УДК 621.383.523

А.С. Задорин, А.В. Максимов, Д.А. Махорин, С.О. Чечулин, А.А. Маликов

Скорость генерации кода в системе квантового распределения ключей

Дана расчетная модель скорости генерации секретного кода и вероятности содержания в нем ошибочных символов системой квантового распределения ключей в условиях внешних и внутренних шумов.

Ключевые слова: квантовая криптография, режим счета фотонов, лавинный фотодиод, режим Гейгера.

Непрерывное повышение требований к уровню защищенности цифровых телекоммуникационных систем от несанкционированного доступа стимулирует и развитие криптографической стойкости используемых в них протоколов. Как известно, теоретически абсолютно безопасной криптосистемой является схема одноразового блокнота, к которой наиболее близко из всех возможных на сегодня позиционируется система квантового распределения ключей (КРК) [1]. Практическое распространение технологий КРК стало возможным после появления на рынке лавинных фотодиодов (ЛФД) с большим коэффициентом лавинного размножения M, способных работать в режиме счета фотонов [1, 2]. В данной связи прикладной интерес представляет адаптация известных методик расчета оптических фотоприемных устройств (ФПУ) [3, 4] для оценки предельных параметров систем КРК. Данная работа преследует именно эту цель.

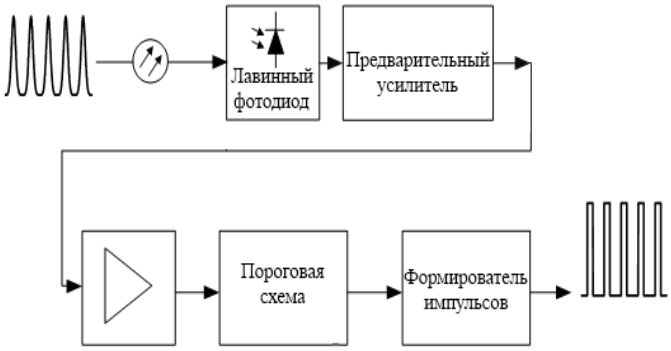

Рис. 1. Структурная схема КРК

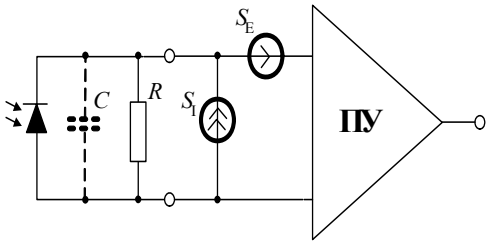

Рис. 2. Структурная схема ФПУ

Рассмотрим структурную схему ФПУ канала КРК (рис. 1). В дальнейшем будем считать, что данный канал построен на основе оптического волокна (ОВ) длиной L и с погонным затуханием α[дБ/км]. Будем полагать, что ЛФД работает в ждущем режиме (Гейгера). Его квантовую эффективность, коэффициент лавинного умножения и уровень темнового тока обозначим как η, M и i_{tt} соответственно. Внутренние шумы предварительного усилителя ФПУ, структурная схема которого представлена на рис. 2, представим приведенными к входу шумовыми источниками тока и напряжения S_E, S_I [3]. На рис. 2 нагрузочный резистор ЛФД и суммарная емкость выходной цепи ПУ обозначены как R и C.

Во всех протоколах технологии КРК секретный ключ K, как известно, формируется путем многоступенчатой рандомизации «сырого ключа» K_0, первоначально создаваемого на одном конце канала (Алиса) и передаваемого ею «Бобу» путем кодирования каких-либо неортогональных состояний однофотонных посылок светового сигнала [1, 2]. Обозначим битовую скорость этого исходного ключа как B_0, а среднюю скорость генерации символов секретного ключа – B. Разность значений скоростей B_0-B может быть весьма значительной. Она зависит от параметров ЛФД (η, M, i_{tt}), потерь в волокне, порога срабатывания ФПУ U_0 и др. и тесно связана с другой базовой характеристикой приемника – помехоустойчивостью, т.е. вероятностью генерации ложных символов P_f в ключе K. При отыскании оптимальных схемотехнических решений ФПУ необходимо установить и контролировать обе указанные зависимости. Рассмотрим каждую из них.

Прежде всего заметим, что при формировании Алисой однофотонных посылок на основе первоначального кода K_0 вероятность обнаружения в тактовом интервале n фотонов $p(n)$, при их среднем числе m, описывается пуассоновской статистикой. При этом значение m на практике берется ~0,1[1, 2], так, что $p(1)\approx 0{,}1$, а $p(0)\approx 0{,}9$. Отсюда следует, что уже на этапе передачи в системе КРК возникает рандомизация последовательности K_0. Происходит это, однако, за счет многократного снижения скорости генерации ключа.

Другие механизмы случайного удаления однофотонных посылок из последовательности K_0 в рассматриваемой технологии связаны с поглощением фотонов в оптическом волокне, ограниченной квантовой эффективностью ЛФД η, а также особенностями протоколов КРК. Так, в протоколе BB84 коэффициент k_p априорного снижения скорости B_0 составляет 0,5, а в протоколе B92 – 0,25 [1, 2].

Еще один фактор снижения скорости B обусловлен внутренними шумами ФПУ, 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 K. С учетом изложенного, находим оценку для скорости B:

$$B = B_0(1-P_l)\,p(1)k_p\exp(-\alpha L). \tag{1}$$

Для отыскания P_l и P_f воспользуемся стандартной методикой расчета помехоустойчивости оптической системы передачи (ОСП) [3, 4], учитывая при этом малость времени τ реакции ФПУ на однофотонную посылку по сравнению с длительностью тактового интервала $T = 1/B_0$. Данная особенность технологии КРК избавляет от необходимости введения высокочастотной коррекции АЧХ ФПУ, которая обычно используется для восстановления формы принимаемых символов. Здесь становится возможным, наоборот, сужение полосы частот системы относительно $1/\tau$ и снижение шумов приемника в $\sim T/\tau$ раз.

С учетом сделанных замечаний зададим основные шумовые источники канала КРК, определяющие вероятности P_l и P_f [3, 4]:

• Плотность вероятности (ПВ) дробовых шумов темнового тока i_{tt} подчиняется распределению Пуассона со средним числом n_{tt} темновых фотоэлектронов на измерительном интервале пороговой схемы ФПУ τ:

$$n_{tt} = (i_{tt}\cdot\tau)/e, \tag{2}$$

где e – заряд электрона.

• Шум нагрузки ЛФД и предварительного усилителя будем считать гауссовым и представим безразмерным температурным параметром W, имеющим смысл эквивалентного числа фотоэлектронов, порождаемых тепловыми шумами нагрузочного резистора и шумами источников S_E, S_I усилителя на указанном интервале τ:

$$W = \frac{2kt\tau}{R\cdot e^2}\left(\frac{\tau}{T}\right) + \frac{S_I\tau}{e^2}\left(\frac{\tau}{T}\right) + \frac{S_E\tau}{2e^2R^2}\left(\frac{\tau}{T}\right), \tag{3}$$

где t – температура в градусах Кельвина; k – постоянная Больцмана.

Опираясь на статистическую независимость названных шумовых источников, несложно отыскать суммарную ПВ в присутствии и в отсутствие сигнальной посылки p_c и p_n. При этом в качестве аргументов указанной композиции удобно использовать введенные выше числа фотоэлектронов n. В таком случае искомые вероятности P_l и P_f запишутся как

$$P_l = \int_{-\infty}^{U_0} p_c(n)dn,\ P_f = \int_{-U_0}^{\infty} p_n(n)dn, \tag{4}$$

где U_0 – порог срабатывания ФПУ, выраженный через n.

Изложенная выше методика была использована нами для моделирования канала КРК на основе кварцевого ОВ длиной 20 км, α=0,25 дБ/км, работающего при комнатной температуры, и реальных параметров ЛФД и ФПУ, взятых из [4]: $i_{tt} = 10^{-9}$ А; $R = 10^6$ Ом; η = 0,8; $M = 100$; $B_0 = 10^6$ Мбит/с; τ = 20 нс. Для указанных параметров и $U_0 = 190$ расчетные значения P_l и P_f оказались равными 0,012 и 0,783 соответственно, а средняя скорость генерации ключа B для протокола BB84 оказалась равной ~34,4 Кбит/с.

Интерес представляет зависимость B от вариации номинала R (рис. 3), при расчете каждой точки которой U_0 подбирался из условия $P_f = 0{,}1$. Монотонный, асимптотический характер этой кривой указывает на существование предельной скорости генерации секретного ключа системой $B_{\max}$. В

рассматриваемом случае $B_{max} \sim 145$ Кбит/с. Из рис. 3 можно также заключить, что реализация режима, близкого к B_{max}, достигается уже при сравнительно небольшом номинале $R \sim 300 \div 400$ кОм. Схемотехнически такой режим наиболее просто обеспечивается трансимпедансными усилителями.

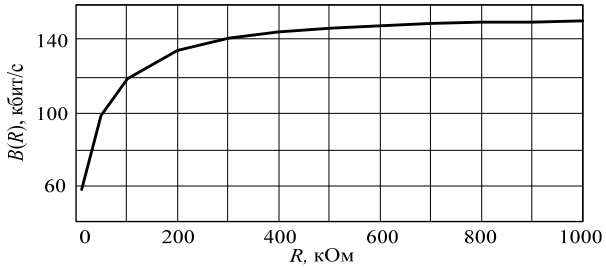

Рис. 3. Зависимость B от R

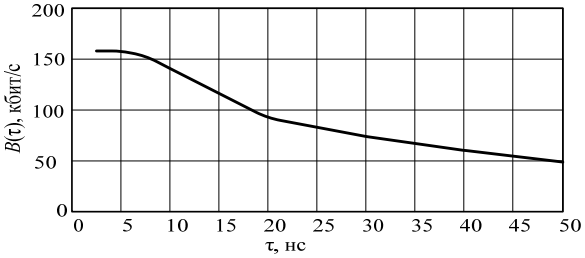

Рис. 4. Зависимость B от τ

На рис. 4 приведена аналогично рассчитанная зависимость скорости B от другой переменной – времени τ активации гейгеровского режима ЛФД и опроса пороговой схемы. Как видим, предельные скорости B_{max} в системе достижимы лишь при $\tau \sim 10^{-9}$с. Однако, как видно из рис. 4, в области малых времен кривая $B(\tau)$ меняется слабо. Это дает возможность на порядок снизить требования к быстродействию указанных блоков ФПУ, сохраняя при этом скорость близкой к B_{max}.

Литература

1. Молотков С.Н. Квантовая криптография и теоремы В.А. Котельникова об одноразовых ключах и об отсчетах // Успехи физических наук. – 2006. – Т. 176, № 7. – С. 777–788.

2. Elliott C. Quantum cryptography in practice // C. Elliott, D. Pearson, G. Troxel // SIGCOMM '03: Proceedings of the 2003 conference on applications, technologies, architectures, and protocols for computer communications. – New York, USA, 2003. – P. 227–238.

3. Keiser G. Optical fiber communications / Gerd Keiser. – Second Edition. – Singapore: McGraw-Hill, 2000. – 243 p.

4. Волоконно-оптические системы передачи: учеб. для вузов / М.М. Бутусов, С.М. Верник, С.Л. Галкин и др. – М.: Радио и связь, 1992. – 173 с.

Задорин Анатолий Семенович
Зав. каф. РЗИ ТУСУРа
Эл. почта: Anatoly.Zadorin@rzi.tusur.ru

Максимов Анатолий Владимирович
Инженер каф. РЗИ ТУСУРа
Эл. почта: MaksimovAV@rzi.tusur.ru

Махорин Дмитрий Алексеевич
Аспирант каф. радиоэлектроники и защиты информации (РЗИ) ТУСУРа
Эл. почта: mda.tomsk@gmail.com

Чечулин Сергей Олегович
Аспирант каф. радиоэлектроники и защиты информации (РЗИ) ТУСУРа
Эл. почта: ChechulinSO@rzi.tusur.ru
Сот. тел.: +7-923-401-1275

Маликов Алмас Аскарович
Магистрант гр. 141м, каф. РЗИ ТУСУРа

Zadorin A.S., Maksimov A.V., Mahorin D.A., Chechulin S.O., Malikov A.A.

Code generation rate in quantum key distribution system

Computational model of secret code generation speed and incorrect symbol existence probability by quantum key distribution system with internal and external noise is given.

Keywords: quantum cryptography, photon counting mode, avalanche photodiode, Geiger mode.