ЭКСПЕРИМЕНТАЛЬНЫЕ ИССЛЕДОВАНИЯ В ОБЛАСТИ КВАНТОВОЙ КРИПТОГРАФИИ*

В.Л. Курочкин, Институт физики полупроводников СО РАН, Новосибирский государственный университет; А.В. Зверев, Институт физики полупроводников СО РАН; Ю.В. Курочкин, Московский физико-технический институт; И.И. Рябцев, Институт физики полупроводников СО РАН, Новосибирский государственный университет, И.Г. Неизвестный, Институт физики полупроводников СО РАН

Представлен краткий обзор экспериментальных работ в области квантовой криптографии. Рассмотрены экспериментальные установки по распределению квантового ключа через воздушный промежуток и по оптоволоконной линии связи, созданные в ИФП СО РАН. Приведены результаты исследования параметров квантовой эффективности, вероятности появления после импульсов и уровня шумов для различных режимов работы InGaAs-InP лавинных фотодиодов.

ВВЕДЕНИЕ

Развитие экспериментальной квантовой физики в последние десятилетия привело к интересному результату. Абстрактные идеи квантовой механики начинают постепенно находить практическое применение. Благодаря новым технологическим возможностям квантовые приборы и устройства появляются в серийном производстве. В области квантовой оптики можно, прежде всего, выделить направления, связанные с созданием квантового компьютера и квантовых телекоммуникаций – квантовой криптографии. 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 такого метода состоит в распространении секретного ключа между пространственно удаленными пользователями.

В квантовой криптографии случайный ключ формируется путем организации передачи последовательности нулей и единиц 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

* Перепечатано из журнала "Микроэлектроника" с разрешения издательства "Академиздатцентр "Наука" РАН, Москва.

состояния фотона в строго определенном базисе. Безусловная секретность квантовой криптографии базируется на следующих запретах квантовой физики, которые накладываются на любой измерительный прибор. Первый – 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 которым факт вторжения может быть выявлен.

В 1984 году был предложен первый протокол, а в 1992 году осуществлена экспериментальная демонстрация генерации квантового ключа с помощью передачи одиночных, поляризованных в двух неортогональных базисах, фотонов по открытой линии связи [4,5]. Этот протокол получил общепринятое название BB84. В дальнейшем фундаментальные научные исследования в этой области постепенно перешли к проблеме создания практических квантовых систем связи и появлению первых коммерческих устройств. На данный момент исследования в области квантовой криптографии вызывают большой интерес в мире [6,7]. Разработки в области практической квантовой криптографии ведутся во многих странах и телекоммуникационных компаниях. Как и в классических видах связи, представляет интерес развитие методов распределения квантового ключа по открытому пространству и оптоволокну.

РАСПРЕДЕЛЕНИЕ КВАНТОВОГО КЛЮЧА ПО ОТКРЫТОМУ ПРОСТРАНСТВУ

При распространении излучения через атмосферу поляризация излучения подвергается незначительным изменениям, поэтому поляризационный метод кодирования используется при организации квантовых каналов через открытое пространство [8], причем в перспективе рассматривается возможность связи с орбитальными спутниками [9,10]. В спектре пропускания атмосферы есть окна с хорошей прозрачностью для излучения с длинами волн в районе 0,8 мкм. Считается, что вертикальная оптическая плотность атмосферы эквивалентна расстоянию примерно 8 км при нормальных условиях [8–10], поэтому потери фотонов на поглощение при связи со спутниками довольно малы. Генерация квантового ключа между наземными источниками и приемниками также представляет значительный интерес. Рассмотрим более подробно основные проблемы, возникающие при генерации квантового ключа.

Поскольку для секретности передачи требуется присутствие не более одного фотона в каждом лазерном импульсе, то к фотодетекторам приемного узла предъявляются высокие требования. Детекторы одиночных фотонов являются одним из важнейших элементов любой системы связи, построенной на принципах квантовой криптографии. Они должны обладать высокой квантовой эффективностью регистрации, малыми шумами и достаточно высокой скоростью счета. Наилучшими однофотонными детекторами в этой области являются кремниевые лавинные фотодиоды (ЛФД) [6], которые обычно применяются в криптосистемах для передачи ключа по открытому пространству. Для счета отдельных фотонов ЛФД включают так, чтобы они работали в так называемом гейгеровском режиме [11,12], когда

один фотон способен вызвать лавину носителей заряда. Если приложить к фотодиоду напряжение свыше некоторого порогового, то при попадании на него фотона происходит лавинное размножение носителей заряда, а коэффициент усиления таких ЛФД может составлять 10^5–10^6. Вероятность регистрации одного фотона достигает 50% для длины волны 830 нм. Для уменьшения собственных шумов лавинные диоды обычно охлаждаются полупроводниковыми микрохолодильниками. Частота появления шумовых импульсов ЛФД в гейгеровском режиме зависит от температуры и приложенного к нему напряжения сверх порогового. Для обеспечения стабильной работы и увеличения скорости генерации ключа необходимо тем или иным образом быстро остановить возникшую лавину, чтобы ЛФД был готов к приему следующего фотона. Для этого используются различные схемы включения с пассивным или активным гашением лавины, либо с импульсным питанием, когда напряжение на ЛФД поддерживается ниже порогового, а для регистрации одиночных фотонов его кратковременно (на несколько наносекунд) увеличивают выше порога [6, 11, 12]. Применение активной схемы гашения повышает скорость счета фотонов [11–13].

Если в первой экспериментальной установке [5] расстояние между передатчиком и приемником (длина квантового канала) была 0,3 м, то в дальнейшем наблюдался быстрый прогресс в сторону увеличения дальности связи. Так, в 2001 году был поставлен эксперимент по организации передачи на 1,9 км [14]. Распределение ключа на расстояния свыше эффективной толщины атмосферы было продемонстрировано в работах, например, [15] – 10 км, [8] – 23 км на основе протокола BB84 и используя перепутанные [16] состояния на 13 км [17]. Рекорд на данный момент принадлежит группе авторов работы [18], в которой представлены результаты по передаче ключа на расстояние 144 км. В 2008 году проведился эксперимент со спутником, когда был зарегистрирован отраженный однофотонный сигнал от лазерного импульса, посланного с земли [19]. Для подавления фоновых засветок от солнечного или лунного света применяют спектральные, пространственные и временные фильтры [20].

Нами в Институте физики полупроводников СО РАН в 2003 году была создана экспериментальная установка для проведения исследований по распределению квантового ключа через открытое пространство [21,22]. Передающий узел (Алиса) состоял из четырех полупроводниковых лазеров, каждый из которых генерировал импульсы излучения с одной из четырех поляризаций: 0°, 45°, 90° и -45°. Их лучи совмещались системой зеркал в один луч, ослаблялись на выходе поглощающими фильтрами до уровня одиночных фотонов и направлялись через воздушный промежуток 70 см в приемный узел (Боб). Полупроводниковые лазеры с модулированным по току источником питания работали в импульсном режиме с длительностью импульса 8–10 нс. Длина волны генерации излучения находилась вблизи 830 нм. Каждый лазер генерировал импульс когерентного излучения при подаче на его источник питания управляющего импульса от компьютера. Ослабленные лазерные импульсы попадали на вход приемного узла и разделялись на два луча светоделительным 50% зеркалом. Анализ поляризации фотонов производился с помощью двух призм Глана и четырех однофотонных счетчиков.

Схема приемного узла позволяет настроить передающий узел так, чтобы в каждом лазерном импульсе после выходного ослабителя находилось основном не более одного фотона, а доля двух и более фотонных импульсов была мала. Фотон любой поляризации, переданный Алисой, может попасть на три фотоприемника: в своем базисе на один (на второй его не пропускает поляризационная делительная призма) и в чужом базисе на два с равной вероятностью. Если одновременно регистрировать сигналы со всех четырех фотоприемников и дополнительно считать количество одновременных срабатываний двух и более фотоприемников, то, основываясь на статистике Пуассона, можно рассчитать долю многофотонных импульсов в передаче. Последовательно настраивая мощность генерации каждого из лазеров, можно установить требуемое среднее число фотонов в световых импульсах передающего узла.

В качестве однофотонных детекторов применялись специально отобранные лавинные фотодиоды (ЛФД) C30902S производства фирмы EG&G – одни из наиболее чувствительных для диапазона 0,8 мкм. Они работали в гейгеровском режиме [11,12] с пассивным гашением лавины.

Процесс генерации квантового ключа в нашем эксперименте происходил следующим образом. Компьютер Алисы задавал тактовую частоту повторения лазерных импульсов. На каждый такт вырабатывался синхроимпульс (строб), который посылался Бобу для синхронизации передачи-приема. Одновременно со стробом другой импульс подавался случайным образом на один

из четырех лазеров, этот лазер генерировал световой импульс длительностью 10 нс. Для выработки случайного числа использовался программный генератор случайных чисел, хотя, в общем случае, предпочтительнее применять генератор случайных чисел на основе естественных шумовых процессов [6]. Боб, получив синхроимпульс, вырабатывал дополнительно собственный строб-импульс длительностью 20 нс. Импульсы с фотоприемников регистрировались только во время подачи строба. Это позволяло избавиться от большей части собственных шумовых импульсов фотоприемников. Данные с четырех ЛФД считывались по синхроимпульсу компьютером Боба. В этой установке использовался один и тот же компьютер для Алисы и Боба, что не меняет общности проведения эксперимента, но позволяет слегка упростить его в аппаратурном исполнении. Если с какого-либо фотодиода приходил импульс в течение строб-импульса, то Боб запоминал эти данные, номер тактового импульса, и вырабатывал для Алисы сигнальный импульс, по которому она запоминала номер импульса и какой из лазеров в этом такте сработал. Поскольку среднее число фотонов в световом импульсе было много меньше единицы, то запоминать всю передачу не было необходимости. Боб случайным образом выбирал базис измерения поступивших фотонов. Если базисы Боба и Алисы совпали, то результатам измерений присваивался очередной порядковый номер и они заносились в файл создания ключа, в противном случае данные отбрасывались. В соответствии с протоколом BB84, после такой процедуры у Алисы и Боба генерировался согласованный случайный секретный ключ.

Скорость генерации ключа зависит от тактовой частоты повторения лазерных импульсов, количества $\bar{n}$ фотонов в импульсе и частотных характеристик ЛФД. В нашем эксперименте скорость генерации ключа ограничивалась темпом обмена данными между компьютером и приемопередающими узлами, что соответствовало тактовой частоте передачи 100 кГц.

В эксперименте при передаче с $\bar{n}$ ~0,1 на 10^6 тактовых импульсов был сформирован ключ длиной 10721 бита, из них только 104 бита (0,97%) оказались ошибочными (значения битов у Алисы и Боба не совпадали). При передаче с $\bar{n}$ ~0.2 длина ключа составила 18306 бита, а ошибка была в 174 битах (0,95%). Для используемой тактовой частоты 100 кГц это соответствовало скорости генерации ключа ~1 кбит/с и 1,8 кбит/с. На этой же установке нами была смоделирована ситуация несанкционированного перехвата подслушивателем всех фотонов своими детекторами и попытка передачи перехваченных данных Бобу. При сравнении полученного кода в этом случае по открытому каналу сразу же выяснилось, что процент ошибок в коде увеличился в десятки раз и факт присутствия подслушивателя на квантовой линии связи был выявлен.

ОПТОВОЛОКОННЫЕ КВАНТОВЫЕ ЛИНИИ СВЯЗИ

Оптоволоконные линии связи нашли широкое применение в классической связи, и первая работа по распределению квантового ключа по оптоволоконному квантовому каналу появилась уже в 1993 году [23]. Для квантовой криптографии используется стандартное одномодовое оптоволокно. Передача данных ведется обычно на телекоммуникационной длине волны 1550 нм, которая соответствует наименьшему затуханию и минимальной дисперсии в волокне [6].

На сегодняшний день наилучшими однофотонными детекторами в этой спектральной

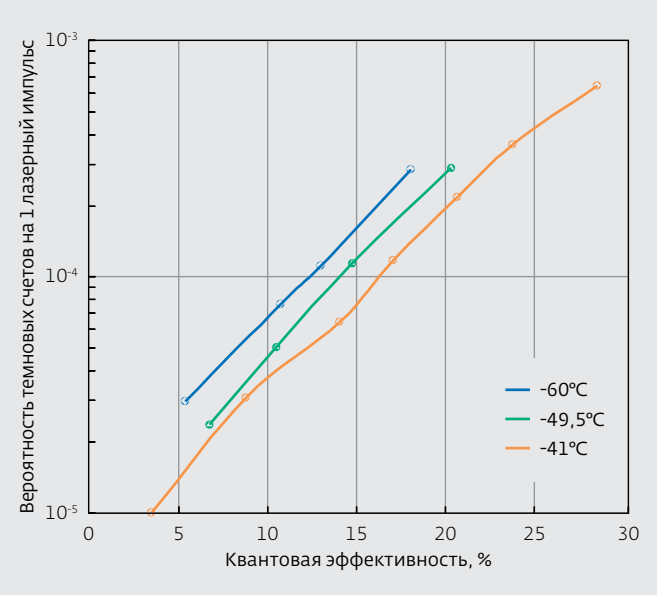

Рис.1. *Измеренные зависимости квантовой эффективности детекторов одиночных фотонов от величины темновых шумов на один лазерный импульс для различных температур*

области для практического использования являются лавинные InGaAs-InP фотодиоды (ЛФД) [6, 24–28]. По сравнению с кремниевыми фотодиодами они обладают меньшей квантовой эффективностью, обычно на уровне 10%, и большими шумами. Для регистрации отдельных фотонов ЛФД включают так, чтобы они работали в гейгеровском режиме [15, 20, 21]. Для этого обратное напряжение питания на них поднимают выше порогового напряжения пробоя. Чем выше напряжение над порогом, тем выше вероятность регистрации фотона. Однако при этом обычно значительно возрастают темновые шумы и вероятность появления так называемых послеимпульсов. При протекании тока лавины после срабатывания фотодиода от фотона или теплового шумового импульса могут заряжаться так называемые ловушки в объеме полупроводника, и затем, с некоторой задержкой, они начинают спонтанно разряжаться и могут приводить к появлению новой лавины заряда. Это вызывает ложные срабатывания фотодетектора. Эффект послеимпульсов сильно ограничивает максимальную частоту счета фотонов.

Для уменьшения влияния этих нежелательных эффектов применяют ряд специальных мер. Например, охлаждение ЛФД дает заметное уменьшение темновых шумов. Обычно температуру InGaAs-InP ЛФД понижают до -40°...-70°C с помощью микрохолодильников на основе элементов Пельтье. Однако понижение температуры приводит и к увеличению времени жизни заряженных ловушек, что также уменьшает скорость счета. Для снижения вероятности появления послеимпульсов применяют метод активного гашения лавины [26–28] 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 [24,23]. После прохождения лавины напряжение понижают ниже порога на некоторое время (5–20 мкс), чтобы дать возможность ловушкам разрядиться.

Более 10 лет назад была предложена одна удачная схема импульсного питания InGaAs-InP лавинных фотодиодов, на основе которой были измерены основные характеристики диодов и сделаны многие эксперименты по оптоволоконной квантовой криптографии [24,29]. С использованием этой схемы нами были экспериментально измерены основные рабочие характеристики нескольких лавинных фотодиодов [30]. В качестве детекторов одиночных фотонов были протестированы специально отобранные лавинные

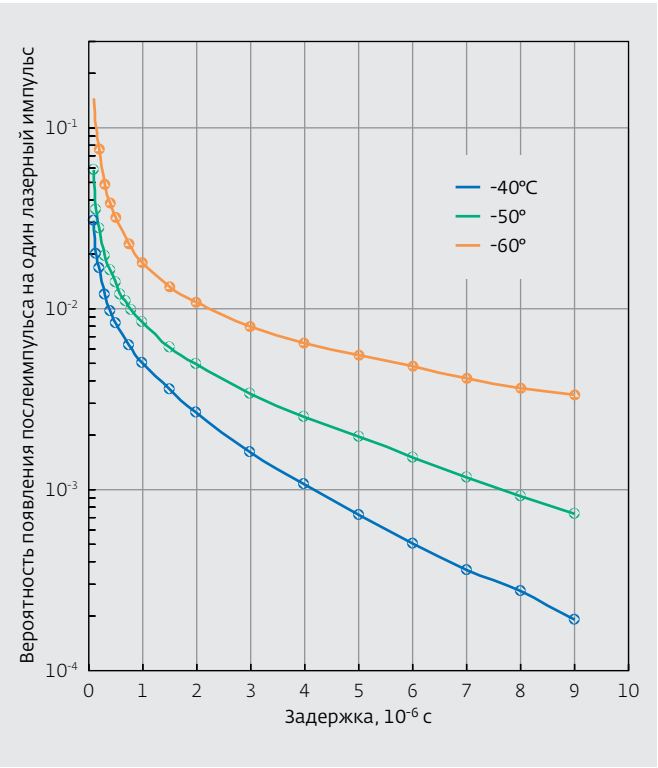

Рис.2. *Измеренные зависимости вероятности послеимпульсов детекторов одиночных фотонов от времени задержки после лазерного импульса для различных температур*

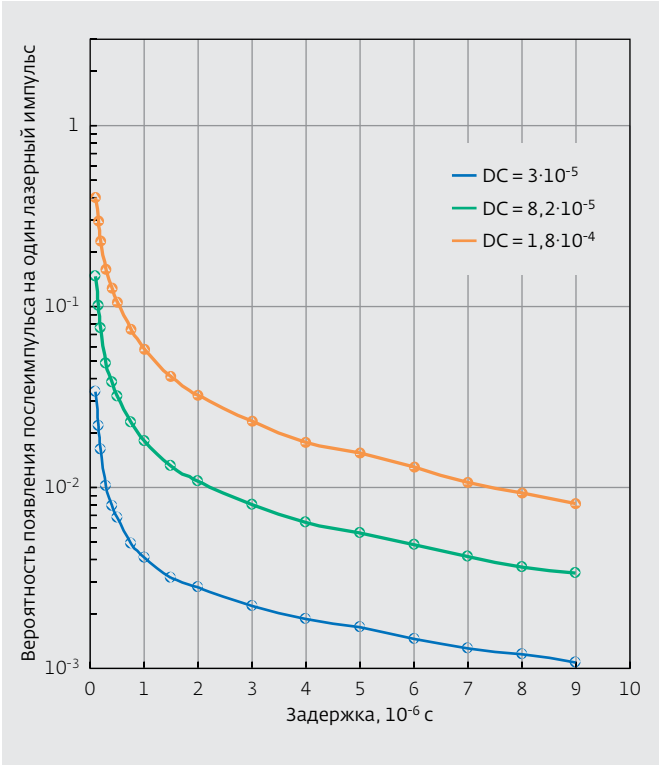

Рис.3. *Измеренные зависимости вероятности послеимпульсов детекторов одиночных фотонов от времени задержки после лазерного импульса для различных уровней темнового шума при температуре -60°С. DC – вероятность появления шумового импульса на один лазерный импульс*

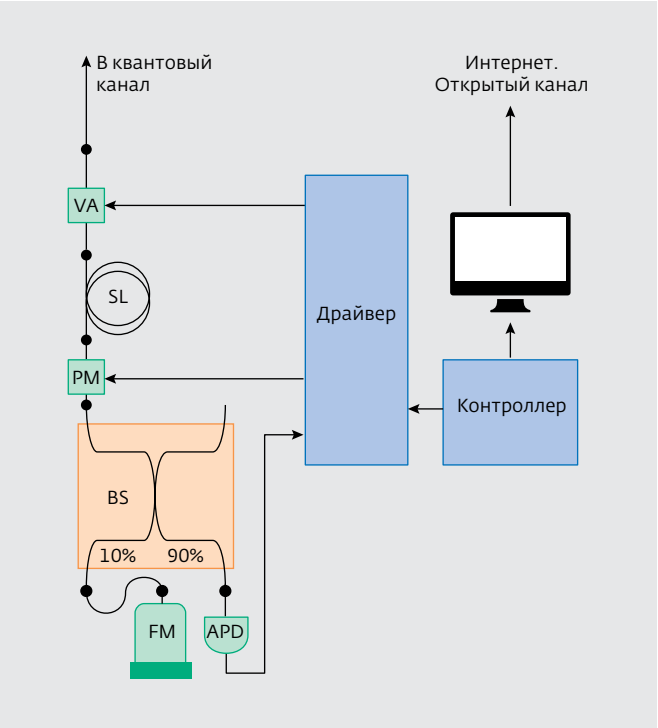

Рис.4. *Схема передающего узла (Алиса) оптоволоконной экспериментальной установки для генерации квантового ключа. VA – электрооптический аттенюатор, SL – накопительная линия, PM – фазовый модулятор, BS – оптоволоконный светоделитель 10%/90%, FM – зеркало Фарадея, APD – лавинный фотодиод*

InGaAs-InP фотодиоды ETX40 (Epitax, США), совмещенные с оптоволокном и работающие в режиме с импульсным питанием. Импульсы имели трапециевидную форму с 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 температуры -40°...-60°С. На рис.1 приведены измеренные нами зависимости квантовой эффективности регистрации от величины шумов в пересчете на один импульс для различных температур. При этих измерениях излучение импульсного лазера с частотой повторения лазерных импульсов 1 МГц ослаблялось оптоволоконными аттенюаторами до уровня 0,1 фотона на импульс. В момент прихода фотона на ЛФД подавался импульс питания, и фотодиод переходил в гейгеровский режим для регистрации одиночных фотонов.

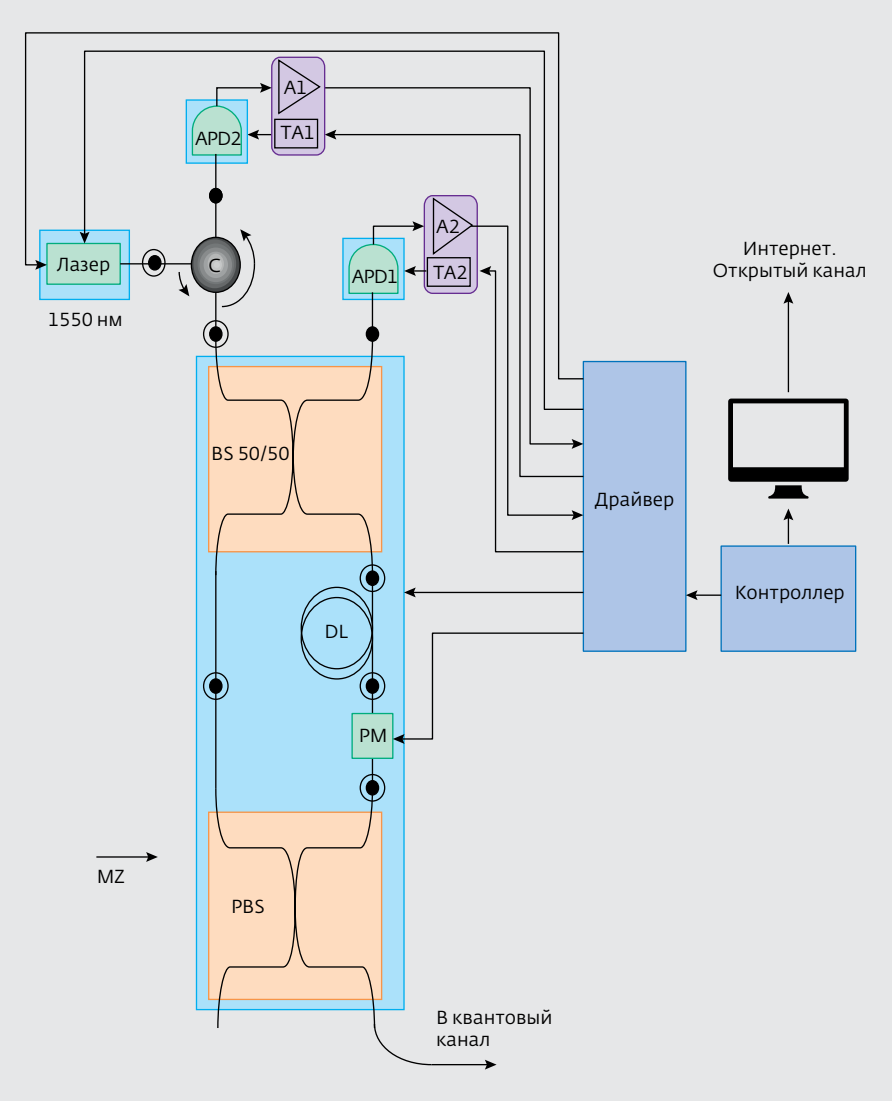

Рис.5. *Схема приемного узла (Боб) оптоволоконной экспериментальной установки для генерации квантового ключа. APD1 и APD2 –лавинные фотодиоды, A1 и A2 – усилители, TA1 и TA2 – триггеры запуска, C – циркулятор, BS50/50 – оптоволоконный светоделитель 50%/50%, DL – линия задержки, PM – фазовый модулятор, PBS – поляризационный светоделитель, MZ – интерферометр Маха-Цендера*

Вероятность регистрации и уровень темнового шума определялись суммарным обратным напряжением смещения ЛФД, которое варьировалось при проведении измерений.

На рис. 2 приведена зависимость вероятности появления послеимпульсов от времени задержки для различных температур. 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 влияние послеимпульсов от соседних световых импульсов [24,25]. 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 APD 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. На рис. 3 также приведена измеренная зависимость вероятности появления послеимпульсов от времени задержки, полученная для различного уровня шума при температуре фотодиода -60˚C. Уровень шумов задавался обратным напряжением смещения ЛФД в гейгеровском режиме.

Проведенные измерения показали, что характеристики наших детекторов, созданных на основе ЛФД ETX40, близки к данным, сообщаемым зарубежными исследователями [24]. Используя измеренные параметры фотодиода, можно выбрать рабочую точку для режима регистрации одиночных фотонов, исходя из допустимого уровня ложных срабатываний и квантовой эффективности, требуемых для конкретной задачи.

Для оптоволоконных линий связи применяются различные способы кодирования квантовых состояний фотонов [6, 7]. Например, одни из первых криптосистем работали на основе поляризационного кодирования [23, 31]. В последующих работах была продемонстрирована дальность связи свыше 100 км [32, 33]. Частотно-фазовое кодирование использовалось в [34, 35], временной способ был предложен и реализован авторами [36, 37]. Наиболее широкое применение нашло фазовое

кодирование с использованием интерферометров Маха-Цендера [2], где уже продемонстрирована генерация квантового ключа на расстояния свыше 100 км с помощью полупроводниковых детекторов одиночных фотонов [38, 39], и свыше 200 км со сверхпроводящими детекторами [40, 41].

Отдельно стоит отметить появление двухпроходной автокомпесационной оптической схемы для фазового кодирования [42], которая отличается устойчивой работоспособностью при изменяющихся внешних условиях и на основе которой построены коммерческие квантовые оптоволоконные криптосистемы [43, 44, 45].

Рассмотрим подробнее особенности работы такой оптической схемы [42] на примере экспериментальной установки, созданной нами в ИФП СО РАН. Эта установка может служить прототипом для создания практической квантовой криптосистемы.

Она состоит из передатчика Алиса (рис.4) и приемника Боб (рис. 5), которые соединены между собой одномодовым оптоволокном SMF-28 (квантовый канал) 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 C и направляется на первый светоделитель 50/50 (BS). Далее одна часть импульса поступает на вход поляризационного светоделителя PBS по короткому плечу оптоволоконного интерферометра Маха-Цендера MZ. Вторая часть импульса приходит на PBS, пройдя длинное плечо, образованное линией задержки длиной 10 м и оптоволоконным фазовым модулятором PM. Оптические элементы в длинном плече выполнены из поляризационно стойкого оптоволокна. Это позволяет сориентировать поляризацию излучения так, чтобы обе части импульса вышли через выход PBS и направились от Боба к Алисе по протяженному одномодовому оптоволокну (квантовому каналу связи).

После прохождения квантового канала лазерный импульс поступает на вход Алисы, проходит через накопительную линию SL (рис.4) длиной 25 км, фазовый модулятор PM, и отражается от так называемого фарадеевского зеркала FM, которое поворачивает поляризацию излучения на 90° для автокомпенсации поляризационных искажений оптоволокна. На обратном пути, на выходе из Алисы, лазерный импульс ослабляется перестраиваемым аттенюатором VA 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 PBS (рис. 5) они направляются в другое плечо интерферометра MZ, после прохождения которого соединяются на выходе BS, где они интерферируют. Результат интерференции регистрируется лавинным фотодиодом APD1 в одном плече, либо, после прохождения циркулятора C, на APD2 в другом плече. Поскольку эти две части импульса проходят одинаковый путь, причем в обратном порядке внутри Боба, этот интерферометр автоматически скомпенсирован. Это большое достоинство интерферометра такого типа и, например, коммерческие системы [43, 44, 45] построены именно на таком принципе.

Для реализации протокола BB84 Алиса случайным образом с помощью PM прикладывает в нужный момент времени фазовый сдвиг 0 или π (первый базис), либо π/2 или 3π/2 (второй базис) к световому импульсу, пришедшему от Боба. Боб, получив отраженные от Алисы одиночные

фотоны, также случайным образом выбирает базис для измерения, прикладывая сдвиг 0 (первый базис) или π/2 (второй базис) на свой фазовый модулятор PM в соответствующий момент времени.

В такой оптической схеме, когда импульсы распространяются вперед и назад, обратное рэлеевское рассеяние света может значительно увеличить шум, регистрируемый детекторами APD1 и APD2, 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 SL, вставленной для этой цели после аттенюатора VA в оптическую схему Алисы. Благодаря этому однофотонные импульсы, распространяющиеся обратно, больше не пересекаются в квантовом канале с многофотонными импульсами, идущими от Боба к Алисе. В нашей системе для накопительной линии длиной 25 км цуг импульсов 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, при этом регулируемый аттенюатор VA у Алисы устанавливается на полное пропускание. Боб принимает отраженный сигнал и на основании этих измерений устанавливает положение во времени строба длительностью 2,5 нс для детекторов APD1 и APD2, когда они должны регистрировать сигнал. Детекторы при этом работают в линейном режиме регистрации многофотонных световых импульсов. После этого устанавливается режим генерации квантового ключа. Обратное напряжение на лавинных фотодиодах поднимается выше порогового напряжения пробоя, и они переходят в режим регистрации одиночных фотонов. В качестве детекторов одиночных фотонов нами были использованы лавинные InGaAs-InP фотодиоды ETX40 (Epitax, США) совмещенные с оптоволокном и работающие в режиме с импульсным питанием. Рабочие характеристики этих детекторов были описаны выше. Боб испускает цуг лазерных импульсов. Аттенюатор VA у Алисы открыт на пропускание. Когда цуг импульсов заполнит накопительную линию SL, этот быстрый, электрически управляемый аттенюатор уменьшает свое пропускание до такого уровня, чтобы от Алисы к Бобу выходили световые импульсы с содержанием фотонов на уровне 0,1–0,3 фотона на импульс.

Далее светоделитель BS10/90 Алисы направляет 90% мощности излучения приходящих световых импульсов на вспомогательный многофотонный детектор APD. Он генерирует сигнал запуска, который используется для синхронизации опорного 20-МГц генератора Алисы 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 свой компьютер как порядковый номер импульса, так и базис измерения одиночных фотонов, зарегистрированных детекторами APD1 и APD2. 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 персональными компьютерами, которые задают режим работы оптоэлекторонных компонентов установки с помощью быстродействующей программируемой матрицы высокой степени интеграции.

На описанной экспериментальной установке нами были проведены тестовые эксперименты по генерации квантового ключа в протяженной оптоволоконной линии связи между Алисой и Бобом длиной 25 км. Предварительно проводилось измерение контраста интерферометра Маха-Цендера у Боба, который является источником дополнительных ошибок при генерации ключа [42]. Измерения выполнялись в многофотонном режиме, когда отсутствуют шумы, обусловленные собственными шумами однофотонных детекторов, работающих в гейгеровском режиме. Для регистрации оптического сигнала использовался фотодетектор с линейным диапазоном выходного сигнала 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 [42].

В начале каждого эксперимента проводилась процедура настройки всей системы в многофотонном режиме. 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 экспериментах была получена генерация квантового ключа со скоростью 450 бит/с. Общее количество ошибок в ключе не превышало 3,7%. Учитывая, что максимальная допустимая ошибка в квантовой передаче не должна превышать 11% [15], полученный результат можно считать вполне удовлетворительным для экспериментальной генерации ключа.

В заключение отметим, что используемая нами импульсная схема питания ЛФД с длительностью импульса в несколько наносекунд [24,29] обладает ограничением на тактовую частоту подачи импульсов на фотодиод в 5–10 МГц. В последние годы было найдено оригинальное техническое решение, позволяющее преодолеть этот недостаток и увеличить тактовую частоту и, соответственно, скорость счета фотонов. В работах [46–51] напряжение на фотодиоде поднималось выше порогового на доли наносекунды, что позволило увеличить частоту вплоть до 2 ГГц и получить скорость счета фотонов в сотни мегагерц. Опубликованы экспериментальные результаты распределения квантового ключа с такими детекторами [52]. Научные коллективы [50, 51] объявили о создании квантовых оптоволоконных криптосистем связи, которые будут работать на тактовых частотах выше 2 ГГц.

ЗАКЛЮЧЕНИЕ

Экспериментальные исследования в области квантовой криптографии вызывают все возрастающий интерес в мире. Практические разработки интенсивно ведутся во многих научных учреждениях и телекоммуникационных компаниях. Начиная с первой экспериментальной работы [5], где расстояние между передатчиком и приемником было 30 см, пройден большой путь развития. Передача ключа по открытому пространству продемонстрирована на 144 км [18], и теперь усилия направлены на глобальное географическое распределение ключа [9, 10, 19]. Экспериментальные ограничения, связанные с малой скоростью генерации ключа, в ближайшее время будут преодолены. Ожидается появление высокоскоростных квантовых криптосистем, работающих на тактовой частоте в несколько гигагерц [50–52]. Это позволит поднять скорость генерации квантового ключа до уровня, удовлетворяющего стандартные требования к телекоммуникационным системам связи.

ЛИТЕРАТУРА

1. **Shannon C.E.** Communication Theory of Secret Systems. – Bell Syst. Tech. Jour., 1949, v. 28, p. 658–715.
2. **Bennet C.H.** Quantum Cryptography Using any Two Nonorthogonal States Phys. – Rev. Lett., 1992, v.68, p. 3121–3124.
3. **Wooters W.K., Zurek W.H.** A single quantum cannot be cloned. – Nature, 1982, v.299, p. 802–803.
4. **Bennet C.H. Brassard G.** Quantum Cryptography: Public Key Distribution and Coin Tossing. – Proc. of IEEE Int. Conf. on Comput. Sys. and Sign. Proces., Bangalore, India, December 1984, p. 175–179.
5. **Bennet C.H. Bessette F. Brassard G. et.al.** Experimental Quantum Cryptography. – J.Cryptology, 1992, v. 5, p. 3–28.
6. **Gisin N., Ribordy G., Title W. et al.** Quantum Cryptography. – Rev. of Mod. Phys., 2002, v. 74, p. 145–175.
7. **Scarani V., Pasquinucci H., Cerf N. et al.** The security of practical quantum key distribution. – Rev. of Mod. Phys., 2009, v. 81. p. 1301
8. **Kurtsiefer C., Zarda P., Halder M. et al.** Quantum cryptography: A step towards global key distribution. – Natura, 2002, v. 419, p. 450.
9. **Rarity J.G., Tapster P.M., Gorman P.M., Knight P.** Ground to Satellite Secure Key Exchange Using Quantum Cryptography. – New J. Physics, 2002, v. 4, p. 82.1–82.21.
10. **Ursin R., Jennewein T., Koer J et.al.** Space-QUEST: Experiments with quantum entanglement in space. 2008, arxiv:quant-ph/0806.0945
11. **Ghioni M., Cova S., Zappa F. et al.** Compact active quenching circuit for fast photon counting with avalanche photodiodes. – Rev. Sci. Instrum., 1996, v. 67, № 10, p. 3440–3448.
12. **Cova S., Ghioni M., Laciata A.** Avalanche photodiodes and quenching circuits for single-

photon detection . – Applied optics, 1996, v. 35. № 12, p. 1956-1976.
13. **Kurochkin V.L., Ovchar V.K.** Free space quantum key distribution system with hight rate counter single photon detectors. Abstract of EQIS' Conf., Tokyo, Japan, September 1–5, 2004, p.116–117.
14. **Raritya J.G.; Tapstera P.R.; Gormana P.M.** Secure free-space key exchange to 1,9 km and beyond. –J. Modern Optics, 2001, v.48, № 13, p.1887 – 1901.
15. **Hughes R.J., Nordholt J.E., Derkacs D., Peterson C.G.** Practical free-space quantum key distribution over 10 km in daylight and at night. – New J. Physics, 2002, v. 4, p. 43.1 – 43.14.
16. **Ekert A.K.** Quantum Cryptography Based on Bell's Theorem. – Phys. Rev. Lett., 1991, v. 67, p. 661–663.
17. **Peng C., Yang T., Bao X. et al.** Experimental Free-Space Distribution of Entangled Photon Pairs Over 13 km: Towards Satellite-Based Global Quantum Communication. –Phys. Rev. Lett. 2005,v.94, p.150501.
18. **Ursin R., Tiefenbacher F., Schmitt-Manderbach T. et al.** Entanglement based quantum communication over 144 km.– Nature Physics, 2007, p.3, p.481–486.
19. **Villoresi P., Jennewein T., Tamburini F. et al.** Experimental verification of the feasibility of a quantum channel between space and earth. –New J. Phys., 2008, v.10, № 3, p.033038.
20. **Miao Er-long, Han Zheng-fu, Gong Shun-sheng et al.** Background noise of satellite-to-ground quantum key distribution. – New Journal of Physics, 2005, v.7, № 1, p.215.
21. **Курочкин В.Л., Рябцев И.И., Неизвестный И.Г.** Генерация квантового ключа на основе кодирования поляризационных состояний фотонов.– Оптика и спектроскопия, 2004, т. 96, вып.5, с. 772–776.
22. **Курочкин В.Л., Рябцев И.И., Неизвестный И.Г.** Квантовая криптография и генерация квантового ключа с использованием одиночных фотонов. – Микроэлектроника, 2006, т. 35, №1, с. 41–47.
23. **Muller A., Breguet J., Gisin N.** Experimental Demonstration of Quantum Cryptography Using Polarized Photons in Optical Fibre over More than 1 km. – Europhys. Lett. 1993, v.23, № 6, p.383–388.
24. **Ribordy G., Gautier J D, Zbinden H. Gisin N.** Performance of InGaAs/InP avalanche photodiodes as gated-mode photon counters. – Appl. Opt., 1998, v.37, № 12, p.2272–2277
25. **Trifonov A., Subacius D., Berzanskis A., Zavriev A.** Single photon counting at telecom wavelength

and quantum key distribution. – J. Mod. Optics, 2004,v.51, № 9–10, p.1399–1415.
26. **Thew R. T., Stucki D., Gautier J.-D. , Zbinden H., Rochas A.** Free-running InGaAs/InP avalanche photodiode with active quenching for single photon counting at telecom wavelengths. – Appl. Phys. Lett., 2007, v. 91, p. 201114.
27. **Rochas A., Guillaume-Gentil C., J.-D.Gautier et al.** ASIC for high speed gating and free running operation of SPADs. – Proc. of SPIE, 2007, v. 6583, p. 65830F.
28. **Zhang J., Thew R., Gautier J., Gisin N., Zbinden H.** Comprehensive Characterization of InGaAs–InP Avalanche Photodiodes at 1550 nm With an Active Quenching ASIC IEEE.– J. of Quantum Electronics, 2009, v.45, № 7, p.792–799.
29. **Stucki D., Ribordy G., Stefanov A. et al.** Photon counting for quantum key distribution with Peltier cooled InGaAs/InP APD's. – J. Mod. Opt., 2001, v. 48, № 13, p.1967–1981.
30. **Курочкин В.Л., Зверев А.В., Курочкин Ю.В. и др.** Применение детекторов одиночных фотонов для генерации квантового ключа в экспериментальной оптоволоконной системе связи. – Автометрия, 2009, т.45, №4, с. 110-119.
31. **Muller A., Zbinden H., Gisin N.** Quantum cryptography over 23 km in installed under-lake telecom fibre. – Europhys. Lett., 1996,v.33, № 4. p.335–339.
32. **Wu G., Chen J., Yao Li, Zeng H.** Stable polarization-encoded quantum key distribution in fiber. 2006, arXiv:quant-ph/0606108.
33. **Peng C., Zhang J., Dong Yang et al.** Experimental Long-Distance Decoy-State Quantum Key Distribution Based on Polarization Encoding. – Phys. Rev. Letters, 2007, v.98, № 1, p.010505.
34. **Mazurenko Y., Giust R., Goedgebuer J.** Spectral coding for secure optical communications using refractive index dispersion. – Opt. Commun. 1997, v.133, p.87–92.
35. **Merolla J-M., Mazurenko Y., Goedgebuer J. P., Rhodes W. T.** Single-photon interference in sidebands of phase-modulated light for quantum cryptography. – Phys. Rev. Lett., 1999, v.82, p.1656–1659.
36. **Debuisschert T., Boucher W.** Time coding protocols for quantum key distribution. – Phys. Rev. A , 2004, v.70, p.042306.
37. **Boucher W., Debuisschert T.** Experimental implementation of time-coding quantum key distribution. – Phys. Rev. A., 2005, v.72, № 6, p. 062325.
38. **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. – Electronics let., 2003, v. 39, p. 1119–1201.
39. **Kimura T., Nambu Y., Hatanaka T. et al.** Single-Photon Interference over 150-km Transmission Using Silica-Based Integrated-Optic Interferometers for Quantum Cryptography. 2004, arxiv:quant-ph/0403104.
40. **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, v. 1, p. 343–348.
41. **Stucki D., Walenta N., Vannel F. et al.** High rate, long-distance quantum key distribution over 250km of ultra low loss fibres. – 2009, arxiv:quant-ph/0903.3907.
42. **Stucki D., Gisin N., Guinnard O. et al.** Quantum key distribution over 67 km with a plug&play system. – New Journal of Physics. 2002, v.4, p. 41.1–41.8.
43. http://www.magiqtech.com
44. http://www.idquantique.com
45. http://www.smartquantum.com
46. **Namekata N., Sasamori S., Inoue S.** 800MHz Single-photon detection at 1550-nm using an InGaAs/InP avalanche photodiode operated with a sine wave gating. – Opt. Express, 2006, v.14, p.10043.
47. **Yuan Z. L, Kardynal B. E, Sharpe A. W., Shields A. J.** High speed single photon detection in the near infrared – Appl. Phys. Lett., 2007, v.91, p. 041114.
48. **Zhang J., Thew R., Barreiro C., Zbinden H.** Practical fast gate rate InGaAs/InP single-photon avalanche photodiodes. –Appl. Phys. Lett., 2009, v.95, № 9, p.091103.
49. **Namekata N., Adachi S., Inoue S.** 1.5 GHz single-photon detection at telecommunication wavelengths using sinusoidally gated InGaAs/InP avalanche photodiode. – Optics Express , 2009, v.17, № 8, p.6282–6275.
50. **Yuan Z.L., Sharpe A.W., Dynes J.F. et al.** Multi-gigahertz operation of photon counting InGaAs avalanche photodiodes. – Appl. Phys. Lett., 2010, v.96, №7, p.071101.
51. **Zhang J., Eraerdsa P., Walentaa N. et al.** 2.23GHz gating InGaAs/InP single-photon avalanche diode for quantum key distribution. 2010, arXiv:1002.3240.
52. **Dixon A. R., Yuan1 L., Dynes1 J. F. et al.** Gigahertz decoy quantum key distribution with 1 Mbit/s secure key rate. – Optics Express, 2008, v.16, № 23, p.18790–18797.