Уменьшение уровня засветки оптоволокна в однопроходной системе квантовой криптографии

К. А. Балыгин,[1,2,а] В. И. Зайцев,[1,2] А. И. Климов,[1,2,б] А. Н. Климов,[2] С. П. Кулик,[2,3] С. Н. Молотков[2]

[1] *Национальный исследовательский центр "Курчатовский институт". Россия, 123182, Москва, пл. Академика Курчатова, д. 1.*
[2] *Центр квантовых технологий МГУ имени М. В. Ломоносова;*
[3] *Московский государственный университет имени М. В. Ломоносова, физический факультет. Россия, 119991, Москва, Ленинские горы, д. 1, стр. 2.*

Поступила в редакцию 11.07.2019, после доработки 25.11.2019, принята к публикации 26.11.2019.

Предложен способ запуска лазерного диода синхронизации в однопроходной системе квантовой криптографии, позволяющий уменьшить на ∼2 порядка уровень «засветки» в оптоволокне от рассеивания лазерного излучения и увеличить протяженность одноволоконной линии связи при выработке секретного ключа до 95 км.

Ключевые слова: системы квантовой криптографии, однофотонный детектор, лазер.
УДК: 53.088.22. PACS: 42.50.Ex.

ВВЕДЕНИЕ

Практически все современные системы передачи и обработки конфиденциальной информации используют криптографические средства защиты [1, 2]. Однопроходные системы квантовой криптографии позволяют достичь больших скоростей и дальностей распределения ключей по сравнению с двухпроходными системами. Однопроходные системы требуют наличия двух каналов связи: один — для квантового канала, второй — для канала синхронизации. Уровень сигнала в квантовом канале на выходе передающей аппаратуры составляет, в зависимости от протокола, примерно 0.1–1 фотон на импульс. Для стабильной работы системы синхронизации необходимый уровень сигнала на входе приемной аппаратуры должен составлять десятки тысяч фотонов. Для исключения перекрестных помех между каналами проще всего использовать два раздельных волокна. Однако это не всегда возможно на практике, учитывая конкретные технические и экономические обстоятельства.

Поскольку в квантовой криптографии принципиально невозможно отличить ошибки, связанные с несовершенством используемой аппаратуры, в том числе с перекрестными помехами, их необходимо снижать. Для снижения перекрестных помех необходимо применять разделение квантового канала и канала синхронизации по длинам волн (используя WDM-фильтр) и по времени прихода сигнала на однофотонный детектор

В работе предложен способ запуска лазера синхронизации, позволяющий обеспечить уровень перекрестных помех на уровне темновых отсчетов детектора при использовании обычных телекоммуникационных CWDM (Coarse WDM)-фильтров (светоделителей). Первыми WDM-системами, нашедшими практическое применение, стали двухволновые фильтры, объединившие две основные несущие длины волн 1310 нм и 1550 нм из 2-го и 3-го окон прозрачности в одном одномодовом волокне [3].

Уровни сигналов в квантовом канале, через который передаются квантовые состояния, ослабленные до квазиоднофотонного уровня и в канале синхронизации, через который передаются интенсивные импульсы синхронизации, отличаются на несколько порядков. Это обстоятельство приводит к дополнительным «засветкам» в квантовом канале. Для устранения таких паразитных «засветок» используются WDM-светоделители, которые позволяют снизить уровень паразитного сигнала (уровень помех) от канала синхронизации на ∼ 40 дБ. В системах квантовой криптографии даже при нулевой длине линии сигнал в квантовом канале на 40–50 дБ ниже сигнала в канале синхронизации, а с увеличением длины линии это соотношение только увеличивается. Это связано с тем, что уровень сигнала в квантовом канале на выходе передающей аппаратуры должен иметь квазиоднофотонный уровень — это параметр протокола, интенсивность сигнала в канале синхронизации с ростом длины линии должна возрастать. Помимо разделения по длине волны, необходимо также разделить сигналы по времени. Внутренние ошибки также можно разделить на ошибки от электронной аппаратуры, например «темновые» шумы лавинных однофотонных детекторов и ошибки от нестабильности оптической части системы.

1. ПОСТАНОВКА ЗАДАЧИ

Целью данной работы является уменьшение уровня паразитных засветок квантового канала от сигналов синхронизации до уровня, сравнимого с уровнем собственных шумов однофотонного детектора.

На рис. 1, *а* представлена схема однопроходной системы квантовой криптографии с фазовым кодированием: МЛ1 — лазерный диод с длиной волны излучения $\lambda = 1.5$ мкм, МЛ2 — источник классических импульсов синхронизации — лазерный диод с длиной волны излучения $\lambda = 1.3$ мкм. В случае строго однофотонного состояния импульсы кодируются в относительную разность фаз двух «половинок» единого квантового состояния, локализованных в разных временных окнах. На передающей стороне данная пара состояний получается из одного состояния при помощи волоконного интерферометра Маха—Цандера с разной длиной плеч (ИМЦ1) (рис. 1, *а*). Относительная разность фаз изменяется

[а] E-mail: kirill.balygin@gmail.com
[б] E-mail: nrc.klimov@gmail.com

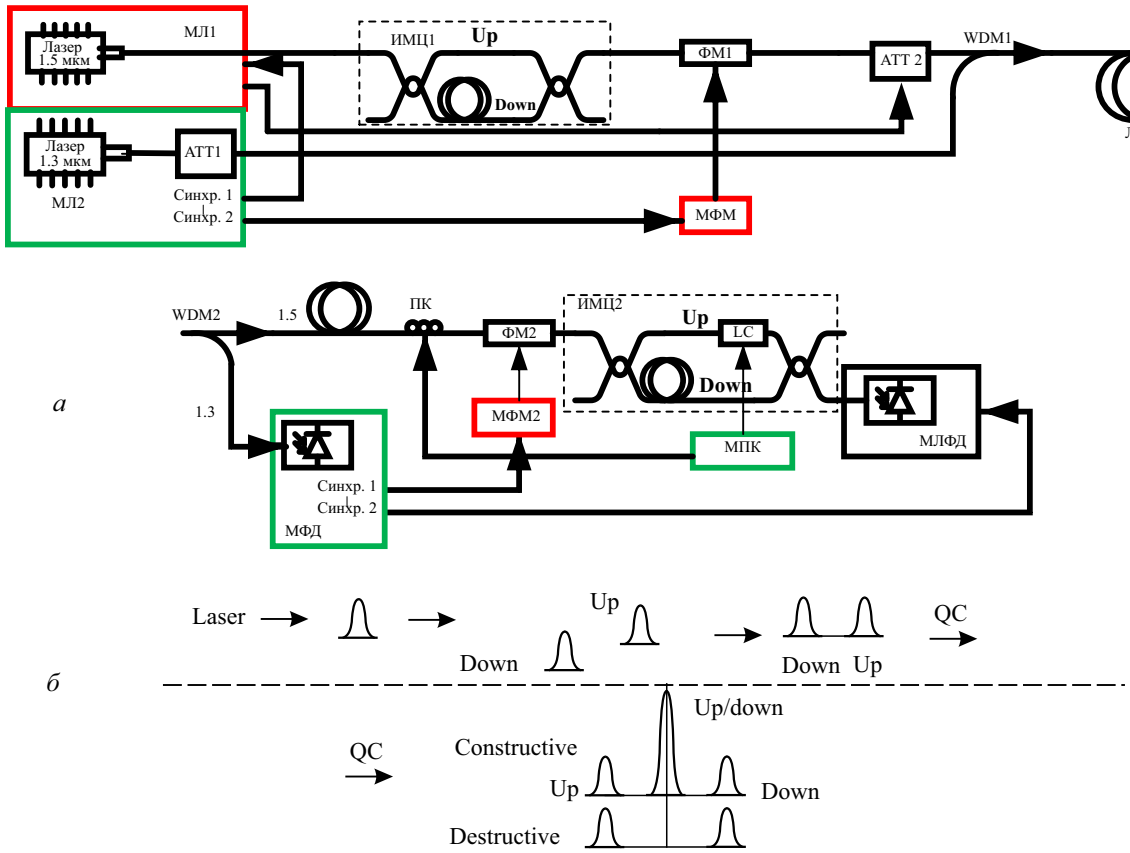

Рис. 1. Волоконно-оптическая схема однопроходной системы квантовой криптографии. МЛ1, МЛ2 — лазеры — источники излучения; МЛФД — однофотонный детектор; МФД — pin-диод; WDM1, WDM2 — первый и второй волоконные светоделители; ИМЦ1, ИМЦ2 — волоконные интерферометры Маха—Цандера; ФМ1, ФМ2 — фазовые модуляторы; ПК — контроль поляризации; Линия — оптоволоконная линия связи; ЛЗ — оптоволоконная линия задержки; АТТ1, АТТ2 — аттенюаторы; МФМ1, МФМ2 — блоки управления фазовыми модуляторами; LC — пьезоэлемент

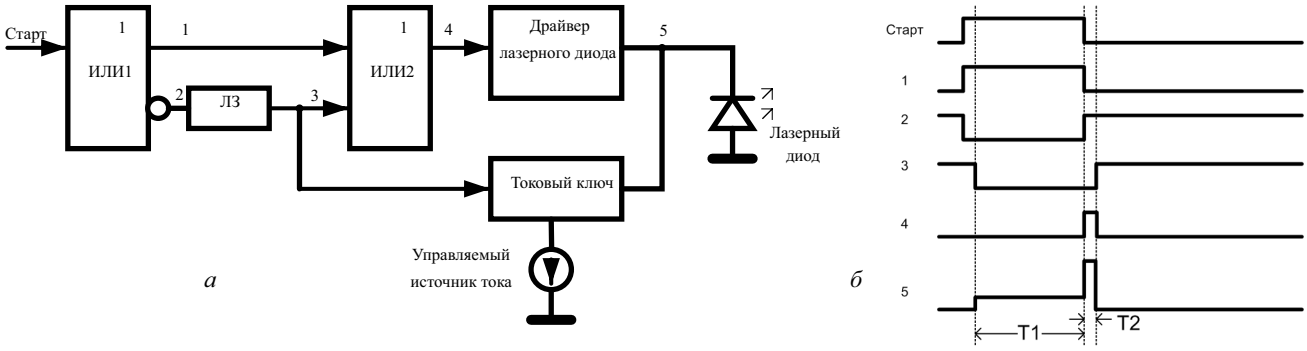

Рис. 2. Функциональная схема формирователя импульса запуска лазерного диода (*а*) и временная диаграмма его работы (*б*)

во время прохождения через фазовый модулятор, который активируется в нужном временном окне. На приемной стороне так же добавляется относительная разность фаз аналогичным фазовым модулятором. С помощью пьезоэлемента LC, включенного в одно из плеч интерферометра Маха—Цандера, производится при необходимости его точная подстройка. Состояния, разделенные во времени, на приемной стороне, «собираются» вместе при помощи точно такого же интерферометра (ИМЦ2) [4]. Это дает либо конструктивную, либо деструктивную интерференцию в центральном временном окне (рис. 1, *б*).

2. ФОРМИРОВАТЕЛЬ СИГНАЛА ЗАПУСКА ЛАЗЕРА

Для передачи синхросигналов в линию используется лазер с распределенной обратной связью DFB (distributed feedback) — инжекционный полупроводниковый лазер, в нашем случае, это полупроводниковый лазер DFB Laser Module 1310 nm 14 BF фирмы Nolatech [5]. В телекоммуникационных системах на передающей стороне через лазер пропускается непрерывный ток, который модулируется передаваемым сигналом. Это позволяет держать лазерный диод в открытом состоянии и обеспечивать высокую скорость модуляции. В квантовых криптографических системах, использующих один оптоволоконный

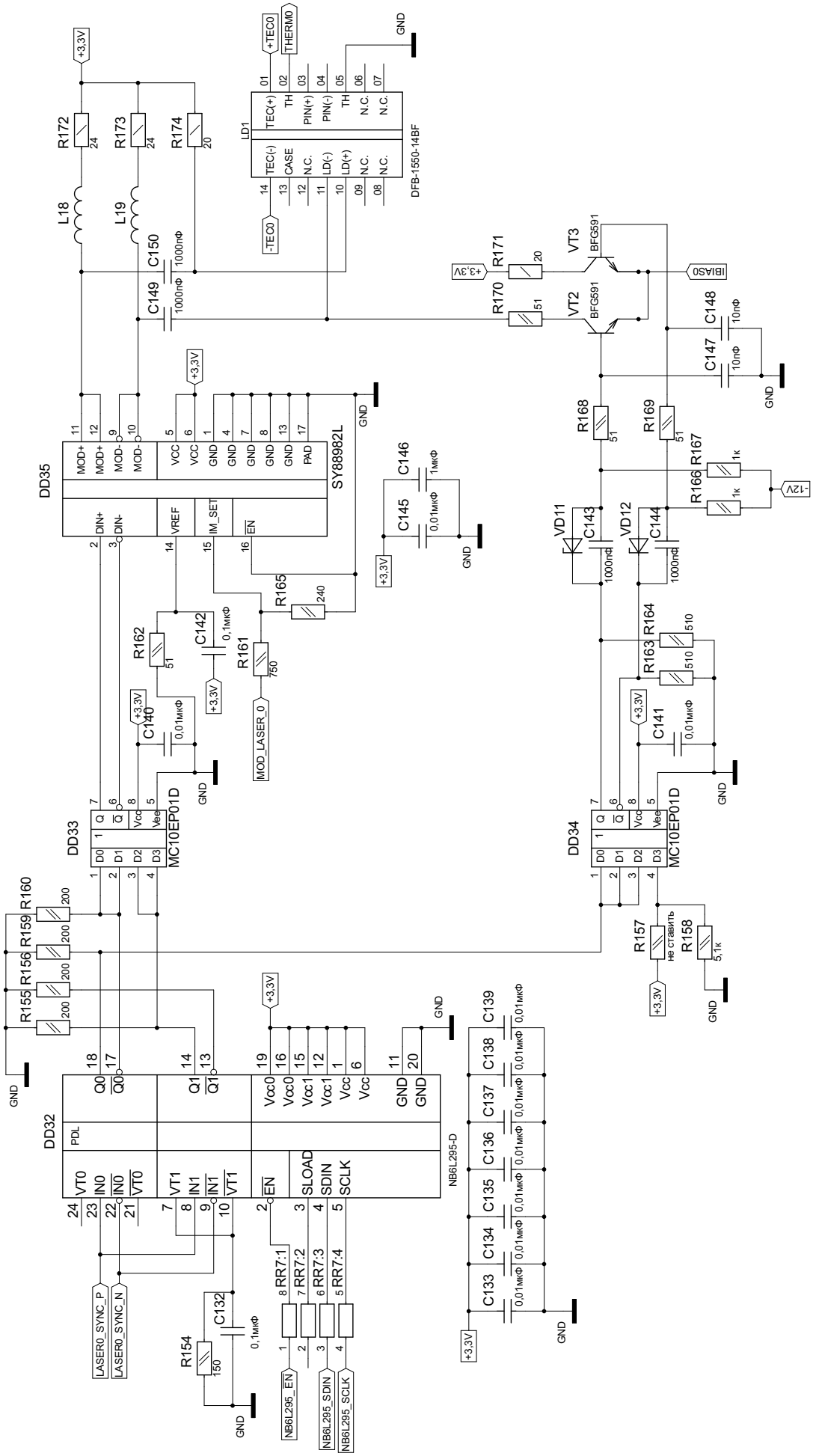

Рис. 3. Принципиальная схема формирователя импульса запуска лазера

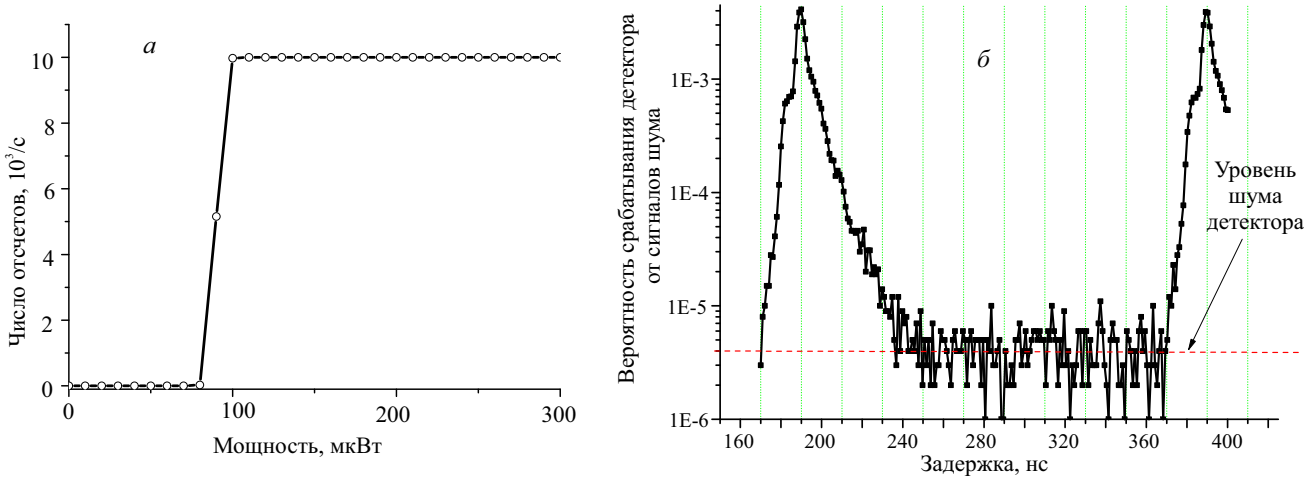

Рис. 4. а — Пороговая характеристика детектора синхронизации; *б* — вероятность срабатывания однофотонного детектора от задержки относительно импульсов синхронизации, уровень «шума» детектора равен 4×10^{-6} 1/с

канал, такой режим работы лазера синхронизации недопустим из-за наличия перекрестных помех на квантовый канал. С увеличением длины оптоволоконной линии связи мощность излучения лазера синхронизации приходится увеличивать. Чрезмерная интенсивность лазера синхронизации приводит к увеличению рассеяния фотонов в квантовом канале и возрастанию ошибки QBER (Quantum Bit Error Rate) при формировании секретного ключа [6].

На рис. 2, *а* представлена функциональная схема формирователя сигнала запуска лазера синхронизации. На вход «старт» формирователя поступают импульсы длительностью $T_1 \sim 30$ нс с выхода элемента ИЛИ1 положительный сигнал передается на первый вход элемента ИЛИ2, а отрицательный сигнал через элемент задержки, величиной T_2, на второй вход элемента ИЛИ2 и на токовый ключ (рис. 2, *а, б*). Элемент ИЛИ2 выполняет функцию дифференцирующего звена, на выходе которого формируется сигнал запуска лазера, длительностью $T_2 = 2{-}3$ нс, поступающий на вход драйвера лазерного диода. В результате суммирования двух импульсов схемы токового ключа и драйвера на вход лазерного диода поступает короткий импульс запуска лазера ($T_2 = 2{-}3$ нс), расположенный в конце импульса «полочки» $T_1 = 30$ нс. На рис. 3 представлена принципиальная схема формирователя, выполненная на быстродействующих 2-канальных программируемых элементах задержки (NB6L295-D) с дифференциальным LVPECL выходом, позволяющих устанавливать величину задержки в диапазоне 0–6 нс, с дискретностью 11 пс, а также драйвер запуска телекоммуникационного DFB-лазера (SY88982L), обеспечивающего скорость передачи данных до 2.7 Гбит/с. В качестве токового ключа используются широкополосные 7 ГГц *n-p-n*-транзисторы с током коллектора до 200 мА (BFG-591).

3. ЭКСПЕРИМЕНТАЛЬНЫЕ РЕЗУЛЬТАТЫ

Проведены измерения уровней «засветки» однофотонного детектора, вызываемой сигналами синхронизации на длине волны $\lambda = 1310$ нм. Мощность сигнала синхронизации выбиралась такой, чтобы обеспечить надежное срабатывание детектора при выборе соответствующей длины линии связи.

На рис. 4, *а* представлена пороговая характеристика детектора синхронизации при использовании оптоволоконной линии связи SMF-28 длиной 25 км, при этом мощность сигнала лазера не превышала $W = 30$ мкВт в импульсе длительностью $T = 3$ нс. При увеличении длины линии связи из-за затухания излучения в оптоволокне приходится увеличивать мощность излучения лазера синхронизации и при $L = 95$ км мощность излучения лазера в импульсе составила $W = 4.6$ мВт.

Проведены измерения уровней засветки однофотонного детектора на разных длинах линии связи (5, 25, 50, 85, 95 км). Результаты измерений представлены на рис. 5. Верхняя кривая получена при «засветке» однофотонного детектора импульсами лазера синхронизации, работающего в режиме пропускания непрерывного тока, который модулируется передаваемым сигналом (режим CW). Уровень «засветки» существенно (~ на 2 порядка) превышает уровень собственных шумов однофотонного детектора на всех используемых в нашем случае длинах линии связи. Нижняя кривая получена при запуске лазера синхронизации в режиме так называемой «полочки». Короткий импульс запуска лазера ($T_2 = 2{-}3$ нс) формируется в конце импульса длительностью $T_1 = 20{-}30$ нс с помощью специальной схемы формирователя (рис. 2, *а*). Измерения по опре-

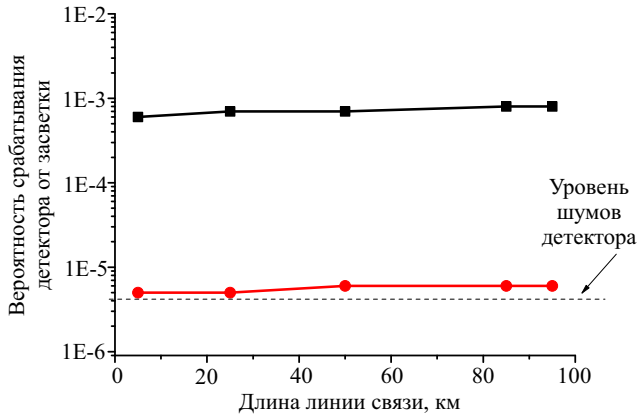

Рис. 5. Вероятности срабатывания однофотонного детектора от «засветки», связанной с рассеиванием излучения от лазера синхронизации

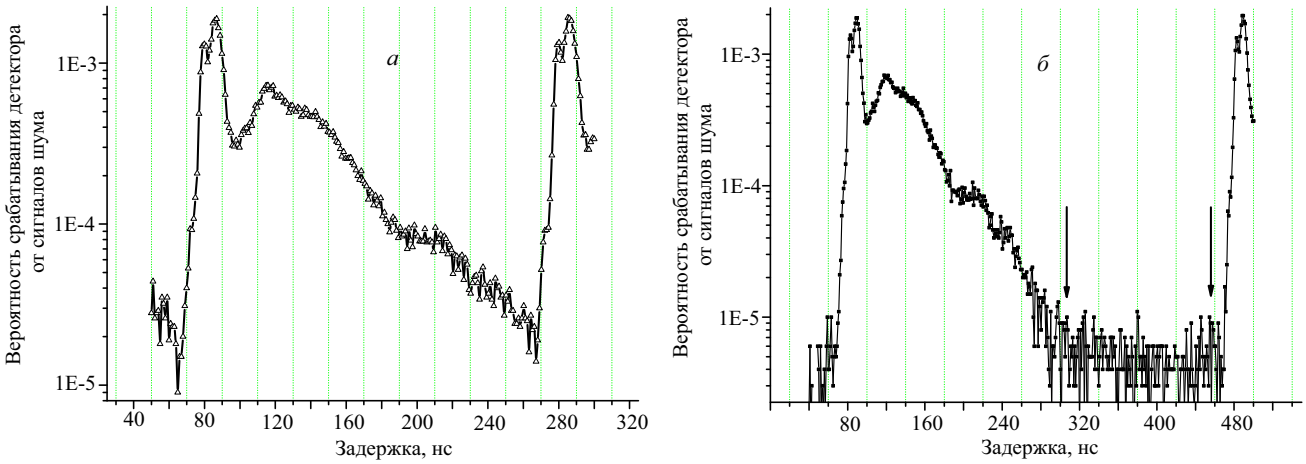

Рис. 6. Вероятности срабатывания однофотонного детектора от сигналов лазера синхронизации: *а* — режим импульсной «засветки», $F = 5$ МГц, уровень «шума» равен 8×10^{-4} 1/с; *б* — режим импульсной «засветки», $F = 2.5$ МГц, уровень «шума» равен 4×10^{-6} 1/с на участке, обозначенном стрелками, и сравним с собственным уровнем «шума» детектора

делению уровня «засветки» проводились на частотах 2.5 и 5 МГц; следует отметить, что на частоте 5 МГц уровень «засветки» не успевает снизиться до уровня собственных шумов однофотонного детектора (рис. 6, *а*), при работе на частоте 2.5 МГц, через $T = 300$ нс после импульса синхронизации (рис. 6, *б*) уровень шумов сравним с уровнем собственных шумов детектора.

ЗАКЛЮЧЕНИЕ

Из представленных данных рис. 6, *а, б* видно, что при длине линии связи 95 км и режиме запуска лазера с непрерывном током, уровень шумовой «засветки» однофотонного детектора между импульсами запуска значительно превышает собственный уровень шумов детектора (4×10^{-6} 1/с). В случае запуска лазера в режиме предварительного формирования короткого ($T_1 = 20–30$ нс) импульса «полочки», в конце которой поступает запускающий импульс ($T_2 = 2–3$ нс), уровень шумовой «засветки» не превышает значения собственных шумов детектора.

Таким образом, предложенный оригинальный способ запуска DFB-лазера синхронизации и применение временной селекции сигналов синхронизации и квазиоднофотонных импульсов позволяют уменьшить ошибку (QBER) при выработке секретного ключа и увеличить протяженность одноволоконной линии связи до 95 км.

СПИСОК ЛИТЕРАТУРЫ

1. *Muller A., Zbinden H., Gisin N.* // Europhysics Letters. 1996. **33**, N 5. P. 335.
2. *Балыгин К. А., Зайцев В. И., Климов А. Н.* и др. // Письма в ЖЭТФ. 2017. **105**, № 9. С. 570.
3. *Наний О. Е.* // Lightwave Russian Edition. 2004. N 2. P. 47.
4. *Кулик С. П., Молотков С. Н., Потапова Т. А.* // Письма в ЖЭТФ. 2013. **98**, № 10. С. 700.
5. www.nolatech.ru
6. *Patel K. A., Dynes J. F., Choi I.* et al. // Phys. Rev. X 2012. **2**. 041010.

Reducing the Level of Stray Exposure of an Optical Fiber in a Single-Pass Quantum Cryptography System

K. A. Balygin[1,3,a], **V. I. Zaitsev**[1,3], **A. I. Klimov**[1,3,b], **A. N. Klimov**[3], **S. P. Kulik**[2,3], **S. N. Molotkov**[3]

[1]*National research center "Kurchatov Institute". Moscow 123182, Russia*
[2]*Faculty of physics;* [3]*The center for quantum technologies, Lomonosov Moscow State University. Moscow 119991, Russia.*
E-mail: [a]*kirill.balygin@gmail.com*, [b]*nrc.klimov@gmail.com*.

A method for triggering a laser synchro-signal diode in a single-pass quantum cryptographic system is proposed. The method allows reducing the level of stray in fluence in an optical fiber from scattered laser radiation by ~ 2 orders of magnitude and increasing the length of a single-fiber communication line when generating a secret key to 95 km.

Keywords: quantum cryptography systems, single-photon detector, laser.
PACS: 42.50.Ex.
Received 11 July 2019.

English version: *Moscow University Physics Bulletin*. 2020. **75**, No. 2. Pp. 175–180.

Сведения об авторах

1. Балыгин Кирилл Алексеевич — науч. сотрудник; e-mail: kirill.balygin@gmail.com.
2. Зайцев Владимир Иванович — науч. сотрудник; e-mail: vl-i-z@yandex.ru.
3. Климов Анатолий Иванович — канд. техн. наук, вед. науч. сотрудник; e-mail: nrc.klimov@gmail.com.
4. Климов Андрей Николаевич — науч. сотрудник.
5. Кулик Сергей Павлович — доктор физ.-мат. наук, вед. науч. сотрудник; e-mail: sergei.kulik@physics.msu.ru.
6. Молотков Сергей Николаевич — доктор физ.-мат. наук, вед. науч. сотрудник; e-mail: sergei.molotkov@gmail.com.