Письма в ЖЭТФ, том 96, вып. 5, с. 374 – 380 © 2012 г. 10 сентября

О стойкости релятивистской квантовой криптографии в открытом пространстве при конечных ресурсах

С. Н. Молотков

Академия криптографии РФ, 103025 Москва, Россия

Институт физики твердого тела РАН, 142432 Черноголовка, Россия

Факультет вычислительной математики и кибернетики, МГУ им. Ломоносова, 119991 Москва, Россия

Поступила в редакцию 1 июня 2012 г.

После переработки 10 июля 2012 г.

Секретность ключей для базового нерелятивистского протокола BB84 исследовалась более полутора десятков лет. Только недавно было получено простое доказательство секретности в случае однофотонного источника квантовых состояний и конечных последовательностей с использованием энтропийных соотношений неопределенностей. Однако на сегодняшний день источники состояний не являются строго однофотонными. Неоднофотонность вместе с заранее неизвестными и меняющимися потерями в квантовом канале – открытом пространстве – приводит к тому, что нерелятивистские системы квантовой криптографии в открытом пространстве не могут гарантировать безусловную (unconditional) секретность ключей. Предложенная недавно релятивистская квантовая криптография снимает принципиальные ограничения, связанные с неоднофотонностью источника и потерями в открытом пространстве. Исследована стойкость принципиально нового семейства протоколов релятивистского квантового распределения ключей через открытое пространство в реальной ситуации конечных длин передаваемых последовательностей квантовых состояний. Данная система оказывается стойкой при реальных источниках неоднофотонных состояний (ослабленном лазерном излучении) и произвольных потерях в открытом пространстве.

Введение. Секретность ключей в квантовой криптографии гарантируется фундаментальными запретами квантовой механики [1, 2]. Основная мотивация использования дополнительных фундаментальных релятивистских ограничений в квантовой криптографии [3] *для открытого пространства* связана с тем, что все протоколы, секретность которых базируется только на ограничениях квантовой механики, не могут гарантировать секретности ключей при неоднофотонном источнике, больших и заранее не известных потерях в квантовом канале связи [4]. Релятивистская квантовая криптография гарантирует секретность ключей при любых потерях (любой дальности [5]).

Другая проблема со всеми базовыми протоколами, включая BB84 [6], связана с их уязвимостью по отношению к атаке с “ослеплением” детекторов [7]. Это было продемонстрировано как для оптоволоконных систем, так и для систем в открытом пространстве [8]. Релятивистская квантовая криптография оказывается устойчивой и к атаке с “ослеплением” фотодетекторов [9]. Стойкость базовых протоколов квантового распределения ключей в асимптотическом пределе бесконечно длинных последовательностей была доказана в ряде работ [10, 11]. В реальной ситуации длина передаваемой последовательности всегда конечна. Доказательство стойкости при конечных ресурсах (длине последовательности) было недавно дано в работах [12, 13] для базового протокола BB84.

Принципиальное отличие релятивистской квантовой криптографии от систем нерелятивистской квантовой криптографии связано с тем, что в последних важны только геометрические свойства квантовых состояний, точнее неортогональность информационных состояний фотонов. Пространственно-временная структура и факт распространения состояний с предельно допустимой скоростью света в пространстве-времени Минковского никак не используется.

В релятивистском случае принципиально важна пространственная протяженность состояний в пространстве-времени. Из-за нормировки квантового состояния вероятность исхода в некоторой пространственно-временной области для *любого измерения* не может превышать долю нормировки, которая набирается в этой области. Доступ к области пространства-времени, в которой сосредоточено квантовое состояние, из-за существования предельной скорости света требует конечного времени. Это неизбежно приводит к задержкам при подслушивании передаваемых состояний [5].

Анализ секретности ключей в квантовой криптографии фактически сводится к установлению коли-

чественной связи между возмущением квантовых состояний, приводящим к ошибкам на приемной стороне, и информацией, которую получает подслушиватель, производя данные возмущения. На решение данной задачи, которая является крайне нетривиальной, было затрачено немало усилий теоретиков [2, 4, 6, 10–14]. С момента появления протокола BB84 [6], всем интуитивно было понятно, что секретность протокола базируется на невозможности безошибочного измерения неортогональных состояний, которая, в свою очередь, гарантируется соотношениями неопределенностей. Однако установить данную связь явно и в прозрачной форме долгое время не удавалось. В значительной степени это было связано с тем, что соотношения неопределенностей в форме Гайзенберга–Робертсона [15, 16] не имеют теоретико-информационной интерпретации. Поэтому они неприменимы к доказательству секретности.

Совсем недавно связь между секретностью ключей для протокола BB84 и энтропийными соотношениями неопределенностей [17–22] была установлена в явной форме сначала в асимптотическом пределе бесконечно длинных последовательностей, а затем для реалистического случая – конечных передаваемых последовательностей [13].

Основными величинами, фигурирующими в доказательстве [13], являются так называемые сглаженные условные энтропии Реньи для составных квантовых систем[1)] нулевого (минимальная – max, $H^{\varepsilon}_{\max}(A|B)$) и бесконечного (максимальная – min, $H^{\varepsilon}_{\min}(X|B)$) порядков [13]. Данные энтропии имеют прозрачный операциональный смысл [23], если одна из подсистем, например A, является классической битовой строкой X и $\varepsilon \to 0$. Тогда $H^{\varepsilon}_{\min}(X|B)$ равна числу случайных равномерно распределенных бит, которые можно получить из строки X и которые теперь никак не коррелированы с подсистемой B. Аналогично $H^{\varepsilon}_{\max}(X|B)$ равна минимальному числу бит, которых не хватает пользователю, обладающему подсистемой B, чтобы полностью узнать битовую строку X, не имея к ней прямого доступа.

В длину секретного ключа входят (см. ниже) величина $H^{\varepsilon}_{\min}(X|E)$, где X – битовая строка Алисы (передающая сторона), E – квантовая система подслушивателя (Евы), и величина $H^{\varepsilon}_{\max}(X|B)$, где B – квантовая система на приемной стороне (Боб). Наиболее сложной для вычисления является величина $H^{\varepsilon}_{\min}(X|E)$. Обе упомянутые величины входят в соотношения неопределенностей, что и позволяет напрямую связать длину секретного ключа с энтропийными соотношениями неопределенностей.

В релятивистском случае ограничения на различимость состояний, диктуемые соотношениями неопределенностей, оказываются более мягкими, чем ограничения, связанные с релятивистской причинностью. Соображения, связанные с релятивистской причинностью, позволяют получить нижнюю границу для величины $H^{\varepsilon}_{\min}(X|E)$, которая определяет недостаток информации Евы о битовой строке X, простым способом.

Ниже будет приведено доказательство секретности релятивистской квантовой криптографии в реальной ситуации конечных длин передаваемых последовательностей как для однопроходной реализации с синхронизацией часов на передающей и приемной сторонах [5], так и для двухпроходной, когда синхронизации часов (общего начала отсчета времени) не требуется [5].

Min и max энтропии. Наиболее адекватным и удобным является использование так называемых min и max сглаженных квантовых энтропий (энтропии Реньи бесконечного и нулевого порядка [14]). Данные величины являются обобщением энтропий Шеннона в классическом случае и фон Неймана в квантовом и имеют прозрачную теоретико-информационную интерпретацию [23]. Они удобны, когда истинная матрица плотности точно не известна, но известно, что в определенном смысле (метрике) матрица плотности близка к истинной. Именно такая ситуация имеет место в квантовой криптографии, когда матрица плотности оценивается по конечной последовательности измерений. По определению min и max энтропий имеем (подробности см. в [14])

$$\begin{aligned} H_{\min}(A|B) &= -\sup_{\sigma_B} \log\lambda, \\ H_{\max}(A|B) &= \sup_{\sigma_B} \log\{\mathrm{Tr}[\rho^0_{AB}(I_A \otimes \sigma_B)]\}, \end{aligned} \tag{1}$$

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 $\mathcal{H}_A$, $\rho^0_{AB} = \mathrm{supp}(\rho_{AB})$ – проектор (носитель матрицы плотности) на пространство, где действует оператор ρ_{AB}. По определению [14] сглаженные min и max квантовые энтропии равны

$$\begin{aligned} H^{\varepsilon}_{\min}(A|B) &= \sup_{\overline{\rho}_{AB} \in \mathcal{B}^{\varepsilon}(\rho_{AB})} H_{\min}(A|B)_{\overline{\rho}_{AB}}, \\ H^{\varepsilon}_{\max}(A|B) &= \inf_{\overline{\rho}_{AB} \in \mathcal{B}^{\varepsilon}(\rho_{AB})} H_{\max}(A|B)_{\overline{\rho}_{AB}}, \end{aligned} \tag{2}$$

где точные верхняя и нижняя грани берутся по всем матрицам плотности $\overline{\rho}_{AB}$, находящимся в шаре

[1)] Квантовая система состоит из двух подсистем, A и B, вообще говоря находящихся в запутанном коррелированном состоянии.

$\mathcal{B}^{\varepsilon}(\rho_{AB})$ радиуса ε с центром в ρ_{AB}, $\mathcal{B}^{\varepsilon}(\rho_{AB}) = \{\overline{\rho}_{AB} : ||\rho_{AB} - \overline{\rho}_{AB}||_1 \le \mathrm{Tr}\{\overline{\rho}_{AB}\} \cdot \varepsilon\}$. Удобной мерой близости между парой матриц плотности является следовое расстояние [14]:

$$d_1(\rho,\overline{\rho}) = \frac{1}{2}||\rho - \overline{\rho}||_1 = \frac{1}{2}\mathrm{Tr}[|\rho - \overline{\rho}|] = \frac{1}{2}\mathrm{Tr}[\sqrt{(\rho - \overline{\rho})^2}]. \tag{3}$$

Для дальнейшего нам потребуется еще одна величина, описывающая меру близости между матрицами плотности, соответствие (*fidelity*). При этом имеют место соотношения (см., например, [24])

$$F(\rho,\overline{\rho}) = \mathrm{Tr}[|\sqrt{\rho}\sqrt{\overline{\rho}}|],$$
$$1 - F(\rho,\overline{\rho}) \le d_1(\rho,\overline{\rho}) \le \sqrt{1 - F^2(\rho,\overline{\rho})}. \tag{4}$$

Критерий стойкости при конечных ресурсах. После измерений ситуация описывается матрицей плотности ρ_{XYE}, где битовые строки Алисы и Боба $X, Y = \{0,1\}^n$. Корреляции между Алисой (X) и Бобом (Y) описываются совместной функцией распределения $\rho_{XYE} = \sum_{x,y} \rho_E^{xy} |x\rangle\langle x| \otimes |y\rangle\langle y|$, $\rho_{XY} = \sum_{x,y} P_{XY}(x,y)|x\rangle\langle x| \otimes |y\rangle\langle y|$, $P_{XY}(x,y) = \mathrm{Tr}_E\{\rho_E^{xy}\}$, ρ_E^{xy} – корреляции между X, Y и Евой, которые заключены в квантовой системе Евы. Под стойкостью понимается корректность и секретность протокола распределения ключей [14]. Протокол ε_{EC} корректен, если после исправления ошибок вероятность того, что битовая строка Алисы x отличается от битовой строки Боба $\hat{x}$, оказывается не более ε_{EC}. Протокол Δ секретен, если после сжатия очищенного ключа $x \to z$. Здесь z – расстояние до идеальной ситуации, когда корреляции между ключом легитимных пользователей и квантовой системой Евы

$$\Pr[\hat{x} \ne x] = d_1(\rho_{X\hat{X}}, \rho_{XX}) = d_1(P_{X\hat{X}}, P_{XX}) < \varepsilon_{EC},$$
$$d_1(\rho_{ZFE}, \rho_{UZ} \otimes \rho_{FE}) < \Delta, \tag{5}$$

где $P_{X\hat{X}}$, P_{XX} – совместная функция распределения после коррекции ошибок, описывающая идеальные корреляции, ρ_{ZFE} и ρ_{UZ} – матрица плотности после сжатия очищенного ключа и матрица, отвечающая однородному распределению ключей. *Оказывается, что критерии корректности и секретности протокола выражаются через сглаженные max и min энтропии соответственно.*

Корректность протокола, исправление ошибок. Исправление ошибок происходит через аутентичный открытый канал связи. Информация при обмене доступна Еве. Найдем связь утечки информации с параметром корректности (5). Исправление ошибок можно рассматривать как хэширование. Этот подход развивался в [25], а применительно к квантовой криптографии – в [14]. Алиса, имея битовую строку x, вычисляет хэш-значение $z = f(x)$. При этом хэш-функции выбираются открыто, случайно и равновероятно из множества универсальных хэш-функций второго порядка [26], которые обладают тем свойством, что вероятность совпадения хэш-значений при несовпадающих значениях аргумента не более $f \in \mathcal{F} : X = \{0,1\}^N \to Z = \{0,1\}^k$, $\Pr_f[f(\hat{x}) = f(x)] \le 1/|Z| = 2^{-k}$, $\hat{x} \ne x$. Алиса сообщает через открытый канал Бобу $(f, f(x))$. Поскольку выбор хэш-функции является открытым, число бит дополнительной информации, доступное Еве, есть число бит для сообщения хэш-значения $f(x)$, т.е. k бит. Утечка информации leak_{EC} в битах равна k. Утечка информации выражается через max энтропию (детали см. в [14]):

$$k = \mathrm{leak}_{EC} \le H_{\max}(P_{XY}|Y) + \log 1/\varepsilon_{EC},$$
$$H_{\max}(P_{XY}|Y) = \log \max_{y \in Y} |\mathrm{supp}(P_X^y)|. \tag{6}$$

Max энтропия вычисляется по распределению $P_{XY}(x,y)$, где $\hat{\mathcal{X}}_y = \mathrm{supp}(P_X^y)$ – множество значений y, в которые могут перейти различные x. Соответственно $|\mathrm{supp}(P_X^y)|$ – наибольшее число элементов по y и по x при всех x. Цель Боба, 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 $f(\hat{x}_y) = f(x)$. Боб получает $\hat{x}$ из своей битовой строки y, меняя 0 на 1 и наоборот в части позиций, число которых зависит от вероятности наблюдаемой ошибки. Фактически такая процедура сводится к перебору, но пока это не важно.

Ошибка при декодировании определяется вероятностью того, что существует такое $\hat{x}_y \in \hat{\mathcal{X}}_y = \mathrm{supp}(P_X^y)$, не равное x, при котором хэш-значения $f(\hat{x}) = f(x)$. Имеем (см. также [14, 26])

$$\Pr[x \ne \hat{x}] \le \Pr_f[\exists x \in \hat{\mathcal{X}}_y = \mathrm{supp}(P_X^y), \hat{x} \ne x \wedge f(\hat{x}) = f(x)] \le |\mathrm{supp}(P_X^y)| 2^{-k}. \tag{7}$$

Из (6) видно, что $\max_y |\mathrm{supp}(P_X^y)| = 2^{H_{\max}(P_{XY}|Y)}$. Получаем

$$\Pr[\hat{x} \ne x] \le 2^{H_{\max}(P_{XY}|Y) - [H_{\max}(P_{XY}|Y) + \log(1/\varepsilon_{EC})]} \le \varepsilon_{EC}. \tag{8}$$

Истинная матрица плотности ρ_{XY} и распределение $P_{XY}(x,y)$ неизвестны. Их оценки $\overline{\rho}_{XY}$ и $\overline{P}_{XY}(x,y)$ возникают при подсчете числа наблюдаемых ошибок. Если из этой оценки следует, что (см. ниже)

$$d_1[P_{XY}(x,y), \overline{P}_{XY}(x,y)] \le \varepsilon_{EC}, \tag{9}$$

то, поскольку

$$H^{\varepsilon'}(P_{XY}|Y) = \min_{\overline{P}_{XY}(x,i)\in\mathcal{B}^{\varepsilon'}[P_{XY}(x,y)]} H(\overline{P}_{XY}|Y),$$

утечка информации для любого распределения $\overline{P}_{XY}(x,y)$ ε'-близкого к $P_{XY}(x,y)$, оказывается не более $\mathrm{leak}_{EC} \le H(\overline{P}_{XY}|Y) + \log(2/\varepsilon_{EC})$. В итоге утечка информации

$$\mathrm{leak}_{EC} \le H^{\varepsilon'}(P_{XY}|Y) + \log(2/\varepsilon_{EC}), \quad \varepsilon' = \varepsilon_{EC}/2 \tag{10}$$

(множитель 2 под логарифмом возникает из дополнительного фактора $1/2$ в определении следового расстояния, в отличие от расстояния в шаре).

Оценка параметров. Для двухпроходной схемы оцениваются два параметра: доля η задержанных отсчетов и вероятность ошибки Q. Для однопроходной схемы оценивается только вероятность ошибки. Сначала сделаем оценки для двухпроходной схемы. Примерно в половине случаев Ева ошибается, что приводит к задержке классического сигнала. Эти посылки отбрасываются. Примерно в половине она угадывает. Оценка $\overline{\eta}$ доли угаданных производится по доле ошибок. Это дает долю посылок с подменой классического сигнала. Вероятность того, что наблюдаемое число $\overline{\eta}$ превышает точное значение η на величину ξ, оказывается не более (данная оценка следует из вероятности больших уклонений; детали см. в [27])

$$\Pr[\overline{\eta} \ge \eta + \xi] \le e^{-2n\xi^2} = \varepsilon_\xi^2. \tag{11}$$

Введем распределение $\overline{P}(X,Y)_{\overline{\eta},Q}$, которое дает $\overline{\eta} < \eta + \xi$ задержанных отсчетов и является ε_ξ-близким к истинному (лежит в шаре $\overline{P}(X,Y)_{\overline{\eta},Q} \in \mathcal{B}^{\varepsilon_\xi}[P(X,Y)_{\eta,Q}]$). Имеем

$$\overline{P}(X,Y)_{\eta,Q} = P(X,Y)_{\eta,Q}/\Pr[\overline{\eta} < \eta + \xi], \ \overline{\eta} < \eta + \xi;$$
$$\overline{P}(X,Y)_{\eta,Q} = 0, \ \ \overline{\eta} \ge \eta + \xi. \tag{12}$$

Выражая следовое расстояние d_1 через соответствие (fidelity) (4) и учитывая, что

$$\Pr[\eta \ge \eta + \xi] + \Pr[\eta < \eta + \xi] = 1,$$

и

$$F[P(X,Y)_{\eta,Q}, \overline{P}(X,Y)_{\eta,Q}] =$$
$$= \sum_{\overline{\eta}<\eta+\xi} \sqrt{P(X,Y)_{\eta,Q}\overline{P}(X,Y)_{\eta,Q}} =$$
$$= \sqrt{\Pr[\overline{\eta} < \eta + \xi]} = \sqrt{1-\varepsilon_\xi^2},$$

получаем

$$d_1[P(X,Y)_{\eta,Q}, \overline{P}(X,Y)_{\eta,Q}] \le$$
$$\le \sqrt{1 - F^2[P(X,Y)_{\eta,Q}, \overline{P}(X,Y)_{\eta,Q}]} < \varepsilon_\xi. \tag{13}$$

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

$$d_1[P(X,Y)_{\eta,Q}, \overline{P}(X,Y)_{\eta,Q}] \le \varepsilon_\xi. \tag{14}$$

Следующий шаг состоит в оценке величины истинной вероятности ошибки по наблюдаемой в раскрытой части последовательности для распределения $\overline{P}(X,Y)_{\eta,Q}$. Пусть раскрываемая доля из N посылок есть ν, а не раскрываемая для ключа – $(1-\nu)$. Тогда полная ошибка в последовательности $\overline{Q} = \nu Q_{\mathrm{obs}} + (1-\nu)Q_{\mathrm{key}}$. По раскрытой части делается оценка вероятности ошибки. Согласно неравенству для вероятности уклонения наблюдаемого значения от истинного по выборке без возвращения (детали см. в [28]) получаем

$$\Pr[Q_{\mathrm{key}} \ge \overline{Q} + \zeta] \le e^{-2\frac{kn}{N}\frac{k}{k+1}\zeta^2} = \varepsilon_\zeta^2,$$
$$k = \nu N, \quad n = (1-\nu)N. \tag{15}$$

Протокол не прерывается, если величина ошибки $\overline{Q}$ не превосходит критической величины для протокола. Введем новое распределение вероятностей:

$$\widehat{\overline{P}}(X,Y)_{\eta,\overline{Q}} = \overline{P}(X,Y)_{\eta,Q}/\Pr[Q_{\mathrm{key}} < \overline{Q} + \zeta],$$
$$Q_{\mathrm{key}} < \overline{Q} + \zeta, \ \ \widehat{\overline{P}}(X,Y)_{\eta,Q} = 0, \tag{16}$$
$$Q_{\mathrm{key}} \ge \overline{Q} + \zeta.$$

Данное распределение производит не более $\overline{Q}+\zeta$ ошибок при заданном значении $\overline{\eta}$. Аналогично анализу, сделанному выше (см. (12)–(14)), получаем, что распределения $\overline{P}(X,Y)_{\eta,Q}$ и $\widehat{\overline{P}}(X,Y)_{\eta,Q}$ являются ε_ζ-близкими:

$$d_1[\overline{P}(X,Y)_{\eta,Q}, \widehat{\overline{P}}(X,Y)_{\eta,Q}] \le \varepsilon_\zeta. \tag{17}$$

Для расстояния между истинным и эмпирическим распределениями с учетом (16), (17) имеем

$$d_1[P(X,Y)_{\eta,Q}, \widehat{\overline{P}}(X,Y)_{\eta,Q}] \le$$
$$\le \sqrt{1 - F^2[P(X,Y)_{\eta,Q}, \widehat{\overline{P}}(X,Y)_{\eta,Q}]} = \varepsilon_\zeta. \tag{18}$$

Окончательно находим, что распределение $\widehat{\overline{P}}(X,Y)_{\eta,Q}$ оказывается $\varepsilon_{\xi,\zeta} = \varepsilon_\xi + \varepsilon_\zeta$-близким к истинному. Действительно, используя (14), (17), (18) и неравенство треугольника, имеем

$$d_1[P(X,Y)_{\eta,\overline{Q}}, \widehat{\overline{P}}(X,Y)_{\eta,Q}] \le$$
$$\le d_1[P(X,Y)_{\eta,Q}, \overline{P}(X,Y)_{\eta,Q}] +$$
$$+ d_1(\overline{P}(X,Y)_{\eta,Q}, \widehat{\overline{P}}(X,Y)_{\eta,Q}) \le \varepsilon_{\xi,\zeta}. \tag{19}$$

Определение утечки информации. Найдем величину $H_{\max}^{\varepsilon_{\xi,\zeta}}[P(X,Y)_{\eta,Q}|Y]$, определяющую согласно (10) утечку информации в битах при

коррекции ошибок в конечной последовательности. Фактически $H_{\max}[\overline{P}_{\eta,Q}(X,Y)|Y)]$ равна логарифму произведения числа способов раскидать не более $nQ_{\rm key}=n(\overline{Q}+\zeta)$ ошибок по n позициям. Величина $H_{\max}^{\varepsilon_{\xi,\zeta}}[P(X,Y)_{\eta,Q}]$ является точной нижней границей (в нашем случае минимумом) по всем распределениям в шаре $\overline{P}(X,Y)_{\eta,Q}\in\mathcal{B}^{\varepsilon_{\eta,\zeta}}[P(X,Y)_{\eta,Q}]$. Воспользовавшись неравенствами (см., например, [29]) $\sum_{k=0}^{x}\frac{n!}{(n-i)!i!}\le 2^{nH(x)}$, получаем

$$H_{\max}^{\varepsilon_{\xi,\zeta}}[P(X,Y)_{\eta,Q}|Y]\le H_{\max}[\overline{P}_{\eta,Q}(X,Y)|Y)]\le$$
$$\le\log\left(\sum_{i=0}^{nQ_{\rm key}}\frac{n!}{(n-i)!i!}\right)\le nH(\overline{Q}+\zeta),\qquad(20)$$

где $H(x)=-x\log x-(1-x)\log(1-x)$, $\varepsilon_{\xi,\zeta}=(\varepsilon_\xi+\varepsilon_\zeta)/2$ для двухпроходной и $\varepsilon_{\xi,\zeta}=\varepsilon_\zeta/2$ для однопроходной схемы. Отметим, что доля $\overline{\eta}$ посылок, где Ева угадала момент посылки классического сигнала, "невидима" для легитимных пользователей, т.к. не дает ошибок.

Вычисление длины секретного ключа. После исправления ошибок происходит сжатие (усиление секретности – *privacy amplification* [30]) очищенного ключа до финального секретного ключа при помощи случайных универсальных хэш-функций второго порядка f [26]: $X=\{0,1\}^N\to Z=\{0,1\}^{l_{\rm secr}}$ (множество хэш-функций F). *Степень сжатия определяется сглаженной min энтропией, которая зависит от протокола квантового распределения ключей.* Согласно теореме о хэшировании (Leftover Hash [31]) расстояние до идеальной ситуации после сжатия становится равным

$$d_1(\rho_{FZEF},\rho_{UZ}\otimes\rho_{EF})=$$
$$=\frac{1}{2}||\rho_{FZEF}-\rho_{UZ}\otimes\rho_{EF}||_1=$$
$$=\Delta<\varepsilon+\tfrac{1}{2}\sqrt{2^{-[l_{\rm secr}-H_{\min}^{\varepsilon}(X|EC)]}}.\qquad(21)$$

Матрица плотности после хэширования $\rho_{FZEF}=\sum_f\sum_z p_f|f\rangle\langle f|\otimes|z\rangle\langle z|\otimes\rho_E^{fz}$, где $\rho_E^{fz}=\sum_{x:f^{-1}(x)=z}\rho_E^x$, $p_f=1/|F|$, $\rho_E^{fz}=\sum_{x,x=f^{-1}(z)}\rho_E^x$. $\rho_{EF}={\rm Tr}_Z\{\rho_{FZEF}\}$ – матрица плотности Евы после хэширования, ρ_{UZ} – матрица плотности, отвечающая однородному распределению. Напомним, что здесь $\varepsilon=\varepsilon_\zeta$ для однопроходной и $\varepsilon=\varepsilon_\zeta+\varepsilon_\zeta$ для двухпроходной схемы. Min энтропия, обусловленная классическими сообщениями C, есть (детали см. в [14]) $H_{\min}^{\varepsilon}(X|EC)\ge H_{\min}^{\varepsilon}(X|E)-{\rm leak}_{EC}$. Если длина секретного ключа выбрана как

$$l_{\rm secr}\le H_{\min}^{\varepsilon}(X|E)-{\rm leak}_{EC}-2\log(1/2\overline{\varepsilon}),\qquad(22)$$

то расстояние до идеальной ситуации $\Delta<\varepsilon+\overline{\varepsilon}$. Остается оценить $H_{\min}^{\varepsilon}(X|E)$ до сжатия ключа. *При этом будут принципиально важны релятивистские ограничения.* Поскольку $H_{\min}^{\varepsilon}(X|E)=\sup_{\overline{\rho}_{XE}\in\mathcal{B}^{\varepsilon}(\rho_{XE})}H_{\min}(X|E)_{\overline{\rho}_{XE}}$, для любого $\overline{\rho}_{XE}\in\mathcal{B}^{\varepsilon}(\rho_{XE})$ сглаженная min энтропия не меньше чем $H_{\min}(X|E)_{\overline{\rho}_{XE}}$. Оценка для $\overline{\rho}_{XE}$ получается после стадии оценки параметров.

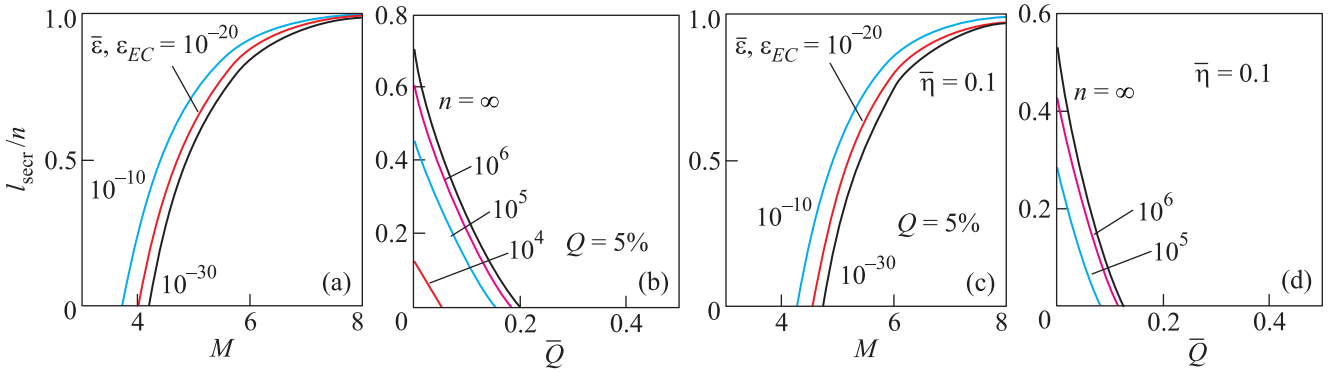
Однопроходная схема (детали см. в [5]). Часы синхронизированы. Алиса посылает пару ослабленных когерентных состояний, отвечающих 0 и 1: $|\varphi_{0,1}\rangle=|e^{i\theta_A^{0,1}}\alpha\rangle_1\otimes|\alpha\rangle_2$ ($|\alpha|^2\ll 1$). Состояния $|e^{i\theta_A^{0,1}}\alpha\rangle_1$ и $|\alpha\rangle_2$ разнесены во времени. Фаза комплексного параметра α когерентного состояния в каждой посылке случайна. Второе состояние, $|\alpha\rangle_2$, служит реперным для первого [5]. Боб, зная момент посылки и расстояние, добавляет свою относительную фазу $|e^{i(\theta_A^{0,1}-\theta_B^{0,1})}\alpha\rangle_1$ на первую половинку, затем сводит состояния вместе и производит измерения. Отсчеты с задержкой по времени отбрасываются. Поскольку измерения с определенным исходом приводят к задержкам из-за необходимости доступа к обеим половинкам [5], оптимальной является атака со светоделителем [5]. Задержки при этом не возникают. При такой атаке информация Евы ограничена фундаментальной верхней границей информации, которую можно извлечь из квантового ансамбля $\{|\varphi_0\rangle,|\varphi_1\rangle\}$. Данная граница совпадает с границей Холево [32]. В нашем случае это означает, что к каждому биту x Алисы "привязано" состояние $|\varphi_{0,1}\rangle$, т.е. $\overline{\rho}_{XE}=\sigma_{XE}^{\otimes n}$, где $\sigma_{XE}=\frac{1}{2}\sum_x|x\rangle\langle x|\otimes|\varphi_x\rangle_{EE}\langle\varphi_x|$ ($x=0,1$). Используя неравенство для min энтропии от тензорного произведения [14], находим

$$H_{\min}^{\varepsilon}(X|E)\ge H_{\min}(\sigma_{XE}^{\otimes n}|\sigma_E^{\otimes n})=$$
$$=n\left[H(\sigma_{XE})-H(\sigma_E)\right]=n\left[1-\overline{C}(\varphi_{0,1})\right],\qquad(23)$$

где $H(\sigma)=-{\rm Tr}\{\sigma\log\sigma\}$ – энтропия фон Неймана, $\overline{C}(\varphi_{0,1})=-\lambda_+\log\lambda_+-\lambda_-\log\lambda_-$ – классическая пропускная способность квантового канала связи со входным ансамблем $\{|\varphi_0\rangle,|\varphi_1\rangle\}$ ($\lambda_\pm=(1\pm\lambda)/2$, $\lambda=|\langle\varphi_0|\varphi_1\rangle|$) [32]. Окончательно для длины ключа с учетом (21)–(23) получаем

$$l_{\rm secr}\le n[1-\overline{C}(\varphi_{0,1})-H(\overline{Q}+\zeta)]-\log(2/\varepsilon_{EC})-$$
$$-2\log(1/2\overline{\varepsilon}),\ \text{где}\ \varepsilon_{EC}=\varepsilon_\zeta.\qquad(24)$$

Двухпроходная схема [5]. Здесь синхронизации часов не требуется. Алиса посылает в один из двух случайных моментов времени, t_0 или t_1, пару интенсивных (классических) когерентных состояний, $|\varphi_{t_{0,1}}^{\rm clas}\rangle=|\alpha_c\rangle_{t_{0,1},1}\otimes|\alpha_c\rangle_{t_{0,1},2}$ ($|\alpha_c|^2\gg 1$), сдвинутых друг относительно друга так же, как и в однопроходной схеме. Боб регистрирует время прилета классического состояния в данной посылке и время между соседними посылками. Затем он ослабляет (пропус-



Зависимости отношения длины ключа к длине последовательности от логарифма длины переданной последовательности N ($M = \log_{10} N$) (a, b) и наблюдаемой доли ошибок $\overline{Q}$ (b, d). Панели a, b относятся к однопроходной схеме, а c, d – к двухпроходной. Доля раскрываемой части последовательности для оценки параметров $\nu = 1/2$ ($n = k = \nu N$). Остальные параметры приведены на рисунке. Скалярное произведение информационных состояний $|\langle\varphi_0|\varphi_1\rangle| = 0.9$

кая, например, через сильно асимметричный светоделитель) их до квазиоднофотонного уровня, кодирует их (добавляет относительную фазу между парой состояний) и посылает Алисе. Алиса также добавляет свою относительную фазу, компенсируя фазу Боба, и сводит половинки вместе, а затем регистрирует фотодетектором аналогично однопроходной схеме. Кроме того, Алиса фиксирует моменты посылки и прилета состояний. Задержанные состояния отбрасываются. Отбрасываются также и посылки, в которых состояние прибыло к Бобу не вовремя. В этой схеме, в отличие от однопроходной, Ева может попытаться угадать один из двух случайных моментов посылки классического состояния. Примерно в половине случаев Ева может угадать и пройти тест на задержку. Если доля таких посылок 2η, то она будет знать примерно η бит ключа (детали см. в [5]). Для остальной доли посылок оптимальной является стратегия, аналогичная однопроходной схеме. Оценка матрицы плотности дает $\overline{\rho}_{XE} = (\sigma_{XX})^{\otimes n\overline{\eta}} \otimes \sigma_{XE}^{\otimes n(1-\overline{\eta})}$ ($\sigma_{XX} = \frac{1}{2}\sum_x |x\rangle\langle x| \otimes |x\rangle_{EE}\langle x|$). Первый сомножитель отражает тот факт, что Ева достоверно знает бит Алисы–Боба в $n\overline{\eta}$ посылках. Консервативно считаем, что все эти посылки сосредоточены в нераскрываемой при коррекции ошибок части последовательности, фигурирующей в очищенном ключе. Для min энтропии имеем

$$H_{\min}^{\varepsilon}(X|E) \geq H_{\min}(\overline{\rho}_{XE}) = n[1-\overline{\eta}][1-\overline{C}(\varphi_{0,1})] - \overline{\eta}. \quad (25)$$

Тогда для длины секретного ключа с учетом (21), (22), (25) находим (ниже $\varepsilon_{EC} = (\varepsilon_\eta + \varepsilon_\zeta)/2$)

$$l_{\text{secr}} \leq n\left\{1-\overline{\eta})[1-\overline{C}(\varphi_{0,1})] - \overline{\eta} - H(\overline{Q}+\zeta)\right\} - \\ - \log(2/\varepsilon_{EC}) - 2\log(1/2\overline{\varepsilon}). \quad (26)$$

Отметим, что потери в квантовом канале связи не входят в длину секретного ключа (24), (26).

Численные результаты. Конечная цель протокола – получить заданную длину ключа при задаваемых легитимными пользователями параметрах (корректности, секретности протокола и длине передаваемой последовательности N).

Однопроходная схема. Выразим из (15) величину уклонения ζ от параметров корректности ($\varepsilon_{EC} = \varepsilon_\zeta$) и секретности ($\Delta = \overline{\varepsilon} + \varepsilon_\zeta$) протокола ($\zeta = \sqrt{N(k+1)\ln(1/\varepsilon_\zeta)/k^2 n}$) и от наблюдаемого числа ошибок $\overline{Q}N$ в последовательности. Подставляя ее в (24), получаем зависимость длины секретного ключа от параметров корректности, секретности, наблюдаемой ошибки и длины последовательности N.

Двухпроходная схема. Параметры корректности $\varepsilon_{EC} = \varepsilon_\xi + \varepsilon_\zeta$, а параметр секретности протокола $\Delta = \overline{\varepsilon} + \varepsilon_\xi + \varepsilon_\zeta$. Находя из (11) величину уклонения для числа задержанных посылок ξ ($\xi = \sqrt{\ln(1/\varepsilon_\xi)/N}$) и наблюдаемого числа ошибок ζ ($\zeta = \sqrt{N(k+1)\ln[1/(\varepsilon_\xi+\varepsilon_\zeta)/k^2 n]}$) и затем подставляя их в (24), получаем зависимость длины секретного ключа от параметров протокола.

Пусть длина передаваемой последовательности N фиксирована. Тогда чем меньше параметры секретности и корректности (более жесткие требования), тем больше разброс оценки для величины уклонения параметров от их истинных значений. Оценка уклонения для параметра ξ для ошибки пропорциональна логарифму от обратной величины параметров секретности $\overline{\varepsilon}$ и ε_{EC}. Это означает, что чем меньше величины параметров секретности, тем более консервативной (завышенной) является оценка величины ошибки и доли задержанных состояний (для двухпроходной схемы). Бóльшие значения этих параметров подра-

зумевают завышение информации Евы, которую она получает при вторжении в квантовый канал связи. Важно отметить, что при конечных длинах последовательностей существует некоторая их минимальная критическая длина, начиная с которой вообще можно сгенерировать секретный ключ (рис. a и c). Кроме того, чем меньше длина переданной последовательности, тем больше ошибка в оценке параметров. Это также приводит к завышению информации Евы по отношению к асимптотическому пределу бесконечных последовательностей. Отсюда также 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 задержанных состояний (рис. d).

Заключение. Итак, найдены критерии секретности ключей для случая конечных последовательностей для релятивистской квантовой криптографии. Ненулевая длина ключа может быть получена (в зависимости от параметров корректности и секретности), только если длина передаваемой последовательности превышает некоторую величину. Система обеспечивает секретность ключей даже при не строго однофотонном источнике и произвольных потерях в канале связи, которые не входят в длину секретного ключа.

Выражаю благодарность коллегам по Академии криптографии Российской Федерации за постоянную поддержку. Работа частично поддержана проектом РФФИ # 11-02-00455.

1. W. K. Wootters and W. H. Zurek, Nature **299**, 802 (1982).
2. C. H. Bennett, Phys. Rev. Lett. **68**, 3121 (1992).
3. S. N. Molotkov and D. I. Pomozov, *Relativistic No-Cloning Theorem, NATO Series for Peace and Security, Information and Communication Security* (ed. by M. Zhukowski, S. Kilin, and J. Kowalik), IOS Press, Amsterdam, Berlin, Oxford, Washington, 2007, v. 11, p. 31.
4. V. Scarani, H. Bechmann-Pasquinucci, N. J. Cerf et al., Rev. Mod. Phys. **81**, 1301 (2009).
5. С. Н. Молотков, ЖЭТФ **139**, 429 (2011); Письма в ЖЭТФ **94**, 504 (2011).
6. C. H. Bennett and G. Brassard, *Proc. of IEEE Int. Conf. on Comput. Sys. and Sign. Proces.*, Bangalore, India, 1984, p. 175.
7. L. Lydersen, C. Wiechers, C. Wittmann et al., Nature Photonics **4**, 686 (2010).
8. I. Gerhardt, Q. Liu, A. Lamas-Linares et al., arXiv/quant-ph: 10110105.
9. С. Н. Молотков, ЖЭТФ **141**, 812 (2012).
10. H.-K. Lo and H. F. Chau, Science **283**, 2050 (1999).
11. P. Shor and J. Preskill, Phys. Rev. Lett. **85**, 441 (2000).
12. V. Scarani and R. Renner, Phys. Rev. Lett. **100**, 200501 (2008); arXiv/quant-ph: 08060120.
13. M. Tomamichel, C. C. Wen Lim, N. Gisin, and R. Renner, Nature Communications **3**, 634 (2011).
14. R. Renner, *Security of Quantum Key Distribution*, PhD Thesis, ETH Zürich, Dec. 2005; arXiv/quant-ph: 0512258.
15. W. Heisenberg, Zeit. für Phys. **43**, 172 (1927).
16. H. P. Robertson, Phys. Rev. **34**, 163 (1929).
17. D. Deutsch, Phys. Rev. Lett. **50**, 631 (1983).
18. K. Kraus, Phys. Rev. D **35**, 3070 (1987).
19. H. Maassen and J. B. M. Uffink, Phys. Rev. Lett. **60**, 1103 (1988).
20. J. M. Renes and J.-C. Boileau, Phys. Rev. Lett. **103**, 020402-1 (2009).
21. M. Berta, M. Chritlandl, R. Colbeck et al., arXiv/quant-ph: 0909.0950.
22. M. Tomamichel and R. Renner, arXiv/quant-ph: 1009.2015.
23. R. König, R. Renner, and C. Schaffner, arXiv/quant-ph: 08071338.
24. M. Nielsen and I. Chuang, *Quantum Computation and Quantum Information*, Cambridge Univ. Press, Cambridge, 2000.
25. D. R. Stinson, *On the Connections Between Universal Hashing, Combinatorial Designs and Error-Correcting Codes*, ECCC TR95-052, Electronic Colloquium on Computational Complexity – Reports Series, 1995.
26. J. L. Carter and M. N. Wegman, J. Comp. Syst. Sci. **18**, 143 (1979).
27. W. Hoeffding, J. Amer. Statistical Assoc. **58**, 13 (1963).
28. R. J. Serfling, Ann. Stat. **2**, 39 (1974).
29. В. К. Леонтьев, *Избранные задачи комбинаторного анализа*, М.: Из-во МГТУ, 2001.
30. C. H. Bennett, G. Brassard, C. Crepeau, and U. M. Maurer, IEEE Trans. on Inf. Theory **41**, 1915 (1995).
31. M. Tomamichel, C. Schaffner, A. Smith, and R. Renner, arXiv/quant-ph:10022436.
32. А. С. Холево, *Квантовые системы, каналы, информация*, М.: МЦМО, 2010, с. 327.