

УДК 535.14

## РАСПРЕДЕЛЕНИЕ КВАНТОВОГО КЛЮЧА НА ДАЛЬНИЕ ДИСТАНЦИИ ПО ОПТОВОЛОКНУ СО СВЕРХПРОВОДЯЩИМИ ДЕТЕКТОРАМИ

В. Л. Курочкин<sup>1,2</sup>, А. В. Зверев<sup>1</sup>, Ю. В. Курочкин<sup>3</sup>, И. И. Рябцев<sup>1,2,3</sup>,  
И. Г. Неизвестный<sup>1</sup>, Р. В. Ожегов<sup>4</sup>, Г. Н. Гольцман<sup>4</sup>, П. А. Ларионов<sup>4</sup>

<sup>1</sup>*Институт физики полупроводников им. А. В. Ржанова СО РАН,  
630090, г. Новосибирск, просп. Академика Лаврентьева, 13*

<sup>2</sup>*Новосибирский государственный университет,  
630090, г. Новосибирск, ул. Пирогова, 2*

<sup>3</sup>*Российский квантовый центр,  
143025, Москва, ул. Новая, 100А*

<sup>4</sup>*Московский государственный педагогический университет,  
119991, Москва, ул. Малая Пироговская, 1  
E-mail: kurochkin@isp.nsc.ru*

Представлены результаты экспериментальных исследований по распределению квантового ключа в оптоволоконных линиях связи с применением сверхпроводящих детекторов. Для экспериментальной установки на основе автокомпенсационной оптической схемы получена генерация ключа при длине оптоволоконной линии 101,1 км. На основе поляризационного кодирования фотонов впервые продемонстрирована возможность распределения квантового ключа на расстоянии свыше 300 км по оптоволокну.

*Ключевые слова:* квантовая криптография, детекторы одиночных фотонов.

**Введение.** В первой работе по квантовой криптографии [1] было продемонстрировано распределение квантового ключа с помощью передачи одиночных поляризованных в двух неортогональных друг другу базисах фотонов через открытое пространство на расстоянии 30 см. Усовершенствование техники эксперимента позволило достаточно быстро увеличить дальность связи по открытому пространству [2, 3]. В работе [4] продемонстрирована передача ключа на расстояние 144 км с одного испанского острова (Лас-Пальмас) на другой (Тенерифе) по атмосфере и получены экспериментальные данные, показывающие возможность глобального распределения ключа через спутники [5–7].

В то же время ведутся интенсивные работы по созданию оптоволоконных квантовых систем связи. Современные телекоммуникационные системы связи широко применяют оптическое волокно, и первое исследование по распределению квантового ключа по оптоволоконному квантовому каналу появилось уже в 1993 году [8]. Для квантовой криптографии используется одномодовое оптоволоконно, передача же ведётся обычно на телекоммуникационной длине волны 1550 нм, которая соответствует наименьшему затуханию и минимальной дисперсии для оптоволоконной линии со смещённой дисперсией [2]. Экспериментально реализовано распределение квантового ключа на расстояния свыше 100 км по оптоволокну с полупроводниковыми детекторами [9, 10], функционирующими в режиме стробирования, и на 300 км с детекторами, работающими в ждущем режиме [11]. Появились коммерческие изделия, такие как Cerberis, Vectis и Clavis производства фирмы "IdQuantique" (Швейцария) [12] и MagiQ QPN Security Gateway 7505 фирмы "MagiQ Technologies" (США) [13]. Со сверхпроводящими детекторами одиночных фотонов (СДФ), имеющими значительно меньший уровень темновых шумов, продемонстрирована дальность связи на расстояния 200–300 км [14–19].

В данной работе представлены результаты наших экспериментальных исследований по распределению квантового ключа в оптоволоконных линиях связи с применением сверхпроводящих детекторов. Для экспериментальной установки на основе двухпроходной автокомпенсационной оптической схемы с фазовым кодированием фотонов получена генерация ключа при длине оптоволоконна до 101,1 км. В однонаправленной оптической схеме с поляризационным кодированием фотонов впервые продемонстрирована возможность распределения квантового ключа на расстояния свыше 300 км по оптоволокну.

**Эксперименты с двухпроходной автокомпенсационной оптической схемой и фазовым кодированием одиночных фотонов.** Оптическая часть оптоволоконной экспериментальной установки (рис. 1) собрана по автокомпенсационной двухпроходной схеме, предложенной в работе [20]. Она состоит из передатчика Алиса и приёмника Боб, которые соединены между собой одномодовым оптоволоконном SMF-28 (квантовый канал) длиной 25–101 км. Особенности прохождения оптических сигналов подробно описаны в [20–22].

Для регистрации одиночных фотонов с длиной волны 1550 нм, получаемых в виде сильно ослабленных коротких (1 нс) импульсов излучения полупроводникового лазера с распределённой обратной связью, были применены сверхпроводящие детекторы одиночных фотонов [11, 14]. Их квантовая эффективность и уровень шумов зависят от температуры — наилучшие результаты достигаются при охлаждении ниже температуры жидкого гелия (примерно 2 К). В нашем эксперименте штук с держателем СДОФ и адаптерами тока смещения помещался в сосуд Дьюара с жидким гелием и находился при температуре 4,2 К. Рабочий ток через детекторы задавался с помощью источника смещения. Выходной сигнал с высокочастотных усилителей детекторов поступал на вход контроллера детекторов и далее направлялся в быстродействующий цифровой процессор для обработки. Токи смещения в двух сверхпроводящих детекторах подбирались так, чтобы можно было получить оптимальное соотношение сигнал/шум. При этом квантовая эффективность детекторов составляла около 2 %.

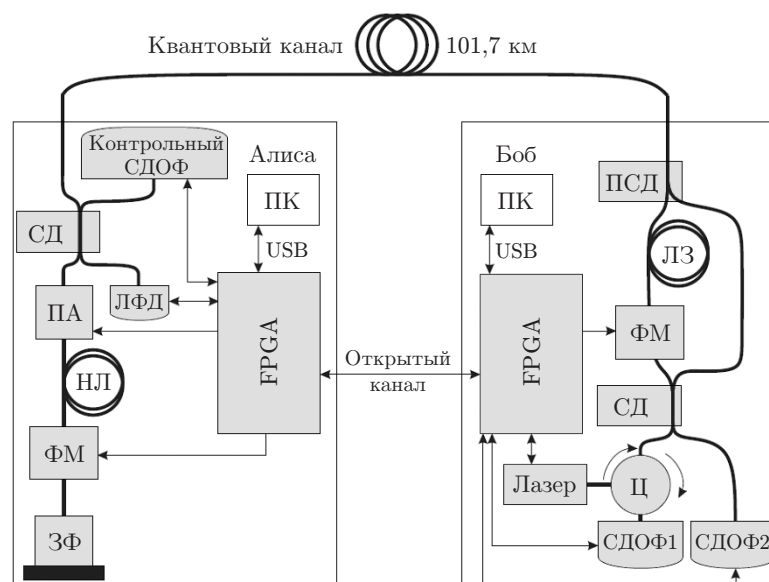


Рис. 1. Блок-схема передатчика Алиса и приёмника Боб (ПСД — оптоволоконный поляризационный светоделитель, ФМ — фазовый модулятор, ЛЗ — линия задержки длиной 10 м, Ц — циркулятор, ЗФ — зеркало Фарадея, ПА — перестраиваемый аттенюатор, НЛ — накопительная линия длиной 25 км, ПК — персональный компьютер, FPGA — программируемая логическая матрица, ЛФД — лавинный фотодиод)

**Экспериментальные данные по генерации квантового ключа  
и количеству ошибок в ключе  
для различной длины квантового канала**

Длина квантового канала, км	Скорость генерации ключа, бит/с	Количество ошибок в ключе, %
25,8	1418	0,25
51,2	748	0,3
76,4	143	0,25
101,7	33	1,57

Перед измерениями проводилась процедура настройки. Модуль приёмника Боб испускал многофотонный лазерный импульс и измерял время его прохождения через квантовый канал с точностью  $\pm 400$  пс. На основании данного измерения задавались моменты открытия временных ворот для регистрации информационных фотонов в однофотонных детекторах. При этом ослабление излучения управляемым аттенуатором и токи смещения в сверхпроводящих детекторах подбирались так, чтобы можно было зарегистрировать многофотонный сигнал. Во время распределения квантового ключа излучение ослаблялось передатчиком Алиса с помощью ПА до уровня 0,4 фотона в лазерном импульсе. Токи смещения в сверхпроводящих детекторах увеличивались, при этом детекторы переключались в однофотонный режим работы и регистрировали однофотонные импульсы в нужный момент времени с временными воротами длительностью 3–4 нс. Частота повторения лазерных импульсов устанавливалась равной 5 МГц.

В нашем эксперименте зарегистрирована генерация квантового ключа с различной скоростью, зависящей от длины оптоволоконного квантового канала 25,8–101,7 км (см. таблицу). Количество ошибок в ключе не превышало 1,57 %. Учитывая, что максимальная допустимая ошибка в квантовой передаче не должна быть выше 11 %, можно считать, что полученные экспериментальные данные удовлетворяют условию секретности распределения квантового ключа.

**Эксперименты с однопроходной оптической схемой и поляризационным кодированием одиночных фотонов.** В двухпроходной схеме для автокомпенсации поляризационных искажений оптический сигнал проходит квантовый канал дважды, что уменьшает скорость генерации квантового ключа. Для увеличения скорости и дальности квантовой связи нами была собрана экспериментальная установка на основе однопроходной оптической схемы с поляризационным кодированием одиночных фотонов (рис. 2). Сверхпроводящие детекторы СДОФ1 и СДОФ2 охлаждались до температуры 2,2 К, при которой квантовая эффективность составляла около 12 %. Для охлаждения детекторов использовался рефрижератор замкнутого цикла SRDK-101D. Измеренная зависимость квантовой эффективности и уровня шумов от тока смещения одного из детекторов приведена на рис. 3.

Процедура распределения квантового ключа велась в соответствии с протоколом BB84. Лазерный импульс на длине волны 1550 нм длительностью 1 нс ослаблялся до уровня 0,2 фотона на импульс аттенуатором 3 (см. рис. 2) Частота повторения лазерных импульсов составляла 32 МГц. Поляризация фотона на выходе передатчика задавалась с помощью поляризационного контроллера 6. Поляризационный контроллер 8 на входе в приёмник восстанавливал линейную поляризацию и задавал базис измерения поляризации прошедшего фотона. После прохождения через одномодовое оптоволокно длиной 25–302,4 км фотоны регистрировались детекторами СДОФ1 и СДОФ2. Квантовая эффективность детекторов зависит от поляризации входного излучения [11, 14]. Для компенсации

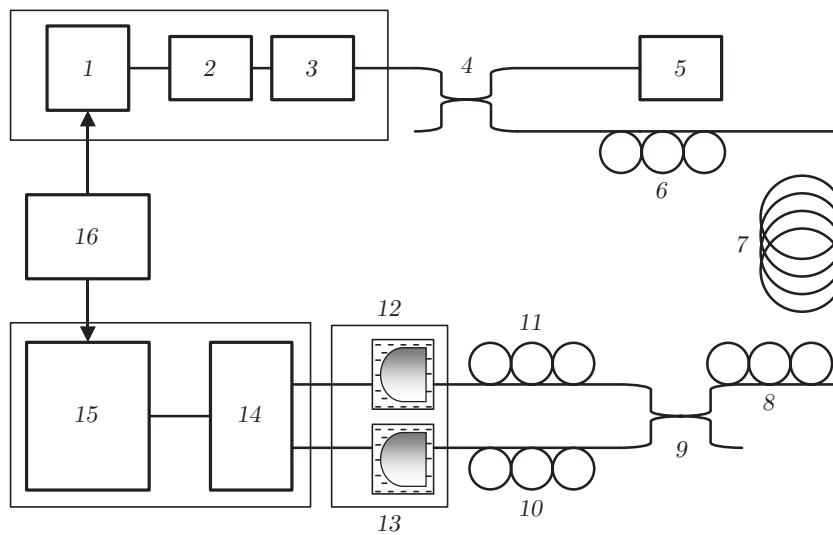


Рис. 2. Блок-схема экспериментальной установки с поляризационным кодированием фотонов: 1 — контроллер передатчика, 2 — лазер, 3 — аттенюатор, 4 и 9 — светоделители 50/50 %, 5 — измеритель мощности, 6, 8, 10 и 11 — поляризационные контроллеры, 7 — квантовый канал (одномодовое оптоволокно), 12 и 13 — сверхпроводящие детекторы, 14 — драйвер детекторов, 15 — контроллер приёмника, 16 — персональный компьютер

этой зависимости на входе детекторов стояли дополнительные поляризационные контроллеры 10 и 11. Передатчик и приёмник синхронизировались во времени. Длительность временных ворот, в которых регистрировался однофотонный сигнал, составляла 6,25 нс.

Для уменьшения затухания фотонов в квантовом канале использовалось оптоволокно Corning SMF-28 ULL с ультранизкими потерями 0,168 дБ/км. При длине оптоволокна 302,4 км полное затухание сигнала составило 50,2 дБ. На рис. 4 представлена измеренная зависимость отношения скорости детектирования фотонов к тактовой частоте передачи квантового ключа от длины квантового канала. При длине 302,4 км скорость генерации квантового ключа составила 7 бит в секунду при количестве квантовых ошибок 5,1 %. Ре-

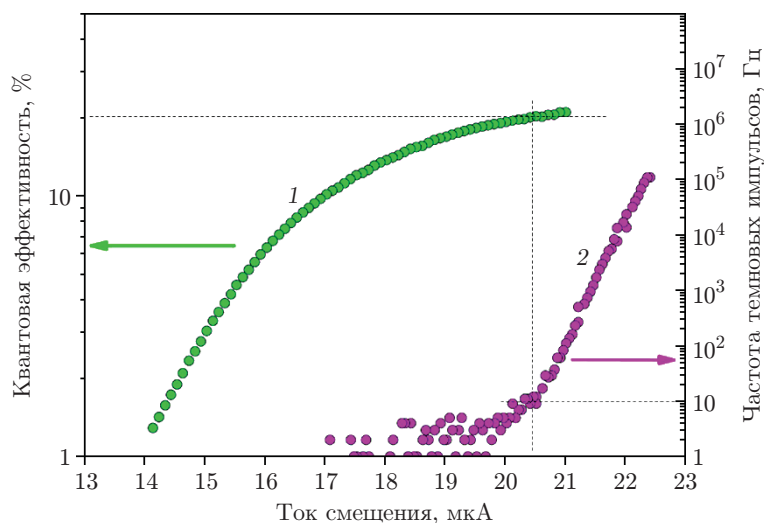


Рис. 3. Измеренная зависимость квантовой эффективности на длине волны 1550 нм (1) и частоты темновых импульсов (2) от тока смещения для одного из сверхпроводящих детекторов (канал 2)

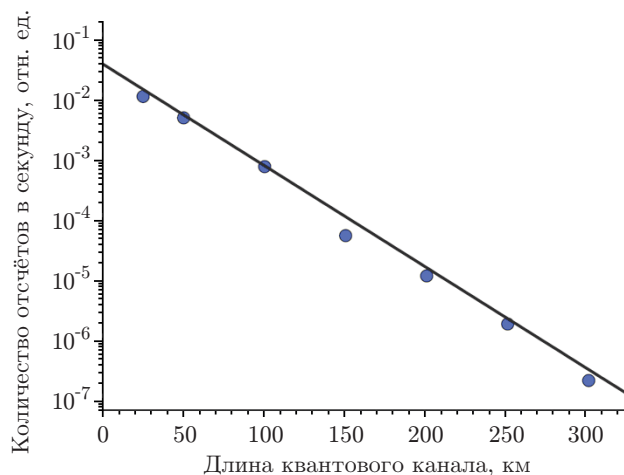


Рис. 4. Измеренная зависимость отношения количества зарегистрированных фотонов в секунду к тактовой частоте передачи квантового ключа от длины квантового канала

зультаты данного эксперимента впервые продемонстрировали возможность распределения квантового ключа по оптоволокну на расстояния свыше 300 км.

**Заключение.** Проведённые эксперименты показали, что применение сверхпроводящих детекторов одиночных фотонов позволяет увеличить дальность распределения квантового ключа в оптоволоконном квантовом канале. При охлаждении детекторов до температуры жидкого гелия, при которой их квантовая эффективность составляла 2 %, на установке с двухпроходной автокомпенсационной оптической схемой и фазовым кодированием фотонов в данной работе была достигнута дальность связи 101,1 км — наибольшая для такой схемы. При охлаждении детекторов до температуры 2,2 К, соответствующей квантовой эффективности 12 %, нами впервые продемонстрирована возможность распределения квантового ключа на расстояния свыше 300 км по оптоволокну на основе поляризационного кодирования фотонов в однопроходной оптической схеме. Дальнейшее увеличение тактовой частоты передачи и уменьшение временных ворот регистрации однофотонных сигналов позволит увеличить дальность и скорость генерации квантового ключа.

## СПИСОК ЛИТЕРАТУРЫ

1. **Bennet C. H.** Quantum cryptography using any two nonorthogonal states // Phys. Rev. Lett. 1992. **68**, Is. 21. P. 3121–3124.
2. **Gisin N., Ribordy G., Title W. et al.** Quantum cryptography // Rev. Mod. Phys. 2002. **74**, Is. 1. P. 145–175.
3. **Scarani V., Bechmann-Pasquinucci H., Cerf N. et al.** The security of practical quantum key distribution // Rev. Mod. Phys. 2009. **81**, Is. 3. P. 1301–1350.
4. **Schmitt-Manderbach T., Weier H., Furst M. et al.** Experimental demonstration of free-space decoy-state quantum key distribution over 144 km // Phys. Rev. Lett. 2007. **98**, Is. 1. 010504.
5. **Villoresi P., Jennewein T., Tamburini F. et al.** Experimental verification of the feasibility of a quantum channel between space and Earth // New Journ. Phys. 2008. **10**, N 3. 033038.
6. **Yin J., Cao Y., Liu S.-B. et al.** Experimental quasi-single-photon transmission from satellite to earth // Opt. Express. 2013. **21**, N 17. 20032.

7. **Vallone G., Bacco D., Dequal D. et al.** Experimental satellite quantum communication // Phys. Rev. Lett. 2015. **115**, Is. 4. 040502.
8. **Muller A., Breguet J., Gisin N.** Experimental demonstration of quantum cryptography using polarized photons in optical fibre over more than 1 km // Europhys. Lett. 1993. **23**, N 6. P. 383–388.
9. **Kosaka H., Tomita A., Nambu Y. et al.** Single-photon interference experiment over 100 km for quantum cryptography system using balanced gated-mode photon detector // Electron. Lett. 2003. **39**, Is. 15. P. 1119–1201.
10. **Kimura T., Nambu Y., Hatanaka T. et al.** Single-photon interference over 150-km transmission using silica-based integrated-optic interferometers for quantum cryptography // Jpn. Journ. Appl. Phys. 2004. **43**, N 9AB. P. L1217–L1219.
11. **Korzha B., Lim C. C.-W., Houlmann R. et al.** Provably secure and practical quantum key distribution over 307 km of optical fibre // Nature Photon. 2015. **9**, N 3. P. 163–168.
12. **IDQ.** URL: <http://www.idquantique.com> (дата обращения: 15.12.2014).
13. **MagiQ.** URL: <http://www.magiqtech.com> (дата обращения: 15.12.2014).
14. **Ozhegov R., Elezov M., Kurochkin Y. et al.** Quantum key distribution over 300 km // Abst. of the Intern. Conf. "Micro- and Nanoelectronics-2014 (ICMNE-2014)". Moscow — Zvenigorod, Russia, October 6–10, 2014. q3-10.
15. **Shibata H., Honjo T., Shimizu K.** Quantum key distribution over a 72 dB channel loss using ultralow dark count superconducting single-photon detectors // Opt. Lett. 2014. **39**, Is. 17. P. 5078–5081.
16. **Stucki D., Walenta N., Vannel F. et al.** High rate, long-distance quantum key distribution over 250 km of ultra low loss fibres // New Journ. Phys. 2009. **11**. 075003.
17. **Wang S., Chen W., Guo J.-F. et al.** 2 GHz clock quantum key distribution over 260 km of standard telecom fiber // Opt. Lett. 2012. **37**, N 6. P. 1008–1010.
18. **Takesue H., Nam S. W., Zhang Q. et al.** Quantum key distribution over a 40-dB channel loss using superconducting single-photon detectors // Nature Photon. 2007. **1**. P. 343–348.
19. **Liu Y., Chen T.-Y., Wang J. et al.** Decoy-state quantum key distribution with polarized photons over 200 km // Opt. Express. 2010. **18**, N 8. P. 8587–8594.
20. **Stucki D., Gisin N., Guinnard O. et al.** Quantum key distribution over 67 km with a plug&play system // New Journ. Phys. 2002. **4**. P. 41.1–41.8.
21. **Курочкин В. Л., Зверев А. В., Курочкин Ю. В. и др.** Применение детекторов одиночных фотонов для генерации квантового ключа в экспериментальной оптоволоконной системе связи // Автометрия. 2009. **45**, № 4. С. 110–119.
22. **Курочкин В. Л., Зверев А. В., Курочкин Ю. В. и др.** Экспериментальные исследования в области квантовой криптографии // Микроэлектроника. 2011. **40**, № 4. С. 264–273.

*Поступила в редакцию 15 декабря 2014 г.*