УДК 621.383.523

А.С. Задорин, А.В. Максимов, Д.А. Махорин

Режимы работы фотоприемного устройства системы квантовой криптографии

Дана сравнительная оценка линейного и ключевого режимов работы лавинных фотодиодов в системе квантового распределения ключей. Показано, что при низких скоростях линейный режим более помехоустойчив, а гейгеровский обеспечивает максимально возможную скорость генерации ключа.

Ключевые слова: квантовая криптография, лавинный фотодиод, счет фотонов, линейный и гейгеровский режимы.

Технические параметры систем квантового распределения ключей (КРК) [1–3] во многом определяются датчиками и схемотехническими решениями фотоприемного устройства (ФПУ). В качестве датчиков ФПУ на практике обычно используются лавинные фотодиоды (APD). В данных устройствах сигнальный ток i_s может быть усилен за счет лавинного размножения фотоэлектронов в обедненной области, когда обратное напряжение питания устройства U_a превышает некоторое пороговое значение U_b.

В линейном режиме работы фотодиода среднее число сигнальных фотоэлектронов n_s остается пропорциональным числу возбуждающих их фотонов n_p так, что $n_s \sim \eta \cdot M\, n_p$. Здесь η и M – квантовая эффективность и коэффициент лавинного умножения APD.

Чувствительность APD в линейном режиме описывается хорошо изученной моделью и ограничена как шумами самого диода (флуктуацией M, дробовым шумом темнового тока i_{tt}, и др.), так и внутренними шумами ФПУ [4]. Характеристики современных фотодиодов в принципе позволяют обеспечить режим счета одиночных фотонов.

Новые возможности в достижении предельной чувствительности ФПУ открывают лавинные фотодиоды специальной конструкции G-SPAD (Single Photon Avalanche Diode), способные работать не только в линейном режиме, но и в сильно нелинейном, ключевом режиме, который в литературе обозначается как «режим Гейгера» [1]. В гейгеровской моде напряжение питания диода U_a превышает пороговое напряжение U_b лавинного пробоя на величину так называемого перенапряжения (U_a–U_b). В этих условиях возбуждение G-SPAD единичным фотоэлектроном приводит к формированию в p–n-переходе диода самоподдерживающегося лавинного процесса с глубокой внутренней положительной обратной связью, приводящего к формированию в нагрузке G-SPAD сигнального отклика i_s макроскопического уровня, на фоне которого внутренние шумы ФПУ оказываются исчезающее малыми. Указанная особенность хорошо сочетается со спецификой детектирования бинарных оптических сигналов, и кроме этого, позволяет упростить схемотехнические решения реализации ФПУ. По указанным причинам именно диоды типа G-SPAD наиболее широко применяются для построения экспериментальных систем КРК.

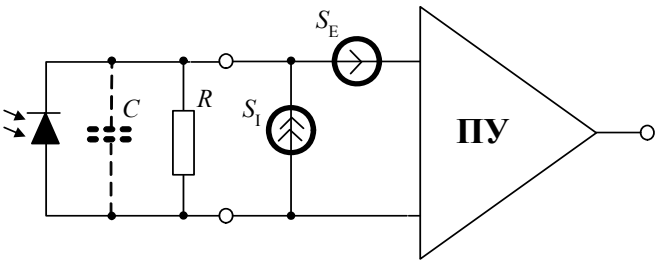

Рис. 1. Эквивалентная схема предварительного усилителя ФПУ

Вместе с тем в литературе отсутствуют сведения о сравнительной оценке линейного и нелинейного режимов APD с точки зрения влияния на помехоустойчивость, чувствительность и среднюю скорость генерации символов ключа B системы. Целью данного сообщения является исследование указанной задачи.

Рассмотрим вначале параметры системы КРК в линейном режиме работы APD. Будем считать, что канал КРК построен на основе оптического волокна (ОВ) длиной L и с погонным затуханием α [дБ/км]. Внутренние шумы предварительного усилителя ФПУ представим приведенными к входу

шумовыми источниками тока и напряжения S_E, S_I (рис. 1) [4]. Ннагрузочный резистор APD и суммарная емкость выходной цепи ФПУ обозначены как R и C.

Как известно, в протоколах КРК ключ K формируется путем многоступенчатой рандомизации «сырого ключа» K_0, первоначально создаваемого на одном конце канала путем кодирования каких-либо неортогональных состояний однофотонных посылок светового сигнала [1–3]. Обозначим битовую скорость этого исходного ключа как B_0, а среднюю 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 K. При отыскании оптимальных схемотехнических решений ФПУ необходимо контролировать обе указанные зависимости. Рассмотрим каждую из них.

Прежде всего заметим, что при формировании в канале КРК 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 [4]

$$p(n) = \frac{(m \cdot \eta)^n e^{-m \cdot \eta}}{n!}, \tag{1}$$

На практике значение m берется ~0,1 [4, 5], так, что $p(1) \approx 0{,}1$, а $p(0) \approx 0{,}9$. Это означает дополнительную рандомизацию последовательности фотонов уже на этапе лазерного излучения.

Другие механизмы случайного удаления однофотонных посылок из последовательности K_0 в рассматриваемой технологии связаны с поглощением фотонов в оптическом волокне, ограниченной квантовой эффективностью SPAD η, а также особенностями протоколов КРК. Так, в протоколе BB84 коэффициент $k_р$ протокольного снижения скорости B_0 составляет 0,5, а в протоколе B92 – 0,25 [3–5].

Еще один фактор снижения 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. По величине P_l можно получить оценку для скорости B:

$$B = B_0 (1 - P_l) p(1) k_p \exp(\alpha L). \tag{2}$$

Для отыскания вероятностей P_f и P_l воспользуемся методикой расчета помехоустойчивости ВОСП [4]. Для этого сделаем несколько допущений. Первое из них будет касаться формы вызываемых лавинными процессами импульсов в нагрузке APD $u_c(t)$, которую аппроксимируем гауссовой кривой

$$u_c(t) = \frac{u_0}{\sqrt{2\pi}\alpha} \exp\left(-\frac{t^2}{2\alpha^2 T^2}\right), \tag{3}$$

где α – параметр формы сигнала, определяющий долю тактового интервала = $1/B_0$, занимаемого сигнальным импульсом $u_c(t)$.

Определим далее вероятности P_l и P_f, связанные с внутренними источниками шума ФПУ. Среди этих источников рассмотрим шумы нагрузки SPAD и предварительного усилителя ФПУ, общее распределение плотности вероятности $p(n)$ которых будем считать гауссовым, с дисперсией, описываемой безразмерным температурным параметром W [4]:

$$W(\alpha) = \frac{I_2(\alpha)}{e^2 B_0}\left(S_I + \frac{4kt}{R}\right) + S_E\left[\frac{I_2(\alpha)}{R^2} + (2\pi C)^2 \frac{I_3(\alpha) B}{e^2}\right], \tag{4}$$

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

Параметр W в (4) имеет смысл эквивалентного числа фотоэлектронов, порождаемых тепловыми шумами нагрузочного резистора и внутренними шумами источников S_E, S_I ФПУ на интервале стробирования τ [4].

Коэффициенты I_2, I_3 в формуле (4) называются интегралами Персоника и устанавливают соотношение между эффективной шумовой полосой частот ФПУ $B_{эф}$ и битовой скоростью B_0 как [4]

$$B_{эф} = B_0 I_2 + C^2 R^2 B_0^3 I_3. \tag{5}$$

При этом второе слагаемое (5) определяет уширение $B_{эф}$, связанное с воздействием на помехоустойчивость КРК внутреннего источника шумового напряжения $e_a(t)$ предварительного усилителя ФПУ. Коэффициенты I_2, I_3 выражаются через отношение спектров огибающей оптического сигнала

на выходе и входе ФПУ. В качестве аргумента этих зависимостей выступает безразмерная нормированная частота $\Omega = \omega / T$:

$$I_2 = \int_0^{\infty} \left| \frac{H'_{\text{вых}}(\Omega)}{H_{\text{вх}}(\Omega)} \right|^2 d\Omega, \quad I_3 = \int_0^{\infty} \left| \frac{H_{\text{вых}}(\Omega)}{H_P(\Omega)} \right|^2 \Omega^2 d\Omega \quad . \tag{6}$$

Особенностью технологии КРК является малость времени τ по сравнению с длительностью тактового интервала $T = 1/B_0$. Это избавляет от необходимости введения высокочастотной коррекции АЧХ ФПУ, которая обычно используется в ВОСП для восстановления формы принимаемых символов. Здесь становится возможным, наоборот, сужение полосы частот ФПУ и снижение шумов приемника. Вследствие указанных особенностей системы тракта КРК сигнал $P_c(t)$ на выходе ФПУ системы КРК может значительно уширятся относительно (3). Допуск на такое отклонения обычно ограничен межсимвольной интерференцией и обеспечивается с характеристикой $H(f)$ тракта вида «приподнятого косинуса» [4].

Соотношения (4)–(6) определяют суммарную плотность вероятности шумов в присутствии и в отсутствие сигнальной посылки p_c и p_n. При этом в качестве аргументов данного распределения удобно использовать числа фотоэлектронов n. В таком случае искомые вероятности P_l и P_f запишутся как

$$P_l = \int_{-\infty}^{U_0} p_c(n)dn, \; P_f = \int_{-U_0}^{\infty} p_n(n)dn, \tag{7}$$

где U_0 – порог срабатывания ФПУ, выраженный через n.

Значение P_f определяет среднюю частоту F_r генерации ложных импульсов кода, вызываемых внутренними шумами ФПУ:

$$F_r = P_f B_0 . \tag{8}$$

Дадим далее оценку P_l и P_f в нелинейном режиме лавинного диода с временным стробированием.

Основной справочной характеристикой чувствительности G-SPAD, определяющей значение P_l, является эффективность регистрации фотонов $\varepsilon = (1 - P_l)$, равная вероятности регистрации падающего на фоточувствительную площадку G-SPAD фотона [5]. Величина ε равна

$$\varepsilon = \eta \cdot A \cdot P_G , \tag{9}$$

где A – геометрическая эффективность G-SPAD и P_G – вероятность возникновения гейгеровского разряда, зависящая от уровня перенапряжения ($U_a - U_b$).

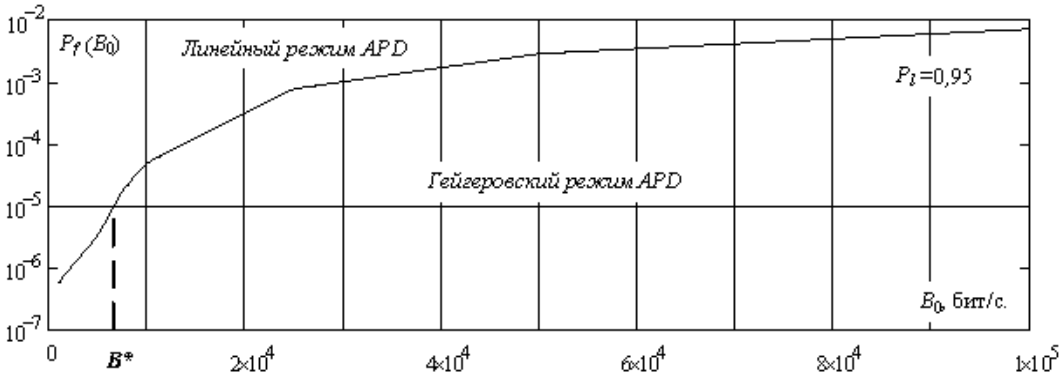

Рис. 2. Зависимости P_f от B_0 и режима APD при фиксированном значении P_l

Как отмечалось выше, сигнальный отклик i_s G-SPAD в гейгеровском режиме намного превышает шумы, поэтому формулы (4)–(6) для расчета вероятностей P_f здесь не применимы. Основными механизмами снижения помехоустойчивости системы в данном случае являются эффекты афтерпалсинга и спонтанного формирования лавин электронами темнового тока i_{tt}, который при перенапряжении перехода диода трансформируется в хаотическую последовательность коротких импульсов, средняя частота которой обозначается как F_{dcr} (DCR – dark count rate) [1, 5]. Если обозначить средние частоты генерации ложных символов, обусловленные указанными эффектами соответственно как F_{ap} и F_{dcr}, то:

$$P_f = (F_{ap} + F_{dcr}) / B_0 . \tag{10}$$

Справочные параметры ε, F_{ap} и F_{dcr} зависят от типа G-SPAD и перенапряжения ($U_a - U_b$), но при использовании в контроллере ФПУ активных способов гашения лавины и коротком времени стробирования τ ~ 1 нс практически не зависят от системной скорости B_0. Этот вывод иллюстрируется графиком на рис. 2, рассчитанным по формуле (10) для G-SPAD SAP500-Series [6].

На этом же графике приведена аналогичная зависимость для Si APD типа S8664-05K [7], работающем в линейном режиме. Кривая рассчитана по формулам (2)–(7) для модели канала КРК на основе кварцевого ОВ длиной 20 км, α = 0,25 дБ/км, работающего при комнатной температуре и параметрах ФПУ, взятых из [4]: i_{tt} = 0,1 пА; M = 100; C = 1 пФ. При расчете каждой точки графика номинал сопротивления нагрузки R APD подбирался из условия: $3 \cdot R \cdot C \approx (B_0)^{-1}$. Из представленных данных видно, что вследствие расширения шумовой полосы частот ФПУ с ростом частоты B_0 вероятность генерации ложных символов в линейном режиме увеличивается монотонно и асимптотически.

На приведенном рисунке интерес представляет точка B^* пересечения графиков $P_f(B_0)$ линейного и ключевого режимов работы APD. В области $B_0 < B^*$ линейный режим APD более помехоустойчив. В противном случае преимущество имеет гейгеровский режим работы диода. Положение границы B^* следует уточнять для каждого типа APD, однако приведенные данные показывают, что ключевой режим работы лавинного диода принципиально обеспечивает максимально возможную скорость генерации ключа.

Литература

1. Avalanche photodiodes and quenching circuits for single-photon detection / S. Cova, M. Ghioni, A. Lacaita et al. // Applied Optics. – 1996. – Vol. 35, No. 12. – P. 1956–1976.
2. Килин С.Я. Квантовая информация / Успехи физических наук. – 1999. – Т. 169. – С. 507–527.
3. 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.
4. Keiser G. Optical Fiber Communications. – New York: McGraw-Hill Inc., 1991. – 461 p.
5. Duarte F.J. Laser Pulse Phenomena and Applications // [Электронный ресурс]. – Режим доступа: http://www.twirpx.com/file/502972/, свободный (дата обращения: 09.12.2012).
6. Данные о кремниевом лавинном диоде, с гейгеровским режимом [Электронный ресурс]. – Режим доступа: http://www.lasercomponents.com/de/?embedded=1&file=fileadmin/user_upload/home/Datash eet/l cd/sap-series.pdf&no_cache=1, свободный (дата обращения: 17.09.2012).
7. Данные о кремниевом лавинном диоде S8664 серии [Электронный ресурс]. – Режим доступа: http://sales.hamamatsu.com/assets/pdf/parts_S/S8664_series.pdf свободный, (дата обращения: 17.09.2012).

Задорин Анатолий Семенович
Д.-р физ.-мат. наук, профессор, зав. каф. радиотехники и защиты информации (РЗИ) ТУСУРа
Тел.: 8 (382-2) 41-33-65
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. РЗИ ТУСУРа
Эл. почта: mda.tomsk@gmail.com

Zadorin A.S., Maksimov A.V., Mahorin D.A.
Working modes of photodetector device of quantum cryptography system

There is given a comparative evaluation of linear and switching mode operation of avalanche photodiodes in a quantum key distribution. It is shown that at low speeds, the linear mode is more resistant to interference, and a Geiger one provides a maximum key generation rate.
Keywords: quantum cryptography, avalanche photodiode photon counting, linear and Geiger modes.