Научная статья

УДК 535.14
DOI 10.25205/2541-9447-2021-16-2-81-93

Исследование долговременной стабильности генерации однофотонного квантового ключа в схеме с поляризационным кодированием

Александр Владимирович Коляко [1], Александр Сергеевич Плешков [2]
Денис Борисович Третьяков [3], Василий Матвеевич Энтин [4]
Игорь Ильич Рябцев [5], Игорь Георгиевич Неизвестный [6]

[1–6] Институт физики полупроводников им. А. В. Ржанова
Сибирского отделения Российской академии наук
Новосибирск, Россия

[1–5] Новосибирский государственный университет
Новосибирск, Россия

[2] Сибирский государственный университет телекоммуникаций и информатики
Новосибирск, Россия

[5] Новосибирский государственный технический университет
Новосибирск, Россия

[1] kolyako@isp.nsc.ru, https://orcid.org/0000-0003-0163-6580
[2] pleshkov@isp.nsc.ru, https://orcid.org/0000-0001-5856-6304
[3] dtret@isp.nsc.ru, https://orcid.org/0000-0002-3708-6253
[4] ventin@isp.nsc.ru, https://orcid.org/0000-0001-5436-2849
[5] ryabtsev@isp.nsc.ru, https://orcid.org/0000-0002-5410-2155
[6] neizv@isp.nsc.ru

Аннотация

Представлены экспериментальные результаты, демонстрирующие долговременную стабильность работы созданной нами атмосферной квантово-криптографической установки, использующей протокол BB84 и поляризационное кодирование. Показано, что скорость генерации «просеянного» квантового ключа и уровень ошибочных битов в ключе оставались постоянными в течение 1 часа и равнялись 10 кбит/с и 6,5 % соответственно при расстоянии между передатчиком и приемником, равном 20 см. Приведены теоретические зависимости скорости генерации секретного квантового ключа от коэффициента пропускания квантового канала для детекторов одиночных фотонов, которые использовались в данном эксперименте, и новых детекторов с пониженным уровнем темновых шумов.

Ключевые слова

квантовая криптография, протокол BB84, поляризационное кодирование, детекторы одиночных фотонов

Источник финансирования

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

Для цитирования

Коляко А. В., Плешков А. С., Третьяков Д. Б., Энтин В. М., Рябцев И. И., Неизвестный И. Г. Исследование долговременной стабильности генерации однофотонного квантового ключа в схеме с поляризационным кодированием // Сибирский физический журнал. 2021. Т. 16, № 2. С. 81–93. DOI 10.25205/2541-9447-2021-16-2-81-93

Investigation of Long-Term Stability of Single-Photon Quantum Key Distribution in a Polarization Coding Scheme

Alexander V. Kolyako [1], **Alexander S. Pleshkov** [2]
Denis B. Tretyakov [3], **Vasiliy M. Entin** [4]
Igor I. Ryabtsev [5], **Igor G. Neizvestny** [6]

[1–6] A. V. Rzhanov Institute of Semiconductor Physics
of the Siberian Branch of the Russian Academy of Sciences
Novosibirsk, Russian Federation

[1–5] Novosibirsk State University
Novosibirsk, Russian Federation

[2] Siberian State University of Telecommunications and Information Science
Novosibirsk, Russian Federation

[5] Novosibirsk State Technical University
Novosibirsk, Russian Federation

[1] kolyako@isp.nsc.ru, https://orcid.org/0000-0003-0163-6580
[2] pleshkov@isp.nsc.ru, https://orcid.org/0000-0001-5856-6304
[3] dtret@isp.nsc.ru, https://orcid.org/0000-0002-3708-6253
[4] ventin@isp.nsc.ru, https://orcid.org/0000-0001-5436-2849
[5] ryabtsev@isp.nsc.ru, https://orcid.org/0000-0002-5410-2155
[6] neizv@isp.nsc.ru

Abstract

Experimental results demonstrating long-term stability of the operation of our atmospheric quantum cryptography set-up using the BB84 protocol and polarization coding are presented. It was shown that the "sifted" quantum key distribution rate and the quantum bit error rate in the key remained constant for 1 hour and were equal to 10 kbit/s and 6.5 %, respectively, at a distance between the transmitter and the receiver equal to 20 cm. Theoretical dependences of the secret quantum key generation rate on a quantum channel transmission coefficient for single-photon detectors, which were used in this experiment, and for new detectors with a reduced level of dark pulses are given.

Keywords

quantum cryptography, BB84 protocol, polarization coding, single-photon detectors

Funding

This work was supported by A. V. Rzhanov Institute of Semiconductor Physics SB RAS and Novosibirsk State University

For citation

Kolyako A. V., Pleshkov A. S., Tretyakov D. B., Entin V. M., Ryabtsev I. I., Neizvestny I. G. Investigation of Long-Term Stability of Single-Photon Quantum Key Distribution in a Polarization Coding Scheme. *Siberian Journal of Physics*, 2021, vol. 16, no. 2, pp. 81–93. (in Russ.) DOI 10.25205/2541-9447-2021-16-2-81-93

Введение

В квантово-криптографических линиях связи защита передаваемой информации от подслушивания обеспечивается законами квантовой механики [1] в отличие от классических криптографических систем, в которых секретность основана на сложности математических вычислений. С помощью передачи квантовых объектов – одиночных фотонов – по оптоволоконной или атмосферной линии связи генерируется секретный двоичный ключ, известный только отправителю (Алисе) и получателю (Бобу). Используя данный ключ, Алиса зашифровывает свое сообщение и передает его Бобу по открытому каналу [2].

Первый квантово-криптографический протокол BB84 был предложен в 1984 г. [3] и экспериментально реализован в 1992 г. [4]. В данном протоколе используются четыре поляризационных состояния одиночных фотонов, ориентированных под углами 0, 90, 45 и –45° по отношению к некоторой оси. Из них первые два состояния составляют вертикально-гори-

зонтальный базис, а вторые два – диагональный. Двоичные значения «0» и «1» произвольно присваиваются одному и другому состоянию в каждом базисе. Далее Алиса случайным образом выбирает одно из четырех поляризационных состояний фотона и посылает фотон Бобу. Боб, получив фотон, измеряет его состояние в случайно выбранном базисе. После сеанса квантовой связи Боб сообщает Алисе по открытому каналу номера тактовых импульсов, в которых был зарегистрирован один фотон. Все остальные тактовые импульсы отбрасываются. Таким образом, Алиса и Боб формируют так называемый «сырой» ключ в виде случайной последовательности битов. Далее Алиса и Боб обмениваются информацией о выбранных базисах для каждого бита и отбрасывают те биты, для которых базисы не совпали. В результате получается «просеянный» ключ, который у Алисы и Боба будет отличаться вследствие того, что используемая ими аппаратура неидеальна. Чтобы получить идентичный ключ, Алисе и Бобу нужно провести процедуру коррекции ошибок. Вклад в уровень ошибочных битов будет вносить также любая попытка получения злоумышленником (Евой) информации о ключе путем внедрения в квантовый канал. Поэтому Алиса и Боб проводят дополнительную процедуру усиления конфиденциальности, после которой количество информации у Евы о ключе становится ничтожно малым. После этих двух процедур Алиса и Боб получают один секретный ключ, размер которого меньше, чем размер «просеянного» ключа, и тем меньше, чем больше уровень ошибочных битов. Теоретически доказано, что для протокола BB84 при уровне ошибочных битов в «просеянном» ключе больше 11 % сгенерировать секретный ключ становится невозможно [2].

К настоящему времени иностранными группами была успешно продемонстрирована генерация квантового ключа на расстояниях 400÷500 км по оптоволоконным линиям связи [5; 6]. По открытому пространству максимальная длина квантово-криптографической линии связи через спутники составляет уже 7 600 км [7].

В России оптоволоконные квантово-криптографические системы были опробованы в городских условиях на расстоянии нескольких десятков километров [8; 9]. Атмосферные квантовые линии связи реализованы пока на расстояниях 20 м на основе метода боковых частот [10] и 180 м с применением релятивистской квантовой криптографии [11].

Одной из основных целей исследований в области квантовой криптографии, проводимых в мире, является повышение скорости генерации секретного ключа и дальности квантовых линий связи. Препятствием к этому являются неизбежные потери одиночных фотонов при прохождении по квантовому каналу (атмосфере или оптоволокну). Они приводят к увеличению уровня ошибочных битов в «просеянном» ключе и, следовательно, уменьшению скорости генерации секретного ключа. Однако в случаях, когда скорость генерации секретного ключа не обладает большим приоритетом перед секретностью, на первый план выходит долговременная стабильность работы квантово-криптографической системы. Тогда за достаточно долгое время можно сгенерировать секретный ключ нужной длины даже при уровне ошибочных битов, близком к 11 %, и при низкой скорости генерации ключа.

Целью данной статьи являлось исследование долговременной стабильности работы созданной нами атмосферной квантово-криптографической экспериментальной установки, использующей протокол BB84 и поляризационное кодирование. Аналогичная установка, применявшаяся нашей группой ранее [12], была почти полностью модернизирована. В результате была существенно увеличена скорость генерации квантового ключа и улучшена долговременная стабильность работы установки.

Экспериментальная установка

В качестве источников фотонов передатчика использовались четыре полупроводниковых лазера с длиной волны излучения 780 нм, которая соответствует окну прозрачности атмосферы [2]. Каждый из лазеров имел отдельный источник питания, который был способен работать как в импульсном режиме, так и в непрерывном. Лазерные импульсы длительностью

5 нс формировались при подаче на лазеры импульсов тока и использовались для генерации квантового ключа. Запуск импульсов тока осуществлялся тактовыми импульсами с компьютера, подаваемыми отдельно на каждый источник питания лазеров. Непрерывный режим использовался для предварительной настройки оптической схемы передающего и приемного узлов.

На рис. 1 показана оптическая схема передатчика. В схеме задавалась поляризация излучения каждого лазера. Поскольку из лазеров излучение выходило уже поляризованным, то их корпуса были повернуты так, чтобы излучения 1-го и 4-го лазеров имели поляризацию относительно плоскости оптического стола 90°, а 2-го и 3-го лазеров – 0°. Далее излучения 1-го и 4-го лазеров отражались от призм Глана, а излучения 2-го и 3-го лазеров проходили через них. В данном случае призмы Глана использовались в качестве как отражающих элементов, так и дополнительных поляризаторов. Далее поляризация излучения 3-го и 4-го лазеров поворачивалась на 45° с помощью полуволновой пластинки. В итоге 1-й и 2-й лазеры посылали фотоны, поляризованные в вертикально-горизонтальном базисе, а 3-й и 4-й – в диагональном.

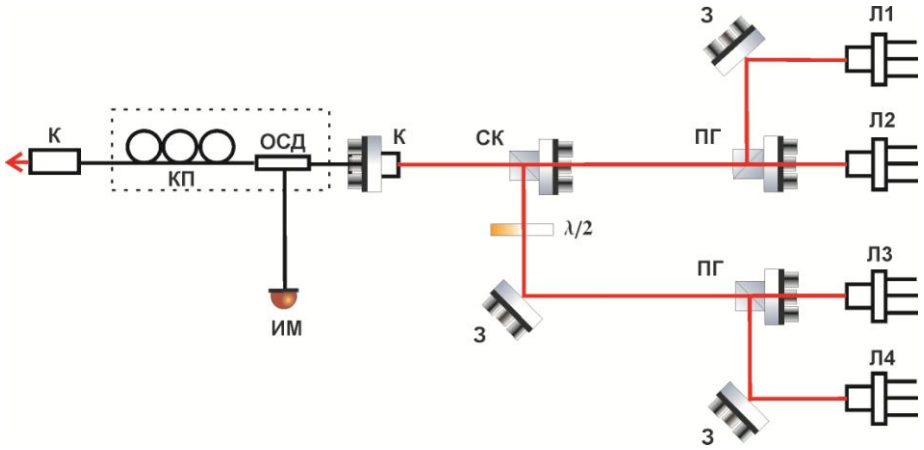

Рис. 1. Оптическая схема передатчика (Алисы): Л1, Л2, Л3, Л4 – лазеры, З – зеркала, ПГ – призмы Глана, λ/2 – полуволновая пластинка, СК – светоделительный кубик (50 : 50), К – коллиматор, ОСД – оптоволоконный светоделитель (50 : 50), ИМ – измеритель мощности, КП – контроллер поляризации. Пунктирной линией обозначен теплоизоляционный кожух
Fig. 1. Optical scheme of the transmitter (Alice): Л1, Л2, Л3, Л4 – lasers, З – mirrors, ПГ – Glan prisms, λ/2 – half-wave plate, СК – beam splitter cube (50 : 50), К – collimator, ОСД – fiber-optics beam splitter (50 : 50), ИМ – power meter, КП – polarization controller. The dotted line indicates the thermal insulation jacket

Лучи всех четырех лазеров совмещались на светоделительном 50 : 50 кубике и заводились в оптоволоконный кабель. На выходе кабеля стоял коллиматор, из которого выходил пучок диаметром 3 мм и посылался к приемному узлу (Бобу).

Заведение в оптоволоконный кабель было использовано для точного совмещения лучей от лазеров в один луч и пространственной фильтрации, а также для удобства соединения передающего узла с телескопом с большой апертурой, который планируется использовать в будущем для генерации квантового ключа на большом расстоянии между передатчиком и приемником. Кроме того, если использовать не обычный кабель, а светоделитель с двумя выходами, то второй выход можно использовать для контроля мощности выходящего излучения (см. рис. 1).

Однако использование оптоволоконного кабеля приводит к искажению поляризации входного излучения, поэтому на кабель необходимо установить контроллер поляризации, восста-

навливающий на выходе поляризацию входного излучения. Кроме того, поляризация выходного излучения зависит от температуры оптоволоконного кабеля. Поэтому также необходимо, особенно при работе установки на открытом воздухе, обеспечить тепловую изоляцию оптоволоконных компонент и в зависимости от ситуации применить активную стабилизацию температуры волокна.

Следует заметить, что использование оптического волокна с сохранением поляризации невозможно, поскольку данное волокно сохраняет линейную поляризацию излучения только в том случае, если поляризация входного излучения ориентирована вдоль одной из двух выделенных перпендикулярных осей волокна, в то время как для реализации протокола BB84 при поляризационном кодировании требуются четыре поляризационных состояния фотонов.

Для получения одиночных фотонов мы использовали стандартный метод сильного ослабления мощности лазерного излучения [2]. Тогда число фотонов в лазерном импульсе описывается распределением Пуассона. С помощью четырех калиброванных поглощающих фильтров (не показаны на рисунках) мы ослабляли мощность излучения лазеров передатчика до такой степени, чтобы среднее число фотонов на импульс по теоретическим расчетам составляло $\mu = 0{,}1$. В этом случае вероятность «пустых» импульсов равняется 0,905, вероятность однофотонных импульсов – 0,09, а многофотонных – 0,005. Косвенным доказательством того, что передатчик является квазиоднофотонным источником света, является соответствие частоты срабатывания фотодетекторов в приемнике и эффективности однофотонной регистрации фотодетекторов, приведенной в техническом описании. При многофотонном режиме частота срабатывания будет завышена.

Расстояние от коллиматора передатчика до входа в установку приемника составляло 20 см. Луч проходил от коллиматора внутри непрозрачной трубки для изоляции от внешних засветок.

Оптическая схема приемника показана на рис. 2. Лазерное излучение разделялось на два луча светоделительным 50 : 50 кубиком, один из которых потом шел на регистрацию фотонов в вертикально-горизонтальном базисе, а другой – в диагональном. В каждом базисе фотоны разделялись по поляризации с помощью призм Глана и регистрировались однофотонными детекторами: 1-й и 2-й фотодетекторы использовались для регистрации фотонов в вертикально-горизонтальном базисе, 3-й и 4-й – в диагональном. Для регистрации фотонов в диагональном базисе использовалась полуволновая пластинка, поворачивающая поляризацию фотонов на угол 45°.

Основу однофотонных детекторов составляли кремниевые лавинные фотодиоды (ЛФД) C30902S производства фирмы «EG&G Optoelectronics». Для регистрации одиночных фотонов ЛФД вводились в постоянный гейгеровский режим, для чего напряжение питания ЛФД поднималось выше напряжения пробоя. Использовалась схема с пассивным гашением лавины. Импульсы с ЛФД длительностью 50 нс усиливались и посылались на блок стробирования, в котором дискриминировались по амплитуде для отсечения паразитных наводок и стробировались для уменьшения уровня темновых импульсов. Длительность строб-импульса составляла 20 нс. В блоке стробирования сигналы с фотодетекторов преобразовывались в стандартные

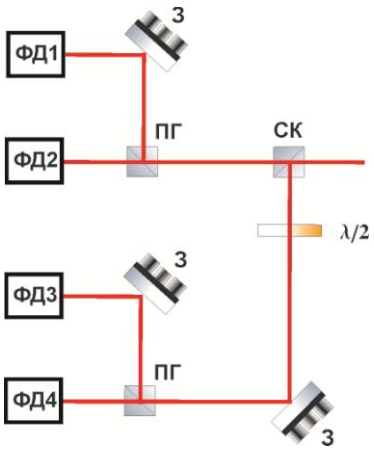

Рис. 2. Оптическая схема приемника (Боба): ФД1, ФД2, ФД3, ФД4 – фотодетекторы, З – зеркала, ПГ – призмы Глана, λ/2 – полуволновая пластинка, СК – светоделительный кубик (50 : 50)

Fig. 2. Optical scheme of the receiver (Bob): ФД1, ФД2, ФД3, ФД4 – photodetectors, З – mirrors, ПГ – Glan prisms, λ/2 – half-wave plate, СК – beam splitter cube (50 : 50)

TTL-импульсы и направлялись на вход счетчика. Частота темновых импульсов уменьшалась также за счет охлаждения корпусов ЛФД до температуры 0 °C с помощью элементов Пельтье. Для защиты от внешних засветок установка находилась в непрозрачном кожухе.

Однофотонные детекторы на основе ЛФД не различают число зарегистрированных фотонов, что для генерации квантового ключа не является важным, но может оказаться полезным для обнаружения атаки с делением числа фотонов. Данная атака может быть выявлена по отклонению распределения числа фотонов в импульсе от статистики Пуассона. Однако, как указано в нашей статье [13], для регистрации изменения распределения числа фотонов в импульсе необязательно иметь детектор, различающий число фотонов, а можно использовать два обычных фотодетектора.

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

Предварительная настройка системы

Предварительная настройка системы проводилась с лазерами, работающими в непрерывном режиме. Поляризационные элементы Алисы и Боба настраивались так, чтобы излучение от 1-го лазера попадало в основном на первый фотодетектор, 2-го лазера – на второй и т. д. При этом в каждом базисе значение контраста поляризации, который находится как отношение мощности излучения, идущего на смежный фотодетектор, к мощности излучения, идущего на основной фотодетектор, должно было быть минимальным для уменьшения уровня ошибочных битов в ключе. Поскольку в блоке Алисы до оптического волокна поляризация излучений всех четырех лазеров была с высокой точностью настроена с помощью призм Глана, основная проблема заключалась в восстановлении этой поляризации при прохождении излучения через оптическое волокно с помощью контроллера поляризации. Однако при настройке контраста для одного базиса у Боба на уровне 0,1 % во втором базисе контраст ухудшался и составлял 3÷4 %. Поэтому в результате приходилось настраивать контроллер поляризации таким образом, чтобы контраст для обоих базисов составлял 1÷2 %.

Окончательная проверка настройки всей системы проводилась в импульсном режиме работы лазеров. Специально написанная для настройки программа в среде LabVIEW позволяла подавать тактовые импульсы на один из четырех лазеров и измерять частоты срабатывания всех четырех фотодетекторов.

В табл. 1 и 2 приведены результаты данной проверки, из которых можно получить значения параметров нашей системы.

В табл. 1 во второй колонке приводятся частоты темновых импульсов $f_{\text{темн}}$ для каждого фотодетектора. В третьей колонке – частоты срабатывания фотодетекторов $f_{\text{лазер+темн}}$ при включении одного основного лазера для каждого фотодетектора. Например, для ФД1 включен лазер 1, для ФД2 – лазер 2 и т. д. В четвертой – уровень темновых импульсов $\varepsilon_{\text{темн}}$, найденный по формуле $\varepsilon_{\text{темн}} = (f_{\text{темн}}/f_{\text{лазер+темн}}) \times 100$ %. В пятой колонке приводится эффективность регистрации одного фотона, найденная по формуле $\eta = (f_{\text{лазер+темн}} - f_{\text{темн}})/(0{,}5 \cdot \mu \cdot f_{\text{такт}}) \times 100$ %, где $\mu = 0{,}1$ – среднее число фотонов в лазерном импульсе, $f_{\text{такт}} = 10^6$ Гц – частота тактовых импульсов. Коэффициент 0,5 в знаменателе возникает из-за того, что луч лазера делится пополам на светоделительном кубике, и фотон с вероятностью 50 % проходит прямо или отражается.

В табл. 2 приводятся частоты срабатывания всех четырех фотодетекторов при включении одного из лазеров.

Таблица 1

Измеренные параметры фотодетекторов

Table 1

Measured parameters of the photodetectors

№ ЛФД	$f_{темн}$, Гц	$f_{лазер+темн}$, Гц	$\varepsilon_{темн}$, %	η, %
1	510	12 045	4,2	23,1
2	501	11 259	4,4	21,5
3	505	8 337	6,0	15,7
4	493	8 010	6,2	15,0

Таблица 2

Частоты срабатывания фотодетекторов при включении одного из лазеров

Table 2

Frequency of counts of photodetectors when one of the lasers is working

№ лазера	*f*, Гц			
	ФД1	ФД2	ФД3	ФД4
1	12 045	651	4 702	3 773
2	639	11 259	4 290	4 105
3	6 581	6 173	8 337	625
4	6 231	6 222	648	8 010

Исследование параметров генерации «просеянного» квантового ключа

Программа для исследования скорости генерации «просеянного» квантового ключа и уровня ошибочных битов подавала тактовые импульсы с частотой следования 1 МГц на запуск одного из четырех лазеров в случайной последовательности и на запуск блока стробирования. Время одного сеанса равнялось 1 с. Среднее число фотонов в лазерном импульсе составляло $\mu = 0{,}1$. После каждого тактового импульса программа проверяла срабатывание всех четырех фотодетекторов. При одновременном срабатывании более одного фотодетектора, а также в случае несовпадения базисов Алисы и Боба эти тактовые импульсы отбрасывались. В случае совпадения базисов подсчитывалось общее количество срабатываний фотодетекторов, которое для времени сеанса 1 с равнялось скорости генерации «просеянного» ключа R, а также уровень ошибочных битов как отношение количества срабатывания смежных фотодетекторов к общему количеству срабатываний.

Скорость генерации «просеянного» ключа R для протокола BB84 при среднем числе фотонов в импульсе $\mu << 1$ находится по следующей формуле [12]: $R = 0{,}5 \cdot f_{такт} \cdot \mu \cdot \eta \cdot T$, где η – эффективность регистрации детекторами одного фотона, T – коэффициент пропускания квантового канала (в наших экспериментах он равен 1). Множитель 0,5 возникает, поскольку отбрасывается примерно половина данных при несовпадении базисов Алисы и Боба. В случае, когда эффективность регистрации детекторов разная, ожидаемую скорость генерации «просеянного» ключа можно найти по следующей формуле:

$$R = 0{,}5 \cdot f_{такт} \cdot \mu \cdot \eta_{ср} \cdot T, \quad (1)$$

где $\eta_{ср}$ – средняя эффективность однофотонной регистрации всех четырех детекторов. В нашем случае $\eta_{ср} = 18{,}8$ % и $R = 9\,400$ бит/с.

Уровень ошибочных битов в «просеянном» ключе (QBER – Quantum Bit Error Rate) находится по следующей формуле [2]:

$$\mathrm{QBER} = \frac{N_{\text{ошиб}}}{N_{\text{прав}} + N_{\text{ошиб}}} = \frac{R_{\text{ошиб}}}{R_{\text{прав}} + R_{\text{ошиб}}}, \tag{2}$$

где $N_{\text{ошиб}}$ – количество ошибочных битов в ключе, $N_{\text{прав}}$ – количество правильных битов, $R_{\text{ошиб}}$ – скорость передачи ошибочных битов, $R_{\text{прав}}$ – скорость передачи правильных битов. Используя выражение (2), из табл. 2 можно найти ожидаемое значение уровня ошибочных битов в «просеянном» ключе для наших экспериментальных условий по следующей формуле:

$$\mathrm{QBER} = \frac{1}{4}\sum_{i=1}^{4} f_i \Big/ \sum_{i=1}^{4}(F_1 + f_i), \tag{3}$$

где i – номер лазера в табл. 2, F_i – частота срабатываний основного фотодетектора для i-го лазера, f_i – частота срабатываний смежного фотодетектора для i-го лазера. Найденное ожидаемое значение QBER = 6 %.

Вклад в уровень ошибочных битов дают темновые импульсы фотодетекторов и несовершенство оптической системы. Вклад от темновых импульсов можно найти, подставив в уравнение (3) на место f_i значения частот темновых импульсов из табл. 1. Тогда $\mathrm{QBER}_{\text{темн}}$ = = 4,8 %. Вклад в уровень ошибочных битов вследствие несовершенства оптической системы будет равняться разности общего уровня ошибочных битов и части от темновых импульсов $\mathrm{QBER}_{\text{опт}} = \mathrm{QBER} - \mathrm{QBER}_{\text{темн}}$ = 1,2 %, что совпадает с контрастом поляризации, измеренным в непрерывном режиме.

На рис. 3 показаны экспериментальные зависимости скорости генерации «просеянного» квантового ключа и уровня ошибочных битов от времени. Каждая точка соответствует одному сеансу передачи битов длительностью 1 с. Временной интервал между сеансами – 9 с. Количество сеансов – 360, т. е. общая продолжительность приведенного периода времени работы установки составляет 3 600 с = 1 час.

Как видно из рис. 3, значение скорости генерации «просеянного» квантового ключа находится в пределах R = 10 000÷10 500 бит/с. Наблюдается небольшое отличие в 600÷1 100 бит/с от ожидаемого значения 9 400 бит/с, найденного по формуле (1). Это объясняется тем, что вклад в скорость генерации «просеянного» ключа дают и темновые импульсы фотодетекторов, суммарные значения которых в одном базисе составляют 1 000 Гц (см. табл. 1). Вклад от этих импульсов не учитывается в формуле (1), поскольку эта формула работает при условии $f_{\text{темн}} = 0$.

Уровень ошибочных битов находится в пределах QBER = 6÷7 %, что совпадает с ожидаемым значением 6 %.

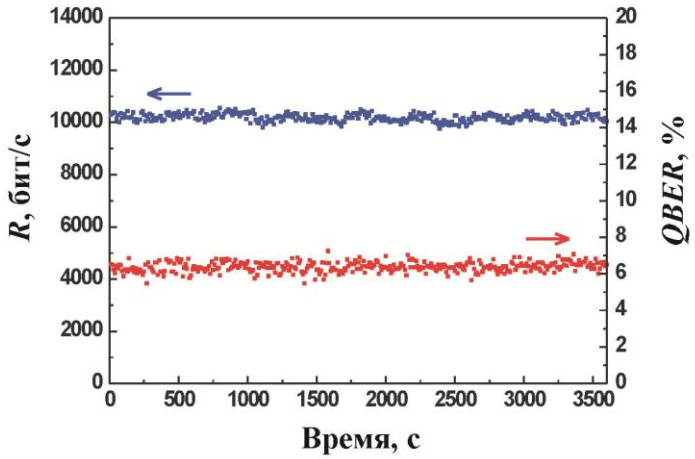

Рис. 3. Экспериментальные зависимости скорости генерации «просеянного» квантового ключа (синие символы, левая шкала) и уровня ошибочных битов (красные символы, правая шкала) от времени
Fig. 3. Experimental dependences of the “sifted” quantum key distribution rate (blue symbols, left scale) and the error bits level (red symbols, right scale) on time

Обсуждение

Для генерации секретного ключа Алиса и Боб должны применить к «просеянному» ключу классические протоколы обработки информации, а именно коррекцию ошибок и усиление конфиденциальности. Первый протокол необходим для получения Алисой и Бобом идентичного ключа, а второй – непосредственно для обеспечения его секретности. Скорость генерации секретного ключа $R_{\text{секр}}$ обратно пропорциональна относительному количеству ошибочных битов в «просеянном» ключе и описывается следующим выражением [2]:

$$R_{\text{секр}} = R\left[I(\alpha,\beta) - I^{\max}(\alpha\varepsilon) \right], \tag{4}$$

где $I(\alpha, \beta)$ – мера информации по Шеннону, которая оказывается общей у Алисы и Боба после генерации «просеянного» ключа, а $I^{\max}(\alpha, \varepsilon)$ – максимальная мера информации по Шеннону, которую может извлечь Ева в процессе подслушивания. Обе величины зависят от уровня ошибочных битов в ключе. Для нахождения $I(\alpha, \beta)$ и $I^{\max}(\alpha, \varepsilon)$ мы использовали выражения, приведенные в [2] для симметричных индивидуальных атак. Тогда для уровня ошибочных битов QBER = 6,5 % и скорости генерации «просеянного» ключа R = 10 000 бит/с скорость генерации секретного ключа будет составлять $R_{\text{секр}}$ = 4 700 бит/с.

В наших экспериментах расстояние между передатчиком и приемником составляло 20 см, и потери фотонов практически отсутствовали. Однако увеличение расстояния приведет к дифракционной расходимости лазерного луча и потерям фотонов, а также к уменьшению скорости генерации ключа и увеличению уровня ошибочных битов QBER в ключе в соответствии с формулой (2). Как уже было сказано, в общем случае при QBER > 11 % для протокола BB84 сгенерировать секретный ключ становится невозможно [2]. Одним из методов уменьшения QBER является понижение частоты темновых импульсов фотодетектора с помощью охлаждения корпуса ЛФД. В текущих экспериментах мы охлаждаем корпуса всех четырех ЛФД до 0 °С, поскольку при более низких температурах происходит намерзание инея на площадку ЛФД. Для работы при отрицательных температурах нами был изготовлен и испытан новый фотодетектор, в котором ЛФД находится в герметичном корпусе. Внутри корпуса помещается силикагель для осушения воздуха. Понижение температуры корпуса ЛФД до –20 °С привело к значительному падению частоты темновых импульсов, что дало возможность поднять напряжение питания ЛФД и увеличить эффективность регистрации одиночных фотонов до η = 48 %. С учетом стробирования частота темновых импульсов составляла $f_{\text{темн}}$ = 180 Гц.

На рис. 4 показана теоретическая зависимость скорости генерации секретного квантового ключа от коэффициента пропускания квантового канала при использовании новых фотодетекторов. Расчет сделан по формуле (4). При коэффициенте пропускания T = 0,1 скорость генерации секретного ключа составляет $R_{\text{секр}}$ = 1 000 бит/с. На этом же рисунке для сравнения приведена зависимость скорости генерации секретного ключа при использовании старых фотодетекторов. В этом случае скорость генерации секретного ключа $R_{\text{секр}}$ = 1 000 бит/с соответствует коэффициенту пропускания T = 0,5.

Коэффициент пропускания атмосферного квантового канала во многом зависит от параметров приемо-передающей оптической системы. В частности, чем больше апертура передающей и принимающей оптики, тем меньше потери фотонов, связанные с дифракционной расходимостью лазерного пучка.

В работе [14] коэффициент пропускания атмосферного квантового канала длиной 0,95 км составлял T = 0,14 при использовании телескопов с апертурой 89 мм. В работе другой группы [15] коэффициент пропускания канала длиной 23,4 км составлял T = 0,01 при использовании телескопов с апертурой 40 мм у передатчика и 250 мм у приемника.

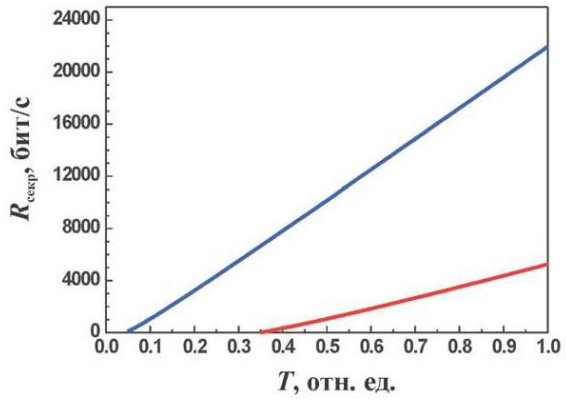

Рис. 4. Теоретические зависимости скорости генерации секретного квантового ключа от коэффициента пропускания квантового канала при использовании новых (синяя кривая) и старых (красная кривая) фотодетекторов
Fig. 4. Theoretical dependences of the secret quantum key distribution rate on the quantum channel transmission coefficient when using new (blue curve) and old (red curve) photodetectors

В наших будущих экспериментах мы планируем использовать телескопы с апертурой 150 мм. Судя по работам [14; 15], мы можем достичь на расстоянии 1÷10 км коэффициента пропускания T = 0,01÷0,1. Тогда скорость генерации секретного ключа будет составлять $R_{секр}$ = 100÷1 000 бит/с в соответствии с рис. 4.

В статье [16] скорость «просеянного» ключа при передаче фотонов со спутника на наземную станцию на расстояние 530 км составляла R = 40 кбит/с, а на расстояние 1 034 км – R = 1,2 кбит/с с уровнем ошибок QBER = 1÷3 %. Данные параметры были достигнуты за счет большой частоты следования лазерных импульсов (100 МГц), низкого уровня темнового шума однофотонных детекторов (25 Гц), высокой эффективности регистрации одиночных фотонов (50 %), применением широкоапертурных телескопов (диаметр 0,3 м у передатчика и 1 м у приемника), а также использованием протокола с «состояниями-ловушками» (decoy states) [17], в котором среднее число фотонов в импульсе составляет μ = 0,8.

Заключение

Созданная нами лабораторная система атмосферной квантово-криптографической связи стабильно проработала в течение как минимум одного часа при скорости генерации «просеянного» квантового ключа R = 10 кбит/с и уровне ошибочных битов QBER = 6,5 % при расстоянии между приемником и передатчиком 20 см и отсутствии потерь фотонов. При имеющихся параметрах фотодетекторов данную систему можно использовать для генерации секретного ключа со скоростью $R_{секр} \geq$ 1 000 бит/с в квантовых каналах с коэффициентом пропускания $T \geq$ 0,4.

Для квантовых каналов с коэффициентом пропускания T = 0,01÷0,1, с соответствующей длиной 1÷10 км потребуется увеличение частоты следования лазерных импульсов, использование фотодетекторов с более низким уровнем темновых импульсов и более высокой эффективностью однофотонной регистрации, применение широкоапертурных телескопов, а также протоколов, способных обеспечить не только секретность, но и дальность связи, например, протокол с «состояниями-ловушками» (decoy states) [17]. В данном протоколе для генерации квантового ключа используются лазерные импульсы со средним числом фотонов в импульсе μ ~ 1 [16], что может значительно увеличить расстояние между Алисой и Бобом.

Список литературы

1. **Wooters W. K., Zurek W. H.** A Single Quantum Cannot Be Cloned. *Nature*, 1982, vol. 299, pp. 802–803.
2. **Gisin N., Ribordy G., Tittel W., Zbinden H.** Quantum cryptography. *Rev. of Mod. Phys.*, 2002, vol. 74, pp. 145–195.

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, pp. 175–179.
4. **Bennet C. H., Bessette F., Brassard G., Salvail L.** Experimental quantum cryptography. *J. Cryptology*, 1992, vol. 5, pp. 3–28.
5. **Boaron A. et al.** Secure Quantum Key Distribution over 421 km of Optical Fiber. *Phys. Rev. Lett.*, 2018, vol. 121, 190502.
6. **Chen J.-P. et al.** Sending-or-Not-Sending with Independent Lasers: Secure Twin-Field Quantum Key Distribution over 509 km. *Phys. Rev. Lett.*, 2020, vol. 124, 070501.
7. **Liao S.-K. et al.** Satellite-Relayed Intercontinental Quantum Network. *Phys. Rev. Lett.*, 2018, vol. 120, 030501.
8. **Duplinskiy A. V. et al.** Quantum-Secured Data Transmission in Urban Fiber-optics Communication Lines. *Journal of Russian Laser Research*, 2018, vol. 39, p. 113.
9. **Глейм А. В. и др.** Многоузловая квантовая сеть на основе технологии квантовой коммуникации на боковых частотах // Проблемы техники и технологий коммуникаций: Сб. тр. XVIII Междунар. науч.-техн. конф. Казань, 2017. С. 65–66.
10. **Kynev S. M., Chistyakov V. V., Smirnov S. V., Volkova K. P., Egorov V. I., Gleim A. V.** Free-space subcarrier wave quantum communication. *J. Phys.: Conf. Ser.*, 2017, vol. 917, 052003.
11. **Kravtsov K. S., Radchenko I. V., Kulik S. P., Molotkov S. N.** Relativistic quantum key distribution system with one-way quantum communication. *Scientific Reports*, 2018, no. 8, 6102.
12. **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.
13. **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.
14. **Buttler W. T. et al.** Practical Free-Space Quantum Key Distribution over 1 km. *Phys. Rev. Lett.*, 1998, vol. 81, no. 15, pp. 3283–3286.
15. **Kurtsiefer C. et al.** Quantum Cryptography: A step towards global key distribution. *Nature*, 2002, vol. 419, p. 450.
16. **Sheng-Kai Liao et al.** Satellite-to-ground quantum key distribution. *Nature*, 2017, vol. 549, pp. 43–47.
17. **Hwang Won-Young.** Quantum Key Distribution with High Loss: Toward Global Secure Communication. *Phys. Rev. Lett.*, 2003, vol. 91, 057901.

References

1. **Wooters W. K., Zurek W. H.** A Single Quantum Cannot Be Cloned. *Nature*, 1982, vol. 299, pp. 802–803.
2. **Gisin N., Ribordy G., Tittel W., Zbinden H.** Quantum cryptography. *Rev. of Mod. Phys.*, 2002, vol. 74, pp. 145–195.
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, pp. 175–179.
4. **Bennet C. H., Bessette F., Brassard G., Salvail L.** Experimental quantum cryptography. *J. Cryptology*, 1992, vol. 5, pp. 3–28.
5. **Boaron A. et al.** Secure Quantum Key Distribution over 421 km of Optical Fiber. *Phys. Rev. Lett.*, 2018, vol. 121, 190502.
6. **Chen J.-P. et al.** Sending-or-Not-Sending with Independent Lasers: Secure Twin-Field Quantum Key Distribution over 509 km. *Phys. Rev. Lett.*, 2020, vol. 124, 070501.

7. **Liao S.-K. et al.** Satellite-Relayed Intercontinental Quantum Network. *Phys. Rev. Lett.*, 2018, vol. 120, 030501.
8. **Duplinskiy A. V. et al.** Quantum-Secured Data Transmission in Urban Fiber-optics Communication Lines. *Journal of Russian Laser Research*, 2018, vol. 39, p. 113.
9. **Gleim A. V. et al.** Multi-node quantum network based on quantum communication side fre quencies technology. In: Proc. of XVIII Int. sci.-tech. conference "Problems of technics and technologies of communications". Kazan, 2017, pp. 65–66. (in Russ.)
10. **Kynev S. M., Chistyakov V. V., Smirnov S. V., Volkova K. P., Egorov V. I., Gleim A. V.** Free-space subcarrier wave quantum communication. *J. Phys.: Conf. Ser.*, 2017, vol. 917, 052003.
11. **Kravtsov K. S., Radchenko I. V., Kulik S. P., Molotkov S. N.** Relativistic quantum key distribution system with one-way quantum communication. *Scientific Reports*, 2018, no. 8, 6102.
12. **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, pp. 453–461. (in Russ.)
13. **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 information. *Siberian Journal of Physics*, 2018, vol. 13, no. 4, pp. 91–104. (in Russ.)
14. **Buttler W. T. et al.** Practical Free-Space Quantum Key Distribution over 1 km. *Phys. Rev. Lett.*, 1998, vol. 81, no. 15, pp. 3283–3286.
15. **Kurtsiefer C. et al.** Quantum Cryptography: A step towards global key distribution. *Nature*, 2002, vol. 419, p. 450.
16. **Sheng-Kai Liao et al.** Satellite-to-ground quantum key distribution. *Nature*, 2017, vol. 549, pp. 43–47.
17. **Hwang Won-Young.** Quantum Key Distribution with High Loss: Toward Global Secure Communication. *Phys. Rev. Lett.*, 2003, vol. 91, 057901.

Информация об авторах

Александр Владимирович Коляко, инженер
WoS Researcher ID AAD-8523-2021
Scopus Author ID 56369246900
Александр Сергеевич Плешков, младший научный сотрудник
WoS Researcher ID ABG-6199-2020
Scopus Author ID 56401232600
Денис Борисович Третьяков, кандидат физико-математических наук
WoS Researcher ID AAD-9791-2021
Scopus Author ID 6507147052
Василий Матвеевич Энтин, кандидат физико-математических наук
Игорь Ильич Рябцев, доктор физико-математических наук, член-корреспондент РАН
Scopus Author ID 7004241094
Игорь Георгиевич Неизвестный, доктор физико-математических наук, член-корреспондент РАН

Information about the Authors

Alexander V. Kolyako, Engineer
WoS Researcher ID AAD-8523-2021
Scopus Author ID 56369246900
Alexander S. Pleshkov, Junior Research Fellow
WoS Researcher ID ABG-6199-2020
Scopus Author ID 56401232600
Denis B. Tretyakov, Candidate of Science (Physics and Mathematics)
WoS Researcher ID AAD-9791-2021
Scopus Author ID 6507147052
Vasiliy M. Entin, Candidate of Science (Physics and Mathematics)
Igor I. Ryabtsev, Doctor of Science (Physics and Mathematics), Corresponding Member of RAS
Scopus Author ID 7004241094
Igor G. Neizvestny, Doctor of Science (Physics and Mathematics), Corresponding Member of RAS

Статья поступила в редакцию 26.02.2021;
одобрена после рецензирования 01.04.2021; *принята к публикации 01.04.2021*
The article was submitted 26.02.2021;
approved after reviewing 01.04.2021; *accepted for publication 01.04.2021*