Письма в ЖЭТФ, том 95, вып. 6, с. 361 – 366 © 2012 г. 25 марта

О геометрически однородных когерентных состояниях в квантовой криптографии

С. Н. Молотков

Академия криптографии РФ, 121552 Москва, Россия

Институт физики твердого тела РАН, 142432 Черноголовка, Россия

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

Поступила в редакцию 10 января 2012 г.

После переработки 14 февраля 2012 г.

Предложено семейство однотипных протоколов квантового распределения ключей на геометрически однородных когерентных состояниях лазерного излучения. Проведен анализ их криптографической стойкости относительно унитарной атаки, атаки с расщеплением когерентного состояния и атаки с измерениями с определенным исходом. Выбор того или иного протокола может осуществляться автоматически в зависимости от параметров системы и требуемой длины линии.

Введение. Целью квантовой криптографии является передача криптографических ключей по открытым, доступным для прослушивания и любой модификации каналам связи при помощи специальных протоколов, использующих квантовые состояния, таким образом, чтобы на приемной (обычно называемой Бобом) и передающей (Алиса) стороне возник идентичный и известный только им секретный ключ – случайная строка бит. На практике такими каналами являются либо оптоволоконные линии связи, либо открытое пространство. В канале без потерь фундаментальные законы квантовой механики гарантируют детектирование любых попыток вторжения в канал связи. Величина возмущения (ошибки) связана с утечкой информации к подслушивателю. Поэтому чем больше критическая ошибка, тем бóльшие собственные шумы и более интенсивные вторжения в канал связи, при которых все еще гарантируется секретность передаваемых ключей, допустимы. Ошибки на приемной стороне также возникают из-за неидеальностей аппаратуры (в основном из-за темновых шумов лавинных детекторов). Поскольку ошибки от шумов и действий подслушивателя принципиально неразличимы, все ошибки приходится списывать на действия подслушивателя. Поэтому одно из главных требований, предъявляемых к квантовым протоколам распределения ключей, состоит в том, чтобы допустимая критическая ошибка, до которой гарантируется секретное распределение ключей, имела максимально возможное значение.

Ситуация радикально меняется, если канал имеет потери и источник квантовых состояний не является строго однофотонным. В этом случае возможны атаки, при которых при длине линии выше некоторой критической подслушиватель получает всю информацию о ключе и не производит ошибок на приемной стороне (подробности см. в [1]).

На сегодняшний день не существует технологически приемлемого однофотонного источника излучения на телекоммуникационной длине волны. В качестве квазиоднофотонных состояний используются ослабленные когерентные состояния (лазерное излучение). Неоднофотонность источника, потери в оптоволокне и темновые шумы фотодетекторов являются факторами, ограничивающими дальность передачи ключей. Были предложены различные протоколы для увеличения дальности передачи: SARG04, decoy state, DPS, COW и т.д. [1–6]. Разнородность протоколов приводит к тому, что для каждого протокола необходимо использовать свои оптоволоконную схему и управляющую электронику, проводить отдельный анализ криптографической стойкости. Для ряда протоколов ввиду их непрозрачности и сложности полный анализ до сих пор не сделан. Несмотря на это, в Евросоюзе начат процесс стандартизации протоколов и систем квантовой криптографии (см. [7]). *Возникла насущная практическая необходимость* иметь набор (стэк) однородных и однотипных протоколов, которые были бы прозрачны для анализа стойкости, обеспечивали бы максимальную дальность передачи ключей, могли бы быть реализованы на одной и той же базовой оптоволоконной схеме и общей управляющей электронике. При этом выбор того или иного протокола должен осуществляться автоматически в зависимости от длины оптоволоконного канала связи. В работе предлагается стэк протоколов на геометрически однородных когерентных состояниях. Проведен анализ их стойкости.

Протокол квантового распределения ключей и информационные состояния. Протокол состоит из стандартной последовательности шагов: 1) Алиса выбирает протокол, фактически фиксирует N; 2) случайно и равновероятно выбирает один из базисов b из $N/2$ штук; 3) случайно и равновероятно выбирает одно из информационных состояний внутри базиса (значение бита), 0 – $|\varphi_{0b}\rangle$ или 1 – $|\varphi_{1b}\rangle$; 4) Боб случайно и равновероятно и независимо от Алисы выбирает базис и *одно из двух измерений* в этом базисе. Каждое измерение имеет два исхода. Один из исходов фактически отвечает проектированию на ортогональное состояние одного из состояний в базисе. Второй исход в каждом измерении является исходом с неопределенным результатом и далее отбрасывается; 5) через открытый канал Алиса и Боб согласуют базисы. Посылки, где базисы не совпадали, а также посылки при совпадающих базисах, где у Боба были неопределенные исходы, отбрасываются. После этой стадии Алиса и Боб имеют битовые строки. Строка Боба содержит ошибки; 6) часть последовательности раскрывается для оценки вероятности ошибки. Эта раскрытая часть далее отбрасывается; 7) если наблюдаемая ошибка меньше критической, то через открытый канал происходит коррекция ошибок. Теперь Алиса и Боб имеют одинаковые битовые строки. Ева имеет частичную информацию об этом очищенном ключе; 8) очищенный ключ хэшируется (сжимается) до битовой строки меньшего размера при помощи универсальной хэш-функции второго порядка, которая выбирается случайно и открыто через классический канал связи. Сжатая битовая строка является секретным ключом, о котором подслушиватель не имеет никакой информации (детали см. в [8]).

Далее удобно воспользоваться версией на запутанных состояниях, которая является формальным приемом и эквивалентна версии приготовление–посылка, изложенной выше. Версия на запутанных состояниях позволяет воспользоваться формальным аппаратом, развитым в [8], и сократить вычисление длины секретного ключа, поскольку в этой версии возможно прямое вычисление условных энтропий фон Неймана, через которые выражается длина ключа (см. ниже).

В этой версии Алиса выбирает только базис и готовит запутанное состояние, которое потенциально содержит оба информационных состояния подсистемы Боба в выбранном базисе. Подсистема A остается в распоряжении Алисы, а подсистема B направляется Бобу. Для того чтобы фиксировать информационное состояние Боба, Алиса делает измерения над своей подсистемой в базисе $\{|0_b\rangle_A, |1_b\rangle_A\}$ (некоторые формальные ортогональные состояния). В результате подсистема Боба случайно и равновероятно переходит в одно из информационных состояний, $|\varphi_{0b}\rangle_B$ или $|\varphi_{1b}\rangle_B$, над которыми Боб производит одно из двух своих измерений. Остальные шаги протокола остаются прежними.

Алиса равновероятно выбирает базис и готовит состояние $|\Phi_b\rangle_{AB} = \frac{1}{\sqrt{2}}(|0_b\rangle_A \otimes |\varphi_{0b}\rangle_B + |1_b\rangle_A \otimes |\varphi_{1b}\rangle_B)$, $\rho^b_{AB} = |\Phi_b\rangle_{ABAB}\langle\Phi_b|$. Информационными состояниями являются геометрически однородные когерентные состояния вида $|\alpha_j\rangle$, получающиеся геометрическим сдвигом (унитарным поворотом U^j, $U^N = I$, см. рис. 1а) $|\alpha_j\rangle = U^j|\alpha\rangle$, где $\alpha_j = e^{i\frac{2\pi}{N}j}\alpha$ ($j = 0, 1, \ldots, N-1$) В протоколе используется $N/2$ базисов (пример для $N = 4$ и $N = 8$ на рис. 1а), базисы обозначены дугами), в каждом базисе имеется пара неортогональных состояний $|\varphi_{ib}\rangle = |\alpha_j\rangle$, отвечающих 0 и 1 ($i = 0, 1$, b – индекс базиса, $b = 1, \ldots, N/2$).

Любые атаки описываются супероператором $\mathcal{T}$ (отображение матриц плотности в матрицы плотности), который имеет унитарное представление. Атака задается выбором унитарного оператора, причем Ева имеет доступ только к подсистеме B, $|\Psi_b\rangle_{ABE} = U_{BE}\,(|\Phi_b\rangle_{AB} \otimes |E\rangle_E)$, $\widetilde{\rho}^b_{AB} = \mathcal{T}(\rho^b_{AB}) = \mathrm{Tr}_E\{U_{BE}\left[(\rho^b_{AB}) \otimes |E\rangle_{EE}\langle E|\right] U^{-1}_{BE}\}$

Случайный и равновероятный выбор бита $X_A = \{0b, 1b\}$ в базисе b Алиса производит посредством измерения над своей подсистемой. Измерения описываются разложением единицы $I_A = P^A_{0b} + P^A_{1b}$, $P^A_{ib} = |ib\rangle_{AA}\langle ib|$. После измерений Алисы ситуация описывается матрицей плотности $\rho^b_{X_ABE} = \sum_{x_A=0b,1b} P^A_{x_A}\rho^b_{ABE}P^A_{x_A}$, $\rho^b_{ABE} = |\Psi_b\rangle_{ABE\ ABE}\langle\Psi_b|$. Боб в каждой посылке независимо от Алисы случайно и равновероятно выбирает базис и *одно из двух* измерений в данном базисе. Каждое измерение описывается разложением единицы $I_B = P^B_{ib} + P^B_{\perp ib}$, $P^B_{0b,1b} = I_B - |\varphi_{1b,0b}\rangle_{BB}\langle\varphi_{1b,0b}|$. Каждое измерение имеет два исхода. Один исход в каждом измерении – определенный. он фактически сводится к проектированию на состояния, ортогональные состояниям, отвечающим 0 и 1. Второй исход в каждом измерении – неопределенный. Неопределенные исходы, отвечающие $P^B_{\perp 0b,1b}$ отбрасываются, определенные исходы интерпретируются Бобом как $X_B = \{0b, 1b\}$. Выбор измерения фиксируется выбором соответствующих напряжений на фазовом модуляторе (см. ниже).

Поскольку в дальнейшем посылки, в которых базисы не совпадают, отбрасываются, достаточно рассмотреть только те посылки, где базисы совпали. Матрица плотности после измерений Боба и отбрасывания неопределенных исходов равна $\rho_{X_AX_BE} = \sum_{x_B=0b,1b} P^B_{x_Bb}\rho_{X_ABE}P^B_{x_Bb}/\mathrm{Tr}\{P^B_{x_Bb}\rho_{X_ABE}\}$.

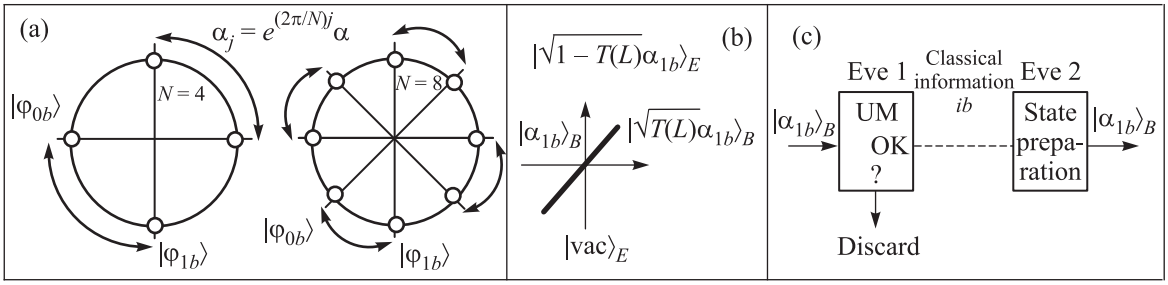

Рис. 1. (a) – Пример информационных состояний, используемых в протоколе для случаев: $N = 2$ базиса $N = 4$ информационных состояний (слева), $N = 4$ базиса, $N = 8$ состояния (справа). Показано соответствие комплексного параметра α_j, описывающего когерентные состояния, информационным состояниям $|\varphi_{0b}\rangle$ (значение бита 0) и $|\varphi_{1b}\rangle$ (1). (b) – Схематическое изображение атаки с расщеплением когерентных состояний при помощи асимметричного светоделителя, коэффициент деления $T(L)$ которого зависит от длины квантового канала связи с потерями. (c) – Схематическое изображение атаки с измерениями с определенным исходом, использующей разрыв исходного канала связи

Длина ключа. Длина секретного ключа в битах после коррекции ошибок и сжатия при помощи хэш-функций второго порядка в асимптотическом пределе длинных последовательностей может быть представлена в виде (детали см. в [8])

$$l_{\mathrm{secret}} \le H(X_A|E) - H(X_A|X_B), \qquad (1)$$

где условная энтропия фон Неймана $H(X_A|E) = H(X_AE) - H(E)$, $H(X_AE) = -\mathrm{Tr}\{\rho_{X_AE}\log\rho_{X_AE}\}$, частичная матрица плотности $\rho_{X_AE} = \mathrm{Tr}_B\{\rho_{X_AX_BE}\}$. Аналогично для других энтропий.

Унитарная атака. В канале без потерь (все посланные Алисой состояния достигают приемной стороны), наиболее эффективной является унитарная атака. Оценка в пользу Евы означает, что если ей известен базис, но не известны состояния, то длина ключа будет меньше, чем в случае когда не известны ни базис, ни состояния в нем. Формально это связано с тем, что дополнительная обусловленность (информация о базисе b), не увеличивает условную энтропию, $H(X_A|Eb) \le H(X_A|E)$. В этом случае задача Евы сводится к оптимальному различению пары неортогональных состояний в известном базисе. Формально это означает, что вспомогательное состояние Евы, $|E_b\rangle_E = |E\rangle_E \otimes |b\rangle_E$, содержит информацию о базисе. Действие унитарного оператора с учетом симметрии между 0 и 1 в этом случае сводится к следующему:

$$U_{BE}(|\Psi_b\rangle_{ABE}) = \\ = \frac{1}{\sqrt{2}}\left(|0_b\rangle_A \otimes |\tilde{\varphi_{0b}}\rangle_{BE} + |1_b\rangle_A \otimes |\tilde{\varphi_{1b}}\rangle_{BE}\right), \qquad (2)$$

$$|\tilde{\varphi_{0b}}\rangle_{BE} = (1-Q)|\varphi_{0b}\rangle_B \otimes |\tilde{E}_{0b}\rangle_E + Q|\varphi_{1b}\rangle_B \otimes |\tilde{E}_{1b}\rangle_E,$$
$$|\tilde{\varphi_{1b}}\rangle_{BE} = (1-Q)|\varphi_{1b}\rangle_B \otimes |\tilde{E}_{1b}\rangle_E + Q|\varphi_{0b}\rangle_B \otimes |\tilde{E}_{0b}\rangle_E.$$

К оператору U_{BE} предъявляется единственное требование унитарности: ${}_{BE}\langle\tilde{\varphi_{0b}}|\tilde{\varphi_{1b}}\rangle_{BE} = {}_{BE}\langle\varphi_{0b}|\varphi_{1b}\rangle_{BE}$. Это условие дает связь между наблюдаемой ошибкой Q на приемной стороне и углом между исходными состояниями. С учетом (1), (2) длина секретного ключа равна

$$l_{\mathrm{secret}}(Q,N,\mu) = 1 - h(Q) - \overline{C}(\varepsilon(N,\mu)) - \\ - \lambda_1\log\lambda_1 - \lambda_2\log\lambda_2, \qquad (3)$$

где

$$\overline{C}(\varepsilon) = -\frac{1-\varepsilon}{2}\log\left(\frac{1-\varepsilon}{2}\right) - \frac{1+\varepsilon}{2}\log\left(\frac{1+\varepsilon}{2}\right),$$

$$\varepsilon(N,\mu) = \frac{\sqrt{1-(1-2Q)^2} - \xi(N,\mu)}{\xi(N,\mu)[\sqrt{1-(1-2Q)^2}\xi(N,\mu) - 1]},$$

$$\xi(N,\mu) = |{}_B\langle\varphi_{0b}|\varphi_{1b}\rangle_B| = e^{-2\mu\sin^2(2\pi/2N)},$$

$$\lambda_{1,2} = \frac{1 \pm \sqrt{1-4\beta(N,\mu)}}{2},$$

$$\beta(N,\mu) = \\ = \frac{(1-Q)+\xi(N,\mu)^2Q)[(1-Q)\xi(N,\mu)^2+Q]-\xi(N,\mu)^2}{1-\xi(N,\mu)^2}.$$

Атака с расщеплением когерентных состояний. Данная атака имеет место в канале с потерями. Она использует тот факт, что на линейном светоделителе когерентные состояния преобразуются самоподобным образом. Среднее число фотонов, достигающих приемной стороны, составляет $\mu(L) = \mu 10^{-\delta L/10} = \mu T(L)$ $(\alpha(L) = \alpha\sqrt{T(L)})$, L – длина оптоволоконного канала связи, $\delta \approx 02$ дб/км – величина затухания для стандартного одномодового волокна SMF-28).

Поскольку в квантовой криптографии квантовый канал связи не контролируется, Ева заменяет исходный канал на канал с меньшими потерями (в пределе без потерь) и отводит часть $1-T(L)$ когерентного состояния в свою квантовую память. Остальная часть направляется через идеальный канал связи (см. рис. 1b). В этом случае Ева, начиная с некоторой критической длины линии. Ева знает весь ключ. При этом она не меняет число отсчетов на стороне Боба и не производит ошибок. Без подслушивателя действие канала с потерями описывается супероператором $\mathcal{T}(\rho_{X_A B}) = |0_{ib}\rangle_{AA}\langle 0_{ib}| \otimes |\alpha_{0b}(L)\rangle_{BB}\langle\alpha_{0b}(L)| + + |1_{ib}\rangle_{AA}\langle 1_{ib}| \otimes |\alpha_{1b}(L)\rangle_{BB}\langle\alpha_{1b}(L)|$.

Атака Евы с расщеплением когерентных состояний описывается действием унитарного оператора следующего вида:

$$U_{BE}^{\text{split}}\left(|\Phi^b\rangle_{AB}\otimes|\text{vac}\rangle_E\right) = = |0_b\rangle_A\otimes|\sqrt{T(L)}\alpha_{0b}\rangle_B\otimes|\sqrt{1-T(L)}\alpha_{0b}\rangle_E + + |1_b\rangle_A\otimes|\sqrt{T(L)}\alpha_{1b}\rangle_B\otimes|\sqrt{1-T(L)}\alpha_{1b}\rangle_E. \quad (4)$$

С учетом (1), (2) получаем длину секретного ключа

$$l_{\text{secret}}(N,\mu,L) = 1-\overline{C}[\varepsilon(N,\mu,L)], \quad \varepsilon(N,\mu,L) = |_E\langle\sqrt{1-T(L)}\alpha_{0b}|\sqrt{1-T(L)}\alpha_{1b}\rangle_E|. \quad (5)$$

Критическая длина линии, до которой гарантируется секретное распределение ключей, определяется из условия $l_{\text{secret}}(N,\mu,L)=0$.

Атака с измерениями с определенным исходом (UM – Unambiguous Measurements). Данная атака имеет место в канале с потерями. Она основана на следующем фундаментальном факте, касающемся измеримости квантовых состояний. *Линейная независимость является необходимым и достаточным условием* существования таких измерений [9]. Для линейно-независимых состояний существуют измерения, которые позволяют различать такие состояния с *определенностью*, хотя и с некоторой вероятностью такого исхода. Любое измерение в квантовой механике описывается разложением единицы: каждому исходу измерений приписываются положительные операторнозначные меры $M_j M_j^+$ (POVM), которые в сумме дают единичный оператор. В нашем случае имеем

$$I_B = \sum_j^N M_j^+ M_j + M_?^+ M_?, \quad \text{Tr}\{|\alpha_j\rangle_{BB}\langle\alpha_j|M_i M_i^+\} = P_{D_j}\delta_{i,j}, \quad \text{Tr}\{|\alpha_j\rangle_{BB}\langle\alpha_j|M_? M_?^+\} = P_{?j} \quad \forall j. \quad (6)$$

Таким образом, если получен определенный исход j, то точно известно, что входным было состояние $|\alpha_j\rangle_B$, и никакое другое. Неопределенный (inconclusive) исход ? имеет место от любого состояния. Для такой атаки Еве не нужны ни квантовая память, ни идеальный квантовый канал связи. Ева разрывает канал связи вблизи передающей и вблизи приемной стороны (рис.1c) и производит измерения (6). Если получен определенный исход, то Ева-1 точно знает состояние и сообщает Еве-2 по классическому каналу связи, какое состояние нужно перепослать. Однофотонные лавинные InGaAS-фотодетекторы не реагируют на вакуумную компоненту когерентного состояния и имеют квантовую эффективность $\eta<1$ (типичное значение $\eta\approx(10-25)\,\%$). Ева-2 может послать когерентное состояние с $\mu^*\gg 1$, чтобы лавинный фотодетектор сработал в каждой перепосланной посылке (чтобы доля невакуумной компоненты составляла $1-e^{-\eta\mu^*}\approx 1$). Если получен неопределенный исход ?, то Ева ничего не перепосылает. Формально посылает вакуумное состояние $|\text{vac}\rangle_B$, на которое детектор не реагирует. При определенной длине линии доля неопределенных исходов равна величине потерь в линии. Начиная с этой длины, Ева знает весь ключ и не производит ошибок на приемной стороне. UM-атака описывается супероператором

$$\mathcal{T}(|i_b\rangle_{AA}\langle i_b|\otimes|\alpha_{ib}\rangle_{BB}\langle\alpha_{ib}|) = = \sum_j^N |i_b\rangle_{AA}\langle i_b|\text{Tr}\{M_j(|\alpha_{ib}\rangle_{BB}\langle\alpha_{ib}|)M_j^+\}\otimes \otimes|\alpha_{ib}^*\rangle_{BB}\langle\alpha_{ib}^*|\otimes|i_b\rangle_{EE}\langle i_b| + + |i_b\rangle_{AA}\langle i_b|\text{Tr}\{M_?(|\alpha_{ib}\rangle_{BB}\langle\alpha_{ib}|)M_?^+\}\otimes \otimes|\text{vac}\rangle_{BB}\langle\text{vac}|\otimes|\text{discard}\rangle_{EE}\langle\text{discard}|. \quad (7)$$

Для геометрически однородных когерентных состояний оптимальные измерения, минимизирующие вероятность исхода ?, могут быть построены явно [9]. POVM для геометрически однородных состояний строятся явно. Пусть спектральное разложение оператора U есть $U=\sum_{j=0}^{N-1}e^{i\frac{2\pi j}{N}}|\lambda_j\rangle\langle\lambda_j|$, где $|\lambda_j\rangle$ – собственные векторы, $\langle\lambda_i|\lambda_j\rangle=\delta_{ij}$. Набор векторов "обратной" решетки $|\alpha_j^\perp\rangle$ также представляет собой геометрически однородные состояния. Таким образом, имеем

$$|\alpha_j\rangle = \sum_{k=0}^{N-1} c_k e^{i\frac{2\pi jk}{N}}|\lambda_k\rangle, \quad |\alpha_j^\perp\rangle = \frac{1}{\sqrt{Z}}\sum_{r=0}^{N-1}\frac{1}{c_r^*}e^{i\frac{2\pi jr}{N}}|\lambda_r\rangle, \quad Z=\sum_{r=0}^{N-1}\frac{1}{|c_r|^2}. \quad (8)$$

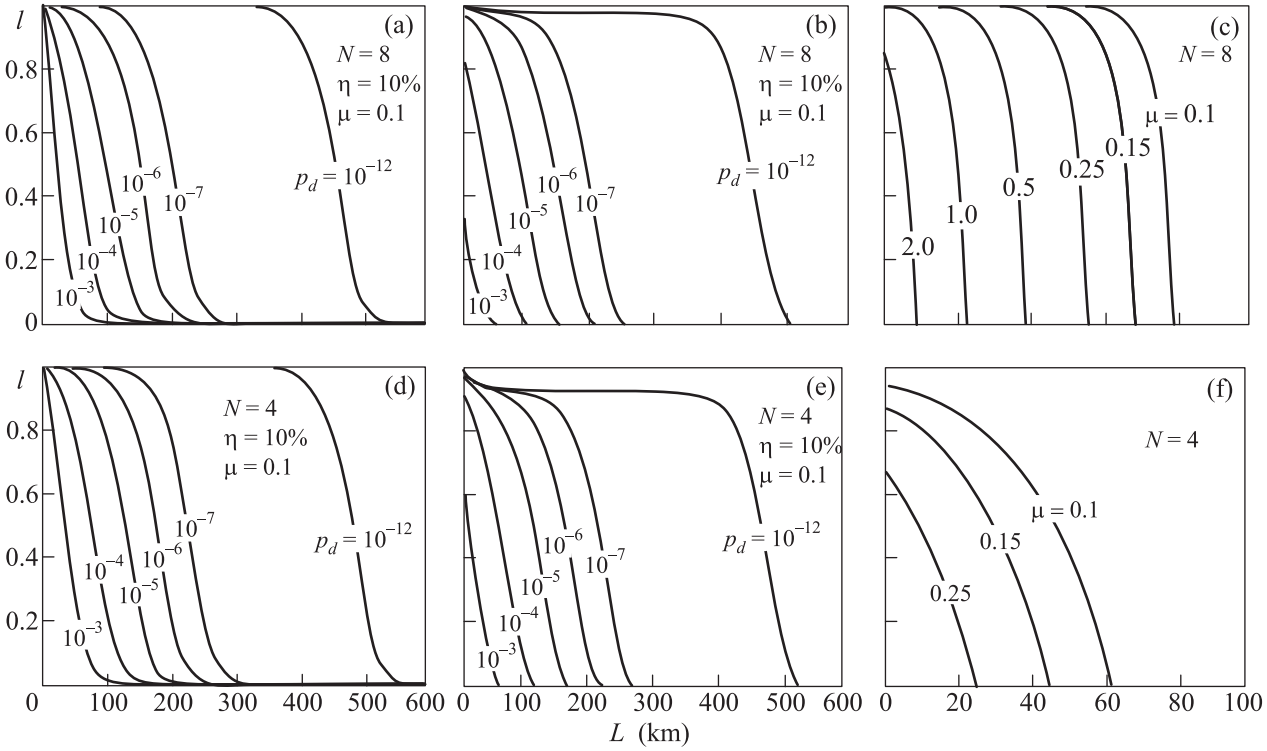

Рис. 2. Доля секретных бит в пересчете на число зарегистрированных у Боба посылок с определенными исходами при совпадающих базисах Алисы и Боба как функция длины линии связи L: (a), (d) – унитарная атака, (b), (e) – атака с расщеплением состояния, (c), (f) – атака с измерениями с определенным исходом (для этой атаки вероятность темновых шумов и квантовая эффективность несущественны) (N – число состояний, μ – среднее число фотонов, η – квантовая эффффективность фотодетекторов, p_d – вероятность темновых шумов

Отвечающие за определенные исходы POVM и нижняя граница вероятности определенных исходов равны

$$M_D = \sum_j^N M_j^+ M_j = \\ = \frac{1}{N^2} \sum_{j,r,r'} P_j c_{r'}^{*-1} c_r^{-1} e^{i\frac{2\pi j(r-r')}{N}} |\lambda_{r'}\rangle\langle\lambda_r|, \qquad (9)$$

$$P_D(N,\mu) \le N \min_r \left(|c_r|^2\right) = \\ = N \min_r \left(\frac{1}{N} \sum_{j=0}^{N-1} e^{\mu\left(e^{i\frac{2\pi j}{N}}-1\right)} e^{-i\frac{2\pi jr}{N}} \right). \qquad (10)$$

С учетом сказанного и (9), (10) для длины секретного ключа получаем

$$l_{\text{secret}}(N,\mu,L) = 1 - e^{-\eta\mu(L)} - P_D(N,\mu). \qquad (11)$$

Критическая длина линии связи, обеспечивающая секретное распределение ключей, определяется из условия $l_{\text{secret}}(N,\mu,L) = 0$.

Учет темновых шумов лавинного фотодетектора. Темновые шумы описываются вероятностью p_d темнового отсчета во временном окне стробирования лавинного детектора. Шумы также могут быть описаны соответствующим супероператором, действующим только на подсистему Боба. Фактически (опуская детали) их учет сводится к замене $Q \to \tilde{Q} = \frac{1}{2}\frac{p_d}{p_d+\tilde{\xi}(N,\mu,L)}$ (где $\tilde{\xi}(N,\mu,L) = e^{-2\mu(L)\sin^2(2\pi/2N)}$). При $L \to \infty$ ошибка стремится к $Q \to \frac{1}{2}$ (отсутствует корреляция между строками бит Алисы и Боба, передача ключей становится невозможной). В результате

1) для унитарной атаки длина ключа вместо (3) становится равной

$$l_{\text{secret}}(N,\mu,L,p_d) = 1 - h(\tilde{Q}) - \overline{C}[\varepsilon(N,\mu)] - \\ - \lambda_1 \log\lambda_1 - \lambda_2 \log\lambda_2; \qquad (12)$$

2) для атаки с расщеплением когерентного состояния вместо (5) имеем

$$l_{\text{secret}}(N,\mu,L) = 1 - h(\tilde{Q}) - \overline{C}[\varepsilon(N,\mu,L)]; \qquad (13)$$

3) для атаки с измерениями с определенным исходом из-за увеличения интенсивности перепосланных Евой состояний темновые шумы несущественны (см. (11)).

Реализация. Оптоволоконная реализация является стандартной. Используются интерферометр Маха–Цандера с разной длиной плеч и фазовые модуляторы на передающей и приемной сторонах. На выходе интерферометра Алисы возникает пара когерентных состояний $|e^{i\varphi_j^A}\alpha\rangle_1 \otimes |\alpha\rangle_2$, сдвинутых по времени (индексы "1" и "2"). Состояние $|\alpha\rangle_2$ всегда имеет одну и ту же фазу и служит реперным. На приемной стороне после прохождения фазового модулятора перед входом в интерферометр состояния принимают вид $|e^{i(\varphi_j^A-\varphi_j^B)}\alpha\rangle_1 \otimes |\alpha\rangle_2$. Они детектируются двумя детекторами после интерферометра. Значения фаз $\varphi_j^{A,B}$ Алисы и Боба выбираются в соответствии с протоколом.

Заключение. Зависимости длины секретного ключа в пересчете на число зарегистрированных посылок для различных числа информационных состояний N, среднего числа фотонов μ, квантовой эффективности фотодетекторов η и вероятности темновых шумов p_d от длины линии L для различных атак Евы показаны на рис. 2. Для унитарной атаки (рис. 2a и b) ошибки обусловлены только шумами детекторов.

Для InGaAs-детекторов типичные значения p_d при охлаждении до $\sim -45\,^\circ$C составляют 10^{-5} counts/gate, а $\eta \approx (10-25)\,\%$ [10]. Вероятность шумов на уровне 10^{-12} в пересчете на строб достигается для сверхпроводящих детекторов. Основным фактором, лимитирующим длину линии для секретной передачи ключей, является атака с UM. Увеличение длины может быть достигнуто за счет увеличения числа информационных состояний и базизов, что уменьшает для Евы вероятность определенных исходов. Скорость генерации ключей при этом падает. Например, при $N = 8$ при $L = 0$ в длину ключа дает вклад только $\sim 5\,\%$ от переданных состояний. Таким образом, принципиально достижимые длины линий связи могут составлять до 400 км. В зависимости от параметров системы и требуемой длины линии может быть выбран один из однотипных протоколов (выбор протокола фиксируется выбором N).

Итак, предложено семейство однотипных протоколов квантового распределения ключей, которые прозрачны для анализа и имеют достаточно широкий диапазон по параметрам (среднему числу фотонов, квантовой эффективности детекторов и вероятности темновых шумов). С их помощью может быть обеспечен достаточно широкий диапазон длин линий связи для гарантированно секретной передачи ключей.

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

1. V. Scarani, H. Bechmann-Pasquinucci, N. J. Cerf et al., Rev. Mod. Phys. **81**, 1301 (2009).
2. V. Scarani, A. Acin, G. Ribordy, and N. Gisin, Phys. Rev. Lett. **95**, 057901-1 (2004); A. Acin, N. Gisin, and V. Scarani, arXiv:quant-ph/0302037.
3. W.-Y. Hwang, Phys. Rev. Lett. **91**, 057901 (2003).
4. K. Inoue, E. Waks, and Y. Yamamoto, Phys. Rev. Lett. **89**, 037902 (2002).
5. N. Gisin, G. Ribordy, H. Zbinden et al., arXiv:quant-ph/0411022.
6. Д. А. Кронберг, С. Н. Молотков, ЖЭТФ **136**, 650 (2009).
7. *European Telecommunications Standards Institute (ETSI)*, http://www.etsi.org.
8. R. Renner, arXiv/quant-ph: 0512258.
9. A. Chefles, arXiv/quant-ph: 9807022; A. Chefles and S. M. Barnett, arXiv/quant-ph: 9807023.
10. А. В. Корольков, К. Г. Катамадзе, С. П. Кулик, С. Н. Молотков, ЖЭТФ **137**, 637 (2010); С. Н. Молотков, С. П. Кулик, А. И. Климов, *Устройство для регистрации слабых оптических импульсов*, Патент РФ, 2339919, 15.06.2007.