УДК 535.14

ИССЛЕДОВАНИЕ ДОЛГОВРЕМЕННОЙ СТАБИЛЬНОСТИ ГЕНЕРАЦИИ КВАНТОВОГО КЛЮЧА В СВОБОДНОМ ПРОСТРАНСТВЕ НА РАССТОЯНИИ 20 М В СХЕМЕ С ПОЛЯРИЗАЦИОННЫМ КОДИРОВАНИЕМ

© **А. С. Плешков, А. В. Коляко, Д. Б. Третьяков, И. И. Рябцев, И. Г. Неизвестный**

Институт физики полупроводников им. А. В. Ржанова СО РАН, 630090, г. Новосибирск, просп. Академика Лаврентьева, 13
E-mail: dtret@isp.nsc.ru

Экспериментально исследована работа созданной нами атмосферной установки для генерации квантового ключа, использующей протокол квантовой криптографии BB84 и поляризационное кодирование. Скорость генерации «просеянного» квантового ключа и уровень ошибочных битов в нём оставались постоянными в течение 1 ч и равнялись 7558 ± 83 бит/с и $5{,}1 \pm 0{,}84$ % соответственно при расстоянии между передатчиком и приёмником 20 м. Для приведённых параметров установки рассчитан минимально возможный коэффициент пропускания квантового канала, обеспечивающий секретность квантового ключа.

Ключевые слова: квантовые коммуникации, протокол BB84, поляризационное кодирование, детекторы одиночных фотонов.

DOI: 10.15372/AUT20240105
EDN: OGYMUW

Введение. В однофотонных квантовых системах связи секретность передаваемой информации обеспечивается законами квантовой механики [1]. С помощью передачи одиночных фотонов по квантовому каналу (оптоволоконной или атмосферной линии связи) генерируется секретный двоичный ключ, который известен только отправителю (Алисе) и получателю (Бобу). Затем Алиса, используя данный ключ, зашифровывает своё сообщение и передаёт его Бобу по открытому каналу [2].

В базовом квантово-криптографическом протоколе BB84 [3, 4] для генерации секретного двоичного ключа используются одиночные фотоны, у которых поляризации ориентированы под углами 0, 90° (вертикально-горизонтальный базис) и ±45° (диагональный базис) по отношению к некоторой оси координат. В каждом базисе поляризационным состояниям присваиваются двоичные значения «0» и «1». Далее Алиса случайным образом выбирает одну из четырёх поляризаций фотона и посылает фотон Бобу по квантовому каналу. Боб измеряет поляризацию полученного фотона в произвольно выбранном базисе, и таким образом генерируется «сырой» ключ в виде случайной последовательности битов. Затем по открытому каналу связи сравниваются базисы передачи и приёма фотонов, отбрасываются те биты, для которых базисы не совпали, и в результате получается так называемый просеянный квантовый ключ. Этот ключ всегда содержит некоторое количество ошибок, обусловленных ложными (темновыми) срабатываниями детекторов одиночных фотонов. Поэтому далее проводят процедуры коррекции ошибок и усиления конфиденциальности путём сравнения части квантового ключа по открытому каналу связи. Таким образом, в конечном итоге Алиса и Боб формируют абсолютно секретный квантовый ключ.

К настоящему времени иностранные группы реализовали генерацию квантового ключа на расстоянии 1000 км по оптоволоконным линиям связи [5]. Максимальная достигнутая длина атмосферно-космических квантовых линий связи через спутники состав-

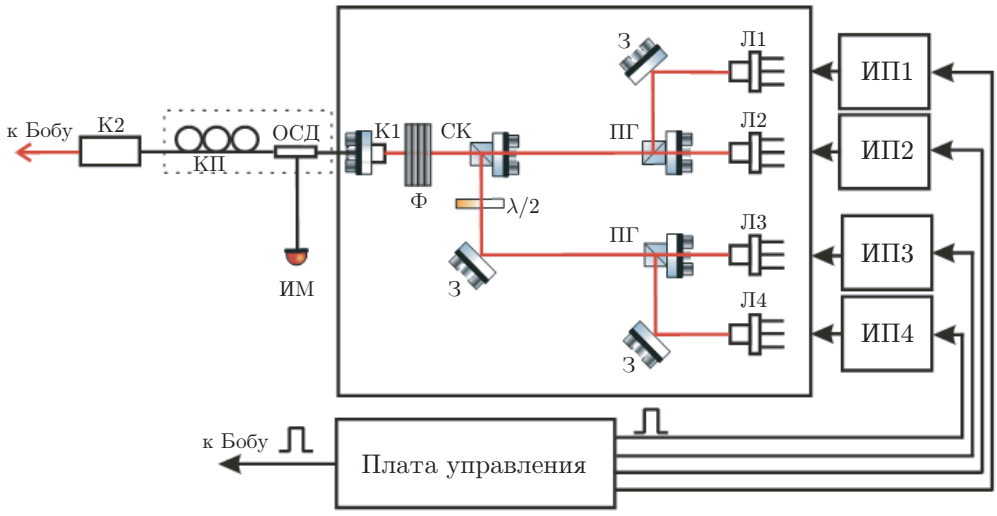

Рис. 1. Общая схема передатчика (Алисы): Л1, Л2, Л3, Л4 — лазеры; ИП1, ИП2, ИП3, ИП4 — источники питания лазеров; З — зеркала; ПГ — призмы Глана; $\lambda/2$ — полуволновая пластинка; СК — светоделительный кубик (50 : 50); Ф — набор фильтров; К1, К2 — коллиматоры; ОСД — оптоволоконный светоделитель (50 : 50); ИМ — измеритель мощности; КП — контроллер поляризации. Пунктирной линией обозначен теплоизоляционный кожух

ляет 7600 км [6]. В России к настоящему времени созданы оптоволоконные квантово-криптографические системы, работающие на расстоянии до 143 км [7, 8]. Квантовые линии связи в свободном пространстве реализованы пока на расстояниях 20 м на основе метода боковых частот [9] и 180 м с применением протокола релятивистской квантовой криптографии [10].

В 2003 г. нашей авторской группой была создана первая лабораторная экспериментальная установка для генерации квантового ключа в свободном пространстве [11], использующая протокол BB84 и поляризационное кодирование. На ней был выполнен ряд экспериментов по отработке основных методик детектирования одиночных поляризованных фотонов и генерации квантового ключа [12–18]. В дальнейшем установка была существенно модернизирована [19] для увеличения быстродействия и вероятности регистрации фотонов. В результате скорость генерации просеянного квантового ключа на расстоянии между передатчиком и приёмником 20 см была увеличена до 10 кбит/с, а также улучшена долговременная стабильность работы установки.

Целью представленной работы являлось исследование долговременной стабильности работы нашей атмосферной квантово-криптографической экспериментальной установки на расстоянии между передатчиком и приёмником, увеличенном до 20 м. Для этого были улучшены параметры фотодетекторов (ФД), изготовлена оптическая система передачи и приёма лазерного излучения и модернизирована управляющая электроника. Насколько нам известно, расстояние 20 м ещё не было достигнуто в России при генерации квантового ключа в свободном пространстве с использованием схемы поляризационного кодирования.

Экспериментальная установка. На рис. 1 показана общая схема установки передатчика. В качестве источников одиночных 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 мог работать как в импульсном, так и в непрерывном режимах. Длительность лазерных импульсов составляла 5 нс. Поляризация излучения каждого лазера выставлялась

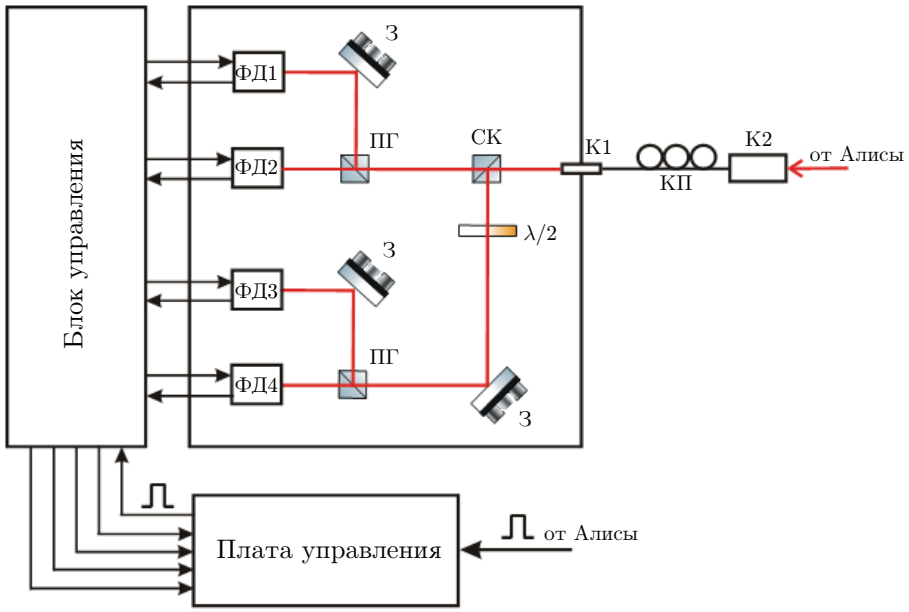

Рис. 2. Общая схема приёмника (Боба): ФД1, ФД2, ФД3, ФД4 — фотодетекторы; З — зеркала; ПГ — призмы Глана; $\lambda/2$ — полуволновая пластинка; СК — светоделительный кубик (50 : 50); К1, К2 — коллиматоры; КП — контроллер поляризации

в соответствии с протоколом BB84. Лучи всех лазеров совмещались с помощью системы зеркал, фокусировались и заводились в одномодовый оптоволоконный кабель (тип оптического волокна 780HP с рабочей длиной волны 780–970 нм и длиной волны отсечки 730 ± 30 нм). На выходе кабеля стоял коллиматор, из которого выходил лазерный пучок диаметром 7,5 мм и посылался к приёмному 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 выходным коллиматором. Для подстройки расходимости лазерного луча имелась возможность регулировки расстояния между линзой коллиматора и торцом коннектора оптоволоконного кабеля. Расстояние от выходного коллиматора передатчика К2 до входного коллиматора приёмника составляло 20 м. Для генерации квантового ключа мощность излучения лазеров передающего узла ослаблялась до однофотонного уровня. В качестве ослабителей использовались четыре калиброванных поглощающих нейтральных оптических фильтра, которые устанавливались перед оптическим волокном.

На рис. 2 показана общая схема установки приёмника. Лазерное излучение, идущее от Алисы, попадало на коллиматор Боба и по одномодовому оптоволоконному кабелю направлялось в оптическую схему приёмника (тип оптического волокна такой же, как у Алисы). Использование заведения в оптическое волокно было обусловлено техническим удобством и достаточной эффективностью передачи излучения в уже настроенную оптическую схему Боба. Заведение излучения в оптоволоконный кабель Боба осуществлялось вручную с помощью юстировочных головок, к которым крепились коллиматоры, и оптических столиков с вертикальным и горизонтальным перемещением. Также имелась возможность регулировки расстояния между линзой коллиматора и торцом коннектора оптоволоконного кабеля для эффективного заведения излучения в оптическое волокно. Поскольку поляризация излучения искажается при прохождении по оптическому волокну, на кабеле был установлен контроллер поляризации для подстройки поляризации фотонов. В оптической схеме приёмника лазерное излучение разделялось на два луча светодели-

тельным 50 : 50 кубиком, один из которых потом направлялся 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. Основу трёх однофотонных детекторов составляли кремниевые лавинные фотодиоды (ЛФД) C30902S производства фирмы EG&G Optoelectronics и одного детектора — ЛФД SAP500S2 производства фирмы Laser Components (последний был использован для замены вышедшего ранее из строя четвёртого ЛФД C30902S). 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. Выходные импульсы с каждого ЛФД проходили через усилитель, а затем посылались на блок стробирования (входит в блок управления на рис. 2), в котором дискриминировались по амплитуде для отсечения паразитных наводок и стробировались для уменьшения количества темновых импульсов. В блоке стробирования сигналы с фотодетекторов преобразовывались в стандартные TTL-импульсы и направлялись на вход счётчика импульсов. Частота темновых импульсов уменьшалась также за счёт охлаждения ЛФД до температуры -20 °C элементами Пельтье. Лавинные фотодиоды находились в герметичных корпусах, внутри которых помещался силикагель для осушки воздуха и предотвращения намерзания инея на входное окно ЛФД. Более подробное описание оптической схемы передатчика и приёмника приведено в [19].

Управление экспериментом осуществлялось отладочной платой на основе программируемой логической интегральной схемы Xilinx Spartan-6 с семисегментным индикатором (см. рис. 1). Плата запускала лазерные импульсы и одновременно отправляла импульсы синхронизации через электрический кабель (витая пара) на такую же плату приёмника, располагающуюся возле установки Боба. Запуск лазерных импульсов производился в двух режимах: 1) запуск отдельного лазера для предварительной настройки системы; 2) запуск случайного лазера для генерации квантового ключа. Согласно протоколу BB84, после генерации «сырого» квантового ключа Алиса и Боб сверяют базисы для последующего формирования просеянного ключа, а затем раскрывают и сверяют часть ключа для оценки уровня ошибочных битов. Поскольку наша установка является экспериментальной, данные процедуры были проведены в реальном времени. Информация о номере запущенного лазера передавалась Алисой Бобу по электрическому кабелю вместе с импульсом синхронизации. На рис. 3 показаны временны́е диаграммы импульсов. Вначале следует импульс синхронизации, затем передаётся в двоичном коде число от 0 до 3, соответствующее номеру лазера: лазер 1 — «0», лазер 2 — «1» и т. д.

Аналогичная электронная плата Боба на основе Xilinx Spartan-6 после приёма импульса синхронизации запускала блок стробирования и осуществляла счёт TTL-импульсов от срабатывания фотодетекторов (см. рис. 2). Количество зарегистрированных импульсов за определённое время выводилось на индикатор для каждого фотодетектора. Также индикатор показывал скорость генерации просеянного ключа и количество ошибочных битов. Вся система позволяла изменять задержку и совмещать лазерные и строб-импульсы во времени с точностью 2,5 нс.

Настройка системы. Первый этап настройки системы проводился с лазерами, работающими в непрерывном режиме. Излучение передатчика подавалось на приёмник по короткому оптоволоконному кабелю. 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. Более подробное описание данного этапа настройки приведено в [19]. На втором этапе измерялись основные параметры, и система переключалась в импульсный режим работы лазеров. Тактовые импульсы подавались на один из четырёх лазеров, и измерялась частота срабатывания соответствующего фотодетектора.

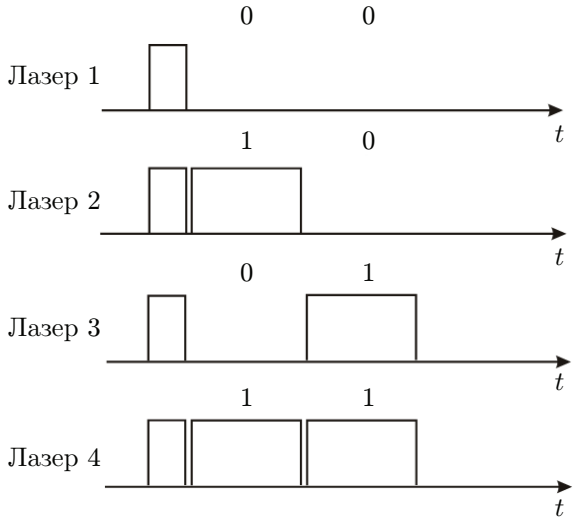

Рис. 3. Временны́е диаграммы импульсов, передаваемых Алисой Бобу по электрическому кабелю. Длительность импульса синхронизации — 7,5 нс, длительности импульсов передачи данных о номере лазера — 25 нс

Таблица 1

Измеренные параметры фотодетекторов

№ ФД	$f_{\text{темн}}$, Гц	$f_{\text{лазер+темн}}$, Гц	$\varepsilon_{\text{темн}}$, %	η, %
1	385 ± 15	17903 ± 49	$2{,}15 \pm 0{,}09$	$35{,}04 \pm 0{,}13$
2	263 ± 13	16881 ± 67	$1{,}58 \pm 0{,}1$	$33{,}24 \pm 0{,}16$
3	215 ± 12	13135 ± 152	$1{,}64 \pm 0{,}11$	$25{,}84 \pm 0{,}33$
4	26 ± 2	5835 ± 45	$0{,}45 \pm 0{,}04$	$11{,}62 \pm 0{,}1$

В табл. 1 приведены полученные значения параметров фотодетекторов. Во второй колонке приводятся частоты темновых импульсов $f_{\text{темн}}$ фотодетекторов (лазерные импульсы не подаются), в третьей — частоты срабатывания фотодетекторов $f_{\text{лазер+темн}}$ при включении одного основного лазера для каждого фотодетектора. Например, для ФД1 включён лазер 1, для ФД2 — лазер 2 и т. д. В четвёртой колонке представлен уровень темновых срабатываний $\varepsilon_{\text{темн}}$, найденный по формуле $\varepsilon_{\text{темн}} = (f_{\text{темн}}/f_{\text{лазер+темн}}) \cdot 100$ %. В пятой колонке приводится эффективность регистрации одного фотона, найденная по формуле $\eta = (f_{\text{лазер+темн}} - f_{\text{темн}})/(0{,}5\mu f_{\text{такт}}) \cdot 100$ %, где $\mu = 0{,}1$ — установленное нами среднее число фотонов в лазерном импульсе, $f_{\text{такт}} = 10^6$ Гц — частота тактовых импульсов. Множитель 0,5 в знаменателе возникает из-за того, что лучи лазеров делятся пополам на светоделительном кубике. В табл. 1 приведены максимальные значения эффективности регистрации фотодетекторов. У ФД4 (SAP500S2) данный параметр оказался значительно ниже, чем у остальных фотодетекторов (C30902S). В то же время уровень темновых срабатываний у ФД4 также в несколько раз ниже.

На третьем этапе лазеры опять переключались в непрерывный режим для измерения коэффициента пропускания квантового канала длиной 20 м для излучения каждого лазера. Данный коэффициент измерялся как отношение мощности излучения на выходном конце оптического кабеля Боба к мощности излучения после выходного коллиматора Алисы K2 (см. рис. 1). Измеренные значения коэффициента пропускания составили для 1-го и 2-го лазера $T_{1,2} = 0{,}5 \pm 0{,}05$, для 3-го — $T_3 = 0{,}59 \pm 0{,}05$ и для 4-го — $T_4 = 0{,}61 \pm 0{,}05$. Различие в значениях коэффициента пропускания для разных лазеров мы связываем с небольшим

Таблица 2

Частоты срабатывания фотодетекторов при включении одного из лазеров и при расстоянии 20 м между передатчиком и приёмником

№ лазера	f(ФД1), Гц	f(ФД2), Гц	f(ФД3), Гц	f(ФД4), Гц
1	9109 ± 18	334 ± 10	4450 ± 23	1497 ± 28
2	522 ± 19	7424 ± 24	3049 ± 29	1457 ± 31
3	2408 ± 10	3162 ± 33	6390 ± 26	67 ± 2
4	4910 ± 11	3330 ± 35	330 ± 10	2692 ± 89

отличием в длинах волн лазеров, которое приводит как к разной расходимости лучей, так и разной эффективности заведения излучения в оптическое волокно.

Окончательная настройка всей системы проводилась в импульсном режиме на расстоянии между приёмником и передатчиком 20 м. Тактовые импульсы подавались на один из четырёх лазеров, и измерялась частота срабатывания каждого фотодетектора. Результаты измерения приведены в табл. 2, согласно которой 1-й и 2-й лазеры составляли вертикально-горизонтальный базис, 3-й и 4-й — диагональный. Поляризация излучения 1-го лазера была вертикальной, 2-го — горизонтальной. Поляризация излучения 3-го лазера выставлялась под углом $+45°$, 4-го — под углом $-45°$ по отношению к вертикальной оси. Соответственно, максимальное количество срабатываний приходилось на основные для каждого лазера фотодетекторы (кроме 4-го лазера, у которого основным является ФД4 с низкой эффективностью регистрации), а минимальное — на смежные фотодетекторы в этом же базисе.

Исследование параметров генерации просеянного квантового ключа. Управляющая плата Алисы в режиме генерации просеянного квантового ключа подавала тактовые импульсы с частотой следования 1 МГц на запуск одного из четырёх лазеров в случайной последовательности и на запуск платы Боба. Время одного сеанса равнялось 1 с. Среднее число фотонов в лазерном импульсе составляло $\mu = 0{,}1$. После каждого тактового импульса плата Боба проверяла срабатывание всех четырёх 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 количество ошибочных битов, равное количеству срабатываний смежных фотодетекторов из того же базиса.

Скорость генерации просеянного ключа R для протокола BB84 при среднем числе фотонов в импульсе $\mu \ll 1$ можно оценить по формуле $R = 0{,}5 f_{\text{такт}} \mu \eta T$ [18], где η — эффективность регистрации детекторами одного фотона, T — коэффициент пропускания квантового канала. Множитель 0,5 возникает, поскольку для получения просеянного квантового ключа отбрасывается примерно половина данных при несовпадении базисов Алисы и Боба. В случае, когда эффективность регистрации фотодетекторов и коэффициент пропускания квантового канала для каждого лазера разные, ожидаемую скорость генерации просеянного ключа можно найти по формуле $R = 0{,}5 f_{\text{такт}} \mu \cdot 0{,}25(\eta_1 T_1 + \eta_2 T_2 + \eta_3 T_3 + \eta_4 T_4)$, где η_i — эффективность регистрации i-го фотодетектора, а множитель 0,25 — вероятность случайного запуска каждого лазера. В нашем случае $R = 7059 \pm 716$ бит/с.

Скорость генерации просеянного ключа также можно оценить, используя значения табл. 2, по формуле $R = 0{,}25 \sum_{i=1}^{4} (F_i + f_i)$, где F_i — частота срабатываний основного

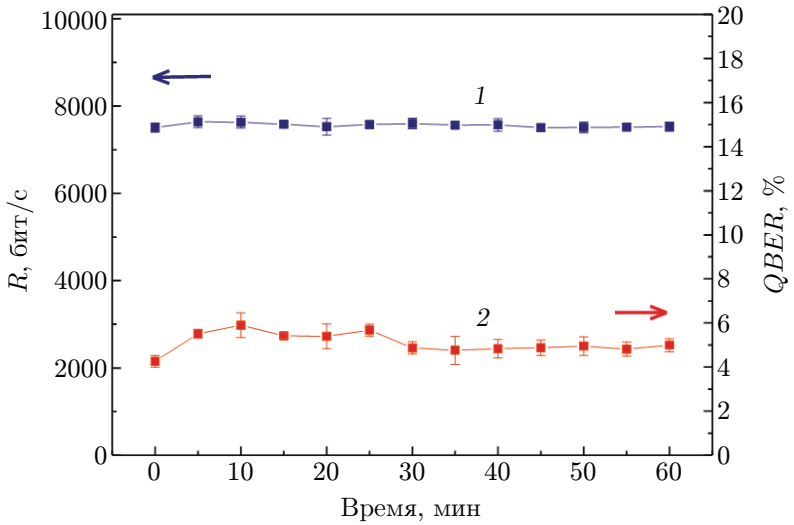

Рис. 4. Экспериментальные зависимости скорости генерации просеянного квантового ключа (кривая *1*, левая шкала) и уровня ошибочных битов (кривая *2*, правая шкала) от времени

фотодетектора для i-го лазера, f_i — частота срабатываний смежного фотодетектора для i-го лазера. Получаем $R = 6717 \pm 50$ бит/с. Уровень ошибочных битов в просеянном ключе ($QBER$ – Quantum Bit Error Rate) находится по следующей формуле [2]:

$$QBER = \frac{N_{\text{ошиб}}}{N_{\text{прав}} + N_{\text{ошиб}}} = \frac{R_{\text{ошиб}}}{R_{\text{прав}} + R_{\text{ошиб}}}, \tag{1}$$

где $N_{\text{ошиб}}$ — количество ошибочных битов в ключе, $N_{\text{прав}}$ — количество правильных битов, $R_{\text{ошиб}}$ — скорость передачи ошибочных битов и $R_{\text{прав}}$ — скорость передачи правильных битов. Тогда с помощью табл. 2 можно найти ожидаемое значение уровня ошибочных битов в просеянном ключе для наших экспериментальных условий по следующей формуле, которая следует из выражения (1): $QBER = \sum_{i=1}^{4} f_i \Big/ \sum_{i=1}^{4} (F_i + f_i)$. Найденное значение $QBER = 4{,}66 \pm 0{,}19$ %.

На рис. 4 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 фиксируемыми сеансами — 5 мин. Количество сеансов 12, т. е. общая продолжительность приведённого периода времени работы установки составляет 1 ч.

Как видно из рис. 4, значение скорости генерации просеянного квантового ключа R находится в пределах 7558 ± 83 бит/с, а уровень ошибочных битов $QBER$ — в пределах $5{,}1 \pm 0{,}84$ %, что в среднем совпадает с ожидаемым значением $4{,}66 \pm 0{,}19$ %. Измеренная скорость генерации ключа превышает примерно на 800 бит/с ожидаемое значение 6717 бит/с. Причина данного расхождения пока не выяснена. Возможно, плата Боба с малой вероятностью ошибается в измерении номера лазера, что приводит к небольшому завышению как количества всех битов в ключе, так и количества ошибочных битов. При этом их соотношение при подсчёте $QBER$ соответствует правильному значению. На данном этапе нашей исследовательской работы отличие в ожидаемой и измеренной скорости генерации просеянного ключа на 10 % не является существенным. В целом результаты эксперимента продемонстрировали стабильную работу нашей установки.

Обсуждение. Для генерации секретного ключа Алиса и Боб должны применить к просеянному ключу классические протоколы обработки информации — коррекцию ошибок и усиление конфиденциальности. Первый протокол необходим для получения Алисой и Бобом идентичного ключа, а второй — 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]:

$$R_{\text{секр}} = R[I(\alpha, \beta) - I^{\max}(\alpha, \varepsilon)], \tag{2}$$

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 данные величины зависят от уровня ошибочных битов в ключе. Для нахождения $I(\alpha, \beta)$ и $I^{\max}(\alpha, \varepsilon)$ мы использовали выражения, приведённые в [2] для симметричных индивидуальных атак. Тогда для уровня ошибочных битов 5 % и скорости генерации просеянного ключа $R =$ 7500 бит/с скорость генерации секретного ключа будет составлять $R_{\text{секр}} = 4200$ бит/с.

В наших предыдущих экспериментах расстояние между передатчиком и приёмником составляло 20 см и потери фотонов практически отсутствовали. Уровень ошибочных битов и скорость генерации просеянного ключа составляли 6,5 % и $R = 10$ кбит/с соответственно, а скорость генерации секретного ключа — $R_{\text{секр}} = 4700$ бит/с. Увеличение расстояния до 20 м привело бы к потерям примерно половины фотонов (измеренный коэффициент пропускания нашего квантового канала длиной 20 м равен 0,5) и, следовательно, к увеличению $QBER$ в ключе до 13 % в соответствии с формулой (1). В общем случае при $QBER > 11$ % для протокола BB84 сгенерировать секретный ключ становится невозможно [2]. Для уменьшения $QBER$ температура ЛФД была понижена до -20 °C, что привело к значительному падению частоты темновых импульсов, дало возможность поднять напряжение питания ЛФД и увеличить эффективность регистрации одиночных фотонов.

Из табл. 2 видно, что частоты срабатывания фотодетекторов в вертикально-горизонтальном базисе (ФД1 и ФД2) примерно в два раза превышают частоты срабатывания фотодетекторов в диагональном (ФД3 и ФД4), что связано с разной эффективностью регистрации фотодетекторов. Подслушиватель может воспользоваться этим и посылать фотоны в два раза чаще в вертикально-горизонтальном базисе, чтобы увеличить количество перехваченной информации. Поэтому в будущем необходимо заменить ФД4 на фотодетектор с более высокой эффективностью регистрации и выровнять частоты срабатывания в каждом базисе.

С помощью формулы (2) и значений параметров, приведённых в табл. 1, можно рассчитать наименьший коэффициент пропускания квантового канала в нашей системе для условно минимальной скорости генерации секретного квантового ключа 500 бит/с, который будет составлять 0,25. Данное значение соответствует расстоянию в несколько сотен метров, как показано в работе [20], где в качестве передающей и принимающей оптических систем использовались телескопы с апертурой 200 мм. В наших будущих экспериментах мы планируем использовать телескопы с апертурой 150 мм. Для повышения скорости генерации квантового ключа будет увеличена частота следования лазерных импульсов до 10 МГц, что также даст возможность в дальнейшем работать с квантовым каналом длиной 1 км и более. Кроме того, электрический кабель, по которому передавался импульс синхронизации и классическая информация, будет заменён на атмосферный оптический канал связи на длине волны, отличной от 780 нм.

Заключение. Созданная нами лабораторная система атмосферной квантово-криптографической связи стабильно проработала в течение как минимум одного часа при скорости генерации просеянного квантового ключа 7558 ± 83 бит/с и уровне ошибочных

битов $5{,}1 \pm 0{,}84$ % при расстоянии 20 м между передатчиком и приёмником. При имеющихся параметрах фотодетекторов её можно использовать для генерации секретного ключа, используя квантовый канал с коэффициентом пропускания не менее 0,25. Для дальнейшего увеличения расстояния между Алисой и Бобом потребуется повышать частоту следования лазерных импульсов. Для реализации квантово-криптографической связи на сотни километров необходимо применять протоколы, способные обеспечить не только секретность, но и дальность связи, например, протокол с «состояниями-ловушками» (decoy states) [21]. В данном протоколе для генерации квантового ключа используются лазерные импульсы со средним числом фотонов в импульсе $\mu \sim 1$ [22], что может значительно увеличить расстояние между Алисой и Бобом.

Финансирование. Исследование выполнено за счёт гранта Российского научного фонда № 23-29-00472, https://rscf.ru/project/23-29-00472/.

СПИСОК ЛИТЕРАТУРЫ

1. **Wooters W. K., Zurek W. H.** A single quantum cannot be cloned // Nature. 1982. **299**. P. 802–803.
2. **Gisin N., Ribordy G., Tittel W. et al.** Quantum cryptography // Rev. Mod. Phys. 2002. **74**, Iss. 1. P. 145–195.
3. **Bennet C. H., Brassard G.** Quantum cryptography: Public key distribution and coin tossing // Proc. of the IEEE Int. Conf. Comput. Systems and Sign. Process. Bangalore, India, 10–12 Dec., 1984. P. 175–179.
4. **Bennet C. H., Bessette F., Brassard G. et al.** Experimental quantum cryptography // Journ. Cryptology. 1992. **5**, Iss. 1. P. 3–28.
5. **Liu Y., Zhang W. J., Jiang C. et al.** Experimental twin-field quantum key distribution over 1000 km fiber distance // Phys. Rev. Lett. 2023. **130**, Iss. 21. 210801.
6. **Liao S.-K., Cai W.-Q., Handsteiner J. et al.** Satellite-relayed intercontinental quantum network // Phys. Rev. Lett. 2018. **120**. 030501.
7. **Duplinskiy A. V., Kiktenko E. O., Pozhar N. O. et al.** Quantum-secured data transmission in urban fiber-optics communication lines // Journ. Russ. Laser Res. 2018. **39**, Iss. 2. P. 113–119.
8. **Bannik O. I., Gilyazov L. R., Gleim A. V. et al.** Subcarrier wave quantum key distribution over 143 km intercity fiber link // Тез. докл. II конференции по фотонике и квантовым технологиям. Казань: ИД «МеДДоК», 2020. С. 35–36.
9. **Kynev S. M., Chistyakov V. V., Smirnov S. V. et al.** Free-space subcarrier wave quantum communication // Journ. Phys.: Conf. Ser. 2017. **917**, Iss. 5. 052003.
10. **Kravtsov K. S., Radchenko I. V., Kulik S. P. et al.** Relativistic quantum key distribution system with one-way quantum communication // Sci. Rep. 2018. **8**. 6102.
11. **Курочкин В. Л., Рябцев И. И., Неизвестный И. Г.** Генерация квантового ключа на основе кодирования поляризационных состояний фотонов // Оптика и спектроскопия. 2004. **96**, № 5. С. 772–776.
12. **Курочкин В. Л., Рябцев И. И., Неизвестный И. Г.** Экспериментальная установка для квантовой криптографии с одиночными поляризованными фотонами // ЖТФ. 2005. **75**, № 6. С. 54–58.
13. **Курочкин В. Л., Рябцев И. И., Неизвестный И. Г.** Квантовая криптография и генерация квантового ключа с использованием одиночных фотонов // Микроэлектроника. 2006. **35**, № 1. С. 41–47.
14. **Курочкин В. Л., Зверев А. В., Курочкин Ю. В. и др.** Экспериментальные исследования в области квантовой криптографии // Микроэлектроника. 2011. **40**, № 4. С. 264–273.

15. **Рябцев И. И., Бетеров И. И., Третьяков Д. Б. и др.** Экспериментальная квантовая информатика с одиночными атомами и фотонами // Вестн. РАН. 2013. **83**, № 7. С. 606–615.
16. **Kolyako A. V., Neizvestny I. G., Kurochkin V. L.** Investigation the bit rate of quantum key using Si single photon detectors // Journ. Phys.: Conf. Ser. 2014. **541**. 012046.
17. **Курочкин В. Л., Коляко А. В.** Исследование скорости распределения квантового ключа через открытое пространство в зависимости от условий передачи // Изв. РАН. Сер. Физическая. 2016. **80**, № 1. С. 6–9.
18. **Третьяков Д. Б., Коляко А. В., Плешков А. С. и др.** Генерация квантового ключа в однофотонных системах связи // Автометрия. 2016. **52**, № 5. С. 44–54. DOI: 10.15372/AUT20160507.
19. **Коляко А. В., Плешков А. С., Третьяков Д. Б. и др.** Исследование долговременной стабильности генерации однофотонного квантового ключа в схеме с поляризационным кодированием // СФЖ. 2021. **16**, № 2. С. 81–93.
20. **Bienfang J. C., Gross A. J., Mink A. et al.** Quantum key distribution with 1.25 Gbps clock synchronization // Opt. Express. 2004. **12**, N 9. P. 2011–2016.
21. **Hwang W.-Y.** Quantum Key Distribution with High Loss: Toward Global Secure Communication // Phys. Rev. Lett. 2003. **91**, Iss. 5. 057901.
22. **Liao S.-K., Cai W.-Q., Liu W.-Y. et al.** Satellite-to-ground quantum key distribution // Nature. 2017. **549**. P. 43–59.

Поступила в редакцию 16.08.2023
После доработки 11.10.2023
Принята к публикации 23.10.2023