (36) видно, что все сказанное выше переносится и на этот случай с заменой в формулах $\varepsilon_{\delta,n}\to\varepsilon_{\delta,n,n_1}$.

Автор выражает благодарность коллегам из Академии криптографии Российской Федерации за обсуждения и поддержку. Автор благодарит И. М. Арбекова за многочисленные и интенсивные обсуждения.

ЛИТЕРАТУРА

1. C. H. Bennett and G. Brassard, in Proc. IEEE Int. Conf. on Comp., Sys. and Signal Process., pp. 175–179, Bangalore, India (1984).
2. P. Shor and J. Preskill, Phys. Rev. Lett. **85**, 441 (2000).
3. D. Mayers, J. ACM **48**, 351 (2001).
4. R. Renner, PhD thesis, ETH Zürich, arXiv:0512258.
5. E. Biham, M. Boyer, P. O. Boykin, T. Mor, and V. Roychowdhury, J. Cryptology **19**, 381 (2006).
6. M. Tomamichel, Ch. Ci Wen Lim, N. Gisin, and R. Renner, arXiv:1103.4130 v2; Nature Communications **3**, 1 (2012).
7. M. Tomamichel and A. Leverrier, arXiv:1506.08458 v2.
8. Won-Young Hwang, Phys. Rev. Lett. **91**, 057901 (2003).
9. Hoi-Kwong Lo, Xiongfeng Ma, and Kai Chen, Phys. Rev. Lett. **94**, 230504 (2005).
10. M. Tomamichel and R. Renner, Phys. Rev. Lett. **106**, 110506 (2011).
11. C. H. Bennett, G. Brassard, C. Crepeau, and U. M. Maurer, IEEE Trans. Inf. Theory **41**, 1915 (1995).
12. J. L. Carter and M. N. Wegman, J. Comp. Syst. Sci. **18**, 143 (1979).
13. M. Tomamichel, C. Schaviner, A. Smith, and R. Renner, IEEE Trans. Inf. Theory **57**, 5524 (2011).
14. R. Renner and S. Wolf, *Advances in Cryptology — ASIACRYPT 2005*, *Proc. 11th International Conference on the Theory and Application of Cryptology and Information Security*, Chennai, India, December 4–8 (2005).
15. W. Hoeffding, J. Amer. Statistical Association **58**, 13 (1963).
16. A. A. Serov and A. M. Zubkov, arXiv:1207.3838 v2.
17. S. Boucheron, G. Lugosi, and P. Massart, *Concentration Inequalities*: *A Nonasymptotic Theory of Independence*, Clarendon Press, Oxford (2012).
18. C. J. Clopper and E. S. Pearson, Biometrika **26**, 404 (1934).
19. C. Portmann and R. Renner, arXiv:1409.3525 v1.
20. И. М. Арбеков, Матем. вопросы криптографии **7**, 39 (2016).
21. И. М. Арбеков, С. Н. Молотков, ЖЭТФ **52**, 62 (2017).
22. R. J. Serfling, Ann. Stat. **2**, 39 (1974).