МЕТОДЫ ИЗМЕРЕНИЯ СРЕДНЕГО ЧИСЛА ФОТОНОВ В ИНФОРМАЦИОННЫХ ИМПУЛЬСАХ СИСТЕМ КВАНТОВОГО РАСПРЕДЕЛЕНИЯ КЛЮЧЕЙ

Methods for Measurement Mean Photon Number in Information Pulses of Quantum Key Distribution Systems

Борисова А.В.[1] (Borisova A.V.), Втюрина А.Г.[1] (Vtyurina A.G.), Бычков С.Б.[2] (Bychkov S.B.), Николаева А.С.[3] (Nikolaeva A.S.)

[1] ОАО «ИнфоТеКС», Москва
JSC "InfoTeCS", Moscow;
[2] ФГУП «ВНИИОФИ», Москва
FGUP "VNIIOFI" The All-Russian Research Institute for Optical and Physical Measurements, Moscow
[3] ФГАОУ ВО МФТИ (НИУ), Московская область, г. Долгопрудный
Moscow Institute of Physics and Technology
National Research University, Dolgoprudny, Moscow Region
Тел.: +79035740565, E-mail: borisova_alina_95@mail.ru

В статье представлены способы измерения среднего числа фотонов в квазиоднофотонных импульсах, используемых для передачи квантовых состояний при квантовом распределении ключей (КРК, QKD).

The article presents several methods for measuring mean photon number in quasi-single-photon pulses that are used for transmitting quantum states in quantum key distribution (QKD).

При изготовлении и проведении проверок безопасности систем квантового распределения ключей (КРК, QKD) обязательным пунктом испытаний является измерение среднего числа фотонов в квазиоднофотонных импульсах, поступающих в квантовый канал. Данный факт обусловлен необходимостью соответствия параметров генерации квантовых состояний протоколу квантового распределения ключей с доказанной секретностью. В противном случае система КРК подвержена атакам на протокол, в частности, при превышении требуемого среднего числа фотонов система подвержена атаке с разделением по числу фотонов.

В настоящее время существует несколько способов счета фотонов:

1. метод TCSPC (Time-correlated single photon counting), основанный на схеме совпадений и широко применяемый для исследования флуоресценции молекул;
2. метод прямого счета однофотонным детектором;
3. с помощью высокочувствительного фотодиода и пикоамперметра.

Описание первого метода можно найти в [1-2], поэтому в данной статье подробнее остановимся на втором и третьем методах.

Так как однофотонный уровень мощности информационных импульсов при настройке системы КРК достигается путем регулировки вносимого

аттенюатором ослабления, то на практике удобно использовать грубый метод оценки среднего числа фотонов, заключающийся в измерении мощности импульсов излучения на выходе лазера, коэффициента ослабления (вносимых потерь) оптической схемы и проведения соответствующих расчетов. Для более точной оценки среднего числа фотонов, например, при аттестации системы КРК, необходимо использовать один из описанных ниже методов.

Измерение с помощью счетчика одиночных фотонов

Под счетчиком одиночных фотонов подразумевается оптоэлектронный модуль, включающий в себя калиброванный однофотонный детектор и схему регистрации с пороговым преобразователем. В качестве детектора зачастую используются однофотонные лавинные фотодиоды (SPAD) или сверхпроводящие однофотонные детекторы (SSPD). Счетчик фотонов считает все импульсы, амплитуда которых значительно превышает значение, выбранное в качестве порога дискриминатора, и сохраняет результат счета во флеш-памяти устройства.

Счетчик одиночных фотонов может представлять собой отдельный измерительный модуль или входить в состав приемной части системы КРК (Боба). При этом независимо от типа устройства, однофотонный детектор должен быть откалиброван, то есть должны быть известны квантовая эффективность (QE или η) и скорость темнового счета (DCR – dark count rate) при рабочих значениях напряжения смещения и температуры.

Для измерения среднего числа фотонов в импульсе, μ, регистрируется количество срабатываний K калиброванного однофотонного детектора при отправке известного количества лазерных импульсов M. Затем рассчитывается частота срабатываний детектора $\nu = K/M$, которая при большом M стремится к вероятности детектирования, p_{det}, непосредственно связанной со средним числом фотонов в импульсе формулой [3]:

$$\frac{K}{M} \xrightarrow[M\to\infty]{} p_{det} = 1 - e^{-\mu\eta}, \qquad (1)$$

где η – квантовая эффективность однофотонного детектора.

Очевидно, что от количества отправленных импульсов M зависит погрешность измерения вероятности детектирования ε, а значит, и погрешность измерения среднего числа фотонов в импульсе. Данная зависимость определяется неравенством Хёфдинга, имеющим вид:

$$P[(p_{det} - \varepsilon)M \le K \le (p_{det} + \varepsilon)M] \ge 1 - 2\,exp\{-2\varepsilon^2 M\}. \qquad (2)$$

Следовательно, перед проведением измерений необходимо задаться допустимой -окрестностью и доверительной вероятностью P нахождения вероятности детектирования p_{det} в заданном доверительном интервале $p_{det} \pm \varepsilon$. Затем по заданным величинам рассчитывается число импульсов M.

В качестве примера возьмем доверительный интервал, равный 1% от вероятности детектирования, т. е. $\varepsilon = 0{,}01 \cdot p_{det}$. В системах КРК среднее число фотонов в импульсе обычно лежит в диапазоне от 0,1 до 0,5; а

квантовая эффективность однофотонных лавинных фотодиодов – от 10% до 20% [4]. Следовательно, минимальная вероятность детектирования составляет $p_{det} \approx \mu\eta = 0{,}1 \cdot 0{,}1 = 0{,}01$, а доверительный интервал – $\varepsilon = 0{,}01 \cdot p_{det} = 0{,}01 \cdot 0{,}01 = 0{,}0001$ отсчета/импульс. Измерения целесообразно проводить с точностью не менее $P = 99{,}9\%$, тогда при данных параметрах количество лазерных импульсов M, по которому оценивается количество отсчетов детектора, составляет:

$$M \geq -\frac{1}{2\varepsilon^2}\ln\left(\frac{1-P}{2}\right) = -\frac{1}{2 \cdot 0{,}0001^2}\ln\left(\frac{1-0{,}999}{2}\right) \approx 4 \cdot 10^8. \quad (3)$$

Для выполнения измерений выход передающей системы КРК (Алисы) подключается напрямую к счетчику одиночных фотонов.

Далее регистрируется количество срабатываний калиброванного однофотонного детектора K при отправке M квазиоднофотонных импульсов и рассчитывается вероятность детектирования в соответствии с левой частью формулы (1). В свою очередь среднее число фотонов в импульсе выражается из правой части той же формулы (1):

$$\mu = -\frac{1}{\eta} \cdot \ln(1 - p_{det}). \quad (4)$$

Диапазон, в котором с заданной вероятностью P (в примере она составляла 0,999) лежит среднее число фотонов в лазерном импульсе, рассчитывается следующим образом:

$$-\frac{1}{\eta}\ln(1 - p_{det} + \varepsilon) \leq \mu \leq -\frac{1}{\eta}\ln(1 - p_{det} - \varepsilon). \quad (5)$$

Таким образом, данный метод позволяет с требуемой точностью измерить среднее число фотонов в импульсе путем накопления необходимой статистики счетным детектором одиночных фотонов.

Измерение с помощью фотодиода и пикоамперметра

Аналогично предыдущему методу для выполнения измерений выход передающей системы КРК (Алисы) подключается напрямую к откалиброванной высокочувствительной измерительной системе. Последняя представляет собой комбинацию из InGaAs-фотодиода и пикоамперметра, для которой известна спектральная чувствительность на рабочей длине волны: при этом коэффициент чувствительности не менее 0,5 А/Вт, диапазон измерения тока до 10^{-13} А. Для повышения точности измерения среднего числа фотонов предварительно рекомендуется измерить уровень темнового тока $I_т$.

Обобщенный порядок выполнения измерений данным методом:

1. Калибровка измерительной системы из фотодиода и пикоамперметра: определение спектральной чувствительности $S_{фд}$.
2. Измерение темнового тока $I_т$.
3. Измерение частоты следования информационных квазиоднофотонных импульсов $f_и$ (данный пункт опускается, если частота заранее известна).

4. Запуск генерации серии импульсов и регистрация протекающего через фотодиод фототока $I_{ф}$.
5. Расчет мощности P квазиоднофотонных импульсов по формуле:

$$P_{ср} = \frac{I_{ф} - I_{темн}}{S_{фд}}. \quad (6)$$

6. Расчет среднего числа фотонов:

$$\mu = \frac{P_{ср} \cdot \lambda}{2 \cdot f_{и} \cdot h \cdot c}, \quad (7)$$

где λ – длина волны оптического излучения, м; h – постоянная Планка ($h \approx 6{,}63 \cdot 10^{-34}$ Дж·с); c –скорость света в вакууме, м/с.

7. Оценка погрешности измерения. Для расчета неопределенности можно использовать формулу:

$$u_{A_\mu} = \sqrt{\left(\frac{\sigma_P}{P_{ср}}\right)^2 + \left(\frac{\sigma_f}{f_{л.и.}}\right)^2}, \quad (8)$$

где σ_P – среднеквадратическое отклонение (СКО) измеренной мощности импульсов, σ_f – СКО измеренной частоты следования импульсов.

Представленный метод имеет преимущество перед ранее описанными ввиду отсутствия необходимости использовать труднодоступные счетчики одиночных фотонов, что позволяет применять данную методику при аттестации систем КРК, требующей использования поверенных измерительных средств.

Заключение

В данной работе приведен обзор существующих методов измерения среднего числа фотонов в квазиоднофотонных импульсах и подробно раскрыты наиболее применимые методики, основанные на прямом счете одиночных фотонов и на регистрации средней мощности излучения высокочувствительной системой. Выбор метода измерений обуславливается как целями исследования, так и имеющимся измерительным оборудованием.

Литература

1. O'Connor, D.V.O., Phillips, D. Time-correlated Single Photon Counting // Academic Press. London. – 1984.
2. Wahl M. Time-correlated single photon counting //Technical Note. – 2014. – С. 1-14.
3. Chunnilall C. J. et al. Metrology of single-photon sources and detectors: a review //Optical Engineering. – 2014. – Т. 53. – №. 8. – С. 081910.
4. Алферов С.В., Балыгин К.А., Борисова А.В., Втюрина А.Г., Климов А.Н. Характеристики InGaAs/InP однофотонных лавинных детекторов производства корейской фирмы WOORIRO // Фотоника. – 2018. – №7. – С. 662–666.