Письма в ЖЭТФ, том 102, вып. 7, с. 530 – 535 

# Какой протокол квантовой криптографии обеспечивает максимальную дальность в случае создания строго однофотонного источника?

*С. Н. Молотков*[1)]

*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 28 июля 2015 г.
После переработки 17 августа 2015 г.

Приведен анализ дальности передачи секретных ключей в случае строго однофотонного источника для протокола BB84 и для протокола с фазово-временны́м кодированием (PTC – Phase Time Coding). Показано, что дальность передачи секретных ключей, которую обеспечивает протокол PTC, превосходит дальность передачи по протоколу BB84 почти на 100 км (при прочих равных параметрах системы).

DOI: 10.7868/S0370274X15190145

**Введение.** Обсуждения проблемы создания однофотонного источника в телекоммуникационном диапазоне длин волн (1.3–1.5 мкм) ведутся с момента появления первого протокола квантовой криптографии BB84 [1] и волоконных систем, использующих этот протокол. При этом всегда произносились слова о том, что строго однофотонный источник обеспечит бóльшую дальность гарантированно секретного распределения ключей. Однако до сих пор внятно не сказано, какую дальность может обеспечить однофотонный источник. Кроме того, неясно, является ли протокол BB84 самым дальнодействующим или существуют другие протоколы, которые обеспечивают большую дальность по сравнению с BB84.

Сразу нужно подчеркнуть, что однофотонный источник – только один из критических элементов систем квантовой криптографии. Есть еще два компонента любой системы, которые определяют дальность секретной передачи ключей. Второй технический элемент – однофотонный детектор. Критические параметры однофотонного детектора – вероятность темновых шумов и квантовая эффективность.

И наконец, третий, самый важный элемент – протокол квантового распределения ключей. На абстрактном уровне под протоколом понимается совокупность действий, включающая набор квантовых состояний, их приготовление, измерение на приемной стороне, коррекцию ошибок в первичных ключах, усиление секретности очищенных ключей. Протокол также включает доказательство секретности ключей с учетом конкретной реализации протокола.

Конкретная реализация протокола может использовать различные способы кодирования – сопоставления квантовых состояний на абстрактном уровне конкретным квантовым состояниям физической системы, например фотона. Возможно кодирование в поляризационные степени свободы фотона. Однако поскольку стандартное волокно не сохраняет поляризацию, для волоконных систем используется фазовое кодирование. Классические биты ключа кодируются в относительную фазу однофотонного пакета.

Протокол BB84 был первым и основным в том смысле, что остальные протоколы являлись развитием BB84 на случай неоднофотонного источника. При неоднофотонном источнике и потерях в линии связи протокол BB84, начиная с некоторой критической длины (порядка 25 км), не позволяет детектировать вторжение в канал подслушивателя и гарантировать секретность ключей. Точнее говоря, PNS-атака и UM-измерения[2)] приводят к тому, что подслушиватель, начиная с некоторой длины линии связи (соответственно, потерь), знает весь ключ, не производит ошибок и не детектируется. Модификации протокола BB84 были направлены на нейтрализацию PNS- и UM-атак (см. обзор [2]).

[1)]e-mail: molotkov@issp.ac.ru

[2)]PNS – Photon Number Splitting attack, атака с расщеплением по числу фотонов; UM – Unambiguous Measurements, измерения с определенным исходом.

В случае однофотонного источника независимо от потерь любая атака при передаче ключей по протоколу BB84 приводит к ошибкам на приемной стороне. Поскольку ошибки на приемной стороне от действий подслушивателя и собственных ошибок системы, например темновых шумов, принципиально неотличимы, все ошибки списываются на действия подслушивателя.

Чем больше длина линии связи, тем меньше фотонов долетает и тем больше ошибка от темновых шумов. Протокол гарантирует секретность ключей, если наблюдаемая ошибка на приемной стороне не превосходит критическую ошибку, которая является константой протокола.

Чем больше критическая ошибка, тем большую дальность передачи секретных ключей обеспечивает протокол. Критическая ошибка протокола BB84 равна $Q_c \approx 11\,\%$ [3, 4].

Существуют протоколы с критической ошибкой, до которой гарантируется секретность ключей, дотягивающей до теоретического предела $Q_c \leq\approx 50\,\%$. Улучшить такую критическую ошибку принципиально уже нельзя. Таким протоколом является протокол с фазово-временным кодированием[3)] (PTC – Phase Time Coding) [5].

Ниже приводится сравнительный анализ BB84 и PTC. Показано, что в однофотонном случае дальность гарантированно секретной передачи ключей по протоколу PTC существенно превышает дальность протокола BB84. Объяснены неформальные причины такой разницы.

**Сравнительный анализ BB84 и PTC.** Для того чтобы понять причину, по которой протокол PTC обеспечивает существенно большую дальность передачи ключей, имеет смысл провести анализ стойкости BB84 и PTC единообразным способом.

*Информационные состояния в протоколе BB84.* В протоколе BB84 с фазовым кодированием используется 4 состояния по 2 в каждом базисе:

$$\left.\begin{aligned} 0 \to |0_+\rangle &= \tfrac{|1\rangle+|2\rangle}{\sqrt{2}},\\ 1 \to |1_+\rangle &= \tfrac{|1\rangle-|2\rangle}{\sqrt{2}},\end{aligned}\right\}\text{базис } +,$$
$$\left.\begin{aligned} 0 \to |0_\times\rangle &= \tfrac{|1\rangle+i|2\rangle}{\sqrt{2}},\\ 1 \to |1_\times\rangle &= \tfrac{|1\rangle-i|2\rangle}{\sqrt{2}},\end{aligned}\right\}\text{базис } \times, \tag{1}$$

где $|1\rangle, |2\rangle$ – однофотонные пакеты, локализованные во временны́х окнах 1 и 2.

На приемной стороне используется пара измерений в базисах $+$ и $\times$, которая выбирается независимо от передающей стороны. Посылки, в которых базисы приготовления состояний и измерения не совпадали, отбрасываются. Два измерения описываются разложениями единицы, $I_2 = |1\rangle\langle 1| + |2\rangle\langle 2|$:

$$I_2 = P_{0_+} + P_{1_+}, \quad I_2 = P_{0_\times} + P_{1_\times}, \tag{2}$$

где $P_{0_+}, P_{1_+}, P_{0_\times}, P_{1_\times}$ – проекторы на информационные состояния (1).

*Информационные состояния в протоколе PTC.* В протоколе PTC с фазовым кодированием используется 8 состояний по 2 в каждом из 4 базисов:

$$\left.\begin{aligned} 0 \to |0_{+L}\rangle &= \tfrac{|1\rangle+|2\rangle}{\sqrt{2}},\\ 1 \to |1_{+L}\rangle &= \tfrac{|1\rangle-|2\rangle}{\sqrt{2}},\end{aligned}\right\}\text{базис } +L,$$
$$\left.\begin{aligned} 0 \to |0_{\times L}\rangle &= \tfrac{|1\rangle+i|2\rangle}{\sqrt{2}},\\ 1 \to |1_{\times L}\rangle &= \tfrac{|1\rangle-i|2\rangle}{\sqrt{2}},\end{aligned}\right\}\text{базис } \times L, \tag{3}$$

$$\left.\begin{aligned} 0 \to |0_{+R}\rangle &= \tfrac{|2\rangle+|3\rangle}{\sqrt{2}},\\ 1 \to |1_{+R}\rangle &= \tfrac{|2\rangle-|3\rangle}{\sqrt{2}}\end{aligned}\right\}\text{базис } +R,$$
$$\left.\begin{aligned} 0 \to |0_{\times R}\rangle &= \tfrac{|2\rangle+i|3\rangle}{\sqrt{2}},\\ 1 \to |1_{\times R}\rangle &= \tfrac{|2\rangle-i|3\rangle}{\sqrt{2}},\end{aligned}\right\}\text{базис } \times R, \tag{4}$$

где $|1\rangle, |2\rangle, |3\rangle$ – однофотонные пакеты, локализованные во временны́х окнах 1, 2 и 3. На приемной стороне используются измерения в базисах $+L$, $+R$ и $\times L$, $\times R$, которые выбираются независимо от передающей стороны. Посылки, в которых базисы приготовления состояний и измерения не совпали, отбрасываются. Два измерения описываются разложениями единицы, $I_3 = |1\rangle\langle 1| + |2\rangle\langle 2| + |3\rangle\langle 3|$:

$$I_3 = P_{0_{+L}} + P_{1_{+L}} + |3\rangle\langle 3|,\ I_3 = P_{0_{\times L}} + P_{1_{\times L}} + |3\rangle\langle 3|, \tag{5}$$

$$I_3 = |1\rangle\langle 1| + P_{0_{+R}} + P_{1_{+R}},\ I_3 = |1\rangle\langle 1| + P_{0_{\times R}} + P_{1_{\times R}}, \tag{6}$$

где $P_{0_{+L,R}}, P_{1_{+L,R}}, P_{0_{\times L,R}}, P_{1_{\times L,R}}$ – проекторы на информационные состояния (3), (4). Проектор $|3\rangle\langle 3|$ в базисе $L$ и проектор $|1\rangle\langle 1|$ в базисе $R$ являются контрольными и играют принципиальную роль для обеспечения большой критической ошибки протокола и, соответственно, дальности. Сразу отметим, что без подслушивателя отсчетов в контрольных временных слотах 1 и 3 быть не должно. Отсчеты возникают только за счет темновых шумов.

Состояния в левом ($L$) базисе смещены по времени по отношению к состояниям в правом ($R$) базисе

[3)] См. также патент РФ RU 2 427 926 C1 *Способ квантового кодирования и передачи криптографических ключей.* Действие патента от 23.07.2010.

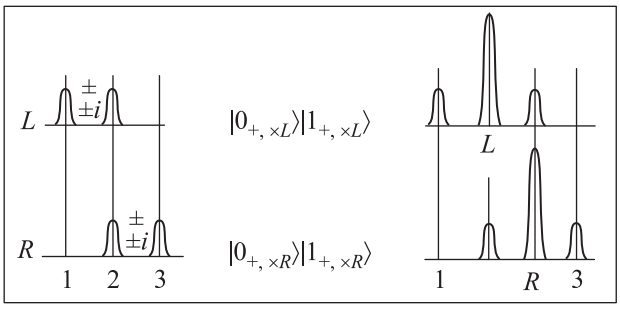


Рис. 1. Информационные состояния протокола РТС на передающей стороне в двух разных посылках в левом и правом базисах. Схематично показана конструктивная интерференция состояний в левом и правом базисах на приемной стороне. Временны́е окна 1 и 3 являются контрольными. В протоколе BB84 во всех посылках используется только один базис, например $L$

(рис. 1). Если использовать состояния только в одном из базисов, $L$ или $R$, то имеет место протокол BB84. Состояния в левом и правом базисах перекрываются (являются неортогональными). Поэтому подслушиватель неизбежно будет ошибаться в выборе между $L$- и $R$-базисами. Последнее приведет к отсчетам в контрольном временно́м слоте 3, если посылались состояния в левом базисе, и к отсчетам во временно́м слоте 1, если в правом (рис. 1).

**Критическая ошибка протоколов BB84 и РТС.** На сегодняшний день доказано, что для протоколов квантовой криптографии, в которых посылки на приемной стороне не зависят друг от друга, оптимальной является коллективная атака [6]. Под оптимальной понимается такая атака, при которой подслушиватель получает максимум информации о ключе при заданной наблюдаемой ошибке на приемной стороне. Неформально коллективная атака сводится к следующему. В каждой посылке подслушиватель готовит свою вспомогательную квантовую систему (ancilla), запутывая ее с передаваемым состоянием. Искаженную анциллу он сохраняет в квантовой памяти, а искаженное состояние отправляет на приемную сторону. После передачи всей серии состояний и индивидуальных измерений на приемной стороне происходит коррекция ошибок через открытый канал, а затем усиление секретности. Только после всех стадий, учитывая информацию, полученную из открытого канала при коррекции ошибок, и усиления секретности подслушиватель проводит коллективные измерения над всей памятью.

Формально задача сводится к построению унитарного оператора подслушивателя, максимизирующего его информацию о ключе после всех стадий. Поскольку информационные состояния есть линейная комбинация базисных состояний $|1\rangle, |2\rangle, |3\rangle$, то достаточно выяснить действие унитарного оператора на базисные состояния. Далее по линейности можно получить его действие на информационные состояния. Имеем

$$U_{BE}(|i\rangle_B \otimes |E\rangle_E) = \sum_{j=1}^{3} |\varphi_{i,j}\rangle_E \otimes |j\rangle_B. \qquad (7)$$

Требования унитарности и симметрии по базисам и состояниям внутри базисов приводят к следующим соотношениям для искаженных состояний подслушивателя:

$$|\varphi_{11}\rangle_E = \sqrt{1-\delta^2}|xx\rangle_E,$$
$$|\varphi_{12}\rangle_E = \frac{\delta}{\sqrt{2}}|xy\rangle_E, \quad |\varphi_{13}\rangle_E = \frac{\delta}{\sqrt{2}}|zx\rangle_E, \qquad (8)$$

$$|\varphi_{21}\rangle_E = \frac{\delta}{\sqrt{2}}[\cos(\alpha)|xy\rangle_E + \sin(\alpha)|yy\rangle_E],$$
$$|\varphi_{22}\rangle_E = \sqrt{1-\delta^2}[\cos(\alpha)|xx\rangle_E + \sin(\alpha)|yx\rangle_E], \qquad (9)$$
$$|\varphi_{23}\rangle_E = \frac{\delta}{\sqrt{2}}[\cos(\alpha)|zz\rangle_E + \sin(\alpha)|xz\rangle_E],$$

$$|\varphi_{33}\rangle_E = \sqrt{1-\delta^2}|xx\rangle_E,$$
$$|\varphi_{32}\rangle_E = \frac{\delta}{\sqrt{2}}|zz\rangle_E, \quad |\varphi_{31}\rangle_E = \frac{\delta}{\sqrt{2}}|yz\rangle_E. \qquad (10)$$

Для информационных состояний, например в базисе $+L$, с учетом (3) получаем

$$U_{BE}(|0_{+L}\rangle_B \otimes |E\rangle_E) = |0_{+L}\rangle_B \otimes |\Phi_{00L}\rangle_E + |1_{+L}\rangle_B \otimes |\Phi_{01L}\rangle_E + |3\rangle_B \otimes |\Psi_{0cL}\rangle_E, \qquad (11)$$

$$U_{BE}(|1_{+L}\rangle_B \otimes |E\rangle_E) = |0_{+L}\rangle_B \otimes |\Phi_{10L}\rangle_E + |1_{+L}\rangle_B \otimes |\Phi_{11L}\rangle_E + |3\rangle_B \otimes |\Psi_{1cL}\rangle_E, \qquad (12)$$

$$|\Phi_{00l}\rangle_E = (|\varphi_{11}\rangle_B + |\varphi_{22}\rangle_B + |\varphi_{12}\rangle_B + |\varphi_{21}\rangle_B)/2,$$
$$|\Phi_{01L}\rangle_E = (|\varphi_{11}\rangle_B - |\varphi_{22}\rangle_B - |\varphi_{12}\rangle_B + |\varphi_{21}\rangle_B)/2,$$
$$|\Phi_{10L}\rangle_E = (|\varphi_{11}\rangle_B - |\varphi_{22}\rangle_B + |\varphi_{12}\rangle_B - |\varphi_{21}\rangle_B)/2, \qquad (13)$$
$$|\Phi_{11L}\rangle_E = (|\varphi_{11}\rangle_B + |\varphi_{22}\rangle_B - |\varphi_{12}\rangle_B - |\varphi_{21}\rangle_B)/2,$$
$$|\Psi_{0cL}\rangle_E = (|\varphi_{23}\rangle_B + |\varphi_{13}\rangle_B)/\sqrt{2},$$
$$|\Psi_{1cL}\rangle_E = (|\varphi_{23}\rangle_B - |\varphi_{13}\rangle_B)/\sqrt{2}. \qquad (14)$$

Переход к протоколу BB84 осуществляется, если положить вероятность отсчетов в контрольных временны́х окнах $\delta^2/2 = 0$. Удобно ввести новые обозначения: $Q = [1-\cos(\alpha)]/2$ – вероятность ошибки в

информационных временны́х окнах, $q = \delta^2/2$ – вероятность отсчета в контрольном временно́м окне.

Далее потребуются частичные матрицы плотности на приемной стороне и со стороны подслушивателя. Вычисляя частичный след в (11), (12), имеем

$$\rho_B(0_{+L}) = |0_{+L}\rangle_{BB}\langle 0_{+L}|\frac{(1-q)(1-Q)}{2} + \\ + |1_{+L}\rangle_{BB}\langle 1_{+L}|\frac{(1-q)Q}{2} + |3\rangle_{BB}\langle 3|q, \qquad (15)$$

$$\rho_B(1_{+L}) = |0_{+L}\rangle_{BB}\langle 0_{+L}|\frac{(1-q)Q}{2} + \\ + |1_{+L}\rangle_{BB}\langle 1_{+L}|\frac{(1-q)(1-Q)}{2} + |3\rangle_{BB}\langle 3|q.$$

Частичная матрица плотности подслушивателя есть

$$\rho_E(0_{+L}) = \frac{|\Phi_{00L}\rangle_{EE}\langle\Phi_{00L}|}{4} + \\ + \frac{|\Phi_{01L}\rangle_{EE}\langle\Phi_{01L}|}{4} + \frac{|\Psi_{0cL}\rangle_{EE}\langle\Psi_{0cL}|}{2}, \qquad (16)$$

$$\rho_E(1_{+L}) = \frac{|\Phi_{10L}\rangle_{EE}\langle\Phi_{10L}|}{4} + \\ + \frac{|\Phi_{11L}\rangle_{EE}\langle\Phi_{11L}|}{4} + \frac{|\Psi_{1cL}\rangle_{EE}\langle\Psi_{1cL}|}{2}.$$

**Зависимость длины секретного ключа от наблюдаемой ошибки для протоколов BB84 и PTC.** Ограничимся асимптотическим пределом. Пусть длина последовательности $n \to \infty$ (число посылок уже в совпадающих базисах). Из-за симметрии по базисам $L$ и $R$ (в протоколе PTC) и состояниям, отвечающим 0 и 1, внутри любого базиса (в протоколах BB84 и PTC) достаточно рассмотреть только один из базисов, например базис $+L$ в протоколе PTC и, соответственно, базис $+$ в протоколе BB84. Длина ключа $R$ (доля секретных бит в пересчете на посылку серии $n$) выражается через условные энтропии фон Неймана [6]. Имеем

$$R \geq H(\rho_{XE}|\rho_E) - H(\rho_{XB}|\rho_B), \qquad (17)$$

$$\rho_{XB} = \frac{1}{2}\big[|0_{+L}\rangle_{AA}\langle 0_{+L}| \otimes \rho_B(0_{+L}) + \\ + |1_{+L}\rangle_{AA}\langle 1_{+L}| \otimes \rho_B(1_{+L})\big], \qquad (18)$$

$$\rho_{XE} = \frac{1}{2}\big[|0_{+L}\rangle_{AA}\langle 0_{+L}| \otimes \rho_E(0_{+L}) + \\ + |1_{+L}\rangle_{AA}\langle 1_{+L}| \otimes \rho_E(1_{+L})\big].$$

Частичные матрицы плотности $\rho_B$ и $\rho_E$ получаются взятием частичного следа от (18) по пространству состояний системы $A$ (передатчика).

*Длина ключа для протокола BB84.* Полагая в (8–10) $q = 0$, получаем знаменитую формулу для длины ключа протокола BB84 как функции от наблюдаемой ошибки на приемной стороне $Q$ [3, 4]:

$$R_{\mathrm{BB84}}(Q) \geq 1 - 2h(Q), \\ h(Q) = -Q\log(Q) - (1-Q)\log(1-Q). \qquad (19)$$

Критическая ошибка дается корнем уравнения $1 = 2h(Q_c)$: $Q_c \approx 11\,\%$. При ошибке больше критической длина секретного ключа обращается в нуль (передача секретных ключей невозможна). (Не нужно забывать, что данная величина критической ошибки подразумевает коррекцию ошибок в шенноновском пределе. Исправление ошибок конструктивными кодами коррекции ошибок уменьшает критическую ошибку.)

*Длина ключа для протокола PTC.* Аналогичные вычисления с использованием (15) дают

$$\overline{R}_{\mathrm{PTC}}(Q,q) \geq (1-q)[1 - h(Q) - h(\eta)] - q, \ \eta = \frac{q}{1-q}. \qquad (20)$$

Удобнее нормировать длину ключа в (20) только на отсчеты в информационных окнах. Число таких отсчетов составляет $1-q$. Итак, имеем

$$R_{\mathrm{PTC}}(Q,q) \geq 1 - h(Q) - h(\eta). \qquad (21)$$

Протокол PTC является двухпараметрическим: длина секретного ключа зависит как от наблюдаемой при измерениях в информационных временны́х окнах ошибки $Q$, так и от вероятности отсчетов в контрольном временно́м окне $q$. Легитимные пользователи могут заранее по своему желанию выбрать порог по величине $q$, например $q_c \approx 0$. Если $q$ превышает порог, протокол прерывается (аналогично тому, как прерывается передача в BB84, если ошибка превысит $11\,\%$). В этом случае в соответствии с (21) секретное распределение ключей гарантируется до ошибки в информационных окнах до $Q \lesssim 50\,\%$.

**Длина секретного ключа для протоколов BB84 и PTC в зависимости от длины линии связи, темновых шумов и квантовой эффективности детектора.** Протокол должен обеспечивать работу и без подслушивателя. В линии с потерями не все фотоны долетают до приемной стороны. Отсчеты в информационных окнах появляются как от долетевших фотонов, так и от темновых шумов (с вероятностью $p_d$). Доля долетевших фотонов составляет $10^{-\xi\mathrm{Len}/10}$, где $\xi$ – потери в волокне (дб/км), Len – длина линии связи. Наблюдаемая ошибка в информационных временны́х окнах для BB84 и PTC одинакова и равна

$$Q(\mathrm{Len}) = \frac{1}{2}\frac{p_d}{p_d + \eta_{\mathrm{APD}}\cdot 10^{-\xi\mathrm{Len}/10}}, \qquad (22)$$

где второе слагаемое в знаменателе представляет собой вероятность регистрации долетевшего фотона лавинным детектором с квантовой эффективностью $\eta_{\mathrm{APD}}$.

Величина $q$ – вероятность отсчета в контрольном временно́м окне при совпадающих базисах на передающей и приемной стороне. В отсутствие подслушивателя данная вероятность определяется только темновыми шумами: $q = p_d$. При идеальном детекторе отсчетов в контрольном временно́м окне быть не должно. Зависимости от длины линии связи длины секретного ключа для разных значений параметров представлены на рис. 2.

**Заключение.** Использование контрольных временны́х окон в протоколе PTC приводит к тому, что в однофотонном случае длина линии, до которой гарантируется секретное распределение ключей превышает длину для протокола BB84 почти на 100 км (при равных значениях других параметров системы).

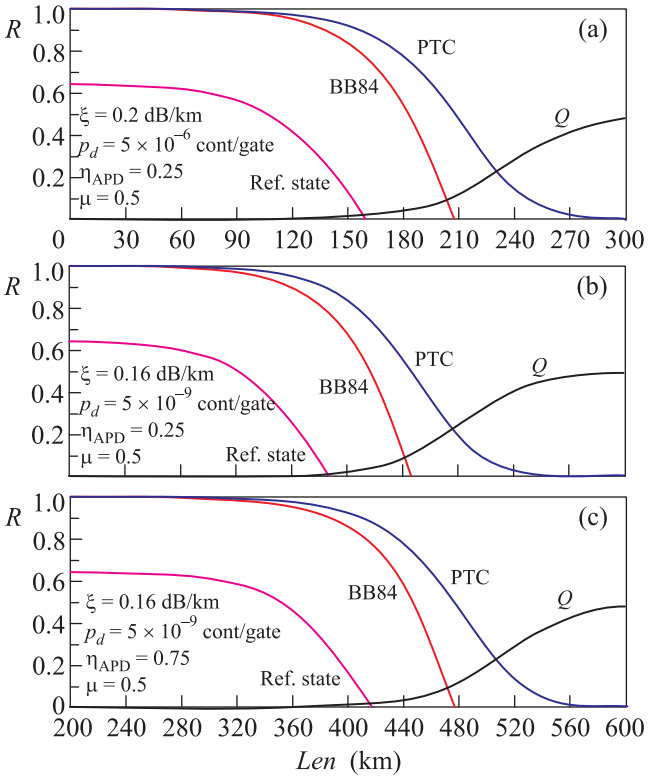


Рис. 2. (Цветной онлайн) Длина секретного ключа $R(Len)$ в пересчете на посылку в совпадающих базисах для разных протоколов в зависимости от длины линии связи. Параметры затухания $\xi$, вероятности темновых шумов $p_d$, квантовая эффективность детектора $\eta_{\mathrm{APD}}$ и среднее число фотонов $\mu$ (для протокола с реперным состоянием с ослабленным лазерным излучением [8]) указаны непосредственно на рисунке. Там же приведена величина наблюдаемой в информационных временны́х окнах ошибки $Q(Len)$, вызванной темновыми шумами детектора, в зависимости от длины линии связи

Максимальная на сегодняшний день длина связи, продемонстрированная для протокола COW (Coherent One Way) [7], где в качестве информационных состояний используется ослабленное лазерное излучение с $\mu \approx 0.5$ ($p_d \approx 5 \cdot 10^{-9}$, $\eta_{\mathrm{APD}} \approx 0.25$, и $\xi \approx 0.16$ дБ/км), составляет 307 км. Однако имеются проблемы со строгим доказательством секретности данного протокола [2]. На рис. 2 приведены также и длины секретного ключа для протокола на квазиоднофотонных состояниях ослабленного лазерного излучения с реперным состоянием (Ref. State) [8].

*Необходимо сделать важное замечание.* Данные результаты относятся к случаю, когда однофотонный источник работает в режиме "on demand", т.е. генерирует однофотонное состояние с вероятностью единица в каждой посылке. Если вероятность излучения однофотонного состояния меньше единицы, то дальность передачи будет меньше[4)]. Однако соотношение дальностей для протоколов BB84 и PTC сохраняется: протокол PTC обеспечивает большую дальность по сравнению с BB84.

Кроме того, приведенные результаты относятся к случаю строго однофотонного источника, что отвечает провалу корреляционной функции второго порядка *строго* до нуля. В противном случае начинают работать все атаки (PNS и UM), имеющие место при ослабленном лазерном излучении, а они существенно уменьшают дальность передачи секретных ключей.

И наконец, отметим, что для открытого пространства системы релятивистской квантовой криптографии принципиально не требуют однофотонного источника и секретность гарантируется при любых потерях, т.к. PNS- и UM-атаки детектируются [9]. Единственным ограничивающим фактором являются темновые шумы лавинных детекторов. Сравнительный анализ дальности передачи для систем релятивистской квантовой криптографии и систем квантовой криптографии с однофотонным источником будет приведен отдельно.

[4)] Данная ситуация легко пересчитывается по формулам, приведенным выше. Для этого нужно включить вероятность излучения как поправочный множитель в квантовую эффективность лавинного детектора. Например, при эффективности излучения в 20 % протокол с реперным состоянием [8] уже начинает превосходить по дальности системы с однофотонным источником.

Автор выражаеь благодарность С.П. Кулику, а также коллегам по Академии криптографии Российской Федерации за полезные обсуждения.

1. C. H. Bennett and G. Brassard, *Quantum Cryptography: Public Key Distribution and Coin Tossing*, Proc. of IEEE Int. Conf. on Comput. Sys. and Sign. Proces., Bangalore, India, December 1984, p. 175.
2. V. Scarani, V. H. Bechmann-Pasquinucci, N. J. Cerf, M. Dušek, N. Lütkenhaus, and M. Peev, Rev. Mod. Phys. **81**, 1301 (2009).
3. P. Shor and J. Preskill, Phys. Rev. Lett. **85**, 441 (2000).
4. С. Н. Молотков, А. В. Тимофеев, Письма в ЖЭТФ **85**, 632 (2007).
5. С. Н. Молотков, ЖЭТФ **133**, 5 (2008).
6. R. Renner, *Security of Quantum Key Distribution*, PhD Thesis, ETH Zürich, Dec. (2005); arXiv/quant-ph: 0512258.
7. 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).
8. С. Н. Молотков, Письма в ЖЭТФ **102**, 436 (2015).
9. S. N. Molotkov, JETP **112**, 370 (2011); JETP Lett. **94**, 469 (2011); JETP Lett. **96**, 342 (2012); S. N. Molotkov and T. A. Potapova, Las. Phys. Lett. **10**, 075205 (2013); I. V. Radchenko, K. S. Kravtsov, S. P. Kulik, and S. N. Molotkov, Las. Phys. Lett. **11**, 065203 (2014); arXiv:quant-ph/1403.3122.