УДК 535.14

ПРИМЕНЕНИЕ ДЕТЕКТОРОВ ОДИНОЧНЫХ ФОТОНОВ ДЛЯ ГЕНЕРАЦИИ КВАНТОВОГО КЛЮЧА В ЭКСПЕРИМЕНТАЛЬНОЙ ОПТОВОЛОКОННОЙ СИСТЕМЕ СВЯЗИ

В. Л. Курочкин[1, 2], А. В. Зверев[1], Ю. В. Курочкин[3], И. И. Рябцев[1, 2], И. Г. Неизвестный[1]

[1] *Институт физики полупроводников СО РАН им. А. В. Ржанова, 630090, г. Новосибирск, просп. Академика Лаврентьева, 13*
E-mail: kurochkin@isp.nsc.ru
[2] *Новосибирский государственный университет, 630090, г. Новосибирск, ул. Пирогова, 2*
[3] *Московский физико-технический институт, 141700, Московская обл., г. Долгопрудный, Институтский пер., 9*

Приведены экспериментальные результаты генерации квантового ключа на созданной оптоволоконной установке на телекоммуникационной длине волны 1555 нм. Оптическая схема установки собрана по автокомпенсационной двухпроходной схеме. Генерация квантового ключа осуществлялась на основе кодирования фазовых состояний одиночных фотонов, излучаемых импульсным полупроводниковым лазером, в двух альтернативных базисах, не ортогональных друг другу. В качестве высокочувствительных фотодетекторов использовались разработанные счетчики одиночных фотонов на основе лавинных фотодиодов InGaAs:InP. Приведены результаты исследования параметров квантовой эффективности, вероятности появления послеимпульсов и уровня шумов для различных режимов работы детекторов в диапазоне температур от –40 до –60 °C. Получена скорость генерации ключа 450 бит/с для одномодового оптоволоконного квантового канала связи между приемником и передатчиком длиной 25 км при тактовой частоте повторения лазерных импульсов 5 МГц и среднем числе фотонов в импульсе около 0,2. Для достигнутых параметров фотодетекторов среднее количество ошибок в квантовом ключе не превышало 3,7 %.

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

Введение. Квантовая криптография, также часто называемая методом генерации квантового ключа, является одним из актуальных направлений квантовой информатики. Основная цель квантовой криптографии состоит в организации абсолютно секретной передачи данных между двумя пользователями, традиционно называемыми Алисой (передатчик) и Бобом (приемник). Секретность и невозможность незаметного перехвата посторонним лицом передаваемых данных основана на фундаментальных законах квантовой механики в противоположность используемым сейчас методам криптографии, которые основаны на математических закономерностях и, в принципе, поддаются расшифровке. В соответствии с математически доказанным утверждением Шеннона [1] передача данных не поддается расшифровке, если сообщение зашифровано одноразовым случайным ключом (длина ключа равна длине сообщения) и этот ключ известен только легитимным пользователям. Основная проблема при реализации данного метода состоит в распространении секретного ключа между пространственно удаленными пользователями.

Такой случайный ключ позволяет сформировать квантовая криптография путем организации передачи одиночными фотонами. Каждый фотон кодируется определенным квантовым состоянием (например, по поляризации или фазе), и принимающая сторона может

извлечь правильное значение зашифрованного бита, проводя измерение квантового состояния фотона в строго заданном базисе. Безусловная секретность квантовой криптографии базируется на следующих запретах квантовой физики, которые накладываются на любой измерительный прибор. Первый запрет — невозможно получить информацию о неортогональных квантовых состояниях без их возмущения [2]. Второй — невозможно достоверно скопировать неизвестное квантовое состояние (теорема о невозможности «клонирования») [3]. Из этих положений следует, что если в качестве носителей информации использовать одиночные квантовые объекты, то любая попытка вторжения несанкционированным лицом в процесс передачи данных неизбежно приведет к необратимому изменению квантовых состояний этих объектов, по которому факт вторжения может быть выявлен.

В работах [4, 5] был предложен первый протокол, а в дальнейшем осуществлена экспериментальная демонстрация генерации квантового ключа с помощью передачи одиночных, поляризованных в двух неортогональных базисах фотонов по открытой линии связи. Этот протокол получил название BB84. Поляризационный метод кодирования используется при организации квантовых каналов через открытое пространство [6], причем в перспективе рассматривается возможность связи с орбитальными спутниками [7, 8]. Для оптоволоконных линий связи чаще применяется фазовое кодирование с использованием интерферометров Маха — Цендера (МЦ) [2], где уже продемонстрирована генерация квантового ключа на расстояния свыше 100 км с помощью полупроводниковых детекторов одиночных фотонов [9, 10] и свыше 200 км со сверхпроводящими детекторами [11, 12]. Также в работе [13] был предложен протокол на основе генерации пар фотонов в перепутанных квантовых состояниях, который был экспериментально реализован, например, в работе [14]. В настоящее время исследования в области квантовой криптографии вызывают большой интерес в мире [15, 16].

В предлагаемой работе приведены результаты генерации квантового ключа, полученные на созданной оптоволоконной экспериментальной установке для квантовой криптографии, работающей на телекоммуникационной длине волны 1555 нм. Генерация ключа осуществлялась на основе кодирования фазовых состояний одиночных фотонов, излучаемых импульсным полупроводниковым лазером, в двух альтернативных квантовых базисах, не ортогональных друг другу (протокол BB84 [4]). Целью данной работы являлось экспериментальное изучение особенностей генерации одиночных фотонов в заданном квантовом состоянии с последующим детектированием этих фотонов и сортировкой по их исходным состояниям при низком уровне ложных измерений. В качестве высокочувствительных фотодетекторов использовались разработанные счетчики одиночных фотонов на основе лавинных фотодиодов InGaAs:InP.

Квантовый протокол BB84. Кратко рассмотрим основные принципы генерации квантового ключа на основе протокола BB84 [4, 15]. Передающая сторона (Алиса) подготавливает однофотонные состояния с линейной поляризацией в двух не ортогональных друг другу базисах. Один базис — назовем его вертикально-горизонтальным — соответствует поляризации фотонов 0 и 90°, другой базис — назовем его диагональным — поляризации 45 и –45°. Алиса и приемная сторона (Боб) договариваются о коде каждой поляризации в двоичном представлении, например фотоны с поляризацией 0 и 45° соответствуют логическому «0», а фотоны с поляризацией 90 и –45° — логической «1».

Для генерации квантового ключа Алиса посылает Бобу последовательность одиночных фотонов, поляризация которых выбрана случайным образом и может составлять 0, 45, 90 и –45°. Эти фотоны распространяются через оптический квантовый канал связи (открытое пространство или оптоволокно). Боб регистрирует пришедшие фотоны, случайным образом выбирая базис измерения для каждого из них. По дополнительному открытому каналу связи (например, сети Интернет) Боб сообщает Алисе, в каком базисе он провел измерение, но не сообщает результат этого измерения. Поскольку поляризация

зарегистрированного фотона может соответствовать как «0», так и «1», то сообщение о факте регистрации фотона по открытому каналу не дает никакой информации постороннему подслушивателю (Ева). Алиса в ответ сообщает Бобу, правильный ли базис измерения был выбран для каждого фотона. Сохраняя в серии только результаты измерений, проведенных в совпадающих поляризационных базисах, Алиса и Боб создают уникальную случайную последовательность «0» и «1», из которой затем и формируют секретный ключ. В случае применения фазового метода кодирования с использованием интерферометра Маха — Цендера в оптоволоконном квантовом канале связи фотон вместо определенной поляризации подвергается дополнительному фазовому сдвигу 0 или π (первый базис) и $\pi/2$ или $3\pi/2$ (второй базис).

Важным этапом квантово-криптографической генерации ключа является проведение проверочного теста на возможный перехват Евой информации по квантовому каналу. Для этого Алиса и Боб по открытому каналу делают проверочное сравнение случайно выбранной части полученного ключа. Если передача не прослушивалась, то сформированный код совпадет. Уровень ошибок в коде будет обусловлен шумами фотодетекторов и неидеальностью оптического канала связи. Если на пути от Алисы к Бобу Ева будет считывать информацию из квантового канала связи, то, поскольку каждый бит передается одиночным фотоном, Ева будет вынуждена пытаться воспроизвести (клонировать) перехваченный фотон и заново отправить его Бобу. В этом случае в соответствии с теоремой о невозможности клонирования состояния произвольного квантового объекта [3] Ева необратимым образом разрушит квантовые состояния фотонов и не сможет их воспроизвести с полной достоверностью. Это вызовет несовпадение в сформированном ключе у Алисы и Боба. Уровень ошибок, который выявится при открытом сравнении данных, будет значительно превышать уровень в передаче без подслушивания. Таким образом будет раскрыт факт несанкционированного подслушивания квантовой линии связи, и легальные пользователи смогут предпринять соответствующие меры безопасности. Фактически использование двух не ортогональных друг другу базисов и уменьшение скорости передачи данных необходимы для достижения гарантии секретности. Также передача должна вестись однофотонными лазерными импульсами, так как присутствие в передаче многофотонных импульсов позволит Еве незаметным образом отвести часть фотонов на свои фотодетекторы, и тогда факт подслушивания не будет зафиксирован.

Оптоволоконная система связи для генерации квантового ключа. Оптическая часть установки собрана по автокомпенсационной двухпроходной схеме [17]. Она состоит из передатчика Алиса (рис. 1) и приемника Боб (рис. 2), которые соединены между собой одномодовым оптоволокном SMF-28 (квантовым каналом) длиной 25 км.

Передача оптических сигналов организована следующим образом. Лазер Боба испускает многофотонный оптический импульс с линейной поляризацией на длине волны 1555 нм и длительностью 1 нс, который проходит через циркулятор и направляется на первый светоделитель 50/50. Далее одна часть импульса поступает на вход поляризационного светоделителя по короткому плечу оптоволоконного интерферометра МЦ. Другая часть импульса приходит на поляризационный светоделитель по длинному плечу, образованному линией задержки длиной 10 м и оптоволоконным фазовым модулятором. Оптические элементы в длинном плече выполнены из поддерживающего поляризацию оптоволокна. Это позволяет сориентировать поляризацию излучения так, чтобы обе части импульса вышли через выход поляризационного светоделителя и направились от Боба к Алисе по протяженному одномодовому оптоволокну (традиционно называемому квантовым каналом связи).

После прохождения квантового канала лазерный импульс поступает на вход передатчика Алиса, проходит через накопительную линию (см. рис. 1) длиной 25 км, фазовый модулятор и отражается от фарадеевского зеркала, которое поворачивает поляризацию

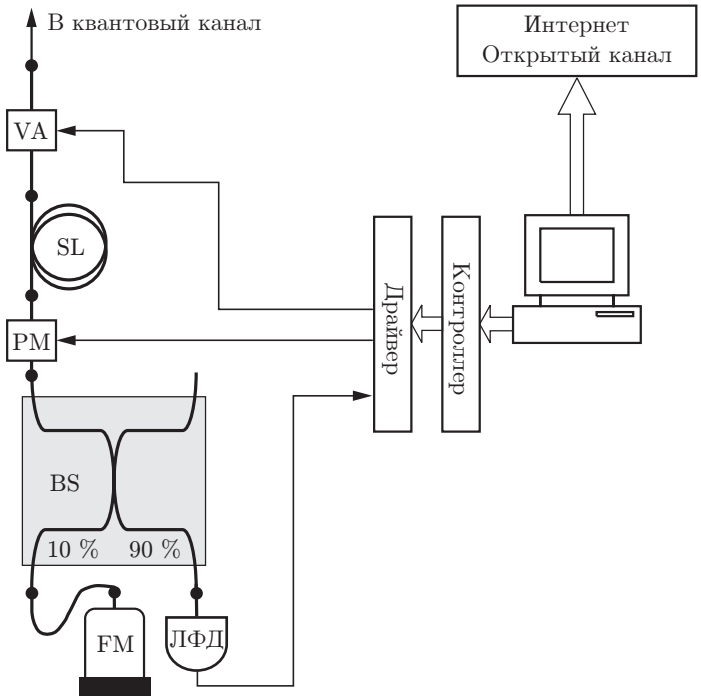

Рис. 1. Схема передающего узла (Алиса) оптоволоконной экспериментальной установки для генерации квантового ключа (VA — электрооптический аттенюатор, SL — накопительная линия, PM — фазовый модулятор, BS — оптоволоконный светоделитель 10/90, FM — зеркало Фарадея)

излучения на 90° для автокомпенсации поляризационных искажений оптоволокна. На обратном пути, на выходе из передатчика Алиса, лазерный импульс ослабляется перестраиваемым аттенюатором до однофотонного состояния (среднее число фотонов на импульс 0,1–0,3). Вернувшиеся от Алисы к Бобу фотоны имеют повернутую на 90° линейную поляризацию, поэтому входным поляризационным светоделителем (см. рис. 2) они направляются в другое плечо интерферометра МЦ, после прохождения которого соединяются на выходе светоделителя, где интерферируют. Результат интерференции регистрируется лавинным фотодиодом (ЛФД1) в одном плече либо после прохождения циркулятора на лавинном фотодиоде (ЛФД2) в другом плече. Поскольку эти две части импульса проходят одинаковый путь, причем в обратном порядке внутри приемника Боб, интерферометр автоматически скомпенсирован. Это большое достоинство интерферометра такого типа. По данному принципу построены, например, коммерческие системы [18, 19].

Для реализации протокола BB84 Алиса с помощью фазового модулятора прикладывает в нужный момент времени фазовый сдвиг 0 или π и $\pi/2$ или $3\pi/2$ к световому импульсу, пришедшему от Боба. Боб, получив отраженные от Алисы одиночные фотоны, случайным образом выбирает базис для измерения, прикладывая сдвиг 0 или $\pi/2$ на свой фазовый модулятор в соответствующий момент времени.

В такой оптической схеме, когда импульсы распространяются вперед и назад, обратное рэлеевское рассеяние света может значительно увеличить шум, регистрируемый детекторами ЛФД1 и ЛФД2, работающими в режиме регистрации одиночных фотонов в процессе генерации квантового ключа. Поэтому лазер испускает импульсы не постоянно, а посылает цуги импульсов в каждом цикле передачи, причем длина этих цугов соответствует длине накопительной линии, вставленной для этой цели после аттенюатора в

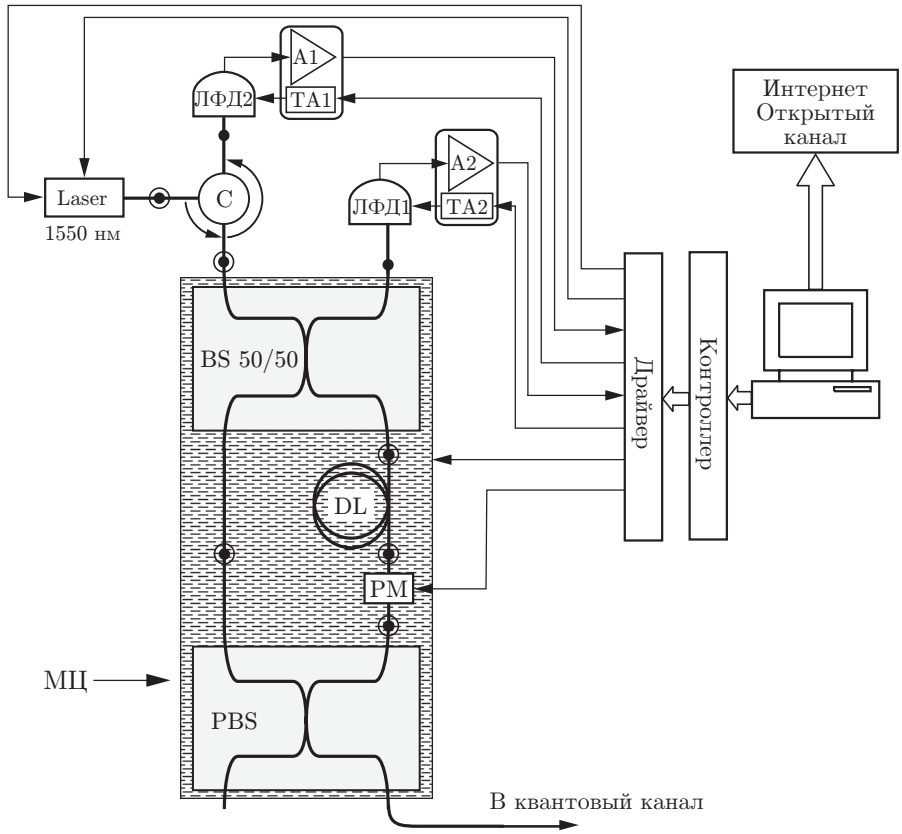

Рис. 2. Схема приемного узла (Боб) оптоволоконной экспериментальной установки для генерации квантового ключа (A1 и A2 — усилители, TA1 и TA2 — триггеры запуска, C — циркулятор, BS — оптоволоконный светоделитель 50/50, DL — линия задержки, PBS — поляризационный светоделитель)

оптическую схему Алисы. Благодаря этому однофотонные импульсы, распространяющиеся обратно, больше не пересекаются в квантовом канале с многофотонными импульсами, идущими от Боба к Алисе. Для накопительной линии длиной 25 км цуг содержит 1200 импульсов при тактовой частоте посылки лазерных импульсов 5 МГц.

Процесс генерации квантового ключа происходит следующим образом. На первом этапе производится калибровка и настройка оптоволоконного канала связи. Для этого точно измеряется длина оптического канала с использованием многофотонных импульсов от Боба и регулируемый аттенюатор у Алисы устанавливается на полное пропускание. Боб принимает отраженный сигнал и на основании этих измерений устанавливает положение строба во времени длительностью 2,5 нс для детекторов ЛФД1 и ЛФД2, когда они должны регистрировать сигнал. Детекторы работают в линейном режиме регистрации многофотонных световых импульсов.

На втором этапе устанавливается режим генерации квантового ключа. Обратное напряжение на лавинных фотодиодах поднимается выше порогового напряжения пробоя, и они переходят в режим регистрации одиночных фотонов (гейгеровский режим счета импульсов). Приемник Боб испускает цуг лазерных импульсов. Аттенюатор Алисы открыт на пропускание. Когда цуг импульсов заполнит накопительную линию, этот быстрый, электрически управляемый аттенюатор уменьшит свое пропускание до такого уровня, при котором от Алисы к Бобу будут выходить световые импульсы с содержанием фотонов на уровне 0,1–0,3 фотон./импульс. В таких условиях вероятность P_n найти n фотонов в

лазерном импульсе подчиняется статистике Пуассона:

$$P_n = \frac{(\bar{n})^n}{n\,!}\,\mathrm{e}^{-\bar{n}}, \tag{1}$$

где $\overline{n}$ — среднее число фотонов в импульсе. В квантовой криптографии импульс считается однофотонным, если $\overline{n}$ находится в пределах 0,1–0,2 [15]. Так, для $\overline{n} = 0{,}1$ доля импульсов с двумя фотонами составляет 5 % от однофотонных, а с тремя фотонами — 0,16 %. В этом случае в девяти из каждых десяти импульсов нет ни одного фотона.

Далее светоделитель 10/90 Алисы направляет 90 % мощности излучения приходящих световых импульсов на многофотонный детектор. Он генерирует сигнал запуска, который используется для синхронизации опорного генератора Алисы (20 МГц) с генератором Боба. Этот синхронизованный генератор позволяет Алисе прикладывать электрический импульс к фазовому модулятору в нужный момент времени для модуляции фазы оптического импульса в соответствии с протоколом BB84. Алиса запоминает порядковый номер каждого импульса и значение приложенной фазы. Случайные числа в эксперименте генерируются обеими сторонами посредством математического датчика псевдослучайных чисел. Боб записывает в буфер и посылает в компьютер как порядковый номер импульса, так и базис измерения одиночных фотонов, зарегистрированных детекторами ЛФД1 и ЛФД2. На основании этих данных, пользуясь открытым каналом между своими компьютерами, Алиса и Боб формируют одинаковый квантовый ключ. Процесс генерации ключа полностью управляется и осуществляется стандартными PCI, которые задают режим работы оптоэлектронных компонентов установки с помощью быстродействующей программируемой матрицы высокой степени интеграции.

Детекторы одиночных фотонов. Поскольку для секретности передачи требуется присутствие не более одного фотона в каждом лазерном импульсе, к фотодетекторам Боба предъявляются высокие требования. Они должны обладать высокой квантовой эффективностью регистрации, малыми шумами и достаточно высокой скоростью счета. Криптосистемы для передачи ключа по оптоволокну обычно работают на телекоммуникационной длине волны 1550 нм, которая соответствует наименьшему затуханию и минимальной дисперсии в волокне [15]. В настоящее время наилучшими однофотонными детекторами в этой области для практического использования являются ЛФД InGaAs:InP [15, 20–23]. При регистрации отдельных фотонов ЛФД включают таким образом, чтобы они работали в гейгеровском режиме [15, 20, 21], когда один фотон способен вызвать лавину носителей заряда. Для этого обратное напряжение питания на них поднимают выше порогового напряжения пробоя: чем больше напряжение над порогом, тем выше вероятность регистрации фотона. Однако при этом обычно значительно возрастают темновые шумы и вероятность появления так называемых послеимпульсов, которые возникают в результате срабатывания ЛФД.

Для уменьшения этих нежелательных эффектов применяют ряд специальных мер. Например, охлаждение ЛФД дает заметное уменьшение темновых шумов. Обычно температуру ЛФД InGaAs:InP понижают до –40 ... –70 °C с помощью микрохолодильников на основе элементов Пельтье. Для снижения вероятности появления послеимпульсов применяют метод активного гашения лавины [22, 23] или работают в режиме с импульсным питанием, когда напряжение на ЛФД поддерживается ниже порогового, а для регистрации одиночных фотонов его кратковременно (на несколько наносекунд) увеличивают выше порога [20, 21].

В качестве детекторов одиночных фотонов были протестированы специально отобранные ЛФД InGaAs:InP ETX40 фирмы "Epitax"(США), совмещенные с оптоволокном и работающие в режиме с импульсным питанием. Импульсы имели трапециевидную форму с

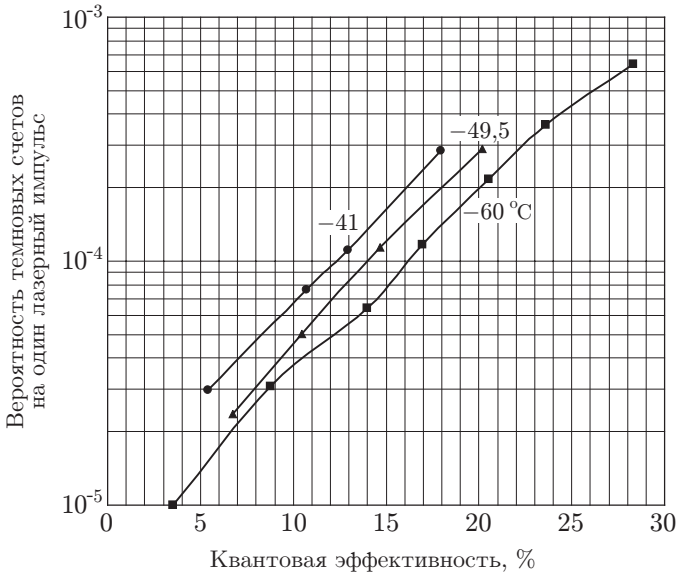

Рис. 3. Измеренные зависимости квантовой эффективности детекторов одиночных фотонов от величины темновых шумов на один лазерный импульс для различных температур

длительностью по полувысоте 3,5 нс и амплитудой 4,2 В. Это напряжение добавлялось к постоянному напряжению смещения ЛФД, которое было ниже порогового. Для уменьшения собственных шумов диоды охлаждались полупроводниковыми микрохолодильниками Пельтье до –40 . . . –60 °C. Измеренные зависимости квантовой эффективности регистрации от величины шумов в пересчете на один импульс для различных температур приведены на рис. 3. При этих измерениях излучение импульсного лазера с частотой повторения лазерных импульсов 1 МГц ослаблялось оптоволоконными аттенюаторами до уровня 0,1 фотон./импульс. В момент прихода фотона на ЛФД подавался импульс питания, и фотодиод переходил в гейгеровский режим для регистрации одиночных фотонов. Вероятность регистрации и уровень темнового шума определялись суммарным обратным напряжением смещения ЛФД, которое варьировалось при проведении измерений.

Зависимости вероятности появления послеимпульсов от времени для различных температур показаны на рис. 4. Измерения выполнялись следующим образом. Частота повторения лазерных импульсов устанавливалась равной 100 кГц для обеспечения временного интервала 10 мкс между лазерными импульсами. Этот интервал достаточно велик, чтобы исключить взаимное влияние послеимпульсов от соседних световых импульсов [20, 21]. Мощность излучения лазера подбиралась так, чтобы полная вероятность детектирования лазерных импульсов была близка к 100 %, т. е. детектор регистрировал около 99 кимп/с. Еще один импульс питания прикладывался к ЛФД с варьируемой задержкой $\tau = (0{,}1–10)$ мкс по отношению к основному, который был синхронен моменту прихода фотонов на ЛФД. Меняя задержку, можно было измерять вероятность появления послеимпульсов во времени относительно основного светового импульса.

Измеренные зависимости вероятности появления послеимпульсов от времени, полученные для различных уровней шума при температуре фотодиода –60 °C, приведены на рис. 5. Уровень шумов задавался обратным напряжением смещения ЛФД в гейгеровском режиме.

Проведенные измерения показали, что характеристики детекторов, созданных на основе ЛФД ETX40, близки к данным зарубежных исследователей [20]. Используя измеренные параметры фотодиода, можно выбрать рабочую точку для режима регистрации одиночных

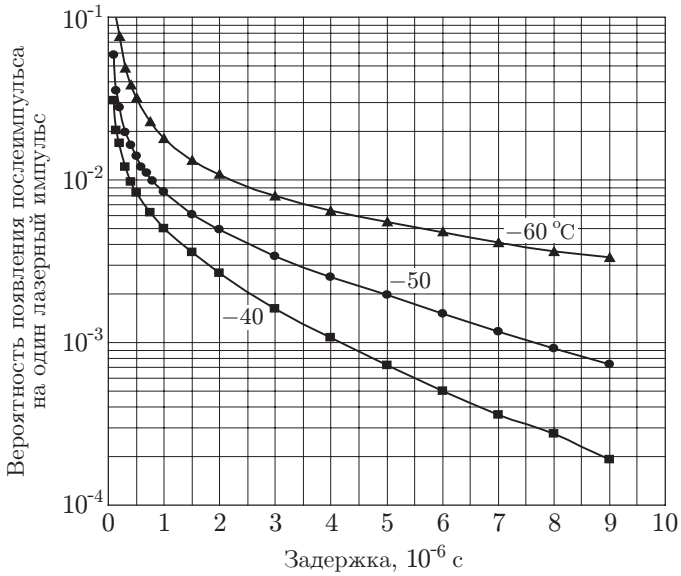

Рис. 4. Измеренные зависимости вероятности послеимпульсов детекторов одиночных фотонов от времени задержки после лазерного импульса для различных температур

фотонов, исходя из допустимого уровня ложных срабатываний и квантовой эффективности, требуемых для конкретной задачи.

Результаты экспериментов по генерации квантового ключа. На созданной экспериментальной установке были проведены тестовые эксперименты по генерации квантового ключа на основе фазового кодирования в протяженной оптоволоконной линии связи между Алисой и Бобом длиной 25 км. Предварительно проводилось измерение контраста интерферометра МЦ, который является источником дополнительных ошибок при генерации ключа [19]. Измерения выполнялись в многофотонном режиме, когда отсутствовали шумы, обусловленные собственными шумами однофотонных детекторов, работающих в гейгеровской моде. Для регистрации оптического сигнала использовался фотодетектор с линейным диапазоном от 10 мВ (уровень собственных шумов) до 800 мВ. Измеренный контраст интерферометра был не хуже 98,5 %, что вполне достаточно, чтобы обеспечить малый вклад ошибок вследствие несовершенства оптической схемы [17].

В начале каждого эксперимента проводилась процедура настройки всей системы в многофотонном режиме. Приемник Боб испускал многофотонный импульс и измерял время прохождения квантового канала с точностью 400 пс. Затем задавались все необходимые временные задержки для управляющих электрических импульсов оптоэлектронных элементов и однофотонных детекторов и контролировалось исполнение алгоритма квантового протокола BB84. На следующей стадии излучение ослаблялось Алисой с помощью быстродействующих оптических аттенюаторов до уровня 0,2 фотона в лазерном импульсе и детекторы переключались в однофотонный режим. Частота повторения лазерных импульсов устанавливалась равной 5 МГц. Данные передавались в соответствии с протоколом BB84.

В тестовых экспериментах была реализована генерация квантового ключа со скоростью 450 бит/с. Общее количество ошибок в ключе не превышало 3,7 %. Учитывая, что максимально допустимая ошибка в квантовой передаче не должна превышать 11 % [15], полученный результат можно считать вполне удовлетворительным для реальной генерации ключа. В то же время полученная скорость генерации была примерно на порядок ниже предельно возможной скорости, теоретически рассчитанной для измеренных параметров

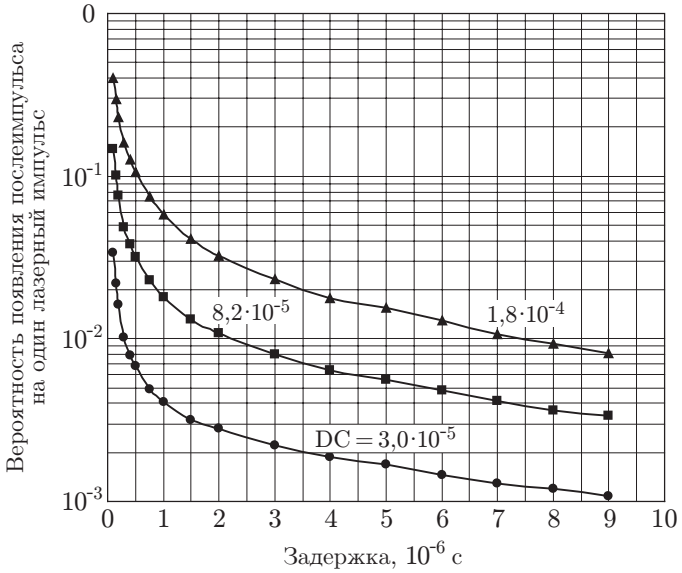

Рис. 5. Измеренные зависимости вероятности послеимпульсов детекторов одиночных фотонов от времени задержки после лазерного импульса для различных уровней темнового шума при температуре –60 °C (DC — вероятность появления шумового импульса на один лазерный импульс)

экспериментальной установки. Это объясняется рядом выявленных проблем в синхронном взаимодействии и обмене данными между компьютером, программируемой матрицей и однофотонными детекторами.

Заключение. В данной работе создана полностью оптоволоконная экспериментальная установка для генерации квантового ключа с процессорным управлением, основанная на телекоммуникационной длине волны. Лазер, оптоволоконный интерферометр, фазовые модуляторы и быстродействующий аттенюатор были выполнены из элементов, согласованных с одномодовым оптоволокном. Автокомпенсационная двухпроходная оптическая схема позволяет работать с каналом связи длиной 25–100 км [15, 17]. В установке применяются специально созданные детекторы одиночных фотонов на базе лавинных фотодиодов InGaAs:InP. Измерены зависимости квантовой эффективности, вероятности появления послеимпульсов и уровни темновых шумов для различных режимов работы ЛФД в диапазоне температур от –40 до –60 °C. При тактовой частоте повторения лазерных импульсов 5 МГц и среднем числе фотонов в импульсе около 0,2 получена скорость генерации квантового ключа 0,45 кбит/с для одномодовой оптоволоконной линии связи между передатчиком и приемником длиной 25 км. Количество ошибок в ключе не превышало 3,7 %.

СПИСОК ЛИТЕРАТУРЫ

1. **Shannon C. E.** Communication theory of secret systems // Bell Syst. Techn. Journ. 1949. **28**. P. 658–715.
2. **Bennet C. H.** Quantum cryptography using any two nonorthogonal states // Phys. Rev. Lett. 1992. **68**. P. 3121–3124.
3. **Wooters W. K., Zurek W. H.** A single quantum cannot be cloned // Nature. 1982. **299**. P. 802–803.
4. **Bennet C. H., Brassard G.** Quantum cryptography: Public key distribution and coin tossing // Proc. of IEEE Intern. Conf. on Comput. Syst. and Sign. Process. Bangalore, India, 1984. P. 175–179.

5. **Bennet C. H., Bessette F., Brassard G. et al.** Experimental quantum cryptography // Journ. Cryptology. 1992. **5**, N 1. P. 3–28.
6. **Kurtsiefer C., Zarda P., Halder M. et al.** Quantum cryptography: A step towards global key distribution // Natura. 2002. **419**. P. 450.
7. **Rarity J. G., Tapster P. M., Gorman P. M., Knight P.** Ground to satellite secure key exchange using quantum cryptography // New Journ. Phys. 2002. **4**. P. 82.1–82.21.
8. **Ursin R., Jennewein T., Koer J. et al.** Space-QUEST: Experiments with quantum entanglement in space // arxiv:quant-ph/0806.0945 (2008).
9. **Kosaka H., Tomita A., Nambu Y. et al.** Single-photon interference experiment over 100 km for quantum cryptography system using balanced gated-mode photon detector // Electron. Lett. 2003. **39**, N 16. P. 1119–1201.
10. **Kimura T., Nambu Y., Hatanaka T. et al.** Single-photon interference over 150-km transmission using silica-based integrated-optic interferometers for quantum cryptography // arxiv:quant-ph/0403104 (2004).
11. **Takesue H., Nam S. W., Zhang Q. et al.** Quantum key distribution over a 40-dB channel loss using superconducting single-photon detectors // Nature Photonics. 2007. **1**. P. 343–348.
12. **Stucki D., Walenta N., Vannel F. et al.** High rate, long-distance quantum key distribution over 250 km of ultra low loss fibres // arxiv:quant-ph/0903.3907 (2009).
13. **Ekert A. K.** Quantum cryptography based on Bell's theorem // Phys. Rev. Lett. 1991. **67**. P. 661–663.
14. **Schmitt-Manderbach T., Weier H., Fürst M. et al.** Experimental demonstration of free-space decoy-state quantum key distribution over 144 km // Phys. Rev. Lett. 2007. **98**. P. 010504.
15. **Gisin N., Ribordy G., Title W. et al.** Quantum Cryptography // Rev. Mod. Phys. 2002. **74**. P. 145–175.
16. **Scarani V., Pasquinucci H., Cerf N. et al.** A framework for practical quantum cryptography // arxiv:quant-ph/0802.4155 (2008).
17. **Stucki D., Gisin N., Guinnard O. et al.** Quantum key distribution over 67 km with a plug&play system // New Journ. Phys. 2002. **4**. P. 41.1–41.8.
18. **http://** www.magiqtech.com
19. **http://** www.idquantique.com
20. **Stucki D., Ribordy G., Stefanov A. et al.** Photon counting for quantum key distribution with Peltier cooled InGaAs/InP APD's // arxiv:quant-ph/0106007 (2001).
21. **Trifonov A., Subacius D., Berzanskis A., Zavriev A.** Single photon counting at telecom wavelength and quantum key distribution // Journ. Mod. Optics. 2004. **51**, N 9–10. P. 1399–1415.
22. **Thew R. T., Stucki D., Gautier J.-D. et al.** Free-running InGaAs/InP avalanche photodiode with active quenching for single photon counting at telecom wavelengths // Appl. Phys. Lett. 2007. **91**. P. 201114.
23. **Rochas A., Guillaume-Gentil C., Gautier J.-D. et al.** ASIC for high speed gating and free running operation of SPADs // Proc. SPIE. 2007. **6583**. P. 65830F.

Поступила в редакцию 19 мая 2009 г.