05;06;07;12

Экспериментальная установка для квантовой криптографии с одиночными поляризованными фотонами

© В.Л. Курочкин, И.И. Рябцев, И.Г. Неизвестный

Институт физики полупроводников СО РАН,
630090 Новосибирск, Россия
e-mail: kurochkin@isp.nsc.ru

(Поступило в Редакцию 16 июня 2004 г.)

Приводятся описание и результаты первых экспериментов на установке для квантовой криптографии с одиночными фотонами. Передача ключа осуществлялась импульсными полупроводниковыми лазерами на основе кодирования поляризованных состояний фотонов в двух альтернативных базисах, не ортогональных друг другу. В качестве детекторов одиночных фотонов использовались специально разработанные высокоскоростные детекторы на основе кремниевых лавинных фотодиодов C30902S. При тактовой частоте повторения лазерных импульсов 100 kHz и среднем числе фотонов в импульсе около 0.2 получена скорость генерации ключа ~ 4 bit/s. Количество ошибок в ключе не превышало 1%.

На сегодняшний день квантовая криптография является наиболее развитой областью квантовой информатики с точки зрения практического применения. Квантовая криптография позволяет реализовать абсолютно секретную передачу данных между двумя легитимными пользователями линии связи. Секретность и невозможность незаметного прослушивания посторонним лицом передаваемых данных основана на фундаментальных законах природы 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 является нерасшифровываемой, 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. Классические методы связи не могут обеспечить, вообще говоря, секретность распространения ключа по открытым каналам связи, так как существуют методы незаметного подслушивания передачи и нет гарантий возможности дальнейшей расшифровки.

Идеи квантовой физики и квантовой информатики, примененные к задачам передачи информации на дальние расстояния, предлагают решение проблемы распространения абсолютно случайного ключа по открытым каналам связи с гарантией его секретности. Безусловная секретность квантовой криптографии базируется на следующих запретах квантовой физики, которые накладываются на любой измерительный прибор: 1) невозможно получить информацию о неортогональных состояниях без из возмущения [2], 2) невозможно достоверно скопировать неизвестное квантовое состояние (теорема „no cloning“) [3]. Из этих положений следует, что если в качестве носителей информации использовать одиночные квантовые объекты, то любая попытка вторжения несанкционированным лицом в процесс передачи неизбежно приведет к необратимому изменению квантовых состояний объектов, по которым факт вторжения может быть выявлен.

Первыми обосновали принципы квантовой криптографии и предложили протокол для их реализации Беннет и Брассард [4] в 1984 г. Появление их первой экспериментальной работы [5] вызвало большой интерес в мире, и с этого момента началось бурное развитие этого направления. В этой работе реализован протокол распространения ключа — секретной последовательности нулей и единиц с помощью одиночных, поляризованных в двух неортогональных базисах фотонов. В дальнейшем этот протокол был назван BB84. Широкое применение в дальнейшем нашел протокол, основанный на фазовом кодировании с использованием интерферометров Маха–Цендера, основные положения которого были заложены в [2]. Принципиально новые идеи выдвинул Экерт [6] для обоснования распределения квантового ключа с помощью перепутанных состояний на базе эффекта Эйнштейна–Подольского–Розена. Идеи и перспективы квантовой криптографии оказались настолько привлекательными, что различные исследовательские группы сражу же начали активную работу по созданию реально работающих установок и устройств. Хороший обзор теоретических и экспериментальных работ в этом направлении сделан в [7]. С момента его опубликования предложено много новых принципов организации квантовых каналов связи. Например, в [8,9] изложены основы релятивистской квантовой криптографии, в [10] предложена частотно-временна́я схема кодирования, в [11,12] для формирования ключа используется фазовый сдвиг между двумя последовательными одиночными когерентными фотонами. Успешно продемонстрировано распространение квантового ключа на десятки километров с помощью однофотонной квантовой криптографии как по оптоволоконным линиям связи, так и по открытому пространству. Отметим, что первые предложенные протоколы оказались и наиболее практичными для организации реальных квантовых каналов связи. Принцип фазового кодирования был реализован в оптоволоконных линиях

связи длиной 67 [13], 100 [14] и 150 km [15]. Протокол на основе поляризационного кодирования BB84, использованный и в нашей работе, применен для организации связи по открытому пространству на 10 [16] и 23 km [17], и в перспективе рассматривается возможность связи с орбитальными спутниками [18].

В данной статье приведены экспериментальные результаты генерации квантового ключа на созданной авторами установке для квантовой криптографии. Передача осуществлялась на основе кодирования поляризационных состояний единичных фотонов, излучаемых импульсными полупроводниковыми лазерами, в двух альтернативных базисах, не ортогональных друг другу (протокол BB84 [4]). Целью работы являлось экспериментальное исследование методов генерации одиночных фотонов в заданном квантовом состоянии и последующего детектирования этих фотонов с разделением по их исходным состояниям при низком уровне ложных измерений. Также была релазиована модель полного перехвата всех фотонов в квантовом канале посторонним лицом и экспериментально продемонстрирована невозможность незаметного присутствия несанкционированного лица в квантовой линии передачи. В качестве детекторов использовались высокоскоростные модули счетчиков одиночных фотонов на основе кремниевых лавинных фотодиодов C30902S с активной схемой гашения лавины.

Кратко рассмотрим основные принципы генерации квантового ключа на основе протокола BB84 [4,7]. Передающая сторона (традиционно называемая в литературе Алисой) подготавливает однофотонные состояния с линейной поляризацией в двух не ортогональных друг другу базисах: один, назовем его вертикально-горизонтальным, с поляризацией фотонов 0 и 90°, второй, назовем его диагональным, с поляризацией 45 и −45°. Алиса и приемная сторона (традиционно называемая Бобом) договариваются о коде каждой поляризации в двоичном представлении: например, фотоны с поляризацией 0 и 45° обозначают число 0, а фотоны с поляризацией 90 и −45° означают число 1. Во время передачи Алиса посылает последовательность фотонов, поляризация которых выбрана случайным образом, и может составлять 0, 45, 90 и −45°. Боб регистрирует пришедшие фотоны и для каждого из них случайным образом выбирает базис измерения. По открытому дополнительному каналу связи Боб сообщает Алисе, в каком базисе он провел измерение, но не сообщает результат этого изменения. Поскольку фотон может иметь значение и 0 и 1, то сообщение о факте регистрации фотона по открытому каналу не дает никакой информации постороннему подслушивателю (обычно называемой Евой). Алиса в ответ сообщает ему, правильный ли базис измерения был выбран для каждого фотона. Сохраняя в серии только измерения, проведенные в правильном базисе, Алиса и Боб создают уникальную случайную последовательность нулей и единиц, из которой затем и формируется секретный ключ.

Важным этапом квантово-криптографической передачи является проведение проверочного теста о возможном перехвате 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 совпадает. Уровень ошибок в коде будет обусловлен шумами детектора и неидеальностью оптического канала связи. Если внешний подслушиватель на пути от Алисы к Бобу будет считывать информацию из квантового канала связи, то, поскольку передача ведется одним фотоном, он будет вынужден пытаться сгенерировать такой же фотон и заново отправить его к Бобу. В этом случае в соответствии с теоремой о невозможности клонирования состояния произвольного квантового объекта [3] он необратимым образом разрушит поляризационные состояния фотонов и не сможет их вопроизвести с полной достоверностью. Это вызовет несовпадение в сформированном коде, и 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 прослушивания не будет зафиксирован.

Схема нашей экспериментальной установки представлена на рис. 1 и 2. Передающий узел (рис. 1) состоял из четырех полупроводниковых лазеров (2) ИЛПН-210, каждый из которых генерировал импульсы излучения с одной из четырех поляризаций 0, 45, 90 и −45°. Их лучи совмещались системой зеркал *5* в один луч, ослаблялись на выходе поглощающими фильтрами *6* и направлялись через воздушный промежуток длиной 70 cm (закрытый от внешнего света) в приемный узел. Полупроводниковые лазеры с модулированным по току источником питания *1* работали в импульсном режиме с длительностью импульса 8–10 ns. Длина волны генерации излучения находилась вблизи 830 nm. Лазеры термостабилизировались с помощью полупроводниковых микрохолодильников *3* на основе элементов Пельтье. Каждый лазер генерировал импульс когерентного излучения при подаче на его источник питания управляющего импульса от компьютера. Ослабленные лазерные импульсы попадали на вход приемного узла (рис. 2) и разделялись на два луча светоделительным 50%-ным зеркалом *1*. Луч, прошедший прямо (рис. 2), направлялся на поляризационную разделительную призму Глана *3*, которая направляла фотоны, пришедшие в вертикально-горизонтальном базисе, каждый в свой фотоприемник *4* с коэффициентом разделения не хуже 10^4. Фотоны, пришедшие в диагональном базисе,

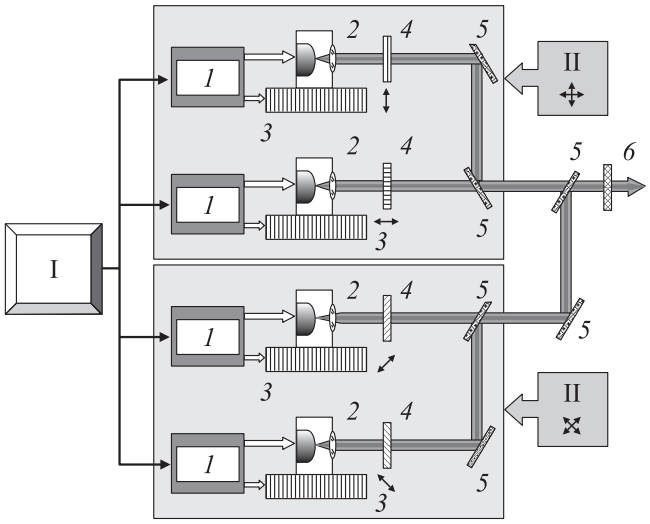

Рис. 1. Схема передающего узла экспериментальной установки для квантовой криптографии с одиночными фотонами: *1* — источник питания полупроводникового лазера, *2* — полупроводниковый лазер, *3* — микрохолодильник на основе элемента Пельтье, *4* — поляризатор (призма Глана), *5* — зеркало, *6* — поглощающий фильтр. I — ЭВМ, II — базис.

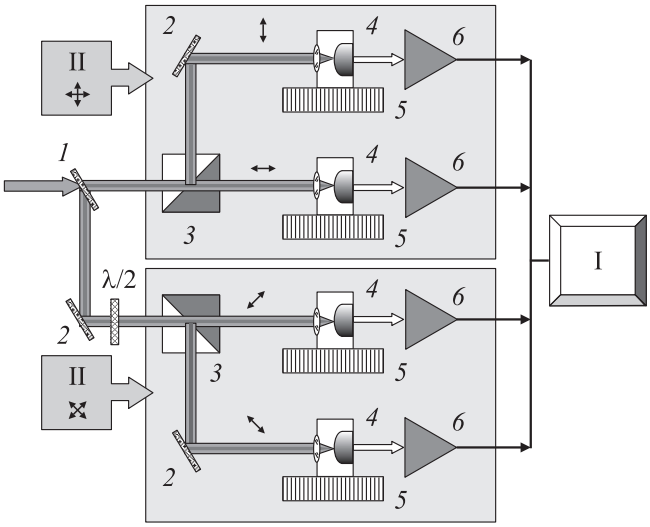

Рис. 2. Схема приемного узла экспериментальной установки: *1* — светоделительное 50%-ное зеркало, *2* — зеркало, *3* — поляризационная разделительная призма Глана, *4* — лавинный фотодиод с собирающей линзой, *5* — микрохолодильник на основе элемента Пельтье, *6* — усилитель, $\lambda/2$ — полуволновая пластинка, I — ЭВМ, II — базис.

с равной вероятностью 50% попадали на любой из этих двух фотоприемников. Вторая часть входного луча, отклоненная входной светоделительной пластинкой, проходила вначале через полуволновую пластинку $\lambda/2$, после которой поляризация фотонов поворачивалась на 45°. В результате пришедшие в диагональном базисе фотоны распределялись с помощью поляризационной разделительной призмы с высоким коэффициентом деления по соответствующим фотоприемникам. Фотоны, пришедшие в другом базисе, попадали на любой из этих двух фотоприемников с равной вероятностью.

Устройство приемного узла позволяет настроить передающий узел так, чтобы в каждом лазерном импульсе после выходного ослабителя находилось в основном не более одного фотона. В таких условиях распределение количества фотонов по импульсам подчиняется статистике Пуассона. В квантовой криптографии сигнал считается однофотонным, если среднее число фотонов $\bar{n}$ в импульсе находится в пределах 0.1–0.2 [7]. Так, для $\bar{n} = 0.1$ доля импульсов с двумя фотонами составляет 5% от однофотонных, трехфотонных — 0.16%. Практически в этом случае из каждых 10 импульсов в 9 нет ни одного фотона. 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.

Поскольку для секретности передачи требуется присутствие не более одного фотона в каждом лазерном импульсе, то к фотодетекторам приемного узла предъявляются высокие требования. Они должны обладать высокой квантовой эффективностью регистрации, малыми шумами и достаточно высокой скоростью счета. Криптосистемы для передачи ключа по открытому пространству [16,17] работают в диапазоне длин волн $\sim 0.85\,\mu$m, который соответствует окну прозрачности атмосферы. На сегодняшний день наилучшими однофотонными детекторами в этой области являются лавинные фотодиоды. В нашей установке в качестве однофотонных детекторов применялись специально отобранные лавинные фотодиоды (ЛФД) C30902S производства фирмы EG&G — одни из наиболее чувствительных для диапазона $0.8\,\mu$m [7,19]. На их основе был разработан и изготовлен высокоскоростной счетчик одиночных фотонов с активной схемой гашения лавины [20,21]. Для счета отдельных фотонов ЛФД включают так, чтобы они работали в гейгеровской моде [19,20,21], когда один фотон способен вызвать лавину носителей заряда. Фотодиоды в трех детекторах (рис. 2, *4*) были подключены по схеме с пассивным гашением лавины, а один — с активным гашением. Балластное сопротивление 200 kΩ ограничивало ток в ЛФД. Сигнал снимался с нагрузочного сопротивления 50 Ω [6], усиливался усилителем *6* и поступал на формирователь стандартных TTL импульсов для сопряжения с компьютером. Если приложить к фотодиоду напряжение свыше некоторого порогового $U(BR)$, то при попадании на него фотона происходит лавинное размножение носителей заряда и коэффициент

усиления у этих ЛФД может достигать 10^5-10^6. Вероятность регистрации одного фотона достигает 50% для всей длины волны 830 nm. Для уменьшения собственных шумов диоды охлаждались полупроводниковыми микрохолодильниками Пельтье до -20°C. Частота появления шумовых импульсов ЛФД в гейгеровской моде зависит от температуры и приложенного к нему напряжения сверх порогового. На рис. 3 приведена измеренная зависимость частоты появления шумовых импульсов от превышения напряжения питания U над пороговым $U-U(BR)$ при температуре диода -20°C.

Один фотодетектор *4* (рис. 2) представлял собой разработанный высокоскоростной счетчик одиночных фотонов с активной схемой гашения лавины [20,21] и скоростью счета на уровне нескольких мегагерц. В отличие от [20,21] наша схема предусматривает возможность работы ЛФД в различных режимах активного ограничения протекающего тока через фотодиод, что позволяет защитить его при яркой засветке. Это — важное достоинство нашей схемы, так как при включении C30902S в гейгеровской моде они могут выходить из строя от излишне высокого светового потока. Амплитуда импульса напряжения гашения лавины регулируется от 5 до 25 V. Имеется дискриминатор уровня сигнала, регулируемый по задержке и длительности строб-импульс. Минимальная длительность строба 30 ns. На выходе счетчика сигнал можно наблюдать в аналоговом режиме или формировать ТТЛ импульс для подачи на компьютер. На рис. 4 приведена измеренная зависимость скорости счета фотонов счетчиком с активным гашением лавины для различных режимов ограничения тока и различных параметрах лазерного импульса: *a* — ограничение скорости счета 2.5 MHz, *b* — 250 kHz.

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 ns. Для выработки случайного числа использовался программный генератор случайных чисел, хотя в общем случае предпочтительнее применять генератор случайных чисел на основе естественных

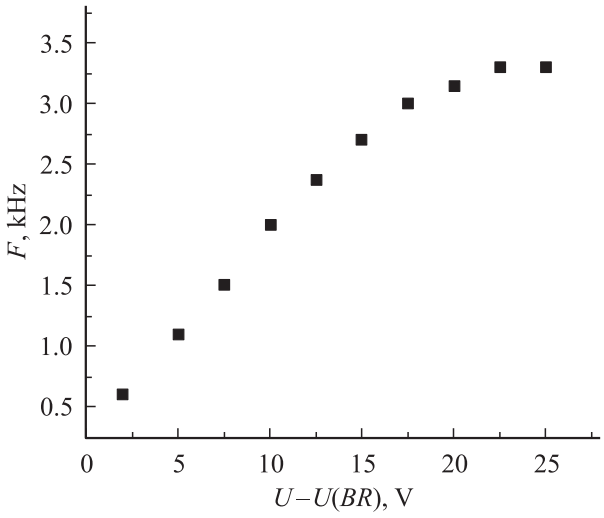

Рис. 3. Зависимость количества шумовых импульсов F лавинного фотодиода C30902S от превышения напряжения питания U над пороговым $U(BR)$ при температуре -20°.

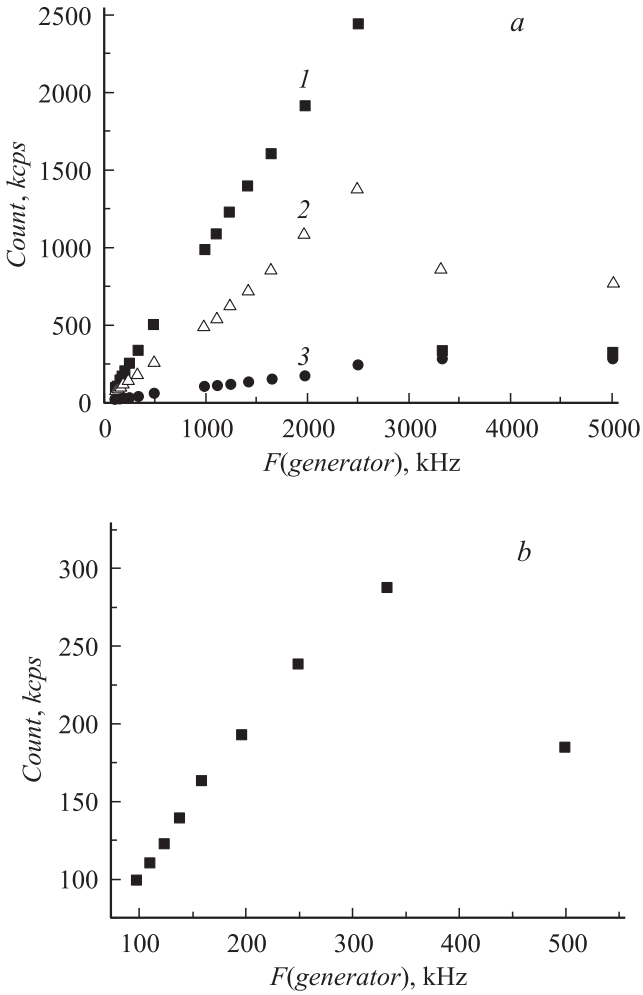

Рис. 4. Зависимость числа счетов COUNT в секунду счетчика одиночных фотонов от частоты $F\,(generator)$ повторения лазурных импульсов. *a* — счетчик включен в режиме ограничения максимальной скорости света $2.5\cdot10^6$ счетов в секунду: *1* — интенсивность лазерного импульса соответствует срабатыванию счетчика с вероятностью *2* — интенсивность лазерного импульса меньше по сравнению с кривой *1* и соответствует срабатыванию счетчика с вероятностью 0.5, *3* — интенсивность лазерного импульса еще меньше и вероятность детектирования этого светового импульса равна 0.1. Это примерно соответствует среднему числу фотонов в импульсе $n\sim0.2$. *b* — счетчик включен в режиме ограничения максимальной скорости счета $2.5\cdot10^5$ счетов в секунду. Интенсивность лазерного импульса соответствует срабатыванию счетчика с вероятностью 1.

шумовых процессов [7]. Боб, получив синхроимпульс, вырабатывал дополнительно собственный строб-импульс длительностью 20 ns. Импульсы с фотоприемнимов регистрировались только во время подачи строба. Это позволяет избавиться от большей части собственных шумовых импульсов фотоприемников. Так, если при температуре -20°C и напряжении над порогом 20 V общее число шумовых импульсов около $3 \cdot 10^3$ в секунду (рис. 3), то при временно́м стробировании сигнала число шумовых импульсов составило около 100 на 10^6 тактовых импульсов передачи. Длительность шумовых и однофотонных импульсов с фотодиода после усилителя составляла 8–10 ns. Предварительное согласование задержки между стробом и импульсом с ЛФД (при срабатывании его от лазерного импульса передатчика) дает возможность значительно улучшить соотношение сигнал/шум и уменьшить количество ошибок в конечном коде. Выходной импульс с ЛФД считался информационным только при временно́м совпадении с лазерным импульсом. Все собственные шумы, не попавшие во время строб-импульса, не доходили до счетчика импульсов. Данные с четырех фотодетекторов считывались по синхроимпульсу компьютером Боба. В данной установке использовался один и тот же компьютер, 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. Входное 50%-ное зеркало *1* случайным образом направляло фотон в вертикально-горизонтальный или диагональный базис для регистрации. 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 n фотонов в импульсе и частотных характеристик ЛФД. В нашем эксперименте скорость генерации ключа ограничивалась темпом обмена данными между компьютером и приемо-передающими узлами, что соответствовало тактовой частоте передачи 100 kHz.

Приведем пример экспериментальных данных по генерации квантового ключа, полученных на нашей установке. При передаче с $\bar{n} \sim 0.1$ на 10^6 тактовых импульсов был сформирован ключ длиной 21 303 bit, из них 209 bit (0.98%) оказались ошибочными (значения битов у Алисы и Боба не совпадали). При передаче с $\bar{n} \sim 0.2$ длина ключа составила 38 578 bit, ошибка была в 371 bit (0.96%). Для используемой тактовой частоты 100 kHz это соответствовало скорости генерации ключа ~ 2.1 и 3.8 kbit/s. Малый уровень ошибок в нашей работе по сравнению с результатами [16] объясняется отсутствием помех и потерь сигнала в оптическом канале связи. На этой же установке нами была смоделирована ситуация несанкционированного перехвата подслушивателем всех фотонов своими детекторами и попытки 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.

Дальнейшие перспективы развития работы предполагают применение протяженных атмосферных и оптоволоконных линий связи и повышение тактовой частоты передачи.

Работа поддержана грантом РФФИ (№ 04-07-90432).

Список литературы

[1] *Shannon C.E.* // Bell Syst. Tech. J. 1949. Vol. 28. P. 658–715.
[2] *Bennet C.H.* // Phys. Rev. Lett. 1992. Vol. 68. P. 3121–3124.
[3] *Wooters W.K., Zurek W.H.* // Nature. 1982. Vol. 299. P. 802–803.
[4] *Bennet C.H., Brassard G.* // Proc. IEEE Intern. Conf. on Comput. Sys. and Sign. Proces., Bangalore (India), 1984. P. 175–179.
[5] *Bennet C.H., Bessette F., Brassard G.* et. al. // J. Cryptology. 1992. Vol. 5. P. 3–28.
[6] *Ekert A.K.* // Phys. Rev. Lett. 1991/ Vol. 67. P. 661–663.
[7] *Gisin N., Ribordy G,m Title W.* et al. // Rev. Mod. Phys. 2002. Vol. 74. P. 145–175.
[8] *Молотков С.Н.* // ЖЭТФ. 2003. Т. 124. Вып. 6. С. 1172–1196.
[9] *Молотков С.Н.* // Письма ЖЭТФ. 2003. Т. 78. Вып. 3. С. 194–200.
[10] *Yelin S.F., Wang B.C.* // arXiv:quant-ph/0309105
[11] *Inoue K., Waks E., Yamamoto Y.* // Phys. Rev. Lett. 2002. Vol. 89. N 3. P. 037902.
[12] *Inoue K., Waks E., Yamamoto Y.* // Phys. Rev. A 2003. Vol. 68. N 3. P. 022317.
[13] *Stucki D., Gisin N., Guinnard O.* et al. // New J. Physics. 2002. Vol. 4. P. 41.1–41.8.
[14] *Kosaka H., Tomita A., Nambu Y.* et. al. // Electron. lett. 2003. Vol. 39. P. 1119–1201.
[15] *Kimura T., Nambu Y., Hatanaka T.* et. al. // arXiv:quant-ph/0403104
[16] *Hughes R.J., Nordholt J.E., Derkacs D., Peterson C.G.* // New J. Phys. 2002. Vol. 4. P. 43.1–43.14.
[17] *Kurtsiefer C., Zarda P., Halder M.* et al. // Natura. 2002. Vol. 419. P. 450.
[18] *Rarity J.G., Tapster P.M., Gorman P.M., Knight P.* // New J. Phys. 2002. Vol. 4. P. 82.1–82.21.
[19] Data Sheet C30902S. EG&G LTD. Canada.
[20] *Ghioni M., Cova S., Zappa F.* et al. // Rev. Scu. Ubstrum. 1996. Vol. 67. N 10. P. 3440–3448.
[21] *Cova S., Ghioni M., Laciata A.* // Appl. Optics. 1996. Vol. 35. N 12. P. 1956–1976.