УДК 535.14
DOI 10.25205/2541-9447-2018-13-4-91-104

Исследование статистики регистрации одиночных фотонов двумя фотодетекторами для применений в квантовой криптографии

Д. Б. Третьяков [1, 2], **А. В. Коляко** [1–3], **А. С. Плешков** [1–3], **В. М. Энтин** [1, 2]
И. И. Рябцев [1, 2], **И. Г. Неизвестный** [1, 4]

[1] *Институт физики полупроводников им. А. В. Ржанова СО РАН*
[2] *Новосибирский государственный университет*
[3] *Институт лазерной физики СО РАН*
[4] *Новосибирский государственный технический университет*
Новосибирск, Россия

Аннотация

Предложен метод обнаружения атаки с делением числа фотонов в квантово-криптографических системах связи по измерению распределения числа фотонов в лазерном импульсе. Вместо использования сложного фотодетектора, способного различать число зарегистрированных фотонов, мы предлагаем использовать два обычных однофотонных детектора на основе лавинных фотодиодов. Представлены результаты экспериментов по измерению числа фотонов в лазерном импульсе и их сравнение с теоретическими расчетами. Обсуждаются пределы применимости предложенного метода.

Ключевые слова

квантовая криптография, атака с делением числа фотонов, детекторы одиночных фотонов

Благодарности

Работа поддержана Институтом физики полупроводников им. А. В. Ржанова СО РАН и Новосибирским государственным университетом

Для цитирования

Третьяков Д. Б., *Коляко А. В.*, *Плешков А. С.*, *Энтин В. М.*, *Рябцев И. И.*, *Неизвестный И. Г.* Исследование статистики регистрации одиночных фотонов двумя фотодетекторами для применений в квантовой криптографии // Сибирский физический журнал. 2018. Т. 13, № 4. С. 91–104. DOI 10.25205/ 2541-9447-2018-13-4-91-104

Investigation of the Statistics of Single-Photon Counting by Two Photodetectors for Applications in Quantum Cryptography

D. B. Tretyakov [1, 2], **A. V. Kolyako** [1–3], **A. S. Pleshkov** [1–3], **V. M. Entin** [1, 2]
I. I. Ryabtsev [1, 2], **I. G. Neizvestny** [1, 4]

[1] *A. V. Rzhanov Institute of Semiconductor Physics SB RAS*
[2] *Novosibirsk State University*
[3] *Institute of Laser Physics SB RAS*
[4] *Novosibirsk State Technical University*
Novosibirsk, Russian Federation

Abstract

A method for revealing a photon-number-splitting attack in quantum-cryptographic communication systems by measuring the photon-number distribution in a laser pulse is proposed. Instead of using a complex photon-number-resolving detector, we propose to use two conventional single-photon detectors based on avalanche photodiodes. The results of experiments on measuring the photon numbers in a laser pulse and their comparison with theoretical calculations are presented. The limits of the applicability of the proposed method are discussed.

Keywords
quantum cryptography, photon-number-splitting attack, single-photon detectors
Acknowledgements
This work was supported by Rzhanov Institute of Semiconductor Physics SB RAS and Novosibirsk State University
For citation
Tretyakov D. B., Kolyako A. V., Pleshkov A. S., Entin V. M., Ryabtsev I. I., Neizvestny I. G. Investigation of the Statistics of Single-Photon Counting by Two Photodetectors for Applications in Quantum Cryptography. *Siberian Journal of Physics*, 2018, vol. 13, no. 4, p. 91–104. (in Russ.) DOI 10.25205/2541-9447-2018-13-4-91-104

Введение

Интерес к быстро развивающейся в последнее время квантовой криптографии обусловлен возможностью создания в ближайшее время квантового компьютера, который, как теоретически доказано, способен взломать самые надежные на сегодняшний день криптографические шифры [1]. Поскольку в квантовой криптографии передача секретной информации происходит посредством квантовых объектов – одиночных фотонов, абсолютная секретность передачи обеспечивается законами квантовой механики, а именно невозможностью измерить и воспроизвести состояние перехваченного одиночного фотона с абсолютной достоверностью [2]. С помощью передачи одиночных фотонов в квантовом канале (оптоволоконной или атмосферной линии связи) генерируется только секретный ключ, который затем используется отправителем (Алисой) и получателем (Бобом) в симметричной криптосистеме, а само зашифрованное сообщение может передаваться по любому открытому каналу [1]. Наибольшая потребность в квантово-криптографических системах связи ожидается в тех случаях, когда абсолютная секретность передачи информации обладает бóльшим приоритетом, чем скорость передачи данных. Дальнейшее развитие квантовых систем связи требует увеличения дальности и скорости генерации квантового ключа, а также степени их защищенности.

В 1984 г. был предложен первый квантово-криптографический протокол BB84 [3], а в 1992 г. осуществлена первая экспериментальная демонстрация генерации квантового ключа по данному протоколу с помощью передачи одиночных, поляризованных в двух неортогональных базисах фотонов по воздушной линии связи [4]. В дальнейшем фундаментальные научные исследования в этой области постепенно перешли к проблеме создания практических квантовых систем связи и появлению коммерческих устройств, таких как система Clavis производства фирмы «ID Quantique» [1].

Поскольку в настоящее время коммерчески доступных истинных источников одиночных фотонов еще не существует, в квантовой криптографии в качестве таких источников применяются сильно ослабленные короткие лазерные импульсы [1]. Если обозначить среднее число фотонов в лазерном импульсе как μ, то вероятность $P(n)$ найти n фотонов в лазерном импульсе подчиняется статистике Пуассона:

$$P(n) = \frac{\mu^n}{n!} e^{-\mu}. \quad (1)$$

При $\mu \ll 1$ доля «пустых» импульсов, вообще не содержащих фотонов, будет равна $P(0) \approx 1 - \mu + \mu^2/2$. Доля импульсов, содержащих один фотон, $P(1) \approx \mu - \mu^2$, а доля импульсов, содержащих два фотона, $P(2) \approx \mu^2/2$. Например, для μ = 0,1 получаем $P(0) \approx 0{,}905$, $P(1) \approx 0{,}09$, $P(2) \approx 0{,}005$. Это означает, что вероятность найти в лазерном импульсе больше, чем один фотон, мала по сравнению с вероятностью однофотонных лазерных импульсов.

[1] https://www.idquantique.com

Основной проблемой квантовых линий связи является потеря одиночных фотонов при передаче по протяженному квантовому каналу, что приводит к уменьшению скорости генерации квантового ключа. Для увеличения скорости генерации квантового ключа можно увеличить среднее число фотонов в лазерном импульсе, однако это будет способствовать тому, что подслушиватель (Ева) применит атаку с делением числа фотонов [5]. В этом типе атак Ева, по предположению обладающая любыми совершенными технологиями, перехватывает каждый импульс, идущий от Алисы, и измеряет число фотонов в импульсе с помощью квантовых неразрушающих измерений [6]. Далее она отделяет от многофотонных импульсов по одному фотону, сохраняет этот фотон в квантовой памяти до конца одиночной сессии между Алисой и Бобом, а оставшиеся фотоны посылает Бобу. При этом однофотонные импульсы Евой не пропускаются. После того, как Алиса и Боб проведут сверку базисов по открытому каналу в соответствии с протоколом BB84, Ева измерит состояния фотонов в нужном базисе, получив таким образом весь ключ, сформированный Алисой и Бобом. После атаки с делением числа фотонов резко уменьшается число фотонов в квантовом канале, что легко может обнаружить Боб, если он знает заранее, сколько примерно фотонов он должен зарегистрировать при генерации квантового ключа. Поэтому данный тип атаки может использоваться только в случае квантового канала с высокими потерями. Тогда Ева может направить Бобу оставшиеся после атаки фотоны не по основному, а по дополнительному каналу без потерь, увеличив таким образом число фотонов, дошедших до Боба. Однако, как показано в работе [5], для того, чтобы Ева отправила Бобу столько фотонов, сколько он должен зарегистрировать в отсутствие атаки, коэффициент пропускания квантового канала T должен быть меньше критического значения T_0:

$$T_0 = 1 - \ln(1+\mu)/\mu. \tag{2}$$

На сегодняшний день разработано несколько протоколов, предназначенных для противодействия атакам с делением числа фотонов в квантовых каналах с большими потерями [7–10]. Одним из наиболее широко применяемых на практике является протокол, использующий импульсы-«ловушки» (decoy state) [10]. В данном протоколе некоторые лазерные импульсы, несущие информацию, заменяются Алисой на импульсы со средним числом фотонов, большим, чем для основных лазерных импульсов. Поскольку Ева не может отличить импульс-«ловушку» от обычного импульса, то она проводит с ним те же операции, что и с обычным. В итоге Алиса и Боб обнаруживают атаку по увеличению числа зарегистрированных импульсов-«ловушек» по отношению к числу обычных импульсов.

В случае, когда коэффициент пропускания квантового канала $T > T_0$ из уравнения (2), Ева, чтобы не внести ошибок в передаваемый ключ, вынуждена будет пропускать однофотонные импульсы и отделять по одному фотону только от многофотонных импульсов. Таким образом, она незаметно получит только часть ключа, сформированного Алисой и Бобом. Однако в этом случае атака с делением числа фотонов делает распределение числа фотонов в лазерном импульсе отличным от пуассоновского (1). Как показано в работе [11], если у Боба имеется фотодетектор, способный различать число зарегистрированных фотонов, то он может выявить атаку с делением числа фотонов по изменению статистики регистрации импульсов с разным числом фотонов. В настоящее время предложено несколько технологий для реализации таких фотодетекторов [12–14], однако все они достаточно сложны в изготовлении и имеют высокую стоимость.

В работе [15] предложен более простой способ обнаружения атаки с делением числа фотонов по измерению распределения числа фотонов в импульсе с использованием двух обычных фотодетекторов, не обладающих разрешением по числу фотонов, перед которыми расположено полупрозрачное зеркало. Идущее от Алисы излучение делится на зеркале пополам таким образом, что одна половина фотонов направляется на один фотодетектор, вторая – на второй. Однако в работе [15] рассматривается специфическая атака с делением числа фо-

тонов, в результате которой распределение числа фотонов в импульсе меняется иначе, чем в классической атаке с делением числа фотонов.

В нашей работе мы рассматриваем метод обнаружения атаки с делением числа фотонов по распределению числа фотонов в импульсе с использованием двух обычных фотодетекторов именно для классического варианта этой атаки. Также представлены результаты простого эксперимента по регистрации одиночных фотонов двумя фотодетекторами и сравнение их с теоретическими расчетами. Обсуждаются пределы применимости предложенного метода.

Теория

После прохождения одиночных фотонов через квантовый канал с коэффициентом пропускания T и регистрации фотонов фотодетектором с эффективностью регистрации η формула (1) преобразуется в следующее выражение:

$$P_{\text{det}}(n) = \frac{(\mu\eta T)^n}{n!} \mathrm{e}^{-\mu\eta T}, \tag{3}$$

где $P_{\text{det}}(n)$ – вероятность зарегистрировать n фотонов в одном лазерном импульсе. Эта формула получается сверткой вероятностей испускания и регистрации определенного числа фотонов [11; 16; 17].

Если фотодетектор различает число зарегистрированных фотонов, то вероятность регистрации одного фотона будет равна

$$P_{\text{det}}(1) = \mu\eta T \cdot e^{-\mu\eta T}, \tag{4}$$

а вероятность регистрации двух фотонов –

$$P_{\text{det}}(2) = (\mu\eta T)^2 \cdot e^{-\mu\eta T}/2. \tag{5}$$

Если фотодетектор не различает число зарегистрированных фотонов, то вероятность срабатывания фотодетектора при регистрации любого числа фотонов будет равна

$$\overline{P}_{1\text{det}} = \sum_{n=1}^{\infty} P_{\text{det}}(n) = 1 - e^{-\mu\eta T}. \tag{6}$$

Если разделить лазерный импульс полупрозрачным зеркалом и направить одну часть фотонов на один фотодетектор, а вторую – на второй, то при условии равенства эффективности регистрации этих фотодетекторов, вероятность срабатывания только одного из них будет выглядеть следующим образом:

$$\overline{P}_{2\text{det}}(1) = 2\left(1 - e^{-\mu\eta T/2}\right) \cdot e^{-\mu\eta T/2}, \tag{7}$$

а вероятность одновременного срабатывания –

$$\overline{P}_{2\text{det}}(2) = \left(1 - e^{-\mu\eta T/2}\right)^2. \tag{8}$$

Формула (7) представляет собой произведение вероятности срабатывания одного из фотодетекторов и вероятности отсутствия срабатывания другого. Произведение умножается на 2,

поскольку та же самая вероятность существует при перестановке фотодетекторов. Показатель экспоненты делится пополам, так как на оба фотодетектора падает импульсное излучение со средним числом фотонов в импульсе $\mu/2$. В свою очередь, формула (8) есть произведение вероятностей срабатывания обоих фотодетекторов.

Если оба фотодетектора различают число зарегистрированных фотонов, то вероятность срабатывания только одного из фотодетекторов будет равна вероятности регистрации одного фотона одиночным фотодетектором, различающим число зарегистрированных фотонов согласно формуле (4).

Наглядно представить различие в статистике регистрации фотонов одним фотодетектором, различающим число зарегистрированных фотонов, и двумя обычными фотодетекторами можно в случае $\mu \cdot \eta \cdot T \ll 1$. Тогда, оставляя члены только первого и второго порядка по $\mu \cdot \eta \cdot T$ (т. е., пренебрегая вероятностью регистрации трехфотонных импульсов), преобразуем выражение (4) в выражение

$$P_{\text{det}}(1) \approx \mu \cdot \eta \cdot T - \left(\mu \cdot \eta \cdot T\right)^2, \tag{9}$$

выражение (5) преобразуем в выражение

$$P_{\text{det}}(2) \approx \left(\mu \cdot \eta \cdot T\right)^2 / 2, \tag{10}$$

выражение (7) преобразуем в выражение

$$\overline{P}_{2\,\text{det}}(1) \approx \mu \cdot \eta \cdot T = 3\left(\mu \cdot \eta \cdot T\right)^2 / 4, \tag{11}$$

а выражение (8) преобразуем в выражение:

$$\overline{P}_{2\,\text{det}}(2) \approx \left(\mu \cdot \eta \cdot T\right)^2 / 4. \tag{12}$$

При сравнении выражения (9) с (11) и выражения (10) с (12) видно, что система из двух обычных фотодетекторов будет различать число зарегистрированных фотонов только частично, так как в половине случаев оба фотона проходят через зеркало или отражаются от него, попадая на один из фотодетекторов, и регистрируются, как один фотон. Мы поставили себе целью проанализировать эти предположения в эксперименте.

Экспериментальная установка

Эксперименты по исследованию статистики регистрации фотонов в лазерном импульсе проводились на основе атмосферной экспериментальной установки для генерации квантового ключа по протоколу BB84, созданной ранее в Институте физики полупроводников СО РАН [16; 17]. На рисунке 1 изображена часть этой установки, используемая в описываемых экспериментах. В качестве источника световых импульсов применялся лазерный диод ADL-78901TL фирмы «Laser components GmbH» с длиной волны излучения 780 нм. Источник тока лазерного диода работал как в непрерывном режиме для настройки оптической схемы, так и в импульсном для проведения экспериментов. Длительность лазерного импульса составляла 5 нс. Излучение лазерного диода заводилось в оптический волоконный светоделитель 50/50. Одна половина излучения направлялась на измеритель мощности, вторая – на детекторы одиночных фотонов. Часть излучения, идущая на фотодетекторы, выводилась из волокна с помощью коллиматора и ослаблялась калиброванными нейтральными фильтрами до уровня мощности, при котором на лазерный импульс приходилось не более одного фотона. С по-

мощью ручного поляризационного контроллера, установленного на волоконный делитель, линейная поляризация выходного излучения выставлялась горизонтальной.

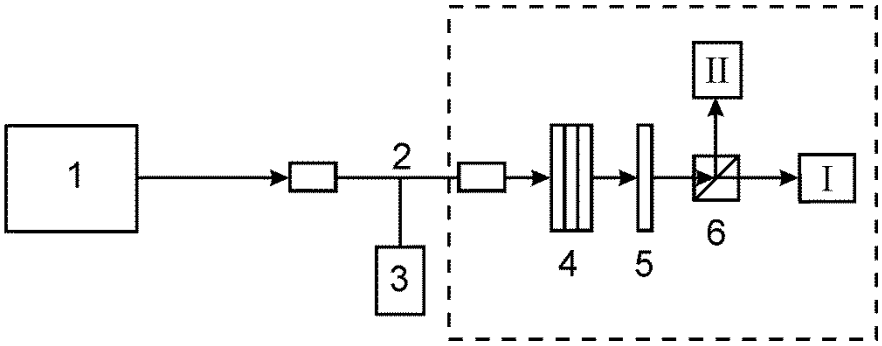

Рис. 1. Схема экспериментальной установки:
1 – лазерный диод; *2* – волоконный светоделитель 50/50; *3* – измеритель мощности;
4 – набор нейтральных светофильтров; *5* – полуволновая пластинка; *6* – призма Глана;
I, *II* – детекторы одиночных фотонов на основе кремниевых лавинных фотодиодов

Fig. 1. Scheme of the experimental setup:
1 – laser diode; *2* – fiber-optics beam splitter 50/50; *3* – power meter;
4 – a stack of neutral optical filters; *5* – half-wave plate; *6* – Glan prism;
I, *II* – single-photon detectors based on silicon avalanche photodiodes

Излучение затем попадало на полуволновую пластинку и призму Глана. При работе с фотодетектором I ось полуволновой пластинки выставлялась под углом 0° по отношению к падающему излучению, что не изменяло поляризацию падающего излучения; при работе с фотодетектором II – под углом 45°, что поворачивало поляризацию падающего излучения на 90°. При работе одновременно с двумя фотодетекторами ось пластинки выставлялась под углом 22,5°, что поворачивало поляризацию падающего излучения на 45°.

Регистрация одиночных фотонов производилась кремниевыми лавинными фотодиодами C30902S производства фирмы «EG&G Optoelectronics», работающими в гейгеровском режиме при температуре 273 К. Выходные импульсы фотодиодов усиливались и поступали на блок амплитудного дискриминирования и временного стробирования, в котором они преобразовывались в стандартные TTL-импульсы и направлялись на вход счетчика импульсов. Длительность строб-импульса составляла 20 нс.

Запуск лазерных импульсов и строб-импульсов тактовыми импульсами с частотой до 1 МГц, а также счет TTL-импульсов с блока стробирования осуществлялись быстродействующей системой на базе программируемой логической платы сбора данных NI 7811 R Series Multifunction RIO компании «National Instruments», встраиваемой в блок персонального компьютера. Система позволяла изменять задержку и совмещать лазерные и строб-импульсы с точностью 5 нс. Система управлялась программой, написанной в среде LabVIEW.

Для защиты от внешнего света часть установки находилась в непрозрачном кожухе, обозначенном на рис. 1 штриховой линией.

Результаты

Далее показаны экспериментальные и теоретические зависимости частоты срабатывания одного или двух фотодетекторов от среднего числа фотонов в лазерном импульсе. Мощность излучения, соответствующая разному среднему числу фотонов в импульсе, выставлялась регулировкой тока лазерного диода и контролировалась измерителем мощности *3* на рис. 1.

Перед проведением основных экспериментов были измерены зависимости частоты срабатывания каждого фотодетектора от частоты следования лазерных импульсов *f*. Данная зависимость должна быть линейной в соответствии с формулой

$$N = \overline{P}_{1\text{det}} \cdot f, \tag{13}$$

где N – частота срабатывания фотодетектора; $\overline{P}_{1\text{det}}$ – вероятность срабатывания фотодетектора при регистрации любого числа фотонов согласно формуле (6).

На рис. 2 приведена типичная экспериментальная зависимость частоты срабатывания фотодетектора I от частоты лазерных импульсов. Среднее число фотонов в лазерном импульсе μ было выставлено равным 0,6. Как видно из графика, при частотах срабатывания фотодетектора более 20 кГц зависимость частоты срабатывания от частоты лазерных импульсов перестает быть линейной, что может быть связано с насыщением фотодетектора. Также на рис. 2 показана аппроксимация экспериментальных данных при низких частотах срабатывания фотодетектора (менее 5 кГц), когда еще не возникает насыщения, и зависимость частоты срабатывания детектора N линейная в соответствии с формулой (13). Значение эффективности регистрации одиночных фотонов было получено из измеренного значения $\overline{P}_{1\text{det}}$ и составило 17 %. Коэффициент пропускания T здесь и везде, где теоретические расчеты сравниваются с экспериментальными данными, берется равным 1 (использовался короткий воздушный промежуток без потерь).

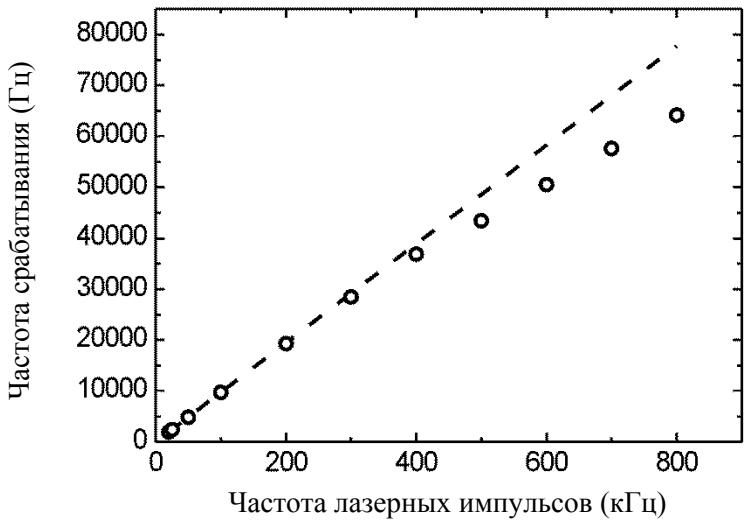

Рис. 2. Экспериментальная зависимость частоты срабатывания фотодетектора I от частоты лазерных импульсов (кружки). Штриховая линия построена по формуле (13)

Fig. 2. Experimental dependence of the frequency of clicks of photodetector I on the frequency of laser pulses (circles). The dashed line is drawn according to equation (13)

Наблюдаемое на рис. 2 насыщение при таких относительно небольших частотах срабатывания фотодетектора оказалось неожиданным, потому что так называемое «мертвое время» (время восстановления после образования лавины) лавинного фотодиода составляет 300 нс, а полоса пропускания усилителя выходных импульсов лавинного фотодиода – 0,5 ГГц. К тому же оказалось, что коэффициент насыщения для разных частот срабатывания не воспроизводится в точности после выключения-включения установки даже при тех же точно выстав-

ленных значениях напряжения питания и температуры лавинного фотодиода. Возможной причиной наблюдаемого насыщения является уменьшение амплитуды выходного импульса фотодетектора при больших частотах срабатывания, поэтому количество импульсов, проходящих через амплитудный дискриминатор, уменьшается.

На рис. 3 представлены экспериментальная и теоретическая зависимости частоты срабатывания фотодетектора I от среднего числа фотонов в импульсе. Частота лазерных импульсов составляла 500 кГц, эффективность регистрации 16,7 %. Для того чтобы избежать насыщения при больших частотах срабатывания фотодетектора, измерения для каждого значения среднего числа фотонов в импульсе проводились при уменьшенных частотах лазерных импульсов, при которых частота срабатывания не превышала 5 кГц. Потом измеренное значение частоты срабатывания умножалось на коэффициент деления частоты лазерных импульсов. Применимость данного метода подтверждается хорошим согласием экспериментальных данных (кружки) и теоретических расчетов (сплошная линия), сделанных по формуле (13). Для каждого значения среднего числа фотонов набиралась статистика из пятикратного измерения частоты срабатывания. Время измерения составляло 5 с. Затем из полученных данных вычислялось среднее значение $N_{\text{ср}}$, представленное на рис. 3. Кроме того, из $N_{\text{ср}}$ вычиталось среднее значение частоты темновых импульсов лавинного фотодиода, которое составляло 65 Гц. Среднеквадратичное отклонение измеренных значений от среднего не превышало теоретического предела, равного $(N_{\text{ср}})^{1/2}$. Поскольку это значение достаточно мало, то погрешность экспериментальных данных на рисунках не приводится.

На рис. 3 для сравнения представлены также две теоретические кривые, одна из которых (штриховая линия) показывает количество зарегистрированных фотонов $\mu \cdot \eta \cdot f$, которое было бы измерено в случае способности фотодетектора различать число зарегистрированных фотонов при той же эффективности регистрации.

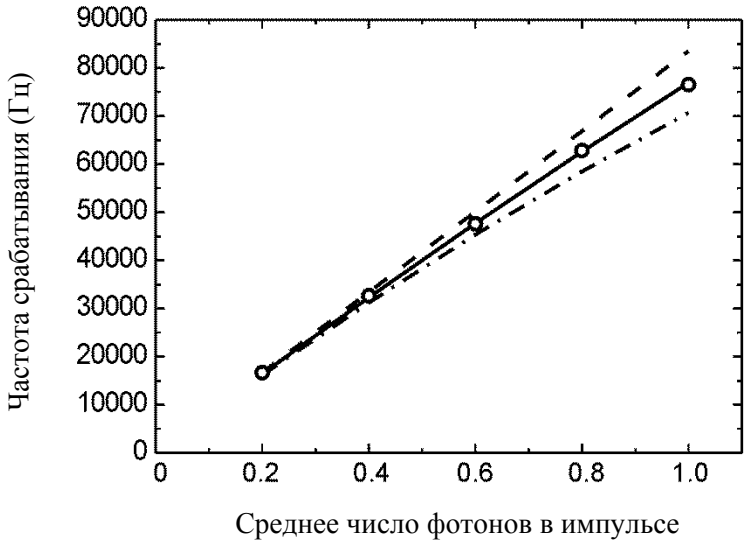

Рис. 3. Экспериментальная (кружки) и теоретическая (сплошная линия) зависимости частоты срабатываний фотодетектора I от среднего числа фотонов в импульсе. Штриховая и штрихпунктирная линии построены для фотодетектора, различающего число зарегистрированных фотонов (см. текст)

Fig. 3. Experimental (circles) and theoretical (solid curve) dependences of the frequency of clicks of photodetector I on the mean photon number per laser pulse. The dashed and dash-dotted lines are drawn for a photodetector that resolves the number of detected photons (see text)

Вторая кривая (штрихпунктирная линия) построена по формуле $P_{\text{det}}(1)\cdot f$, где $P_{\text{det}}(1)$ – вероятность регистрации одного фотона (4) при той же эффективности регистрации.

Аналогичная экспериментальная зависимость была получена и для фотодетектора II.

Далее показаны результаты экспериментов, в которых участвовали оба фотодетектора. Полуволновая пластинка выставлялась под углом 22,5° таким образом, чтобы на фотодетекторы попадало излучение одинаковой мощности. Управляющая программа подсчитывала отдельно частоту событий, в которых срабатывал только один фотодетектор и в которых срабатывали одновременно оба фотодетектора за один лазерный импульс. Эффективность регистрации фотодетекторов выставлялась одинаковой по равенству частот срабатывания каждого из них. Как и в предыдущих экспериментах с одним фотодетектором, для того чтобы избежать насыщения при больших частотах срабатывания фотодетекторов, измерения для каждого значения среднего числа фотонов в импульсе проводились при уменьшенных частотах лазерных импульсов.

На рис. 4 представлены экспериментальная и теоретическая зависимости частоты срабатывания только одного из двух фотодетекторов от среднего числа фотонов в импульсе. Видно, что экспериментальные данные (кружки) и расчет (сплошная линия), сделанный по формуле $\overline{P}_{2\text{det}}(1)\cdot f$, где $\overline{P}_{2\text{det}}(1)$ – вероятность срабатывания одного из двух детекторов (7), хорошо совпадают.

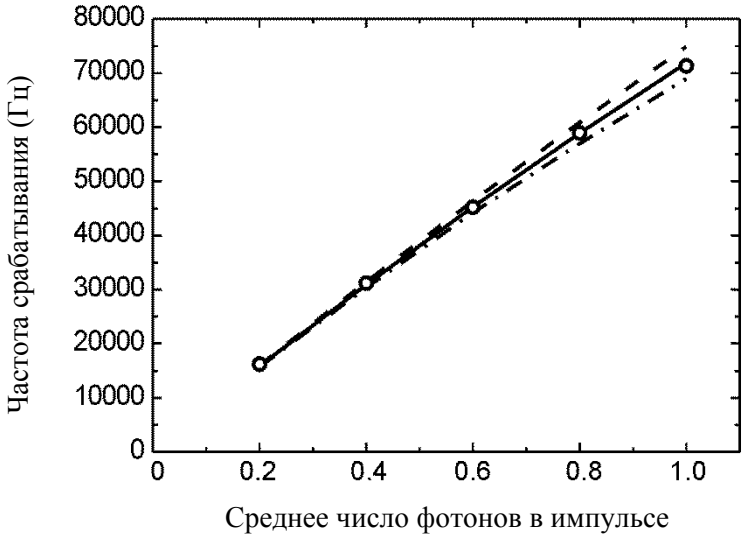

Рис. 4. Экспериментальная (кружки) и теоретическая (сплошная линия) зависимости частоты срабатывания только одного из двух фотодетекторов от среднего числа фотонов в импульсе. Штриховая линия построена по формуле (13), штрихпунктирная – для фотодетектора, различающего число зарегистрированных фотонов (см. текст)

Fig. 4. Experimental (circles) and theoretical (solid curve) dependences of the frequency of clicks of only one of two photodetectors on the mean photon number per laser pulse. The dashed line is drawn according to equation (13), and the dash-dotted line is drawn for a photodetector that resolves the number of detected photons (see text)

Частота лазерных импульсов f составляет 500 кГц, эффективность регистрации обоих фотодетекторов 16,2 %. Штриховой линией для сравнения показана теоретическая зависимость частоты срабатывания одиночного фотодетектора без разрешения числа регистрируемых фотонов, построенная по формуле (13), при той же эффективности регистрации. Штрихпунк-

тирная линия построена по формуле $P_{\text{det}}(1)\cdot f$, где $P_{\text{det}}(1)$ – вероятность регистрации одного фотона фотодетектором, различающим число зарегистрированных фотонов (4), при той же эффективности регистрации.

На рис. 5 представлены экспериментальная и теоретическая зависимости частоты одновременного срабатывания двух фотодетекторов от среднего числа фотонов в импульсе. Также видно, что экспериментальные данные (кружки) и расчет (сплошная линия), сделанный по формуле $\overline{P}_{2\text{det}}(2)\cdot f$, где $\overline{P}_{2\text{det}}(2)$ – вероятность одновременного срабатывания двух детекторов (8), хорошо совпадают. Частота лазерных импульсов f составляет 500 кГц, эффективность регистрации обоих фотодетекторов 16,2 %. Штриховая линия отображает зависимость частоты регистрации двух фотонов фотодетектором, различающим число зарегистрированных фотонов, построенную по формуле $P_{\text{det}}(2)\cdot f$, где $P_{\text{det}}(2)$ – вероятность регистрации двух фотонов (5) при той же эффективности регистрации.

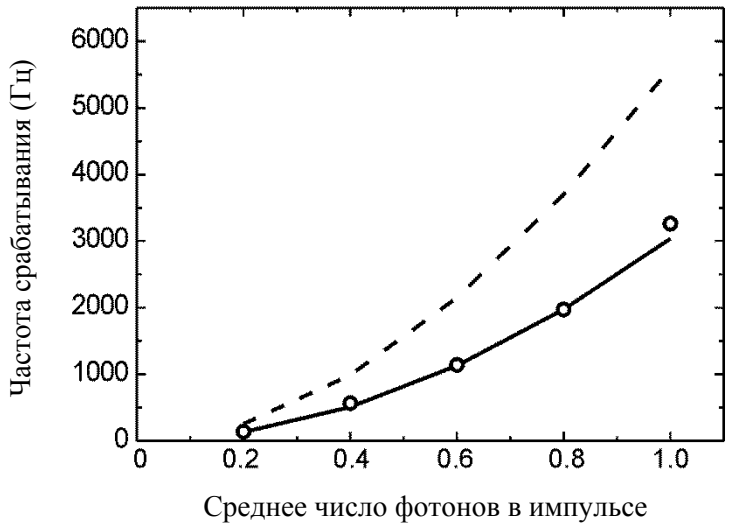

Рис. 5. Экспериментальная (кружки) и теоретическая (сплошная линия) зависимости частоты одновременного срабатывания двух фотодетекторов от среднего числа фотонов в импульсе. Штриховая линия построена для фотодетектора, различающего число зарегистрированных фотонов (см. текст)

Fig. 5. Experimental (circles) and theoretical (solid curve) dependences of the frequency of simultaneous clicks of both photodetectors on the mean photon number per laser pulse. The dashed line is drawn for a photodetector that resolves the number of detected photons (see text)

Обсуждение результатов

В наших экспериментах среднее число фотонов в лазерном импульсе выставлялось косвенно по средней мощности импульсного излучения, измеренной до ослабителя быстрым калиброванным фотоприемником *3* (см. рис. 1). Кроме быстрого фотоприемника, для измерения среднего числа фотонов на импульс может быть использован и обычный детектор одиночных фотонов с известной эффективностью регистрации. Тогда среднее число фотонов в импульсе может быть выставлено напрямую по частоте срабатывания фотодетектора в соответствии с формулой (13).

При атаке с делением числа фотонов для квантового канала с коэффициентом пропускания $T > T_0$ из формулы (2) максимальное количество информации, которое Ева может перехватить без внесения ошибки в квантовый ключ, определяется отношением числа многофо-

тонных импульсов, от которых Ева может отделить по одному фотону, к общему числу импульсов с фотонами. Поэтому чем больше среднее число фотонов в импульсе, тем больше информации получает Ева. Следовательно, Алиса и Боб должны выбрать среднее число фотонов в импульсе таким образом, чтобы оно было наименьшим и в то же время с учетом коэффициента пропускания канала обеспечивало достаточную скорость генерации квантового ключа.

После того как Ева применит атаку с делением числа фотонов непосредственно после Алисы, до Боба дойдет меньшее количество как однофотонных импульсов, так и двухфотонных. Уменьшение общего количества импульсов с фотонами будет сигнализировать Бобу либо об ухудшении пропускания канала, либо об атаке с делением числа фотонов, и может быть обнаружено с помощью даже одного фотодетектора, не различающего число зарегистрированных фотонов. Однако для того чтобы различить случаи ухудшения пропускания канала и атаки с делением числа фотонов, потребуется сравнить количество «пустых», однофотонных и двухфотонных импульсов с распределением Пуассона (3). Для этого потребуется либо фотодетектор, различающий число зарегистрированных фотонов, либо как минимум два обычных фотодетектора.

Как было показано экспериментально и теоретически в предыдущем разделе, вероятность зарегистрировать двухфотонный импульс по одновременному срабатыванию двух обычных фотодетекторов меньше вероятности зарегистрировать двухфотонный импульс фотодетектором, обладающим разрешением по числу зарегистрированных фотонов, в два раза (см. рис. 5). При обнаружении атаки с делением числа фотонов данное уменьшение вероятности не играет существенной роли, так как кратность уменьшения регистрации одно- и двухфотонных импульсов с атакой и без атаки не меняется.

При использовании протокола BB84 можно даже не использовать отдельную контрольную систему из двух фотодетекторов, поскольку такая же система лежит в основе приемного узла. Для этого можно просто измерять вероятности срабатывания только одного из фотодетекторов и одновременного срабатывания двух фотодетекторов и сравнивать их с расчетами по формулам (7) и (8).

Кроме того, как обсуждается в статье [11], Ева может отделять по одному фотону, начиная не с двухфотонных, а с трехфотонных импульсов. Тогда количество информации, которое она получит, уменьшится в несколько раз, но зато такую атаку будет труднее отследить. Это произойдет потому, что теперь на входе Боба сильно изменится число трехфотонных импульсов, в то время как число двухфотонных импульсов радикально не поменяется. В этом случае контрольный фотодетектор с разрешением по числу фотонов будет обладать несомненным преимуществом перед системой из двух обычных фотодетекторов. Выходом из данной ситуации может стать добавление в контрольную систему из двух фотодетекторов третьего фотодетектора.

Заключение

Проведенные нами экспериментальные и теоретические исследования показали, что система из двух обычных детекторов одиночных фотонов в некоторых случаях может заменить фотодетектор, способный различать число зарегистрированных фотонов, для обнаружения классической атаки с делением числа фотонов по изменению распределения числа фотонов в импульсе в квантовом канале с коэффициентом пропускания $T > T_0$ из формулы (2). Вероятность обнаружения двухфотонного импульса для системы из двух обычных фотодетекторов и фотодетектора, различающего число зарегистрированных фотонов, отличается всего в два раза. Данный метод удобен тем, что не требует внесения дополнительных элементов в приемный узел, и может быть реализован программными методами, сравнивающими вероятности срабатывания только одного из детекторов и одновременного срабатывания двух детекторов с расчетами по формулам (7) и (8). Ограничением данного метода может

стать случай, когда Ева отделяет по одному фотону от импульсов, начиная не с двухфотонных, а с трехфотонных импульсов.

Список литературы / References

1. **Gisin N., Ribordy G., Tittel W., Zbinden H.** Quantum cryptography. *Rev. of Mod. Phys*., 2002, vol. 74, p. 145–195.
2. **Wooters W. K., Zurek W. H.** A Single Quantum Cannot Be Cloned. *Nature*, 1982, vol. 299, p. 802–803.
3. **Bennet C. H., Brassard G.** Quantum cryptography: public key distribution and coin tossing. In: Proc. of IEEE Inter. Conf. on Comput. Sys. and Sign. Proces. Bangalore, India, 1984, p. 175–179.
4. **Bennet C. H., Bessette F., Brassard G., Salvail L.** Experimental quantum cryptography. *J. Cryptology*, 1992, vol. 5, p. 3–28.
5. **Dusek M., Haderka O., Hendrych M.** Generalized beam-splitting attack in quantum cryptography with dim coherent states. *Opt. Commun*., 1999, vol. 169, p. 103–108.
6. **Liang L., Lin G. W., Hao Y. M., Niu Y. P., Gong S. Q.** Quantum non-demolition measurement of small photon numbers using stored light. *Phys. Rev. A*, 2014, vol. 90, p. 055801.
7. **Scarani V., Acin A., Ribordy G., Gisin N.** Quantum Cryptography Protocols Robust against Photon Number Splitting Attacks for Weak Laser Pulse Implementations. *Phys. Rev. Lett*., 2004, vol. 92, p. 057901.
8. **Acin A., Gisin N., Scarani V.** Coherent-pulse implementations of quantum cryptography protocols resistant to photon-number-splitting attacks. *Phys. Rev. A*, 2004, vol. 69, p. 012309.
9. **Stucki D., Brunner N., Gisin N., Scarani V., Zbinden H.** Fast and simple one-way quantum key distribution. *Appl. Phys. Lett*., 2005, vol. 87, p. 194108.
10. **Hwang Won-Young.** Quantum Key Distribution with High Loss: Toward Global Secure Communication. *Phys. Rev. Lett*., 2003, vol. 91, p. 057901.
11. **Gaidash A., Egorov V., Gleim A.** Revealing beam-splitting attack in a quantum cryptography system with a photon-numberresolving detector. *Journal of the Optical Society of America B*, 2016, vol. 33, p. 1451–1455.
12. **Lita A. E., Miller A. J., Sae Woo Nam.** Counting near-infrared single-photons with 95 % efficiency. *Optics Express*, 2008, vol. 16, p. 3032–3040.
13. **Kalashnikov D. A., Si Hui Tan, Chekhova M. V., Krivitsky L. A.** Accessing photon bunching with a photon number resolving multi-pixel detector. *Optics Express*, 2011, vol. 19, p. 9352–9363.
14. **Achilles D., Silberhorn C., Sliwa C., Banaszek K., Walmsley I. A.** Fiber-assisted detection with photon number resolution. *Optics Letters*, 2003, vol. 28, p. 2387–2389.
15. **Calsamiglia J., Barnett S. M., Lutkenhaus N.** Conditional beam-splitting attack on quantum key distribution. *Phys. Rev. A*, 2001, vol. 65, p. 012312.
16. **Третьяков Д. Б., Коляко А. В., Плешков А. С., Энтин В. М., Рябцев И. И., Неизвестный И. Г.** Генерация квантового ключа в однофотонных системах связи // Автометрия. 2016. Т. 52. С. 44–54.

    Tretyakov D. B., Kolyako A. V., Pleshkov A. S., Entin V. M., Ryabtsev I. I., Neizvestny I. G. Quantum Key Distribution in Single-Photon Communication System. *Optoelectronics, Instrumentation and Data Processing*, 2016, vol. 52, no. 5, p. 453–461. (in Russ.)
17. **Рябцев И. И., Третьяков Д. Б., Коляко А. В., Плешков А. С., Энтин В. М., Неизвестный И. Г., Латышев А. В., Асеев А. Л.** Элементная база квантовой информатики II:

Квантовые коммуникации с одиночными фотонами // Микроэлектроника. 2017. Т. 46. С. 131–141.

Ryabtsev I. I., Tretyakov D. B., Kolyako A. V., Pleshkov A. S., Entin V. M., Neizvestny I. G., Latyshev A. V., Aseev A. L. Element Base of Quantum Informatics II: Quantum Communications with Single Photons. *Russian Microelectronics*, 2017, vol. 46, no. 2, p. 121–130. (in Russ.)

Материал поступил в редколлегию
Received
08.11.2018

Сведения об авторах / Information about the Authors

Третьяков Денис Борисович, кандидат физико-математических наук, старший научный сотрудник, Институт физики полупроводников им. А. В. Ржанова СО РАН (пр. Академика Лаврентьева, 13, Новосибирск, 630090, Россия); Новосибирский государственный университет (ул. Пирогова, 2, Новосибирск, 630090, Россия)

Denis B. Tretyakov, Candidate of Science (Physics and Mathematics), Senior Researcher, A. V. Rzhanov Institute of Semiconductor Physics SB RAS (13 Academician Lavrentiev Ave., Novosibirsk, 630090, Russian Federation); Novosibirsk State University (2 Pirogov Str., Novosibirsk, 630090, Russian Federation)
dtret@isp.nsc.ru

Коляко Александр Владимирович, Институт физики полупроводников им. А. В. Ржанова СО РАН (пр. Академика Лаврентьева, 13, Новосибирск, 630090, Россия); Новосибирский государственный университет (ул. Пирогова, 2, Новосибирск, 630090, Россия); Институт лазерной физики СО РАН (пр. Академика Лаврентьева, 15Б, Новосибирск, 630090, Россия)

Aleksandr V. Kolyako, A. V. Rzhanov Institute of Semiconductor Physics SB RAS (13 Academician Lavrentiev Ave., Novosibirsk, 630090, Russian Federation); Novosibirsk State University (2 Pirogov Str., Novosibirsk, 630090, Russian Federation); Institute of Laser Physics SB RAS (15B Academician Lavrentiev Ave., Novosibirsk, 630090, Russian Federation)

kolyako@isp.nsc.ru

Плешков Александр Сергеевич, Институт физики полупроводников им. А. В. Ржанова СО РАН (пр. Академика Лаврентьева, 13, Новосибирск, 630090, Россия); Новосибирский государственный университет (ул. Пирогова, 2, Новосибирск, 630090, Россия); Институт лазерной физики СО РАН (пр. Академика Лаврентьева, 15Б, Новосибирск, 630090, Россия)

Aleksandr S. Pleshkov, A. V. Rzhanov Institute of Semiconductor Physics SB RAS (13 Academician Lavrentiev Ave., Novosibirsk, 630090, Russian Federation); Novosibirsk State University (2 Pirogov Str., Novosibirsk, 630090, Russian Federation); Institute of Laser Physics SB RAS (15B Academician Lavrentiev Ave., Novosibirsk, 630090, Russian Federation)

pleshkov@isp.nsc.ru

Энтин Василий Матвеевич, кандидат физико-математических наук, Институт физики полупроводников им. А. В. Ржанова СО РАН (пр. Академика Лаврентьева, 13, Новосибирск, 630090, Россия); Новосибирский государственный университет (ул. Пирогова, 2, Новосибирск, 630090, Россия)

Vasiliy M. Entin, Candidate of Science (Physics and Mathematics), A. V. Rzhanov Institute of Semiconductor Physics SB RAS (13 Academician Lavrentiev Ave., Novosibirsk, 630090, Russian Federation); Novosibirsk State University (2 Pirogov Str., Novosibirsk, 630090, Russian Federation)

ventin@isp.nsc.ru

Рябцев Игорь Ильич, доктор физико-математических наук, член-корреспондент РАН, Институт физики полупроводников им. А. В. Ржанова СО РАН (пр. Академика Лаврентьева, 13, Новосибирск, 630090, Россия); Новосибирский государственный университет (ул. Пирогова, 2, Новосибирск, 630090, Россия)

Igor I. Ryabtsev, Doctor of Science (Physics and Mathematics), Corresponding Member of RAS, A. V. Rzhanov Institute of Semiconductor Physics SB RAS (13 Academician Lavrentiev Ave., Novosibirsk, 630090, Russian Federation); Novosibirsk State University (2 Pirogov Str., Novosibirsk, 630090, Russian Federation)

ryabtsev@isp.nsc.ru

Неизвестный Игорь Георгиевич, доктор физико-математических наук, член-корреспондент РАН, Институт физики полупроводников им. А. В. Ржанова СО РАН (пр. Академика Лаврентьева, 13, Новосибирск, 630090, Россия); Новосибирский государственный технический университет (пр. К. Маркса, 20, Новосибирск, 630073, Россия)

Igor G. Neizvestny, Doctor of Science (Physics and Mathematics), Corresponding Member of RAS, A. V. Rzhanov Institute of Semiconductor Physics SB RAS (13 Academician Lavrentiev Ave., Novosibirsk, 630090, Russian Federation); Novosibirsk State Technical University (20 K. Marx Ave., Novosibirsk, 630090, Russian Federation)

neizv@isp.nsc.ru