Письма в ЖЭТФ, том 102, вып. 6, с. 436 – 443

Аналог дифференциально-фазовой квантовой криптографии на когерентных состояниях с доказуемой криптографической стойкостью

С. Н. Молотков[1)]

Институт физики твердого тела РАН, 142432 Черноголовка, Россия

Академия криптографии РФ, 121552 Москва, Россия

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

Поступила в редакцию 13 июля 2015 г.

Предложен протокол квантовой криптографии, который является аналогом протоколов с распределенным кодированием, работающих на суб- и гигагерцовых тактовых частотах. В отличие от протоколов с распределенным кодированием, секретность которых до сих пор до конца не доказана, данный протокол допускает простое и интуитивно понятное доказательство секретности.

DOI: 10.7868/S0370274X15180150

Введение. Основная цель квантовой криптографии на данный момент состоит в увеличении дальности и скорости распределения ключей. При этом необходимо доказуемо гарантировать секретность ключей. Единственным практическим источником информационных квантовых состояний является сильно ослабленное лазерное излучение – когерентное состояние со средним числом фотонов $\mu \leq \leq 1$. Во всех практических протоколах в волоконной квантовой криптографии используется фазовое кодирование. Информационные состояния представляют собой набор когерентных состояний $\{|\alpha e^{i\varphi_i}\rangle\}_{i=1}^{N}$. Информация о битах ключа кодируется в относительную фазу когерентных состояний. Набор когерентных состояний является линейно-независимым, что служит необходимым и достаточным условием существования измерений с определенным исходом (Unambiguous Measurements) [1]. При таких измерениях неортогональные состояния могут быть идентифицированы однозначно, но с вероятностью, меньшей единицы (определенный исход). Всегда, также с вероятностью $\Pr(?) < 1$, существует неопределенный исход. Если вероятность потерь в канале связи $\Pr(\text{Loss}) \geq \Pr(?)$, то система квантовой криптографии не гарантирует секретности ключей. Другими словами, с некоторой длины L квантового канала связи (и потерь $\Pr(\text{Loss})$) подслушиватель *знает весь ключ, не производит ошибок на приемной стороне и не детектируется* [2]. Для увеличения дальности передачи ключей был предложен ряд протоколов [3–6]. Цель этих протоколов сводится к увеличению вероятности неопределенного исхода $\Pr(?)$. Данная проблема была решена принципиально и радикально для передачи ключей через открытое пространство, где скорость света близка к скорости света в вакууме. Были предложены протоколы распределения ключей, которые используют дополнительные ограничения на измеримость квантовых состояний, диктуемые специальной теорией относительности. Данные системы были названы релятивистской квантовой криптографией [7, 8]. Реализованы макетные варианты таких систем [8]. Важно, что в релятивистских системах квантовой криптографии UM-измерения *всегда (при любых, даже сколь угодно больших потерях), в отличие от нерелятивистских протоколов квантовой криптографии будут приводить к появлению ошибок на приемной стороне*. Кроме того, принципиально важно, что секретность ключей гарантируется даже не при строго однофотонном источнике квантовых состояний.

В протоколе DPS (Differential Phase Shift) [3, 4], перенесенном в квантовую криптографию из классических телекоммуникаций (см. рис. 1a) сечение a – серия ослабленных когерентных состояний, $|\alpha\rangle_1 \otimes \otimes |\alpha\rangle_2 \otimes \ldots \otimes |\alpha\rangle_n$. Сечение b после фазового модулятора – кодирование в разность фаз двух соседних состояний $|+\alpha\rangle_1 \otimes |-\alpha\rangle_2 \otimes \ldots \otimes |+\alpha\rangle_n$. Сечение c – относительный сдвиг на одну позицию серии состояний по верхнему и нижнему плечу интерферометра. Сечение d – конструктивная или деструк-

[1)]e-mail: sergei.molotkov@gmail.ru

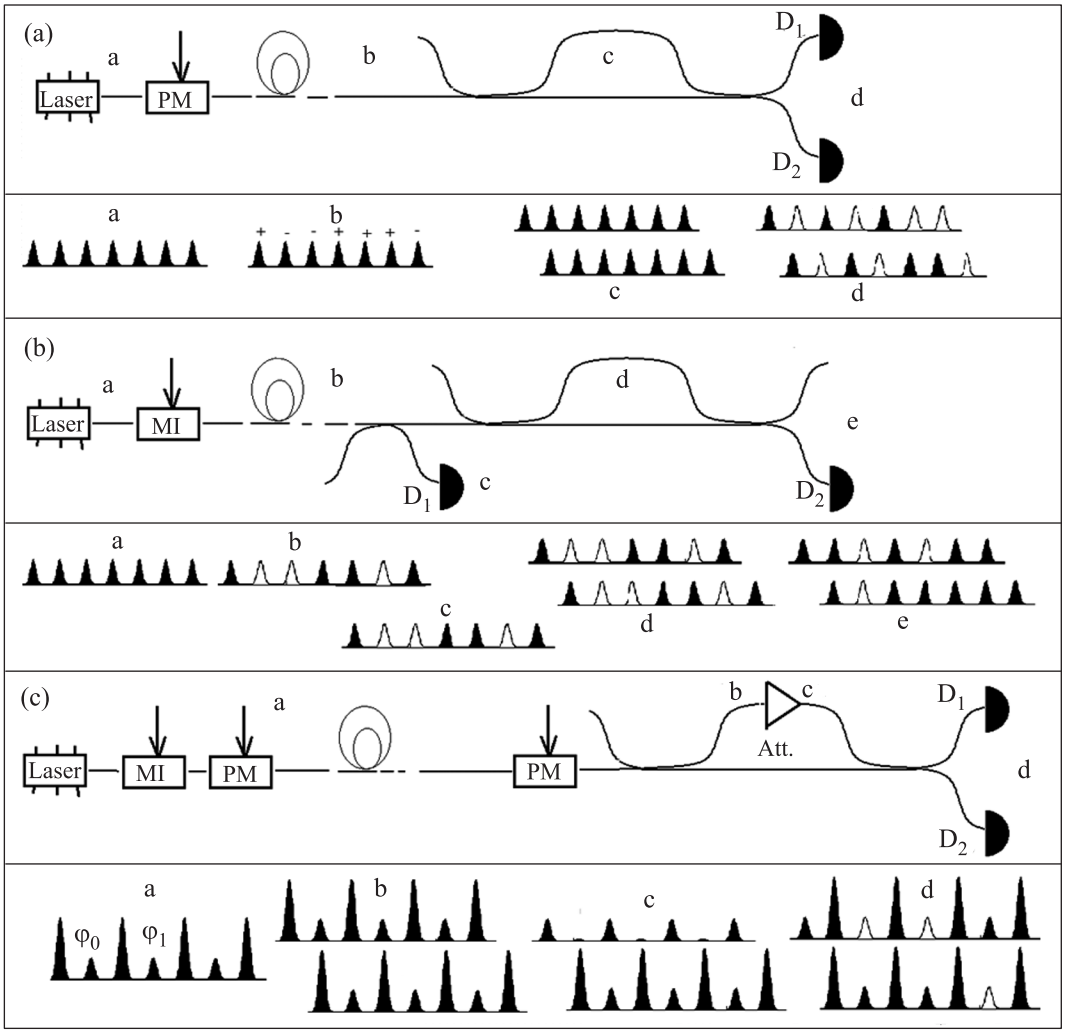

Рис. 1. (a) – Дифференциально-фазовое кодирование (DPS). (b) – Протокол COW. (c) – Кодирование с реперным когерентным состоянием

тивная интерференция на детекторе D_1 или D_2 в зависимости от фазы соседних состояний. Вероятность неопределенного исхода Pr(?) может быть сделана сколь угодно близкой к единице. Для успешных UM-измерений (чтобы подслушиватель не производил ошибок на приемной стороне) требуется различение всей последовательности $|\alpha_1\rangle \otimes |\alpha_2\rangle \otimes \ldots \otimes |\alpha_n\rangle$. Вероятность определенного исхода при этом экспоненциально падает с длиной последовательности n, что в принципе могло бы позволить передавать ключи при больших потерях. Однако секретность данного протокола, несмотря на многочисленные попытки, удовлетворительно не доказана [2]. Существуют доказательства только для отдельных атак, которыми, как все это понимают, ситуация не исчерпывается. Проблемы с доказательством упираются в то, что не работает квантовая теорема de Finnetti [9], поскольку невозможно свести атаку к атаке на отдельные посылки (искажение одного состояния приводит к искажению состояний в соседних посылках и т.д. во всей серии). Матрица плотности Алиса–Боб–Ева ρ^n_{ABE} не сводится к структуре тензорного произведения $\rho^{\otimes n}_{\mathrm{ABE}}$ (точнее, линейной оболочки тензорных произведений). Более того, неизвестна даже критическая ошибка протокола с когерентными состояниями в канале без потерь. Группой из Женевы была предложена модификация протокола DPS. Модифицированный протокол был назван COW (Coherent One Way) [6]. Идея с распределенным кодированием была сохранена, но и проблемы с доказательством секретности остались [2, 10–12]. Работа протокола с пояснениями представлена на рис. 1b. Сече-

ние a – последовательность когерентных состояний, аналогичная предыдущему случаю. Сечение b – после модулятора интенсивности кодирование происходит в пары соседних импульсов, $0 \to |\alpha\rangle_i \otimes |\mathrm{vac}\rangle_{i+1}$, $1 \to |\mathrm{vac}\rangle_i \otimes |\alpha\rangle_{i+1}$, control $\to |\alpha\rangle_i \otimes |\alpha\rangle_{i+1}$. Сечение c – регистрация в соседних временных окнах информационным детектором D_1. Сечение d – сдвиг на одну позицию состояний, распространяющихся по верхнему и нижнему плечу интерферометра. Сечение e – конструктивная или деструктивная интерференция для проверки когерентности в паре соседних импульсов для контрольного состояния.

Протокол квантового распределения ключей с реперным состоянием – аналог дифференциально-фазового кодирования с независимыми посылками. *При больших скоростях передачи ключей (при ГГц) идея распределенного кодирования является довольно естественной, поскольку расстояние по времени между посылками примерно равно длительности самих импульсов. Это также связано с техническими ограничениями. Технически модуляция и синхронизация происходят по гармоническому периодическому сигналу. Поэтому понятия отдельной посылки строго уже не существует. Однако распределенное кодирование приводит к недоказуемости криптографической стойкости таких систем.* Наша идея состоит в том, чтобы сохранить периодичность процесса кодирования, навязанную техническими ограничениями, но при этом отделить кодирование между "отдельными посылками" так, чтобы UM-измерения всегда приводили к ошибкам на приемной стороне, тем самым гарантируя обнаружение подслушивателя и доказуемую секретность ключей. Отметим, что идея реперного состояния восходит к работе [13]. Важность реперного состояния, на наш взгляд, до последнего времени не была до конца осознана. Идея достаточно прозрачна. Она состоит в чередовании через равные временные интервалы реперного (далее будем условно называть его классическим когерентным, см. ниже) и квазиоднофотонного когерентного состояния, в фазу которого кодируется информация о ключе. Реперный импульс не несет никакой информации о ключе. На приемной стороне часть реперного импульса отводится для регистрации, а часть ослабляется до уровня квазиоднофотонного и интерферирует с квазиоднофотонным состоянием (рис. 1). Число реперных импульсов на приемной стороне подсчитывается. Оно должно сохраняться (как мы увидим далее, это требование можно ослабить). Сохранение числа реперных импульсов не позволяет их блокировать. Блокировать или подменять можно лишь квазиоднофотонные состояния, если получен неопределенный исход. Однако из-за того, что часть ослабленного реперного импульса должна интерферировать с квазиоднофотонным импульсом, подмена истинного квазиоднофотонного импульса неизбежно будет приводить к ошибкам на приемной стороне. Используется свойство самоподобного преобразования когерентных состояний при линейном затухании. В линию связи посылается пара соседних когерентных состояний – интенсивное реперное (ref) и квазиоднофотонное (quan): $|\zeta\alpha\rangle_{\mathrm{ref}} \otimes |e^{i\varphi_{0,1}}\alpha\rangle_{\mathrm{quan}}$ ($\mu = |\alpha|^2 < 1$, $\zeta \gg 1$). После прохождения канала длиной L состояния самоподобно затухают: $|\zeta\alpha(L)\rangle_{\mathrm{ref}} \otimes |\alpha(L)\rangle_{\mathrm{quan}}$ ($\alpha(L) = \alpha \cdot 10^{-\delta L/20}$). На приемной стороне часть реперного состояния отводится для регистрации, а часть ослабляется в ζ раз ($|\zeta\alpha(L)\rangle_{\mathrm{ref}} \to |\alpha(L)\rangle_{\mathrm{ref}}$). При этом ослабление каждый раз постоянно и не зависит от длины линии. После ослабления реперное состояние с точностью до фазы эквивалентно квазиоднофотонному состоянию $|e^{i\varphi_{0,1}}\alpha(L)\rangle_{\mathrm{quan}}$, с которым и происходит интерференция (см. рис. 1c). Сечение a – серия одинаковых интенсивных когерентных состояний ослабляется через одно до квазиоднофотонного уровня модулятором интенсивности, а затем кодируется: изменяется фаза ослабленных состояний через одно, $0 \to \varphi_0$, $1 \to \varphi_1$. Перед интерферометром происходит декодирование – изменение фазы через одно состояние – для квазиоднофотонных состояний. На интерферометре состояния по верхнему пути сдвигаются на одну позицию по отношению к состояниям по нижнему пути. Сечение b – до аттенюатора. Сечение c – после аттенюатора. Все состояния ослабляются. Коэффициент ослабления постоянен и подобран так, чтобы ослабить состояния в ζ раз. Затем интенсивные когерентные состояния в верхнем плече становятся такими же по амплитуде, как и квазиоднофотонные состояния в нижнем плече. Сечение d – детекторы D_1 и D_2 стробируются в четных и нечетных временных окнах. Детектор D_1 регистрирует наличие интенсивных реперных состояний, а D_2 – квазиоднофотонные информационные состояния. Интерференция на выходе интерферометра важна для квазиоднофотонных состояний и не важна для реперных.

В результате UM-измерения не позволят подслушивателю знать ключ и не производить ошибок (оставаться недетектируемым) даже при больших потерях из-за невозможности блокировать реперные импульсы. При этом кодирование производится в каждое отдельное квазиоднофотонное состояние, что позволяет доказать секретность протокола.

Доказательство оказывается простым и интуитивно понятным.

Секретность и корректность ключей. После передачи квантовых состояний и их измерения на приемной стороне Алиса и Боб имеют битовые строки длины n: $\mathcal{X}_A = \{0,1\}^n$, $\mathcal{X}_B = \{0,1\}^n$. Строка Боба содержит ошибки. После коррекции ошибок через открытый канал и проверки их идентичности возникает очищенный ключ $\mathcal{X} = \mathcal{X}_A$[2)]. Вероятность того, что ключи отличаются, не превышает $\Pr(X_A \neq X_B) \leq 1/2^M = \varepsilon_{\rm corr}$, где $\varepsilon_{\rm corr}$ – параметр корректности ключей. При коррекции ошибок в битовой последовательности Боба X_B выдается leak_n бит классической информации (с учетом проверки идентичности ключей – $\mathrm{leak}_n + M$ бит). После исправления ошибок происходит сжатие (хэширование – усиление секретности) очищенного ключа длины n до финального секретного ключа длиной $k = [R_k]$ – $\mathcal{X} = \{0,1\}^n \to \mathcal{K} = \{0,1\}^k$, где квадратные скобки обозначают целую часть. Пусть $(k_1, k_2, \ldots, k_k)$ – битовая строка Алисы и Боба – секретный ключ. Ева в конце протокола имеет в распоряжении квантовую систему, коррелированную с данной строкой. Совместная матрица плотности Алиса(Боб)–Ева $\rho_{KE} = |K\rangle\langle K| \otimes \rho_E^K$, $|K\rangle = |k_1\rangle \otimes |k_2\rangle \otimes \ldots \otimes |k_k\rangle$. Информацию о ключе Ева получает в результате измерений, которые описываются некоторым разложением единицы $I = \sum_{K\in\mathcal{K}} \mathcal{M}_K$, где $\mathcal{M}_K$ – операторнозначные меры. Условная вероятность узнать текущий ключ K, имея квантовую систему, есть

$$\Pr_{\rm guess}(K|E) = \mathrm{Tr}\{\mathcal{M}_K \rho_E^K\}. \tag{1}$$

Средняя по всем ключам условная вероятность угадывания ключа Евой при условии, что она имеет доступ к квантовой системе, коррелированной с ключом, согласно [14] ограничена сверху величиной

$$\Pr_{\rm guess}(\mathcal{K}|E) = \frac{1}{2^k} \max_{\mathcal{M}_K} \sum_{K\in\mathcal{K}} \mathrm{Tr}\{\mathcal{M}_K \rho_E^K\} \leq$$

$$\leq \frac{1}{2^k} + D(\rho_{\mathcal{K}E}, \rho_{U\mathcal{K}} \otimes \rho_E), \tag{2}$$

$$D(\rho_{\mathcal{K}E}, \rho_{U\mathcal{K}} \otimes \rho_E) = \frac{1}{2}||\rho_{\mathcal{K}E} - \rho_{U\mathcal{K}} \otimes \rho_{E^n}||_1 = \Delta,$$

$$\rho_{\mathcal{K}E} = \frac{1}{2^k} \sum_{K\in\mathcal{K}} |K\rangle\langle K| \otimes \rho_E^K, \tag{3}$$

где $\rho_{U\mathcal{K}} = \frac{1}{2^k}\sum_{K\in\mathcal{K}} |K\rangle\langle K|$ – однородная по ключам матрица плотности. При $\Delta = 0$ реализуется идеальная ситуация, когда вероятность (2) равна вероятности простого угадывания: $\Pr_{\rm guess}(\mathcal{K}|E) = \frac{1}{2^k}$. Финальный секретный ключ получается после исправления ошибок в исходной битовой строке $\mathcal{X} = \{0,1\}^n$ и дальнейшего сжатия (усиление секретности – privacy amplification) очищенного ключа при помощи случайных универсальных хэш-функций второго порядка [15], $f : \mathcal{X} = \{0,1\}^n \to \mathcal{K} = \{0,1\}^k$ (множество хэш-функций $\mathcal{F}$, которые генерируются публично и доступны Еве). Пусть исходная матрица плотности до всех процедур есть

$$\rho_{\mathcal{X}E} = \frac{1}{2^n} \sum_{X\in\mathcal{X}} |X\rangle\langle X| \otimes \rho_E^X,$$
$$|X\rangle = |x_1\rangle \otimes |x_2\rangle \otimes \ldots \otimes |x_n\rangle. \tag{4}$$

Согласно теореме о хэшировании (теорема Leftover Hash [9, 16]) расстояние до идеальной ситуации после сжатия становится равным ($\rho_{\mathcal{K}E} = \rho_{\mathcal{F}(\mathcal{X})E\mathcal{F}}$ – матрица плотности после хэширования)

$$D(\rho_{\mathcal{K}E}, \rho_{U\mathcal{K}} \otimes \rho_E) = D(\rho_{\mathcal{F}(\mathcal{X})E\mathcal{F}}, \rho_{U\mathcal{K}} \otimes \rho_{E\mathcal{F}}) =$$
$$= \frac{1}{2}||\rho_{\mathcal{F}(\mathcal{X})E\mathcal{F}} - \rho_{U\mathcal{K}} \otimes \rho_{E\mathcal{F}}||_1 =$$
$$= \Delta < \varepsilon + \tfrac{1}{2}\sqrt{2^{-(H_{\min}^{\varepsilon}(X|CE)-R_k)}}, \tag{5}$$

$$\rho_{\mathcal{K}E} = \sum_K |K\rangle\langle K| \otimes \left(\sum_f p_f |f\rangle\langle f| \otimes \rho_E^{fK}\right) =$$
$$= \sum_K |K\rangle\langle K| \otimes \rho_E^K,$$
$$\rho_E^{fK} = \sum_{X, X=f^{-1}(K)} \rho_{XE}, \quad p_f = \frac{1}{|\mathcal{F}|}. \tag{6}$$

Степень сжатия определяется сглаженной min-*энтропией, которая зависит от протокола квантового распределения ключей.* (Определение и свойства сглаженной min-энтропии подробно описаны в [9].) Если длина секретного ключа выбрана

$$R_k \leq H_{\min}^{\varepsilon}(X|CE) - 2\log(1/2\varepsilon), \tag{7}$$

то расстояние до идеальной ситуации $\Delta < \varepsilon$. Остается только оценить $H_{\min}^{\varepsilon}(X|CE)$ до сжатия ключа. Величина C аккумулирует всю информацию, переданную по классическому каналу при коррекции ошибок и проверке идентичности очищенных ключей. Пусть число переданных бит равно leak_n. Тогда имеет место оценка

$$H_{\min}^{\varepsilon}(X|CE) \geq H_{\min}^{\varepsilon}(X|E) - \mathrm{leak}_n - 2\log(1/2\varepsilon). \tag{8}$$

[2)] Проверка сводится к генерированию публично случайной строки бит длиной n, сложению ее по модулю 2 со строками $\mathcal{X}_A$ и $\mathcal{X}_B$ и вычислению бита четности. Процедура повторяется M раз. Если все биты четности совпадают, то имеет место приведенная оценка вероятности. В противном случае ключ отбрасывается.

Для структуры тензорного произведения, $H^{\varepsilon}_{\min}(X|E) = H^{\varepsilon}_{\min}(\rho^{\otimes n}_{XE}|\rho^{\otimes n}_{E})$, имеем (детали см. в [9])

$$H^{\varepsilon}_{\min}(\rho^{\otimes n}_{XE}|\rho^{\otimes n}_{E}) \geq n[H(\rho_{XE}|\rho_{E}) - \delta(\varepsilon)], \qquad (9)$$

где $\delta(\varepsilon) = \log(5)\sqrt{2\log(1/2\varepsilon)/n}$. До сего момента протокол был неважен (лишь бы кодирование производилось независимо в отдельные посылки). Условная сглаженная энтропия (8) содержит в себе всевозможные атаки Евы. Именно вычисление этой величины представляет наибольшую сложность. Неформально величина (9) есть количество бит информации, которых не хватает Еве, чтобы, имея квантовую систему, знать X. Вместо того чтобы перебирать всевозможные атаки Евы, найдем нижнюю фундаментальную границу для этой величины. Если UM-измерения запрещены (в том смысле, что все реперные импульсы должны быть зарегистрированы), то возможна только унитарная атака Евы на передаваемые состояния. В этом случае величина доступной классической информации, которую можно извлечь из квантовых состояний, ограничена фундаментальной величиной Холево [17]. Возмущение состояний приводит к ошибкам на приемной стороне. Поэтому обычный подход сводится к установлению связи между информацией Евы и потоком ошибок на приемной стороне. Мы примем консервативный подход, развязав ошибки от информации Евы. Независимо от потока ошибок величина (9) ограничивается величиной Холево. Ясно, что это завышает информацию Евы, но избавляет от увязывания потока ошибок на приемной стороне с информацией Евы. *Вероятность ошибок Q на приемной стороне входит в финальную длину ключа только через информацию* $\mathrm{leak}_n(Q)$ *– число бит, реально переданных через открытый канал связи при чистке ошибок.*

Асимптотический предел, все реперные импульсы регистрируются. В протоколе используется пара квазиоднофотонных информационных состояний $\{|\alpha e^{i\varphi_0}\rangle_{\mathrm{quan}}, |\alpha e^{i\varphi_1}\rangle_{\mathrm{quan}}\}$ (далее индекс "quan" опускается). Асимптотический предел отвечает ситуации, когда $n \to \infty$, $\varepsilon \to 0$ и $k = \lim_{n\to\infty}\frac{R_n}{n}$. В этом случае наилучшей оценкой в пользу Евы для условной энтропии фон Неймана является нижняя граница, которая определяется величиной Холево $\chi(\rho_A)$. Фактически считается, что Ева имеет прямой доступ к источнику состояний Алисы. В нашем случае величина Холево равна классической пропускной способности идеального квантового канала:

$$H(\rho_{XE}|E) = 1 - \chi(\rho_A), \quad \chi(\rho_A) = \overline{C}(\rho_A),$$
$$\overline{C}(\rho_A) = -\xi_+\log\xi_+ - \xi_-\log\xi_-, \qquad (10)$$

где $\xi_{\pm} = (1 \pm \xi)/2$, $\rho_A = (|\alpha e^{i\varphi_0}\rangle\langle\alpha e^{i\varphi_0}| + |\alpha e^{i\varphi_1}\rangle\langle\alpha e^{i\varphi_1}|)/2$, $\overline{C}(\rho_A)$ – классическая пропускная способность идеального квантового канала связи с квантовым источником состояний $\{|\alpha e^{i\varphi_0}\rangle, |\alpha e^{i\varphi_1}\rangle\}$ и вероятностями $p_0 = p_1 = 1/2$, а величина $\xi = |\langle\alpha e^{i\varphi_0}|\alpha e^{i\varphi_1}\rangle|$ равна вероятности неопределенного исхода для оптимального измерения, различающего пару чистых неортогональных состояний $\Pr(?) = |\langle e^{\alpha\varphi_0}|e^{\alpha\varphi_1}\rangle| = e^{-2\mu\sin^2(\frac{\varphi_0-\varphi_1}{2})}$, $\mu = |\alpha|^2 < 1$.

Утечка информации зависит от процедуры при коррекции ошибок. При коррекции ошибок случайными шенноновскими кодами утечка информации к Еве является минимальной и в асимптотическом пределе равна $\mathrm{leak}_{\mathrm{Shan}}(Q) = \lim_{n\to\infty}\frac{\mathrm{leak}_n(Q)}{n} = h(Q)$ (где Q – наблюдаемая ошибка на приемной стороне). Для реально используемой чистки кодами Хэмминга с дополнительной проверкой на четность $\mathrm{leak}_{\mathrm{Hamm}}(Q) = \lim_{n\to\infty}\frac{\mathrm{leak}_n(Q)}{n} = 1 - \big(0.99827e^{-Q/0.112922} - 0.06851\big)$. Для длины секретного ключа (доли секретных бит в пересчете на посылку) в шенноновском пределе получаем

$$r_k = \lim_{n\to\infty}\frac{R_k}{n} = 1 - h(Q) - \overline{C}(\rho_A). \qquad (11)$$

Интуитивная интерпретация (11) достаточно прозрачна. На качественном уровне секретный ключ представляет собой разницу информации у Боба и у Евы. Информация Боба на посылку есть 1. Информация Евы состоит из двух частей: информации, полученной из открытого классического канала при коррекции ошибок ($\mathrm{leak}_n(Q)$, и информации из квантового канала, которая не превышает фундаментальную величину Холево.

Асимптотический предел, не все реперные импульсы регистрируются. В случае неопределенного исхода подслушиватель может блокировать реперное состояние, чтобы не производить ошибок. В случае определенного исхода Ева может перепосылать достоверно определенное состояние. В остальных посылках, где реперные импульсы не блокируются, ситуация сводится к предыдущему случаю. Пусть Ева делает UM-измерения в доле $n\zeta$ посылок. Пусть часть x реперных импульсов не регистрируется. Подслушиватель проводит UM-измерения. Вероятность неопределенного исхода есть $\Pr(?) = |\langle\alpha e^{i\varphi_0}|\alpha e^{i\varphi_1}\rangle|$. При этом в доле $n\zeta\Pr(?)$ посылок будет получен неопределенный исход, а в остальных $n\zeta[1 - \Pr(?)]$ посылках – определенный исход. Эти

посылки будут отброшены, т.к. они не дают никакой информации Еве, а только приводят к ошибкам на стороне Боба. Полное число зарегистрированных посылок есть $n(1-x) = n(1-\zeta) + n\zeta[1-\Pr(?)]$, где $\zeta = x/\Pr(?)$. Для длины секретного ключа в шенноновском пределе находим

$$r_k = \lim_{n\to\infty} \frac{R_k}{n} = (1-x)[1-h(Q)] - \\ - [1 - x/\Pr(?)]\,\overline{C}(\rho_A) - [(1-\Pr(?)]x/[\Pr(?)]. \quad (12)$$

При коррекции ошибок другой процедурой $h(Q)$ должно быть заменено, например на $\mathrm{leak}_{\mathrm{Hamm}}(Q)$. Неформальная качественная интерпретация (12) достаточно прозрачна. Первое слагаемое, $n(1-x)[1-h(Q)]$ – взаимная информация между Алисой и Бобом после коррекции ошибок. Второе слагаемое, $n[1-x/\Pr(?)]\overline{C}(\rho_A)$ – верхняя граница информации Евы, получаемой ею из $n[1-x/\Pr(?)]$ посылок, в которых (консервативно в ее пользу) она напрямую имеет доступ к источнику квантовых состояний Алисы. Третье слагаемое – информация, которую получает Ева, проводя UM-измерения в $n\zeta = nx/\Pr(?)$ посылках. Число определенных исходов $n[1-\Pr(?)]/[x\Pr(?)]$. Остальные посылки с неопределенным исходом, чтобы не возникло ошибок у Боба, блокируются вместе с реперным состоянием.

Конечная последовательность, не все реперные импульсы регистрируются. Для сглаженной энтропии в этом случае имеет место оценка

$$H_{\min}^{\varepsilon_?+\varepsilon_c}(\rho_{XE}^{\otimes n(1-x)}|\rho_E^{\otimes n(1-x)}) = \\ = H_{\min}^{\varepsilon_?+\varepsilon_c}(\rho_{XE}^{\otimes n\zeta_?}\otimes\rho_{XE}^{\otimes n\zeta_c}|\rho_E^{\otimes n\zeta_?}\otimes\rho_E^{\otimes n\zeta_c}) \geq \\ \geq H_{\min}^{\varepsilon_?}(\rho_{XE}^{\otimes n\zeta_?}|\rho_E^{\otimes n\zeta_?}) + H_{\min}^{\varepsilon_c}(\rho_{XE}^{\otimes n\zeta_c}|\rho_E^{\otimes n\zeta_c}), \quad (13)$$

где неравенство следует из супераддитивности сглаженной энтропии с учетом того, что $\zeta_c = (1-\zeta)$, $\zeta_? = \zeta[1-\Pr(?)]$, $\zeta = x/\Pr(?)$, $1-x = \zeta_c+\zeta_?$. Для энтропии имеет место оценка $H_{\min}^{\varepsilon_?}(\rho_{XE}^{\otimes n\zeta_?}|\rho_E^{\otimes n\zeta_?}) \geq -n\zeta_?\delta(\varepsilon_?)$. Это консервативно в пользу Евы. Ева (при $n\to\infty$) после UM-измерений знает $n\zeta_? = n\zeta[1-\Pr(?)]$ бит. Грубо говоря, при конечных n за счет статистических флуктуаций Ева может знать дополнительно в среднем еще $n\zeta_?\delta(\varepsilon_?)$ бит. Величина $\delta(\varepsilon_?)$ аналогична $\delta(\varepsilon)$, фигурирующей после формулы (9). Далее, для $H_{\min}^{\varepsilon_c}(\rho_{XE}^{\otimes n\zeta_c}|\rho_E^{\otimes n\zeta_c})$ с учетом (13) получаем

$$H_{\min}^{\varepsilon_c}(\rho_{XE}^{\otimes n\zeta_c}|\rho_E^{\otimes n\zeta_c}) \geq n\zeta_c[1-\overline{C}(\rho_A) - \delta(\varepsilon_c)], \quad (14)$$

где $\delta(\varepsilon_c)$ аналогична предыдущему. Длину секретного ключа удобно записать в виде

$$R_k = n(1-x)[1-\mathrm{leak}_n(Q)] - n\left[1 - \frac{x}{\Pr(?)}\right]\times \\ \times C(\rho_A) - n\frac{[1-\Pr(?)]x}{\Pr(?)} - n(1-x)\delta(\varepsilon), \quad (15)$$

где положено $\delta(\varepsilon_c) = \delta(\varepsilon_?) = \delta(\varepsilon)$, $\mathrm{leak}_n(Q)$ – число раскрытых бит (в пересчете на посылку) при коррекции ошибок в последовательности длины $n(1-x)$. Напомним, что $n(1-x)$ – число реально зарегистрированных посылок. *Важно подчеркнуть, что в формулы для длины ключа входят только наблюдаемые на приемной стороне параметры.*

Вычисление длины секретного ключа в зависимости от длины линии. Важным параметром любой системы квантовой криптографии является дальность передачи ключей с гарантией секретности. Оценим дальность передачи секретных ключей в зависимости от длины волоконной линии связи, среднего числа фотонов в информационном состоянии и темновых шумов. В отсутствие подслушивателя ошибки возникают в основном от темновых шумов. Напомним, что ошибки от шумов и подслушивателя принципиально не отличимы. Будем считать, что ошибки возникают только от темновых шумов. Тогда $Q(L) = \frac{1}{2}\frac{p_d}{p_d+n_{\mathrm{reg}}(L)}$; $n_{\mathrm{reg}}(L) = 1 - e^{-\eta\eta_{\mathrm{APD}}\mu(L)}$; $\mu(L) = 2\mu\sin^2(\Delta\varphi)\cdot 10^{-\frac{\delta\cdot L}{10}}$; $\Delta\varphi = \frac{\varphi_0-\varphi_1}{2}$. Здесь L – длина линии связи, $n_{\mathrm{reg}}(L)$ – вероятность зарегистрировать информационное квантовое состояние однофотонным детектором, η_{APD} – квантовая эффективность однофотонного детектора, η – коэффициент светоделителя (см. рис. 1), p_d – вероятность темновых шумов.

Заключение. Как видно из рис. 2a, 3a и 4a, при типичной вероятности темновых шумов $p_d = 5\cdot 10^{-6}$ и стандартном одномодовом волокне с $\delta = 0.2$ дб/км протокол обеспечивает секретность ключей на расстоянии, превышающем 100 км. При этом в отличие от протоколов DPS и COW доказательство секретности данного протокола является прозрачным. Важно, что в формулу для длины секретного ключа не входят никакие параметры однофотонных детекторов, как это неявно имеет место в протоколе Decoy State [18], где в разных посылках требуется отличать квазиоднофотонные состояния с разным числом фотонов. При темновых шумах $p_d = 5\cdot 10^{-9}$ (рис. 3a и 4b) и волокне с уменьшенными потерями ($\delta = 0.16$ дб/км) дальность секретной передачи ключей гарантированно превышает 300 км. Для волокна с потерями ($\delta = 0.1$ дб/км) ожидаемая дальность достигает 500 км. Отметим, что рекорд дальности передачи ключей по протоколу COW был продемонстрирован в работе [19] ($p_d \approx 5\cdot 10^{-9}$ и $\delta = 0.16$ дб/км).

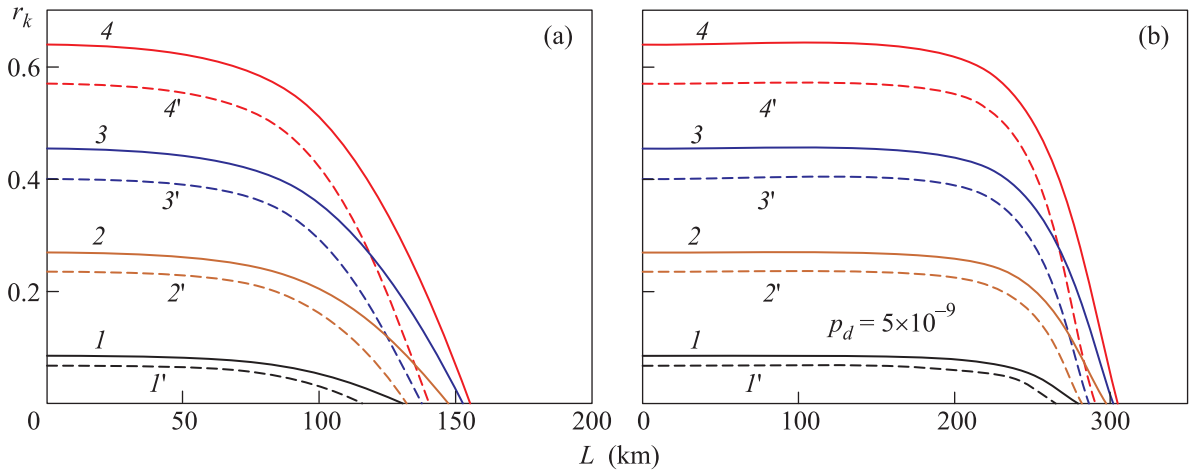

Рис. 2. (Цветной онлайн) Длина секретного ключа r_k в пересчете на посылку в асимптотическом пределе. Кривые с номерами без штрихов – коррекция ошибок случайными шенноновскими кодами, со штрихами – кодами Хэмминга с дополнительной проверкой четности. Общие параметры для кривых: *1*, *1′* – $x = 0.75$; *2*, *2′* — $x = 0.50$; *3*, *3′* – $x = 0.25$; *4*, *4′* – $x = 0.0$. Квантовая эффективность однофотонного детектора $\eta_{\mathrm{APD}} = 0.2$, потери в волокне $\delta = 0.2$ дб/км, среднее число фотонов в квазиоднофотонном состоянии на входе в линию $\mu = 0.5$, $(\varphi_0 - \varphi_1)/2 = \pi/8$. Вероятность темновых шумов на строб для всех кривых: $p_d = 5 \cdot 10^{-6}$ (a) и $5 \cdot 10^{-9}$ (b)

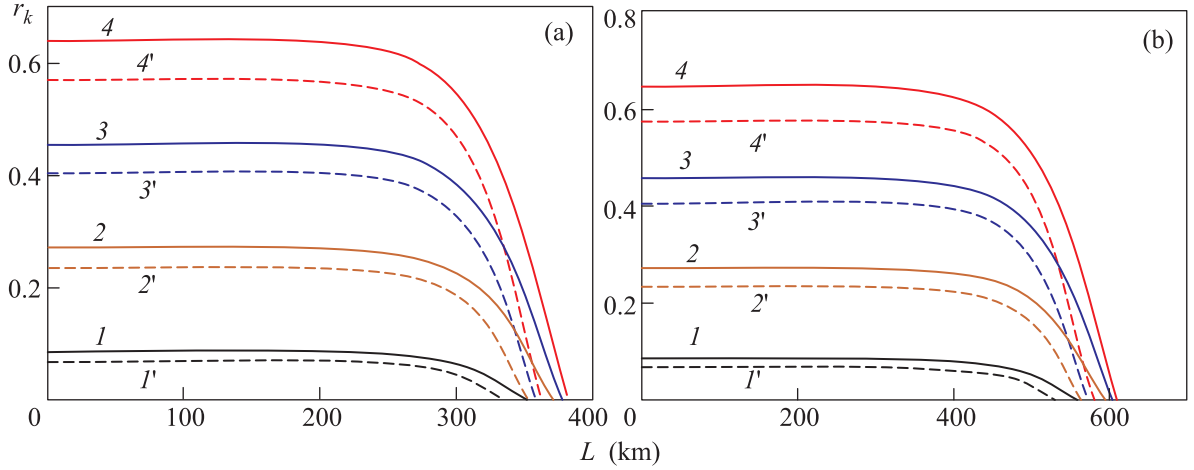

Рис. 3. (Цветной онлайн) Длина секретного ключа r_k в пересчете на посылку в асимптотическом пределе. Все параметры аналогичны параметрам рис. 2, кроме вероятности темновых шумов, $p_d = 5 \cdot 10^{-9}$. Потери в линии $\delta = 0.16$ дб/км (a) и 0.1 дб/км (b)

При этом для достижения такой длины темновые шумы вычитались из длины ключа. Последнее строго недопустимо, поскольку здесь явно используются предположения о свойствах однофотонного детектора, которые могут меняться от посылки к посылке. Несмотря на замечательный результат [19], оценка дальности в ней является завышенной. Это видно из следующих рассуждений. В данном протоколе (при $x = 0$, полный запрет UM-измерений) дальность едва превышает 300 км (рис. 4b). Кроме того, угол между информационными состояниями в канале в нем меньше (отдельные состояния хуже различимы). Поэтому при прочих равных параметрах длина передачи протокола COW не может превосходить длину передачи протокола с реперным состоянием. Как видно из рис. 2–4, достаточно, чтобы реперные состояния регистрировались только в половине посылок. Наш опыт показывает, что однофотонный лавинный детектор срабатывает в каждой посылке при числе фотонов на входе $\mu \approx 50$. Соответственно для срабатывания в половине посылок $\mu \approx 25$. При потерях в линии в 50 дб требуется $\approx 10^6$ фотонов на посылку на входе в канал на передающей станции. При длине 100 км ($\delta = 0.2$ дб/км) требуется $\approx 2.5 \cdot 10^3$ фотонов в реперном импульсе.

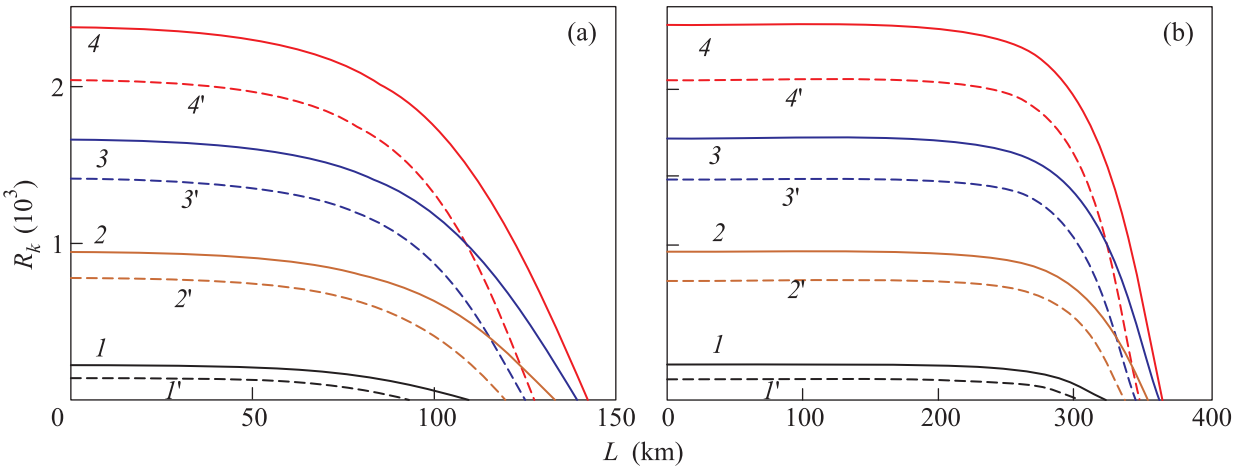

Рис. 4. (Цветной онлайн) Длина секретного ключа R_k в пределе конечных последовательностей. Длина исходного ключа $n = 5 \cdot 10^3$. (a) – $p_d = 5 \cdot 10^{-6}$, $\delta = 0.2$ дб/км; (b) – $p_d = 5 \cdot 10^{-9}$, $\delta = 0.16$ дб/км. Остальные параметры такие же, как на рис. 2. Параметр секретности $\varepsilon = 10^{-20}$. Параметр $M = 0$

Автор выражает благодарность К.А. Балыгину, А.Н. Климову, К.С. Кравцову, С.П. Кулику, И.В. Радченко, а также коллегам по Академии криптографии Российской Федерации за полезные обсуждения.

1. A. Chefles, Phys. Lett. A **239**, 339 (1998); A. Chefles and S. M. Barnett, Phys. Lett. A **250** 223 (1998).
2. V. Scarani, V. H. Bechmann-Pasquinucci, N. J. Cerf, M. Dušek, N. Lütkenhaus, and M. Peev, Rev. Mod. Phys. **81**, 1301 (2009).
3. K. Inoue, E. Waks, and Y. Yamamoto, Phys. Rev. Lett. **89**, 037902 (2002); Phys. Rev. A **68**, 022317 (2003).
4. H. Takesue, S. W. Nam, Q. Zhang, R. H. Hadfield, T. Honjo, K. Tamaki, and Y. Yamamoto, Nat. Photonics **1**, 343 (2007).
5. K. Wen, K. Tamaki, and Y. Yamamoto, arXiv:quant-ph: 0806.2684.
6. D. Stucki, N. Brunner, N. Gisin, V. Scarani, and H. Zbinden, Appl. Phys. Lett. **87**, 194108 (2005).
7. S. N. Molotkov, JETP **112**, 370 (2011); JETP Lett. **94**, 469 (2011); JETP Lett. **96**, 342 (2012); S. N. Molotkov and T. A. Potapova, Laser Phys. Lett. **10**, 075205 (2013).
8. I. V. Radchenko, K. S. Kravtsov, S. P. and S. N. Molotkov, Laser Phys. Lett. **11**,Kulik, 065203 (2014); arXiv:quant-ph/1403.3122.
9. R. Renner, *Security of Quantum Key Distribution*, PhD Thesis, ETH Zürich, Dec. (2005); arXiv/quant-ph: 0512258.
10. C. Branciard, N. Gisin, N. Lütkenhaus, and V. Scarani, Appl. Phys. Lett. **87**, 194108 (2005).
11. C. Branciard, N. Gisin, and V. Scarani, New J. Phys. **10**, 013031 (2008); arXiv:quant-ph:0710.4884.
12. D. Stucki, C. Barreiro, S. Fasel, J.-D. Gautier, O. Gay, N. Gisin, R. Thew, Y. Thoma, P. Trinkler, F. Vannel, and H. Zbinden, Opt. Express **17**, 13326 (2008); arXiv:quant-ph:08095264.
13. C. H. Bennett, Phys. Rev. Lett. **68**, 3121 (1992).
14. C. Portmann and R. Renner, arXiv/quant-ph: 1409.3525.
15. J. L. Carter and M. H. Wegman, J. Comp. Sys. Sci. **18**, 143 (1979).
16. H. Tomamichel, C. Schaffner, A. Smith, and R. Renner, IEEE Trans. Inf. Theory **57**, 5524 (2011); arXiv:quant-ph: 10022436.
17. A. S. Holevo, *Quantum coding theorems*, Rus. Math. Surveys **53,** 1295 (1998).
18. W.-Y. Hwang, Phys. Rev. Lett. **91**, 057901-1 (2003).
19. B. Korzh, C. C. W. Lim, R. Houlmann, N. Gisin, M. J. Li, D. Nolan, B. Sanguinetti, R. Thew, and H. Zbinden, Nat. Photonics **9**, 163 (2014).