УДК 535.14

ОДНОВРЕМЕННАЯ ГЕНЕРАЦИЯ ДВУХ КВАНТОВЫХ КЛЮЧЕЙ ПРИ ПЕРЕДАЧЕ ОДИНОЧНЫХ ФОТОНОВ С ДЛИНАМИ ВОЛН 780 И 850 НМ ПО ОДНОМУ АТМОСФЕРНОМУ КВАНТОВОМУ КАНАЛУ

© **Д. Б. Третьяков, А. В. Коляко, А. С. Плешков, 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

Предложен и реализован экспериментально метод увеличения скорости генерации квантового ключа в атмосферных квантово-криптографических линиях связи за счёт одновременной передачи одиночных фотонов с длинами волн 780 и 850 нм по одному квантовому каналу. Созданная нами лабораторная система продемонстрировала примерно двукратное увеличение скорости генерации так называемого «просеянного» квантового ключа при использовании двух установок, работающих на длинах волн 780 и 850 нм и передающих фотоны по одному квантовому каналу длиной 23 см. Скорость генерации просеянного квантового ключа и уровень ошибочных битов для длины волны 780 нм составили 11502 ± 290 бит/с и $2{,}4 \pm 0{,}4$ %, а для длины волны 850 нм — 10627 ± 290 бит/с и $3{,}9 \pm 0{,}5$ %.

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

DOI: 10.15372/AUT20250107
EDN: ADVZJR

Введение. В основе секретности передаваемой информации в квантово-криптографических линиях связи лежат законы квантовой физики [1]. При передаче одиночных фотонов по квантовому каналу (оптоволоконной или атмосферной линиям связи) генерируется двоичный ключ, известный только отправителю (Алисе) и получателю (Бобу). Далее Алиса зашифровывает своё сообщение с помощью данного ключа и передаёт его Бобу по открытому каналу [2].

В первом квантово-криптографическом протоколе BB84, предложенном в 1984 г. [3] и экспериментально реализованном в 1992 г. [4], для генерации секретного двоичного ключа используются одиночные фотоны, у которых поляризация ориентирована под углами 0, 90 (вертикально-горизонтальный базис) и $\pm 45^\circ$ (диагональный базис) по отношению к некоторой оси. Двоичные значения «0» и «1» произвольно присваиваются одному и другому состояниям в каждом базисе. Далее Алиса посылает Бобу одиночные фотоны по квантовому каналу, случайным образом выбирая одну из четырёх поляризаций. Боб измеряет поляризацию полученного фотона в произвольно выбранном базисе, и, таким образом, генерируется «сырой» ключ в виде случайной последовательности битов. После сеанса передачи фотонов Алиса и Боб сравнивают через открытый канал связи базисы передачи и приёма фотонов и отбрасывают те биты, для которых базисы не совпали. В результате получается просеянный ключ, который у Алисы и Боба будет несколько отличаться вследствие того, что используемая ими аппаратура неидеальна. Поэтому далее проводятся процедуры коррекции ошибок и усиления конфиденциальности [2]. В конечном итоге Алиса и Боб формируют абсолютно секретный квантовый ключ.

К настоящему времени зарубежными группами реализована генерация квантового ключа в оптоволоконных линиях связи на расстоянии до 1000 км [5]. По открытому про-

странству наибольшая длина квантово-криптографической линии связи через спутники составляет 7600 км [6]. Российскими коллективами созданы оптоволоконные квантово-криптографические системы, работающие на расстоянии до 143 км [7, 8]. Атмосферные квантовые линии связи реализованы на расстояниях 20 м на основе метода боковых частот [9] и 180 м с применением протокола релятивистской квантовой криптографии [10]. В настоящее время ведутся работы по реализации квантовой связи с помощью сверхмалого спутника, который будет использоваться в качестве доверенного узла [11].

Нашей группой ещё в 2003 г. создана экспериментальная установка для генерации квантового ключа в свободном пространстве [12] на базе протокола BB84 и поляризационного кодирования. На ней выполнен ряд экспериментов по отработке основных методик детектирования одиночных поляризованных фотонов и генерации квантового ключа [13, 14]. В дальнейшем установка была существенно модернизирована [15] для увеличения быстродействия и вероятности регистрации фотонов. В результате скорость генерации просеянного квантового ключа на расстоянии между передатчиком и приёмником 20 м составила 7,5 кбит/с при уровне ошибочных битов 5,1 % [16].

Последующее развитие квантовых систем связи требует увеличения дальности и скорости генерации квантового ключа, а также степени их защищённости. В качестве основного метода повышения скорости генерации квантового ключа в атмосферных квантово-криптографических линиях связи рассматривается увеличение тактовой частоты при передаче и приёме фотонов [17]. Кроме того, предлагаются и применяются различные протоколы, приводящие к увеличению скорости генерации квантового ключа, например протокол с состояниями-ловушками [18].

В существующих атмосферных квантово-криптографических линиях связи используется лазерное излучение с длиной волны 780 или 850 нм [6, 10]. Данные длины волн попадают в два окна прозрачности атмосферы: 740–785 и 850–890 нм [2].

В данной работе предлагается и реализуется экспериментально метод увеличения скорости генерации квантового ключа в атмосферных квантово-криптографических линиях связи за счёт одновременной передачи одиночных фотонов с длинами волн 780 и 850 нм по одному атмосферному квантовому каналу. Для реализации метода необходимо иметь два передатчика поляризованных фотонов с разной длиной волны и два приёмника, регистрирующих фотоны также с разной длиной волны. Для передачи фотонов по одному квантовому каналу нужно совместить излучения, идущие от двух передатчиков, в один луч и послать его по направлению к двум приёмникам. Перед двумя приёмниками устанавливается дихроичное зеркало, разделяющее с высокой эффективностью фотоны по длинам волн. Далее фотоны с длиной волны 780 нм направляются на один приёмник, а с длиной волны 850 нм — на второй. В итоге происходит одновременная генерация двух квантовых ключей с использованием одного квантового канала. Предложенный метод может быть особенно полезен в случае атмосферных квантовых каналов с малым коэффициентом пропускания. Для реализации данного метода нами изготовлены приёмник и передатчик, аналогичные уже имеющимся, но работающие на длине волны 850 нм.

Экспериментальная установка. На рис. 1 показана общая схема передатчиков. В качестве источников одиночных фотонов использовались полупроводниковые лазеры с длиной волны излучения 780 и 850 нм. Каждый из лазеров имел отдельный источник питания, который мог работать как в импульсном, так и непрерывном режимах. Длительность лазерных импульсов составляла 5 нс. Поляризация излучения каждого лазера выставлялась в соответствии с протоколом BB84. Лучи всех лазеров совмещались с помощью системы зеркал, фокусировались и заводились в одномодовые оптоволоконные светоделители (ОВСД) с использованием входных коллиматоров К1. Один из выходов светоделителей применялся для контроля мощности лазерного излучения. Далее лазерные пучки от двух передатчиков объединялись с помощью оптоволоконного соединителя. На его выходе стоял коллиматор,

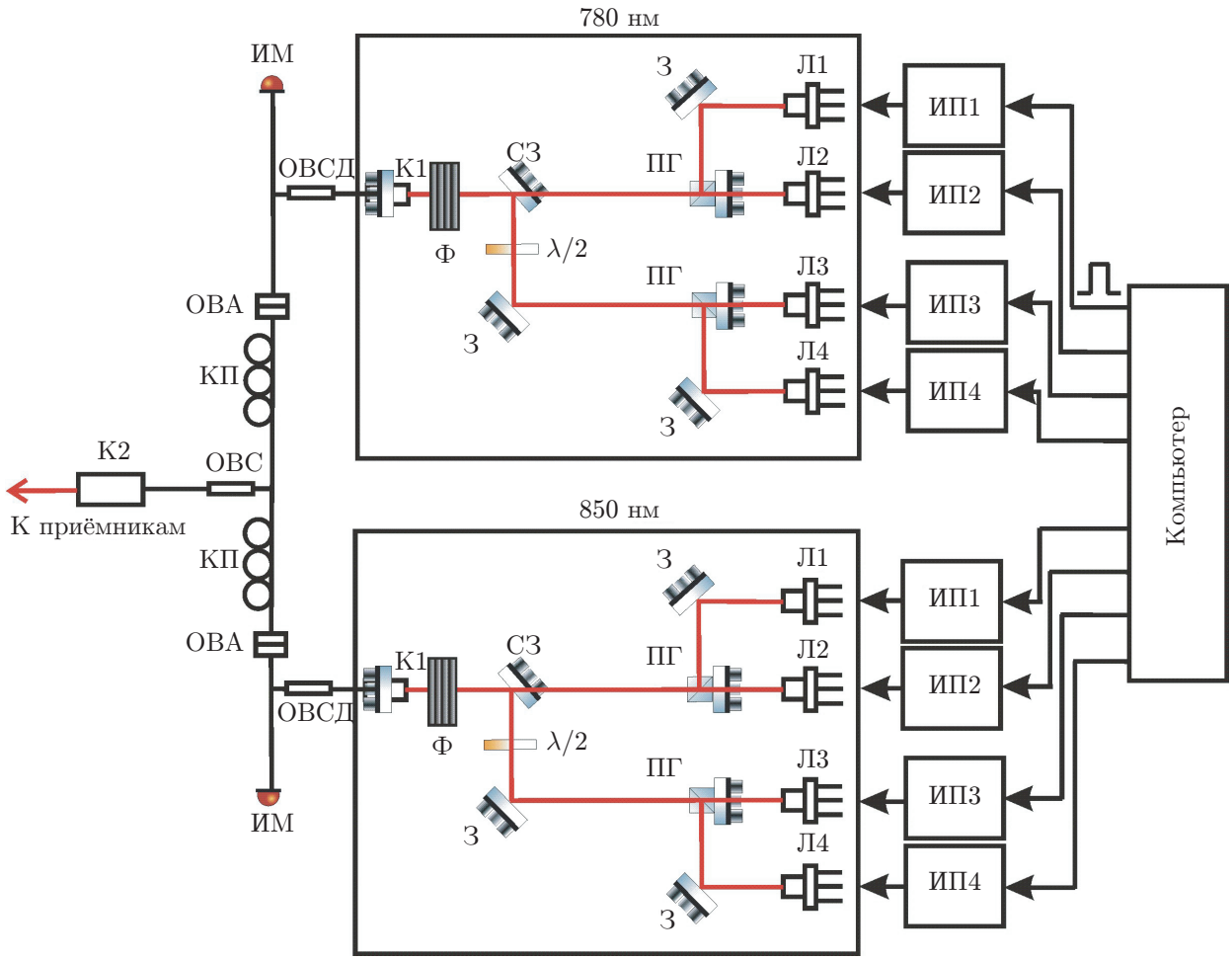

Рис. 1. Общая схема передатчиков: Л1...4 — лазеры; ИП1...4 — источники питания лазеров; З — зеркала; ПГ — призмы Глана; $\lambda/2$ — полуволновые пластинки; СЗ — светоделительные зеркала (50 : 50); Ф — наборы фильтров; К1, К2 — коллиматоры; ОВСД — оптоволоконные светоделители (50 : 50); ОВС — оптоволоконный соединитель; ИМ — измерители мощности; КП — контроллеры поляризации; ОВА — оптоволоконные адаптеры

который формировал лазерный пучок диаметром 7,5 мм, идущий к приёмникам. Заведение в оптоволоконный кабель использовано для точного совмещения лучей от лазеров в один луч и пространственной фильтрации, а также для удобства соединения передающего узла с выходным коллиматором. Поскольку применение оптоволоконных кабелей приводит к искажению поляризации фотонов, на кабели устанавливались ручные контроллеры поляризации, восстанавливающие на выходе поляризацию входного излучения. Для генерации квантового ключа мощность излучения лазеров передающего узла ослаблялась до однофотонного уровня. В качестве ослабителей использовались калиброванные поглощающие оптические фильтры, которые устанавливались перед коллиматорами К1.

На рис. 2 показана общая схема приёмников. Лазерное излучение, идущее от передатчиков, попадало на дихроичное зеркало, которое отражало излучение с длиной волны 850 нм и пропускало излучение с длиной волны 780 нм. Далее лучи заводились с помощью коллиматоров К2 в одномодовые оптоволоконные кабели и направлялись в оптические блоки приёмников. Расстояние от выходного коллиматора К2 передатчиков до дихроич-

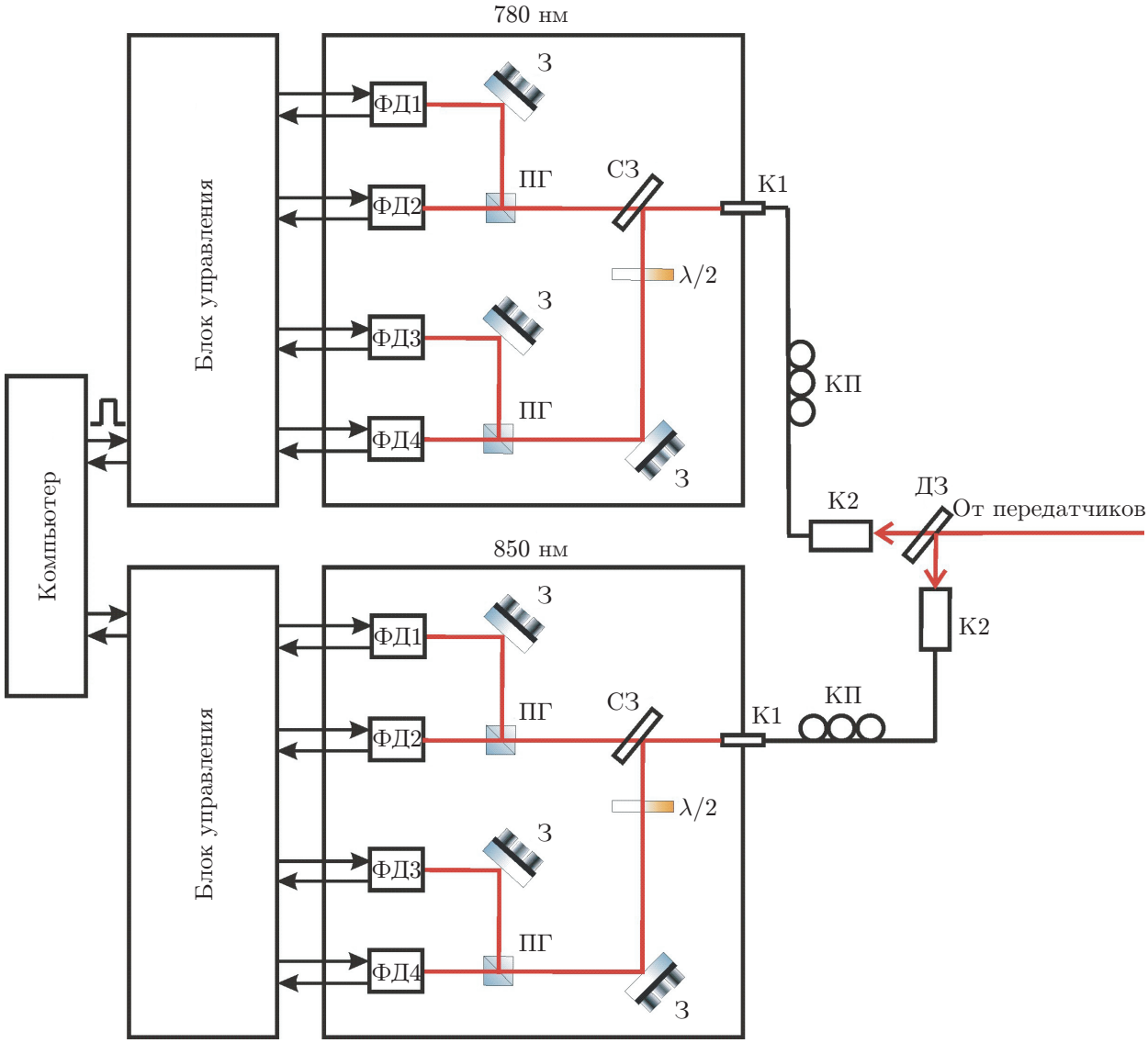

Рис. 2. Общая схема приёмников: ФД1…4 — фотодетекторы; З — зеркала; ПГ — призмы Глана; $\lambda/2$ — полуволновые пластинки; СЗ — светоделительные зеркала (50 : 50); К1, К2 — коллиматоры; КП — контроллеры поляризации; ДЗ — дихроичное зеркало

ного зеркала составляло 23 см, а от дихроичного зеркала до входных коллиматоров К2 приёмников — 7 см. Использование заведения в оптическое волокно обусловлено техническим удобством и достаточной эффективностью передачи излучения в уже настроенную оптическую схему приёмников. Заведение излучения в оптоволоконные кабели осуществлялось вручную с помощью юстировочных головок, к которым крепились коллиматоры, и оптических столиков с вертикальным и горизонтальным перемещениями. Также имелась возможность регулировки расстояния между линзами коллиматоров и торцами коннекторов оптоволоконных кабелей для эффективного заведения излучения в оптическое волокно. Поскольку поляризация излучения искажается при прохождении по оптическому волокну, на каждом кабеле установлен контроллер поляризации для подстройки поляризации фотонов. В оптической схеме каждого приёмника лазерное излучение разделялось на два луча

светоделительным 50 : 50 зеркалом, один из которых потом шёл на регистрацию фотонов в вертикально-горизонтальном базисе, а другой — в диагональном. Таким образом, реализовывался случайный выбор базиса в соответствии с протоколом BB84. В каждом базисе фотоны разделялись по поляризации с помощью призм Глана и регистрировались однофотонными детекторами. В приёмнике излучения с длиной волны 780 нм основу трёх однофотонных детекторов составляли кремниевые лавинные фотодиоды (ЛФД) C30902S производства фирмы EG&G Optoelectronics (Канада) и одного — SAP500S2 производства фирмы Laser Components (Германия), последний использован для замены вышедшего ранее из строя четвёртого ЛФД C30902S. В приёмнике излучения с длиной волны 850 нм использовались четыре ЛФД SAP500S2. Для регистрации одиночных фотонов ЛФД вводились в постоянный гейгеровский режим, для чего напряжение питания ЛФД поднималось выше напряжения пробоя. Применялась схема с пассивным гашением лавины. Выходные импульсы с каждого ЛФД проходили через усилители, а затем посылались на блоки стробирования (входят в блоки управления на рис. 2), в которых 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 всех 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 [15].

Запуск лазерных импульсов и строб-импульсов тактовыми импульсами с частотой следования 1 МГц, а также за счёт TTL-импульсов с блоков стробирования осуществлялся быстродействующей схемой на базе программируемой логической платы сбора данных NI 7811 R Series Multifunction RIO компании National Instruments (США), встраиваемой в системный 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 графической среде.

Настройка системы. Первый этап настройки системы проводился с лазерами, работающими в непрерывном режиме. Излучение передатчика подавалось на соответствующий приёмник по короткому оптоволоконному кабелю. Поляризационные элементы Алисы и Боба настраивались так, чтобы излучение от 1-го лазера попадало в основном на 1-й фотодетектор, 2-го лазера — на 2-й и т. д. Более подробное описание данного этапа настройки приведено в [15].

На втором этапе проводилось измерение коэффициентов пропускания квантового канала длиной 30 см для излучения каждого лазера. Измеренные значения коэффициентов пропускания приведены в табл. 1. Коэффициент пропускания T_{780} измерялся как отношение мощности излучения на выходном конце оптического кабеля, ведущего к приёмнику фотонов с длиной волны 780 нм, к мощности излучения на выходе коллиматора передатчиков K2 (см. рис. 1). Соответственно, коэффициент пропускания T_{850} измерялся как отношение мощности излучения на выходном конце оптического кабеля, ведущего к приёмнику фотонов с длиной волны 850 нм, к мощности излучения на выходе коллиматора передатчиков K2. Также в табл. 1 приведён коэффициент $T_{отн}$, равный отношению T_{850}/T_{780} для лазеров с длиной волны 780 нм и T_{780}/T_{850} для лазеров с длиной волны 850 нм. Данный коэффициент показывает, какая доля фотонов будет попадать на смежный приёмник. Как видно, значения $T_{отн}$ составляют всего доли процента, следовательно, влияние одной установки на другую будет пренебрежимо малым. Различие в значениях коэффициента

Таблица 1

Коэффициенты пропускания квантовых каналов и их отношения для каждого лазера

Коэффициент пропускания	780 нм				850 нм			
	ЛД1	ЛД2	ЛД3	ЛД4	ЛД1	ЛД2	ЛД3	ЛД4
T_{780}, %	58,7 ± 0,1	69,7 ± 0,03	49 ± 0,1	58 ± 0,2	0,01 ± 0,005	0,04 ± 0,01	0,02 ± 0,005	0,02 ± 0,01
T_{850}, %	0,19 ± 0,01	0,04 ± 0,002	0,07 ± 0,007	0,06 ± 0,01	65,6 ± 0,2	66,6 ± 0,2	58,6 ± 0,2	62,3 ± 0,2
$T_{отн}$, %	0,32 ± 0,02	0,06 ± 0,003	0,14 ± 0,01	0,11 ± 0,02	0,02 ± 0,008	0,06 ± 0,02	0,03 ± 0,009	0,03 ± 0,017

Таблица 2

Частоты срабатывания фотодетекторов при включении одного из лазеров

№ лазера		780 нм				850 нм			
		f(ФД1), Гц	f(ФД2), Гц	f(ФД3), Гц	f(ФД4), Гц	f(ФД1), Гц	f(ФД2), Гц	f(ФД3), Гц	f(ФД4), Гц
Лазеры выключены		139 ± 10	118 ± 1	208 ± 5	2 ± 0,5	169 ± 13	206 ± 2	211 ± 9	167 ± 2
780 нм	1	8978 ± 14	280 ± 13	6418 ± 13	1617 ± 7	187 ± 6	207 ± 2	213 ± 12	163 ± 13
	2	219 ± 18	14133 ± 250	6305 ± 39	2488 ± 31	198 ± 7	209 ± 10	211 ± 5	165 ± 7
	3	3486 ± 33	9166 ± 30	11155 ± 54	271 ± 12	187 ± 2	201 ± 10	210 ± 3	166 ± 7
	4	3590 ± 42	2718 ± 20	336 ± 6	2123 ± 15	215 ± 38	212 ± 1	211 ± 3	170 ± 1
850 нм	1	133 ± 4	108 ± 2	204 ± 4	2 ± 0,6	8785 ± 41	322 ± 4	3511 ± 49	5792 ± 45
	2	128 ± 3	111 ± 4	206 ± 9	3 ± 0,5	256 ± 7	7948 ± 25	5138 ± 41	3980 ± 21
	3	137 ± 4	118 ± 4	208 ± 4	3 ± 0,7	4425 ± 151	3720 ± 9	7636 ± 41	546 ± 8
	4	139 ± 1	116 ± 8	208 ± 6	3 ± 0,7	4137 ± 18	4166 ± 15	493 ± 8	8119 ± 18

пропускания для разных лазеров мы связываем с небольшим 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. Тактовые импульсы подавались на один из восьми лазеров, и измерялась частота срабатывания каждого фотодетектора. Мощности лазеров при этом ослаблены до однофотонного уровня, а ЛФД вводились в гейгеровский режим. Для получения максимальной частоты выходных TTL-импульсов проводилось совмещение выходных импульсов ЛФД при регистрации одиночных фотонов со строб-импульсами. Результаты измерения приведены в табл. 2. Первый и второй лазеры составляли вертикально-горизонтальный базис, третий и четвёртый — 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 с длиной волны 780 нм, у которого основным является ФД4 (780 нм) с низкой эффективностью регистрации), а минимальное — на смежные фотодетекторы в этом же базисе. В третьей сверху строке табл. 2 приведены частоты темновых импульсов фотодетекторов. Как видно, при включении лазеров смежного передатчика частота срабатывания фотодетекторов не меняется, что опять же свидетельствует о независимой работе двух установок.

С помощью табл. 1 и 2 можно найти такие параметры фотодетекторов, как эффективность однофотонной регистрации и уровень темновых срабатываний. Частота сраба-

Таблица 3

Измеренные параметры фотодетекторов

Параметры	780 нм				850 нм			
	ФД1	ФД2	ФД3	ФД4	ФД1	ФД2	ФД3	ФД4
η, %	30,1 ± 0,1	40,2 ± 0,7	44,7 ± 0,3	7,3 ± 0,08	26,3 ± 0,2	23,2 ± 0,2	25,3 ± 0,3	25,5 ± 0,1
$\varepsilon_{\text{темн}}$, %	1,55 ± 0,1	0,83 ± 0,02	1,86 ± 0,05	0,09 ± 0,02	1,92 ± 0,16	2,59 ± 0,03	2,76 ± 0,13	2,06 ± 0,03

тываний ФД при включённом основном лазере и при среднем числе фотонов в импульсе $\mu \ll 1$ равняется

$$f = 0{,}5 f_{\text{такт}}\, \mu\, \eta\, T + f_{\text{темн}}, \tag{1}$$

где $\mu = 0{,}1$ — установленное нами среднее число фотонов в лазерном импульсе, $f_{\text{такт}} = 10^6$ Гц — частота тактовых импульсов, η — эффективность регистрации фотодетектором одного фотона, T — коэффициент пропускания квантового канала, $f_{\text{темн}}$ — частота темновых импульсов. Множитель 0,5 возникает из-за того, что лучи лазеров делятся пополам на светоделительном зеркале. Из формулы (1) эффективность регистрации находится как $\eta = (f - f_{\text{темн}})/(0{,}5\, \mu\, T f_{\text{такт}})$. Уровень темновых срабатываний $\varepsilon_{\text{темн}}$ можно найти по формуле $\varepsilon_{\text{темн}} = f_{\text{темн}}/f$. В табл. 3 приведены полученные значения параметров фотодетекторов.

Исследование параметров генерации двух просеянных квантовых ключей. Для исследования параметров генерации двух просеянных квантовых ключей написана программа, которая независимо управляла двумя экспериментальными установками. Далее приведено описание работы программы для одной установки. На запуск одного из четырёх лазеров в случайной последовательности и на запуск блока стробирования подавались тактовые импульсы с частотой следования 1 МГц. Время одного сеанса равнялось 1 с. Среднее число фотонов в лазерном импульсе составляло $\mu = 0{,}1$. После каждого тактового импульса программа 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 уровень ошибочных битов как отношение количества срабатывания смежных фотодетекторов из того же базиса к общему количеству срабатываний.

Скорость генерации просеянного ключа можно предварительно найти, используя значения табл. 2, по формуле $R = 0{,}25 \sum_{i=1}^{4} (F_i + f_i)$, где F_i — частота срабатываний основного фотодетектора для i-го лазера, f_i — частота срабатываний смежного фотодетектора для i-го лазера. Получаем для длины волны 780 нм $R = 9374 \pm 96$ бит/с, для 850 нм — $R = 8526 \pm 38$ бит/с. Уровень ошибочных битов в просеянном ключе $QBER$ (Quantum Bit Error Rate) находится по следующей формуле [2]:

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

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 (2): $QBER = \sum_{i=1}^{4} f_i / \sum_{i=1}^{4} (F_i + f_i)$. Найденное значение для длины волны 780 нм $QBER = 2{,}9 \pm 0{,}1$ %, для 850 нм — $QBER = 4{,}7 \pm 0{,}1$ %.

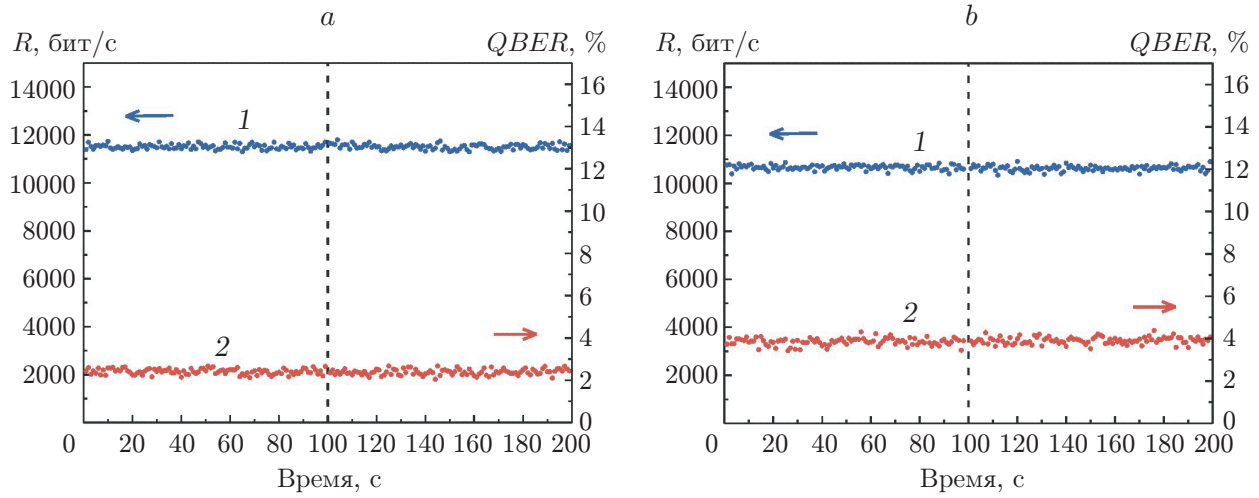

Рис. 3. Экспериментальные зависимости скорости генерации просеянного квантового ключа (точки *1*, *a*, *b*, левая шкала) и уровня ошибочных битов (точки *2*, *a*, *b*, правая шкала) от времени для установок с длиной волны 780 (*a*) и 850 нм (*b*)

На рис. 3 показаны экспериментальные зависимости скорости генерации просеянного квантового ключа и уровня ошибочных битов от времени для обеих установок. Каждая точка соответствует одному сеансу передачи битов длительностью 1 с.

Каждая зависимость разделена пунктирной линией на два временны́х интервала длительностью 100 с, в которых измерения велись в разных условиях. В первом интервале измерения производились при закрытых лазерах другой установки, во втором — две экспериментальные установки работали одновременно. Скорость генерации просеянного квантового ключа для длины волны 780 нм в первом интервале составляет $R = 11504 \pm 220$ бит/с, а уровень ошибочных битов $QBER = 2{,}4 \pm 0{,}3$ %. Во втором $R = 11502 \pm 290$ бит/с, $QBER = 2{,}4 \pm 0{,}4$ %. Для длины волны 850 нм в первом интервале $R = 10663 \pm 280$ бит/с, $QBER = 3{,}9 \pm 0{,}5$ %; во втором — $R = 10627 \pm 290$ бит/с, $QBER = 3{,}9 \pm 0{,}5$ %.

Измеренные значения скорости генерации ключа R превышают ожидаемые значения, вычисленные с помощью табл. 2, на 2100 бит/с для обеих длин волн, что составляет разницу примерно 20 %. Измеренные значения $QBER$ при этом отличаются тоже от ожидаемых значений на 20 %, но в меньшую сторону. Причина данного расхождения пока не выяснена. Возможно, программа при обработке данных с вероятностью 20 % ошибается с измерением номера лазера, что приводит к завышению количества всех битов в ключе и уменьшению $QBER$. На данном этапе нашей исследовательской работы отличие ожидаемых и измеренных параметров генерации просеянного ключа на 20 % не является критичным. В целом результаты эксперимента продемонстрировали способность наших установок работать одновременно, не оказывая никакого взаимного влияния.

Обсуждение. Преимуществом предложенного нами метода увеличения скорости генерации квантового ключа является использование для передачи фотонов с двумя длинами волн одного квантового канала. Объединение излучений с разными длинами волн в один пучок осуществляется с помощью обычного одномодового волоконного соединителя. Разделение фотонов по длинам волн происходит с помощью дихроичного зеркала непосредственно перед оптическими блоками приёмников. В нашем эксперименте длиной

квантового канала является расстояние от выходного коллиматора K2 передатчиков до дихроичного зеркала, равное 23 см. При увеличении данного расстояния могут возникнуть проблемы с передачей мощности, связанные с разной расходимостью лазерных пучков с длинами волн 780 и 850 нм. В будущем планируется увеличить длину квантового канала и исследовать теоретически и экспериментально его коэффициент пропускания для обеих длин волн. Целью исследования будет являться создание оптической системы, обеспечивающей примерно равный коэффициент пропускания квантового канала для фотонов с длинами волн 780 и 850 нм и такой же по величине, как если бы передавались фотоны с одной длиной волны. По результатам исследований будет сделан вывод о применимости данного метода к спутниковым квантовым системам связи.

Описанный в данной работе эксперимент продемонстрировал способность нашей установки генерировать одновременно два просеянных квантовых ключа примерно одного размера. Фактически при объединении данных ключей будет осуществляться двукратное увеличение скорости генерации просеянного квантового ключа. Для генерации секретного ключа Алиса и Боб должны применить к просеянному ключу классические протоколы обработки информации — коррекцию ошибок и усиление конфиденциальности. Скорость генерации секретного ключа $R_{\text{секр}}$ обратно пропорциональна относительному количеству ошибочных битов в просеянном ключе и описывается следующим выражением [2]: $R_{\text{секр}} = R[I(\alpha,\beta) - I^{\max}(\alpha,\varepsilon)]$, 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 данных величины зависят от уровня ошибочных битов в ключе. Для нахождения $I(\alpha,\beta)$ и $I^{\max}(\alpha,\varepsilon)$ мы использовали выражения, приведённые в работе [2] для симметричных индивидуальных атак. Тогда для длины волны 780 нм скорость генерации секретного ключа будет составлять $R_{\text{секр}} = 8830$ бит/с, а для длины волны 850 нм — $R_{\text{секр}} = 6900$ бит/с.

Заключение. Предложенный в данной работе метод увеличения скорости генерации квантового ключа реализован экспериментально. Нами создана лабораторная система атмосферной квантово-криптографической связи, которая состояла из двух установок, работающих на длинах волн 780 и 850 нм и передающих фотоны по одному и тому же квантовому каналу длиной 23 см. Скорость генерации просеянного квантового ключа и уровень ошибочных битов для длины волны 780 нм составили 11502 ± 290 бит/с и $2{,}4 \pm 0{,}4$ %, а для длины волны 850 нм — 10627 ± 290 бит/с и $3{,}9 \pm 0{,}5$ %. Поскольку квантовый ключ представляет собой случайную последовательность битов, то при объединении данных ключей, имеющих примерно одинаковый размер, друг с другом реализуется почти двукратное увеличение скорости генерации просеянного квантового ключа по сравнению со случаем использования только одной установки, работающей на отдельной длине волны. Для дальнейшего увеличения расстояния между передатчиком и приёмником при сохранении одинаковой скорости генерации просеянного квантового ключа на двух длинах волн потребуется создание оптической системы, обеспечивающей примерно равный коэффициент пропускания квантового канала для фотонов с длинами волн 780 и 850 нм и такой же по величине, как если бы передавались фотоны только с одной длиной волны. Планируется провести ряд теоретических и экспериментальных исследований в данном направлении, после чего будет сделан вывод о применимости предложенного метода к спутниковым квантовым системам связи.

Финансирование. Исследование выполнено при поддержке Российского научного фонда (грант № 23-29-00472, https://rscf.ru/project/23-29-00472/).

СПИСОК ЛИТЕРАТУРЫ

1. **Wootters W. K., Zurek W. H.** A single quantum cannot be cloned // Nature. 1982. **299**. P. 802–803.
2. **Gisin N., Ribordy G., Tittel W., Zbinden H.** Quantum cryptography // Rev. Mod. Phys. 2002. **74**, N 1. P. 145–195.
3. **Bennett C. H., Brassard G.** Quantum cryptography: Public key distribution and coin tossing // Proc. of the IEEE Int. Conf. on Comput. Systems & Signal Processing. Bangalore, India, 9–12 Dec., 1984. P. 175–179.
4. **Bennett C. H., Bessette F., Brassard G., Salvail L.** 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 конф. по фотонике и квантовым технологиям. Казань, Россия, 15–17 дек., 2019. 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., Molotkov S. N.** Relativistic quantum key distribution system with one-way quantum communication // Sci. Rep. 2018. **8**. 6102.
11. **Дуплинский А. В., Хмелев А. В., Мерзликин В. Е. и др.** Масштабируемая спутниковая сеть для квантового распределения ключей на основе кубсата // Вестн. ТГУ. 2023. № 63. С. 103–110.
12. **Курочкин В. Л., Рябцев И. И., Неизвестный И. Г.** Генерация квантового ключа на основе кодирования поляризационных состоянии фотонов // Оптика и спектроскопия. 2004. **96**, № 5. С. 772–776.
13. **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.
14. **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.
15. **Коляко А. В., Плешков А. С., Третьяков Д. Б. и др.** Исследование долговременной стабильности генерации однофотонного квантового ключа в схеме с поляризационным кодированием // Сибирский физический журнал. 2021. **16**, № 2. С. 81–93.
16. **Плешков А. С., Коляко А. В., Третьяков Д. Б. и др.** Исследование долговременной стабильности генерации квантового ключа в свободном пространстве на расстоянии 20 м в схеме с поляризационным кодированием // Автометрия. 2024. **60**, № 1. С. 49–58. DOI: 10.15372/AUT20240105.
17. **García-Martínez M. J., Denisenko N., Soto D. et al.** High-speed free-space quantum key distribution system for urban daylight applications // Appl. Opt. 2013. **52**, Iss. 14. P. 3311–3317.
18. **Hwang W.-Y.** Quantum Key Distribution with High Loss: Toward Global Secure Communication // Phys. Rev. Lett. 2003. **91**, Iss. 5. 057901.

Поступила в редакцию 04.10.2024
После доработки 26.11.2024
Принята к публикации 10.01.2025