Скорость формирования квантового распределения ключа в волоконно-оптических системах квантовой криптографии

А. В. Поляков, Е. И. Ляховская

Белорусский государственный университет, Минск,
e-mail: polyakov@bsu.by, elisaveta.lyahovskaya@gmail.com

Предложена математическая модель, описывающая помехоустойчивость систем квантовой криптографии. Проведена оценка битовой скорости формирования квантового распределения ключа (КРК) для двух длин волн 0,85 мкм и 1,55 мкм при использовании Si-ЛФД и InGaAs-ЛФД и скорости генерации псевдослучайной последовательности 1 Мбит в зависимости от длины одномодового волоконного световода. Показано, что не смотря на то, что InGaAs-ЛФД обладает на два порядка большим темновым током и в три раза меньшим коэффициентом лавинного умножения по сравнению с Si-ЛФД, работа системы квантовой криптографии на длине волны 1,55 мкм позволяет увеличить битовую скорость формирования КРК от 1,6 до 15 раз при возрастании длины волокна от 1 до 10 км.

Ключевые слова: квантовая криптография, квантовое распределение ключа, битовая скорость.

Введение

Перспективы создания принципиально новых вычислительных машин, так называемых квантовых компьютеров, позволит значительно увеличить скорость вычислений, что существенно снизит криптостойкость систем с открытым ключом, поэтому актуальной задачей является поиск альтернативных методов шифрования. Развитие науки и техники, практическое применение идей квантовой механики в области квантовых вычислений в последние десятилетия позволило разработать системы квантового шифрования с применением квантового распределения ключа (КРК), использующие симметричное шифрование. В большинстве задач квантовое распределение ключей – это процесс формирования секретного ключа у двух удалённых доверенных пользователей в рамках определённого протокола. В дальнейшем выработанный ключ применяется для классической защиты информации. Технология КРК основывается на применении для связи между легитимными пользователями квантовых частиц – фотонов, свойства которых используются для формирования ключевой последовательности. Системы КРК обладают существенным преимуществом перед существующими методами шифрования, так как их защищенность от перехвата данных являются безусловной, основанной на физических законах, в том числе на теореме о запрете клонирования – о невозможности создания точной копии неизвестного квантового состояния. На данный момент уже созданы коммерческие системы КРК с использованием поляризационного кодирования, фазового кодирования, временного кодирования квантовых состояний [1–4]. Основными причинами, сдерживающими развитие систем квантовой криптографии, являются вероятностный характер измерений в протоколах КРК, низкая эффективность детекторов фотонов и необходимость поддерживать энергию излучения в квантовом канале на однофотонном уровне. Поскольку потери в оптическом волокне растут экспоненциально с увеличением его длины, крайне сложно добиться высоких дальностей передачи данных, когда в волокне распространяются сигналы с энергией порядка энергии одиночных фотонов. На сегодняшний день лучшие лабораторные образцы систем КРК едва преодолели порог дальности 300 км при скоростях порядка 1 бита в секунду [5]. В результате существенно возрастают требования к скорости и точности работы управляющей электроники в блоках отправителя и получателя систем КРК.

1. Помехоустойчивость систем квантовой криптографии

Для оценки битовой скорости генерации ключа рассматривали схему построения системы КРК [1, 6], в которой передающий оптический блок формировал неортогональные кодовые состояния фотонов в соответствии с возбуждающей их двоичной псевдослучайной последовательностью со средней битовой скоростью B_0 на основе временного кодирования согласно протоколу BB84 [7], что позволяло использовать волоконные световоды (ВС) без сохранения поляризации.

В протоколах КРК ключ $\mathbf{k}_{АБ}$ формируется путем многоступенчатой рандомизации «сырого ключа» $\mathbf{k}_0$, первоначально создаваемого на одном конце канала путем кодирования каких либо неортогональных состояний однофотонных посылок светового сигнала. Обозначим битовую скорость этого исходного ключа как B_0, а среднюю битовую скорость генерации символов секретного ключа – B. Разность значений скоростей B_0–B связана с характеристикой помехоустойчивости приемника КРК – вероятностью генерации ложных символов P_f в ключе $\mathbf{k}_{АБ}$. На практике значение среднего числа фотонов в посылке m берется ~0,1 [7], так, что $p(1) \approx 0{,}1$, а $p(0) \approx 0{,}9$. Это обеспечивает дополнительную рандомизацию последовательности фотонов уже на этапе лазерного излучения. Другие механизмы случайного удаления однофотонных посылок из последовательности $\mathbf{k}_{АБ}$ в рассматриваемой технологии связаны с поглощением фотонов в оптическом волокне, а также особенностями протоколов КРК. Так, в протоколе BB84 коэффициент kр протокольного снижения скорости B_0 составляет 0,5, а в протоколе B92 для стандартного случая – 0,25 [8]. Еще один фактор снижения B обусловлен внутренними шумами приемного блока, которые, с одной стороны, с вероятностью P_l, приводят к пропускам сигнальных посылок в моменты опроса пороговой схемы, а с другой, с вероятностью P_f – к генерации ложных символов в ключе $\mathbf{k}_{АБ}$. По величине P_l можно получить оценку для скорости B. В основу для расчетов положили модель, представленную в работе [9], однако при смещении рабочей длины волны в длижнюю ИК-область, где потери в ВС значительно уменьшаются, необходимо дополнительно учитывать потери на стыковку оптоэлектронных элементов с ВС:

$$B = B_0 \left(1 - P_l\right) p(1) k_p 10^{-(\alpha L + \alpha_c)/10}, \tag{1}$$

где α – потери в ВС (дБ/км); α_c – суммарные потери на соединениях элементов (дБ); L – длина ВС (км).

Вероятность P_l выражается как:

$$P_l = \int_{-\infty}^{U_{пор}} p(n / u_c = 0) dn, \tag{2}$$

где $U_{пор}$ – порог срабатывания приемника, выраженный через число электронов n, проходящих через нагрузку ЛФД за время $\tau = 1/B$ – длительность импульсной характеристики приемного блока, обратная ширине полосы частот приемника B.

Распределение плотностей вероятности $p(n)$ числа n фотоэлектронов в нагрузке ЛФД в отсутствии (u_c=0) фотона будем считать гауссовыми:

$$p(n / u_c = 0) = \frac{u_0}{\sqrt{2\pi\sigma}} \exp\left(-\frac{n^2}{2\sigma^2}\right), \tag{3}$$

с безразмерной дисперсией σ [10]:

$$\sigma^2 = \frac{2i_d}{q}\tau I_2(\xi) + \frac{\tau I_2(\xi)}{q^2}\left(S_I + \frac{4k\theta}{R}\right) + S_E\left[\frac{I_2(\alpha)}{R^2} + (2\pi C)^2\frac{I_3(\xi)}{\tau q^2}\right], \quad (4)$$

$$S_I = 2qI_l, \qquad S_E = \frac{4k\theta N_k}{q_m}$$

где q – заряд электрона; θ – температура в градусах Кельвина; k – постоянная Больцмана; i_d – темновой ток; R – нагрузочное сопротивление ЛФД; S_E, S_I – приведенные ко входу шумовые источники тока и напряжения внутренних шумов предварительного усилителя приемного блока; I_l, N_k, q_m – ток утечки затвора, коэффициент шума и крутизна передаточной характеристики полевого транзистора в первом усилительном каскаде, соответственно; C – суммарная емкость выходной цепи приемного блока; ξ – заданный допуск на уширение сигнального импульса в тракте ФПУ вследствие ограничения полосы частот; I_2, I_3 – интегралы Персоника, выражаются через отношение спектров огибающей оптического сигнала на выходе и входе приемного блока [11].

2. Результаты численного моделирования

В системах квантовой криптографии в качестве детекторов приемного оптического модуля при комнатной температуре наибольшее распространение получили лавинные фотодиоды (ЛФД) [12] благодаря наилучшим параметрам при детектировании слабых оптических сигналов. В линейном режиме работы ЛФД основными шумами являются дробовые, шумы темнового тока и поверхностные шумы тока утечки [11]. Наименьшими шумами обладают кремниевые ЛФД. Однако максимум спектральной чувствительности таких фотодиодов приходится на длину волны 0,6 мкм, на которой потери в волоконном световоде (ВС) составляют 9 дБ/км. Кроме того, чтобы добиться коэффициента лавинного умножения M=100, необходимо напряжение обратного смещения не менее 360 В. При этом, как известно, минимальные потери излучения наблюдаются в кварцевых световодах на длине волны 1,55 мкм.

Анализ скорости генерации КРК проводили для двух длин волн: λ_1 = 0,85 мкм и λ_2 = 1,55 мкм. Для численного моделирования использовали следующие параметры: одномодовое волокно Corning SBF-28 с потерями α_1 = 2 дБ/км на λ_1 и α_2 = 0,25 дБ/км на λ_2. Суммарные потери на соединения включали в себя потери стыковки ВС с передающим блоком (1 дБ) и потери стыковки ВС с приемным модулем (0,2 дБ). В качестве ЛФД для λ_1 использовался кремниевый ЛФД Hamamatsu S8664-05K со следующими характеристика: квантовая эффективность η = 0,65, C = 1,5 пФ, θ = 293 K, i_d = 0,2 нА, M = 100, напряжение смещения диода U = 380 В. Для λ_2 применялся InGaAs-ЛФД Hamamatsu G14858 с характеристиками: η = 0,95, C = 2 пФ, θ = 293 K, i_d = 20 нА, M = 30, напряжение смещения диода U = 65 В. Характеристики полевого транзистора первого усилительного каскада следующие: I_l = 1 пА, N_k = 3 дБ, q_m = 40 мСм. Номинал нагрузочного сопротивления ЛФД равнялся 5 МОм, B_0 = 1 Мбит и τ_0 = 2 нс, соответственно.

Безусловная защищенность квантового канала системы КРК ограничена уровнем коэффициента квантовых ошибок Q-BER≈11%. Для систем КРК связь P_l и P_f с помехоустойчивостью более опосредована. Пропущенные символы удаляются из массива $\mathbf{k}_{АБ}$ в ходе протокольных переговоров, поэтому вероятность P_l не вносит никаких ошибок в формирование ключа, а определяет лишь среднюю скорость B его генерации. Уровень ложных сигналов в ключе при этом описывается строго

контролируемым параметром P_f. В простейшем случае в качестве инструмента контроля может использоваться пороговый уровень $U_{\text{пор}}$:

$$P_f = \int_{-U_{\text{пор}}}^{\infty} p(n/u_c \neq 0)dn, \tag{5}$$

$$p(n/u_c = M) = \frac{u_0}{\sqrt{2\pi}\sigma}\exp\left(-\frac{(n-M)^2}{2\sigma^2}\right). \tag{6}$$

Как следует из (2), значение P_l зависит от величины $U_{\text{пор}}$. Уровень $U_{\text{пор}}$ выбирали из условия, чтобы $P_f = 0{,}11$.

Результаты численного моделирования по формулам (1)–(6) представлены на рис. 1. Из полученных данных следует, что не смотря на то, что InGaAs-ЛФД обладает на два порядка большим темновым током и в три раза меньшим коэффициентом лавинного умножения по сравнению с Si-ЛФД, работа системы квантовой криптографии на длине волны 1,55 мкм позволяет увеличить битовую скорость формирования КРК от 1,6 до 15 раз в зависимости от длины волокна.

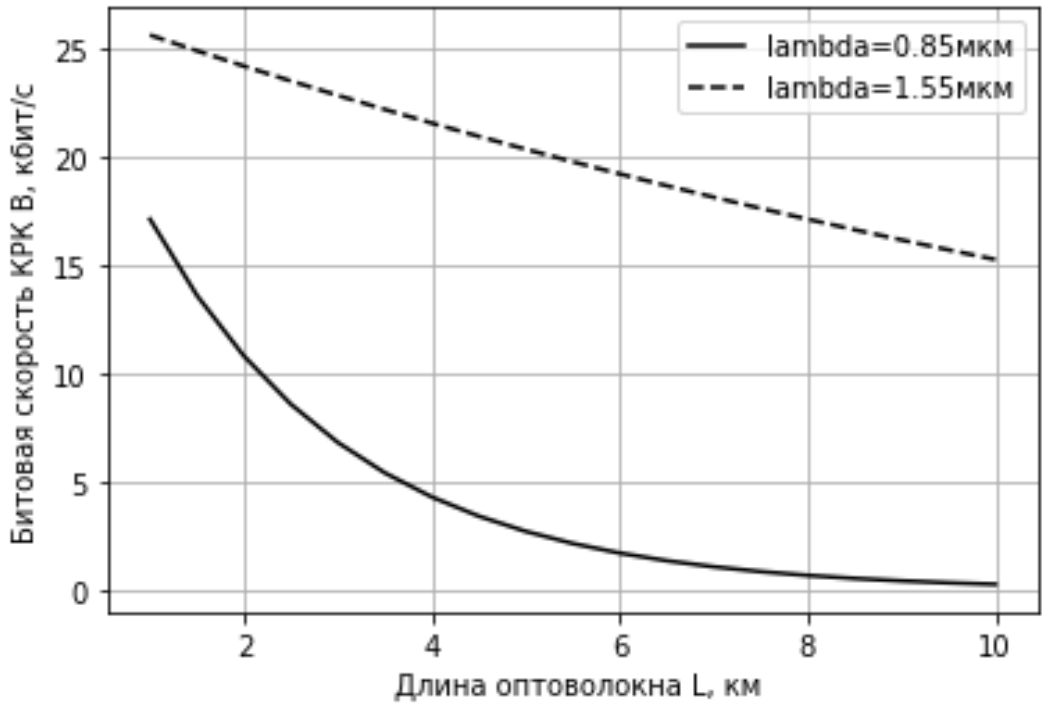

Рис. 1. – Зависимость битовой скорости формирования КРК от длины волоконно-оптической линии.

Заключение

Предложена математическая модель, описывающая помехоустойчивость систем квантовой криптографии. Проведена оценка битовой скорости формирования квантового распределения ключа для двух длин волн 0,85 мкм и 1,55 мкм при использовании Si-ЛФД и InGaAs-ЛФД в линейном режиме и скорости генерации псевдослучайной последовательности 1 Мбит в зависимости от длины одномодового волоконного световода. Учет потерь на стыковку оптоэлектронных элементов с оптоволокном уменьшает скорость формирования КРК на длине волны 1,55 мкм в 1,3

раза, на при этом на порядок больше, чем для длины волны 0,6 мкм, на которой наблюдается максимум спектральной чувствительности Si-ЛФД при длине ВС 1 км [8].

Литература

1. Килин Я. С., Хорошко Д. Б., Низовцев А. П. Квантовая криптография: идеи и практика. Минск: Беларуская навука, 2008.
2. Пустоход, Д. И. Хорошко Д. Б., Килин Я. С. Квантовое распределение ключа на временных сдвигах с использованием “состояний ловушек”. Оптика и спектроскопия. 2010. Т. 108, № 2. С. 366–373.
3. Debuisschert T., Boucher W. Time coding protocols for quantum key distribution. Phys. Rev. A. 2004. Vol. 70, No. 4. P. 042306–042306-16.
4. Молотков С.Н. Мультиплексная квантовая криптография с временным кодированием без интерферометров. Письма в ЖЭТФ. 2004. Т. 79, №. 9. С. 554–559.
5. Козубов А. В., Гайдаш А. А., Кынев С. М., Егоров В. И., Иванова А. Е., Глейм А. В., Мирошниченко Г. П. Основы квантовой коммуникации: часть 1. СПб: Университет ИТМО, 2019.
6. Румянцев К. Е., Голубчиков Д. М. Квантовая связь и криптография: Учебное пособие. Таганрог: ТТИ ЮФУ, 2009.
7. Молотков С. Н. Об интегрировании квантовых систем засекреченной связи (квантовой криптографии) в оптоволоконные телекоммуникационные системы. Письма в ЖЭТФ. 2004. Т. 79. С. 691–704.
8. Bennett C. H. Quantum cryptography using any two nonorthogonal states. Phys.Rev. Lett. 1992. Vol. 68, No 21. P. 3121–3124.
9. Задорин А. С., Максимов А. В., Махорин Д. А. и др. Скорость генерации кода в системе квантового распределения ключей. Доклады ТУСУРа. 2011. №2. С. 139–141.
10. Морен К. Методы гильбертова пространства. М.: Мир, 1965.
11. Keiser G. Optical Fiber Communications. New York : McGraw-Hill Inc., 1991.
12. Cova S., Ghioni M., Lacaita A., Samori C., Zappa F. Avalanche photodiodes and quenching circuits for single-photon detection. Applied Optics. 1996. Vol. 35, No. 12. P 1956-1976.

Quantum key distribution formation rate in the fiber-optic quantum cryptography systems

A.V. Polyakov, E.I. Lyahovskaya

Belarusian State University, Minsk,
e-mail: polyakov@bsu.by, elisaveta.lyahovskaya@gmail.com

A mathematical model is proposed that describes the noise immunity of quantum cryptography systems. The bit rate of a quantum key distribution (QKD) formation for two wavelengths 0.85 μm and 1.55 μm was estimated using Si-APD and InGaAs-APD and the 1 Mbit generation rate of a pseudo-random sequence, depending on the length of a single-mode fiber. It is shown that, despite the fact that InGaAs APD has a dark current large by two orders of magnitude and a three times lower avalanche multiplication factor as compared to Si APD, the operation of the quantum cryptography system at a wavelength of 1.55 μm makes it possible to increase the bit rate of formation QKD from 1.6 to 15 times with an increase in fiber length from 1 to 10 km.

Keywords: quantum cryptography, quantum key distribution, bit rate.