УДК 535.14

ГЕНЕРАЦИЯ КВАНТОВОГО КЛЮЧА В ОДНОФОТОННЫХ СИСТЕМАХ СВЯЗИ*

Д. Б. Третьяков[1,2], А. В. Коляко[1,2,3], А. С. Плешков[1,2,4], В. М. Энтин[1,2], И. И. Рябцев[1,2], И. Г. Неизвестный[1]

[1] *Институт физики полупроводников им. А. В. Ржанова СО РАН, 630090, г. Новосибирск, просп. Академика Лаврентьева, 13*
[2] *Новосибирский государственный университет, 630090, г. Новосибирск, ул. Пирогова, 2*
[3] *Институт лазерной физики СО РАН, 630090, г. Новосибирск, просп. Академика Лаврентьева, 13/3*
[4] *Институт автоматики и электрометрии СО РАН, 630090, г. Новосибирск, просп. Академика Коптюга, 1*
E-mail: ryabtsev@isp.nsc.ru

Представлен краткий обзор экспериментальных работ в области квантовой криптографии и генерации квантового ключа посредством одиночных фотонов в атмосферных и оптоволоконных квантовых линиях связи. Дано описание двух экспериментальных установок для генерации квантового ключа, созданных в Институте физики полупроводников им. А. В. Ржанова СО РАН. Приведены результаты исследования зависимости скорости генерации квантового ключа от среднего числа фотонов μ в лазерном импульсе. Для $\mu > 0{,}3$ обнаружено расхождение между теорией и экспериментом, которое может быть связано с ненулевой вероятностью появления многофотонных импульсов в квантовой передаче, регистрируемых детекторами одиночных фотонов как однофотонные, а также с отбрасыванием при просеивании квантового ключа тех случаев, когда одновременно срабатывают несколько детекторов одиночных фотонов, поскольку тогда результат измерения не определяется.

Ключевые слова: квантовая криптография, генерация квантового ключа, одиночные фотоны.

DOI: 10.15372/AUT20160507

Введение. Основной задачей квантовой криптографии является передача секретной информации посредством квантовых объектов — одиночных фотонов, при этом абсолютная секретность передачи обеспечивается законами квантовой механики: одиночные фотоны не могут быть перехвачены и измерены с абсолютной достоверностью [1]. С помощью одиночных фотонов в квантовом канале (оптоволоконной или атмосферной линии связи) генерируется только секретный ключ, который затем используется отправителем и получателем в симметричной криптосистеме, а само зашифрованное сообщение может передаваться по любому открытому каналу [2–4]. Недавно за рубежом были разработаны коммерческие образцы оптоволоконных квантово-криптографических систем связи [5, 6]. Потребность в таких системах связи ожидается в тех случаях, когда абсолютная секретность передачи информации обладает бóльшим приоритетом, чем скорость передачи данных. Дальнейшее развитие квантовых систем связи требует увеличения дальности и скорости генерации квантового ключа, а также степени их защищённости.

*Работа выполнена при поддержке Российского фонда фундаментальных исследований (грант № 14-07-00809), Сибирского отделения РАН (госзадание № 0306-2014-0020) и Междисциплинарного квантового центра Новосибирского государственного университета.

Одиночный фотон как квантовый объект характеризуется рядом параметров: частотой колебаний электромагнитного поля, направлением распространения (волновым вектором), фазой и поляризацией. В квантовой криптографии для оптоволоконных квантовых каналов применяется фазовое кодирование фотонов с использованием фазовых модуляторов, а декодирование осуществляется с помощью управляемых оптических интерферометров. Для атмосферных каналов применяется поляризационное кодирование и декодирование с помощью поляризационно-чувствительных элементов (призмы Глана или Волластона).

Рассмотрим особенности генерации квантового ключа на примере поляризационного кодирования одиночных фотонов. Согласно законам квантовой механики поляризация фотона может быть определена только в результате измерения, причём одиночное измерение всегда будет иметь некоторую погрешность, а состояние фотона изменится непредсказуемым образом. Если при передаче фотона поляризации передатчика и приёмника совпадут, то будет получен правильный результат измерения, если не совпадут, измерение будет иметь ошибку до 50 %. В квантовой криптографии применяется протокол BB84, в котором передатчик и приёмник по открытому каналу обмениваются информацией о том, в каком поляризационном базисе проводились передача и приём, но не сообщают результат измерения [7]. Далее они сохраняют только те биты ключа, которые получены в идентичных базисах измерения, и формируют так называемый «просеянный» квантовый ключ.

В 1984 г. был предложен первый протокол BB84 [7], а в 1992 г. осуществлена экспериментальная демонстрация генерации квантового ключа с помощью передачи одиночных поляризованных в двух неортогональных базисах фотонов по открытой линии связи [8]. В дальнейшем фундаментальные научные исследования в этой области постепенно перешли к проблеме создания практических квантовых систем связи, что привело к появлению первых коммерческих устройств. Как и в классических видах связи, представляет интерес развитие методов передачи квантового ключа по открытому пространству и оптоволокну.

В данной работе представлен краткий обзор экспериментальных исследований в области квантовой криптографии и генерации квантового ключа посредством одиночных фотонов в атмосферных и оптоволоконных квантовых линиях связи.

Генерация квантового ключа в открытом пространстве. При распространении излучения через атмосферу поляризация излучения подвергается незначительным изменениям, поэтому для организации квантовых каналов через открытое пространство используется поляризационный метод кодирования [9], причём в перспективе рассматривается возможность связи с орбитальными спутниками [10]. В спектре пропускания атмосферы имеются окна прозрачности в диапазоне длин волн 0,8–0,9 мкм. Считается, что вертикальная оптическая плотность атмосферы эквивалентна расстоянию около 8 км при нормальных условиях, поэтому ожидаемые потери фотонов на поглощение при связи со спутниками довольно малы. Генерация квантового ключа между наземными источниками и приёмниками также представляет значительный интерес.

Если в первой атмосферной экспериментальной установке [8] расстояние между передатчиком и приёмником (длина квантового канала) составляло 30 см, то затем наблюдалось быстрое увеличение дальности связи. Так, в 2001 г. был поставлен эксперимент по организации передачи на 1,9 км [11]. Передача ключа на расстояния свыше эффективной толщины атмосферы была продемонстрирована на 10 км в [12], на 23 км в [9] на основе протокола BB84 и с применением перепутанных состояний в [13] на 13 км в [14]. Рекорд на данный момент принадлежит работе [15] (144 км). В 2008 г. проведён эксперимент со спутником и зарегистрирован отражённый однофотонный сигнал от лазерного импульса, посланного с Земли [10]. Для подавления фоновых засветок от солнечного или лунного света необходимо применять спектральные, пространственные и временны́е фильтры. В

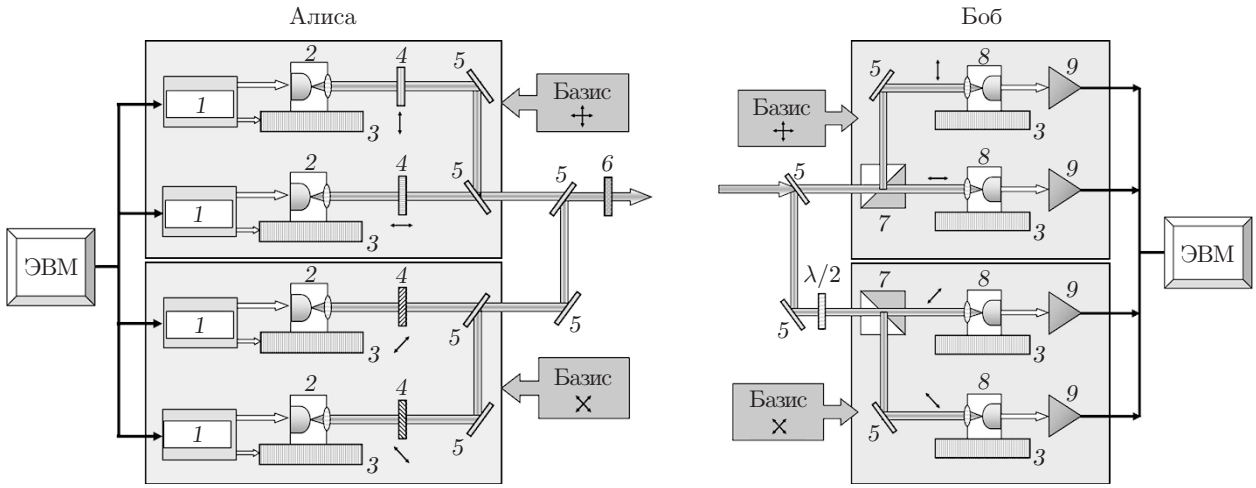

Рис. 1. Схема передающего (Алиса) и приёмного (Боб) узлов экспериментальной установки для генерации однофотонного квантового ключа в атмосферном квантовом канале: *1* — контроллеры полупроводниковых лазеров, *2* — полупроводниковые лазеры с оптическими коллиматорами, *3* — микрохолодильники на элементах Пельтье, *4* — поляризаторы, *5* — зеркала, *6* — набор оптических ослабителей, *7* — призмы Глана, *8* — детекторы одиночных фотонов на основе лавинных фотодиодов, *9* — усилители с формирователями импульсов

России экспериментальными исследованиями в области атмосферной квантовой криптографии занимаются в Московском государственном университете [16] и в Институте физики полупроводников им. А. В. Ржанова Сибирского отделения РАН (ИФП СО РАН) [17–20].

В 2003 г. нами была создана экспериментальная установка для исследования генерации квантового ключа через открытое пространство [17, 18], схема которой аналогична [8] и изображена на рис. 1. Передающий узел (Алиса) состоял из четырёх полупроводниковых лазеров, каждый из которых генерировал импульсы излучения с одной из четырёх 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 длиной 70 см в приёмный узел (Боб). Полупроводниковые лазеры с модулированным по току источником питания работали в импульсном режиме с длительностью импульса 8–10 нс и тактовой частотой $f = 100$ кГц. 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 приёмного узла и случайным образом разделялись на два луча светоделительным 50 %-ным зеркалом. Анализ поляризации фотонов производился с помощью двух призм Глана и четырёх однофотонных детекторов. Генерация квантового ключа осуществлялась согласно протоколу BB84.

В качестве однофотонных детекторов применялись специально отобранные кремниевые лавинные фотодиоды (ЛФД) C30902S производства фирмы EG&G (Канада) — одни из наиболее чувствительных для длин волн вблизи 0,8 мкм. Они работали в гейгеровском режиме счёта фотонов с пассивным гашением лавины. Импульсы фотодетекторов регистрировались компьютером только во время подачи стробирующего импульса длительностью 20 нс. Это позволяло избавиться от большей части собственных шумовых импульсов ЛФД, которые уменьшались за счёт охлаждения до температуры -20 °C. Квантовая эффективность детектирования одиночных фотонов $\eta = 20$–50 % [18].

В стандартном квантовом протоколе BB84 скорость генерации просеянного квантового ключа обычно описывается следующим выражением [2]:

$$R = \frac{1}{2} f \mu \eta T. \tag{1}$$

Здесь множитель 1/2 возникает из-за просеивания ключа по протоколу BB84 (отбрасывается примерно половина данных, когда базисы Алисы и Боба не совпадают); μ — среднее число фотонов на лазерный импульс; T — полное пропускание оптического канала от выхода Алисы до детекторов Боба. Из выражения (1) следует, что скорость генерации квантового ключа должна линейно зависеть от μ.

В современных квантово-криптографических системах связи в качестве источников одиночных фотонов, как правило, используют сильно ослабленные короткие лазерные импульсы, которые имеют пуассоновское распределение по числу фотонов в импульсе n, т. е. вероятность $P(n)$ найти n фотонов в лазерном импульсе даётся выражением

$$P(n) = \frac{\mu^n}{n!} \mathrm{e}^{-\mu}. \tag{2}$$

При $\mu \ll 1$ доля импульсов, вообще не содержащих фотоны, составляет $P(0) \approx 1-\mu+\mu^2/2$. Доля импульсов, содержащих один фотон, — $P(1) \approx \mu - \mu^2$, а доля импульсов, имеющих два фотона, — $P(2) \approx \mu^2/2$. Например, для $\mu = 0{,}1$ получаем $P(0) \approx 0{,}905$, $P(1) \approx 0{,}0905$, $\sum P(n > 1) \approx 0{,}0045$. Это означает, что вероятность найти в лазерном импульсе больше чем один фотон мала по сравнению с вероятностью многофотонных лазерных импульсов. Именно поэтому слабые лазерные импульсы получили широкое применение в квантовой криптографии.

Результаты наших измерений [19, 20] и их сравнение с теорией согласно формуле (1) при значениях $\eta = 30$ %, $T = 85$ % и различных μ представлены на рис. 2, *а*. Из рисунка видно, что при $\mu < 0{,}3$ эксперимент и теория хорошо совпадают. Однако при увеличении μ до 0,4 наблюдается отклонение экспериментальной зависимости от теоретической, связанное, предположительно, с увеличением вероятности появления многофотонных лазерных импульсов и насыщением однофотонных детекторов.

Более тщательный анализ статистики генерации и детектирования одиночных фотонов показывает, что формула (1) не совсем точна. Во-первых, многофотонные лазерные импульсы воспринимаются детектором одиночных фотонов так же, как и однофотонные, поскольку на его выходе может возникнуть только один сигнал с определёнными амплитудой и длительностью независимо от числа пришедших фотонов. Во-вторых, при просеивании квантового ключа Алиса и Боб отбрасывают те случаи, когда одновременно срабатывают не один, а несколько детекторов одиночных фотонов Боба, поскольку результат измерения не определён. Поэтому уточнённая формула для скорости генерации квантового ключа должна быть записана следующим образом:

$$R = \frac{1}{2} f \bar{P}(1). \tag{3}$$

Здесь $\bar{P}(1)$ — вероятность зарегистрировать всеми детекторами Боба только один фотон в лазерном импульсе с учётом конечной квантовой эффективности и потерь в квантовом канале. Эта вероятность описывается модифицированным распределением Пуассона:

$$\bar{P}(n) = \frac{(\mu\eta T)^n}{n!} \mathrm{e}^{-\mu\eta T}, \tag{4}$$

которое получается из свёртки начального распределения Пуассона по числу испущенных фотонов (2) и статистики регистрации фотонов, дошедших до фотодетектора, с учётом конечной квантовой эффективности и потерь в квантовом канале. В итоге имеем уточнённую формулу для зависимости скорости генерации квантового ключа по протоколу BB84 от среднего числа фотонов в лазерном импульсе:

$$R = \frac{1}{2} f \mu \eta T \mathrm{e}^{-\mu\eta T}. \tag{5}$$

Эта функция имеет максимум при $\mu\eta T = 1$. При больших значениях μ предельная скорость генерации просеянного квантового ключа уменьшается и стремится к 0, так как вероятность одновременного срабатывания всех детекторов Боба стремится к 1 из-за большого числа фотонов. Отметим, что при таких высоких значениях μ секретность квантового ключа не обеспечивается, поскольку потенциальный подслушиватель (Ева) может незаметно перехватывать часть фотонов в каждом лазерном импульсе и получать ту же информацию, что и Боб.

На рис. 2, *b* представлено сравнение экспериментальных данных с расчётом по формуле (5). Видно, что теперь при $\mu = 0{,}4$ экспериментальное значение практически совпадает с теоретическим в пределах погрешности наших измерений. Эксперимент подтвердил, что оптимальное среднее число фотонов в лазерном импульсе для генерации секретного квантового ключа $\mu \sim 0{,}1$–$0{,}2$.

Отметим, что в эксперименте тактовая частота генерации квантового ключа составляла 100 кГц и была ограничена скоростью обмена данными между компьютером и приёмопередающими узлами. Для этой частоты продемонстрирована генерация квантового ключа с килобитной скоростью при достаточно малом количестве ошибок в ключе < 2 % (предельное количество ошибок для протокола BB84 не должно превышать 11 %). В дальнейшем увеличение тактовой частоты до 100 МГц может повысить скорость генерации ключа до нескольких мегабит в секунду, что представляет интерес для практического применения атмосферных и спутниковых квантовых линий связи. В настоящее время нами начата работа по подготовке экспериментов по генерации квантового ключа через атмосферу между двумя удалёнными (до 10 км) пользователями на основе модернизированной оптической

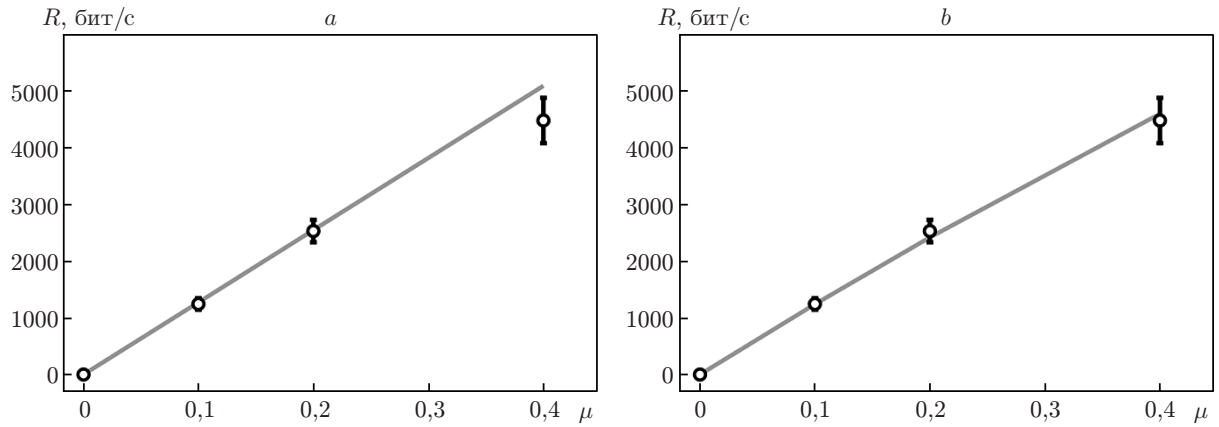

Рис. 2. Сравнение экспериментальной зависимости (кружки) скорости генерации квантового ключа R по протоколу BB84 в атмосферной экспериментальной установке от среднего числа фотонов в лазерном импульсе μ с результатами теоретических расчётов (сплошные линии): *a* — по формуле (1), *b* — по формуле (5)

схемы с телескопическим расширением лазерного пучка для уменьшения дифракционных потерь и с увеличенной тактовой частотой 40 МГц.

Генерация квантового ключа в оптоволоконных линиях связи. Первая работа по генерации квантового ключа в оптоволоконном квантовом канале появилась уже в 1993 году [21]. В ней в качестве квантового канала использовалось стандартное одномодовое оптоволокно SMF-28, применяемое в оптоволоконных коммуникациях. Передача данных велась обычно на телекоммуникационной длине волны 1550 нм, которая соответствовала наименьшему затуханию (0,2 дБ/км) и малой дисперсии в волокне [2]. На сегодняшний день наилучшими однофотонными детекторами в этой спектральной области для практического использования являются лавинные фотодиоды InGaAs/InP [22]. По сравнению с кремниевыми фотодиодами они обладают меньшей квантовой эффективностью, обычно на уровне 10–20 %, и бóльшими шумами. Охлаждение ЛФД до $-40\ldots-70$ °C с помощью микрохолодильников на основе элементов Пельтье даёт заметное уменьшение темновых шумов. Для увеличения быстродействия и снижения вероятности появления послеимпульсов (ложные срабатывания ЛФД после регистрации одиночного фотона или темнового импульса) применяют метод активного гашения лавины [23] или работают в режиме с импульсным питанием [22, 24].

Для оптоволоконных линий связи используются различные способы кодирования квантовых состояний фотонов [2]. Например, одни из первых криптосистем основывались на поляризационном кодировании [21, 25]. В последующих работах была продемонстрирована дальность связи свыше 100 км [26]. Частотно-фазовое кодирование использовалось в [27], а временной способ был предложен и реализован в [28]. Наиболее широкое применение нашло фазовое кодирование с помощью интерферометров Маха — Цендера (МЦ) [2]. Продемонстрирована генерация квантового ключа на расстояния свыше 100 км с полупроводниковыми детекторами одиночных фотонов [29] и свыше 200 км со сверхпроводниковыми детекторами [30, 31].

Отдельно следует отметить появление двухпроходной автокомпенсационной оптической схемы с фазовым кодированием [32], отличающейся устойчивой работоспособностью при изменяющихся внешних условиях, совместимой со стандартными оптоволоконными сетями и на основе которой построены коммерческие квантовые оптоволоконные криптосистемы [5, 6]. Рассмотрим особенности работы такой оптической схемы на примере экспериментальной установки, созданной в ИФП СО РАН [3, 4, 24, 31, 33, 34], которая может послужить прототипом для практической квантовой криптосистемы.

Установка состоит из передатчика Алиса и приёмника Боб (рис. 3), соединённых между собой одномодовым оптоволокном SMF-28 (квантовый канал) длиной 25–100 км. Передача оптических сигналов организована следующим образом. Лазер Боба испускает многофотонный оптический импульс с линейной поляризацией на длине волны 1550 нм и длительностью 1 нс, который проходит через циркулятор (Ц) и направляется на первый светоделитель (СД) 50/50. Далее одна часть импульса поступает на вход поляризационного светоделителя (ПСД) по короткому плечу оптоволоконного интерферометра МЦ. Вторая его часть приходит на ПСД, пройдя длинное плечо, образованное линией задержки (ЛЗ) длиной 10 м и оптоволоконным фазовым модулятором (ФМ). Оптические элементы в длинном плече выполнены из поляризационно-стойкого оптоволокна. Это позволяет сориентировать поляризацию излучения так, чтобы обе части лазерного импульса вышли через ПСД и направились от Боба к Алисе по квантовому каналу связи.

После прохождения квантового канала лазерный импульс поступает на вход Алисы и попадает на светоделитель СД 10/90, где 90 % излучения отводится на контрольный фотодиод (ФД), запускающий систему синхронизации Алисы. Другая часть излучения проходит через накопительную линию (НЛ) длиной 25 км, фазовый модулятор и отражается от зеркала Фарадея (ЗФ), которое поворачивает поляризацию излучения на 90° для авто-

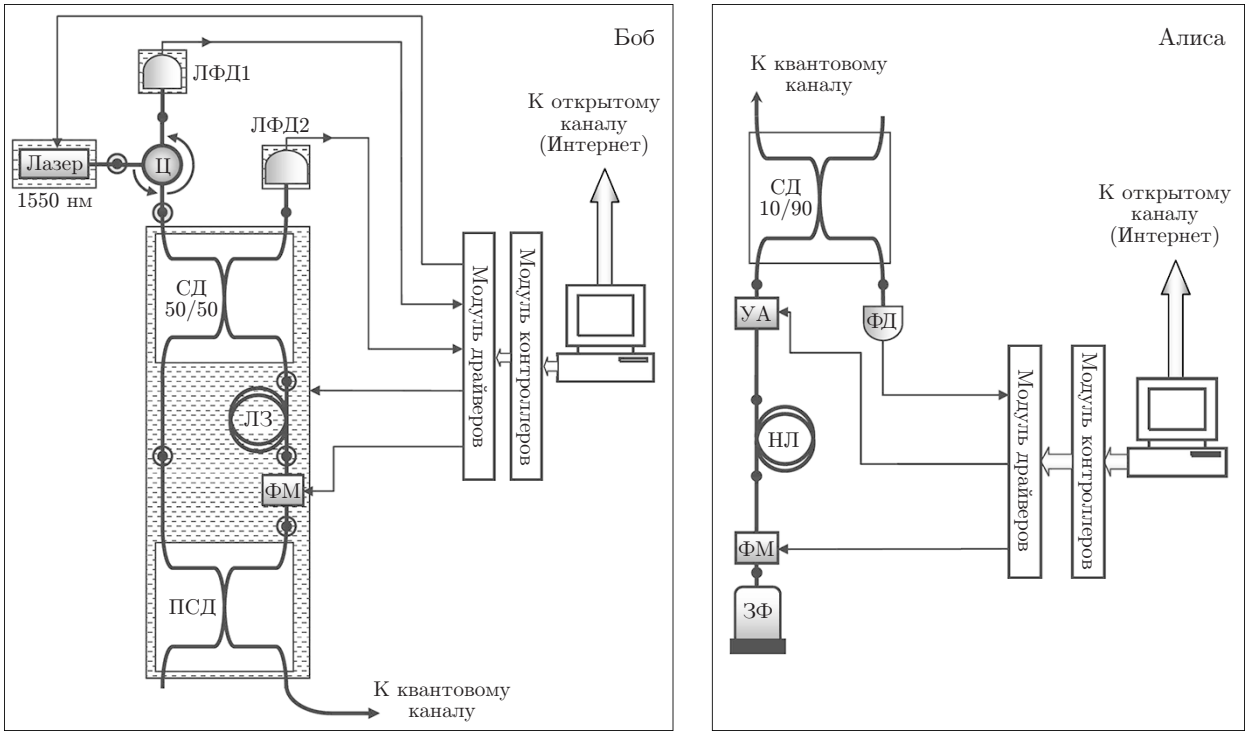

Рис. 3. Схема передающего (Алиса) и приёмного (Боб) узлов экспериментальной установки для генерации однофотонного квантового ключа в оптоволоконном квантовом канале

компенсации поляризационных искажений оптоволокна квантового канала. На обратном пути, на выходе из Алисы, лазерный импульс ослабляется управляемым аттенюатором (УА) до однофотонного состояния (среднее число фотонов на импульс 0,1–0,3). Вернувшиеся от Алисы к Бобу фотоны имеют повёрнутую на 90° линейную поляризацию, поэтому входным ПСД они направляются в другое плечо интерферометра МЦ, нежели на пути к Алисе, после прохождения которого соединяются на выходе СД 50/50, где интерферируют. Результат интерференции регистрируется ЛФД2 в одном плече либо после прохождения циркулятора — ЛФД1 в другом плече (рис. 4). Поскольку эти две части импульса проходят одинаковый путь, причём в обратном порядке внутри Боба, интерферометр оказывается автоматически скомпенсированным, что является большим достоинством интерферометра такого типа. Например, коммерческие системы [5, 6] построены именно по данному принципу. Измеренный контраст нашего интерферометра $V = 98{,}5\ \%$ достаточен для генерации квантового ключа с малым уровнем инструментальных ошибок.

Для реализации протокола BB84 Алиса случайным образом с помощью ФМ прикладывает в нужный момент времени фазовый сдвиг 0 или π (первый базис) либо $\pi/2$ или $3\pi/2$ (второй базис) к световому импульсу, пришедшему от Боба. Боб, получив отражённые от Алисы одиночные фотоны, также случайным образом выбирает базис для измерения, прикладывая фазовый сдвиг 0 (первый базис) или $\pi/2$ (второй базис) на свой фазовый модулятор в соответствующий момент времени. Калибровка фазовых сдвигов осуществляется согласно экспериментально измеренной интерферограмме, представленной на рис. 4.

В такой оптической схеме, когда импульсы распространяются вперёд и назад, обратное рэлеевское рассеяние света может значительно увеличить шум, регистрируемый детекторами ЛФД1 и ЛФД2, работающими в режиме регистрации одиночных фотонов. Поэтому лазер Боба испускает импульсы не постоянно, а посылает цуги импульсов в каждом цикле передачи, причём длина цугов соответствует длине НЛ, вставленной для этой цели

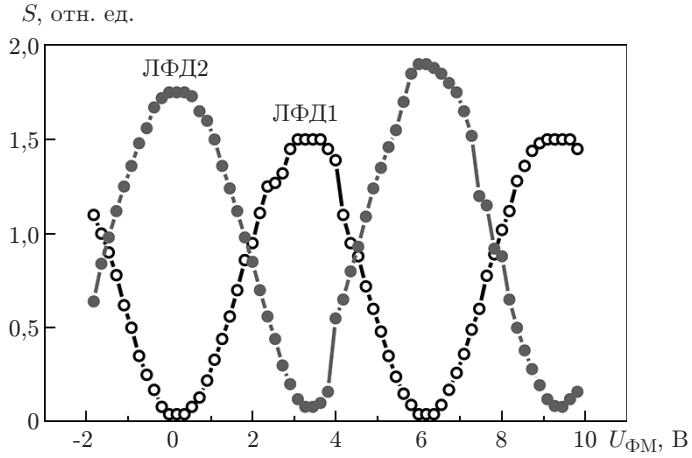

Рис. 4. Зависимость сигналов, регистрируемых детекторами одиночных фотонов ЛФД1 и ЛФД2 модуля приёмника Боб, от напряжения на фазовом модуляторе $U_{ФМ}$. Наблюдаемые осцилляции соответствуют интерференции фотонов в оптоволоконном интерферометре Маха — Цендера

после УА в оптическую схему Алисы. В результате однофотонные импульсы, распространяющиеся обратно, 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 1–5 МГц.

Скорость генерации квантового ключа в оптоволоконной системе также должна описываться формулами (1) или (5). Для их проверки была измерена зависимость скорости генерации квантового ключа от среднего числа фотонов в лазерном импульсе. После предварительной настройки временны́х задержек и напряжений фазовых модуляторов установка переводилась в режим генерации квантового ключа по протоколу BB84 с фазовым кодированием фотонов. Квантовый канал был представлен катушкой одномодового оптоволокна SMF-28 длиной 25 км. Заранее измеренное полное затухание излучения в этой катушке, оптических разъёмах и оптической части Боба составляло 12 дБ, что соответствует $T = 0{,}063$. Частота повторения лазерных импульсов $f = 1$ МГц, а квантовая эффективность детекторов одиночных фотонов $\eta \approx 13$ %. Для измерения зависимости скорости генерации квантового ключа от среднего числа фотонов уровень ослабления УА в модуле Алисы подбирался таким образом, чтобы число фотонов в импульсе на выходе Алисы находилось в диапазоне $\mu = 0{,}01$–1.

Результаты измерений и их сравнение с теорией согласно формуле (1) представлены на рис. 5. Из рисунка видно, что при малом числе фотонов ($\mu < 0{,}3$) эксперимент и теория хорошо совпадают. При увеличении числа фотонов наблюдается отклонение экспериментальной зависимости от теоретической. Однако теоретические расчёты с уточнённой формулой (5) дают практически тот же результат, что и формула (1), так как выражение в показателе экспоненты в формуле (5) очень мало из-за малости T. Таким образом, наблюдаемое на рис. 5 расхождение между теорией и экспериментом связано не с увеличением вероятности появления многофотонных лазерных импульсов, а с какими-то другими факторами. Например, это может быть наличие послеимпульсов в используемых однофотонных детекторах на основе лавинных фотодиодов InGaAs/InP, которые увеличивают мёртвое время детекторов и тем самым ограничивают частотную полосу при регистрации одиночных фотонов такими детекторами.

В любом случае эксперименты с оптоволоконным квантовым каналом длиной 25 км подтвердили, что оптимальное среднее число фотонов в лазерном импульсе для генерации

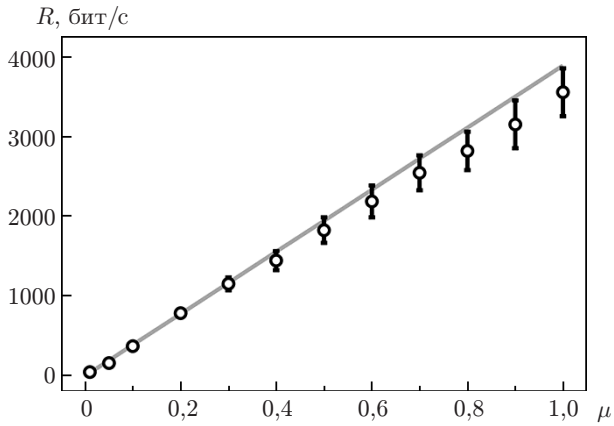

Рис. 5. Сравнение экспериментальной зависимости (кружки) скорости генерации квантового ключа R по протоколу BB84 в оптоволоконной экспериментальной установке от среднего числа фотонов в лазерном импульсе μ с результатами теоретических расчётов (сплошная линия) по формуле (1)

секретного квантового ключа $\mu \sim 0{,}1$–$0{,}3$. В настоящее время нами выполняются работы, направленные на совершенствование детекторов одиночных фотонов и увеличение тактовой частоты генерации квантового ключа до 50–100 МГц. Отметим также, что в России экспериментальными исследованиями в области оптоволоконной квантовой криптографии занимаются в Московском государственном университете [35], Московском педагогическом государственном университете [31] и Университете ИТМО [36].

Заключение. Квантовая криптография является наглядной демонстрацией возможности практического применения квантовых технологий для создания абсолютно защищённых линий связи, безопасность которых обеспечивается на фундаментальном уровне законами квантовой механики. За рубежом и в России проводятся активные экспериментальные и теоретические исследования как оптоволоконных, так и атмосферных квантовых систем связи. Продемонстрирована возможность передачи квантового ключа на расстояния свыше 100 км со скоростью порядка килобит в секунду и выше. Появились первые образцы коммерческих квантовых криптосистем. Потребность в квантово-криптографических системах связи ожидается в тех случаях, когда абсолютная секретность передачи информации будет обладать бóльшим приоритетом, чем скорость передачи данных.

В ИФП СО РАН были созданы атмосферная и оптоволоконная экспериментальные установки для генерации квантового ключа. На этих установках отрабатывались различные методики генерации, детектирования и кодирования одиночных фотонов. Изучены особенности генерации квантового ключа по протоколу BB84 с поляризационным кодированием в однопроходной атмосферной системе связи и с фазовым кодированием в двухпроходной оптоволоконной системе связи. В данной работе была исследована зависимость скорости генерации квантового ключа от среднего числа фотонов в импульсе передачи и сделан вывод, что оптимальным числом фотонов является значение 0,1–0,3. Дальнейшее развитие квантовых систем связи требует увеличения дальности и скорости генерации квантового ключа, а также степени их защищённости.

СПИСОК ЛИТЕРАТУРЫ

1. **Wootters W. K., Zurek W. H.** A single quantum cannot be cloned // Nature. 1982. **299**, Is. 5886. P. 802–803.

2. **Gisin N., Ribordy G., Tittel W., Zbinden H.** Quantum cryptography // Rev. Mod. Phys. 2002. **74**, Is. 1. P. 145–195.
3. **Курочкин В. Л., Зверев А. В., Курочкин Ю. В. и др.** Экспериментальные исследования в области квантовой криптографии // Микроэлектроника. 2011. **40**, № 4. С. 264–273.
4. **Рябцев И. И., Бетеров И. И., Третьяков Д. Б. и др.** Экспериментальная квантовая информатика с одиночными атомами и фотонами // Вестн. РАН. 2013. **83**, № 7. С. 606–615.
5. **IDQ.** URL: http://www.idquantique.com (дата обращения: 11.08.2016).
6. **MagiQ.** URL: http://www.magiqtech.com (дата обращения: 11.08.2016).
7. **Bennett Ch. H., Brassard G.** Quantum cryptography: Public key distribution and coin tossing // Proc. of the IEEE Intern. Conf. on Comput., Systems and Sign. Process. Bangalore, India, 1984. P. 175–179.
8. **Bennett Ch. H., Bessette F., Brassard G. et al.** Experimental quantum cryptography // Journ. Cryptology. 1992. **5**, Is. 1. P. 3–28.
9. **Kurtsiefer C., Zarda P., Halder M. et al.** Quantum cryptography: A step towards global key distribution // Nature. 2002. **419**, Is. 6906. P. 450.
10. **Villoresi P., Jennewein T., Tamburini F. et al.** Experimental verification of the feasibility of a quantum channel between space and Earth // New Journ. Phys. 2008. **10**. 033038.
11. **Rarity J. G., Tapster P. R., Gorman P. M., Knight P.** Ground to satellite secure key exchange using quantum cryptography // New Journ. Phys. 2002. **4**. P. 82.1–82.21.
12. **Hughes R. J., Nordholt J. E., Derkacs D., Peterson Ch. G.** Practical free-space quantum key distribution over 10 km in daylight and at night // New Journ. Phys. 2002. **4**. P. 43.1–43.14.
13. **Ekert A. K.** Quantum cryptography based on Bell's theorem // Phys. Rev. Lett. 1991. **67**. P. 661–664.
14. **Peng Ch.-Z., Yang T., Bao X.-H. et al.** Experimental free-space distribution of entangled photon pairs over 13 km: Towards satellite-based global quantum communication // Phys. Rev. Lett. 2005. **94**. 150501.
15. **Ursin R., Tiefenbacher F., Schmitt-Manderbach T. et al.** Entanglement-based quantum communication over 144 km // Nature Phys. 2007. **3**. P. 481–486.
16. **Radchenko I. V., Kravtsov K. S., Kulik S. P., Molotkov S. N.** Relativistic quantum cryptography // Laser Phys. Lett. 2014. **11**, N 6. 065203.
17. **Курочкин В. Л., Рябцев И. И., Неизвестный И. Г.** Генерация квантового ключа на основе кодирования поляризационных состояний фотонов // Оптика и спектроскопия. 2004. **96**, № 5. С. 771–775.
18. **Курочкин В. Л., Рябцев И. И., Неизвестный И. Г.** Квантовая криптография и генерация квантового ключа с использованием одиночных фотонов // Микроэлектроника. 2006. **35**, № 1. С. 37–43.
19. **Kolyako A. V., Neizvestny I. G., Kurochkin V. L.** Investigation the bit rate of quantum key using Si single photon detectors // Journ. Phys.: Conf. Ser. 2014. **541**. 012046.
20. **Курочкин В. Л., Коляко А. В.** Исследование скорости распределения квантового ключа через открытое пространство в зависимости от условий передачи // Изв. РАН. Сер. Физическая. 2016. **80**, № 1. С. 6–9.
21. **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. **23**, N 6. P. 383–388.
22. **Trifonov A., Subacius D., Berzanskis A., Zavriyev A.** Single photon counting at telecom wavelength and quantum key distribution // Journ. Mod. Opt. 2004. **51**, Is. 9–10. P. 1399–1415.

23. **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**, N 20. 201114.
24. **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. **45**, № 4. С. 110–119.
25. **Muller A., Zbinden H., Gisin N.** Quantum cryptography over 23 km in installed under-lake telecom fibre // Europhys. Lett. 1996. **33**, N 5. P. 335–339.
26. **Peng Ch.-Z., Zhang J., Yang D. et al.** Experimental long-distance decoy-state quantum key distribution based on polarization encoding // Phys. Rev. Lett. 2007. **98**. 010505.
27. **Mérolla J.-M., Mazurenko Yu., Goedgebuer J.-P., Rhodes W. T.** Single-photon interference in sidebands of phase-modulated light for quantum cryptography // Phys. Rev. Lett. 1999. **82**. P. 1656–1659.
28. **Boucher W., Debuisschert Th.** Experimental implementation of time-coding quantum key distribution // Phys. Rev. A. 2005. **72**. 062325.
29. **Kosaka H., Tomita A., Nambu Y. et al.** Single-photon interference experiment over 100 km for quantum cryptography system using a balanced gated-mode photon detector // Electron. Lett. 2003. **39**, Is. 16. P. 1199–1201.
30. **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.
31. **Курочкин В. Л., Зверев А. В., Курочкин Ю. В. и др.** Распределение квантового ключа на дальние дистанции по оптоволокну со сверхпроводящими детекторами // Автометрия. 2015. **51**, № 6. С. 17–22.
32. **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.
33. **Krivyakin G. K., Pleshkov A. S., Zverev A. V. et al.** Noise reduction methods of single photon detector based on InGaAs/InP avalanche photodiodes // Journ. Phys.: Conf. Ser. 2014. **541**. 012050.
34. **Курочкин В. Л., Кривякин Г. К., Зверев А. В. и др.** Оптоволоконная квантовая система связи на основе автокомпенсационной оптической схемы // Изв. РАН. Сер. Физическая. 2016. **80**, № 1. С. 10–13.
35. **Корольков А. В., Катамадзе К. Г., Кулик С. П., Молотков С. Н.** О пассивном зондировании волоконно-оптических линий квантовой связи // ЖЭТФ. 2010. **137**, вып. 4. С. 637–645.
36. **Gleim A. V., Egorov V. I., Nazarov Yu. V. et al.** Secure polarization-independent subcarrier quantum key distribution in optical fiber channel using BB84 protocol with a strong reference // Opt. Express. 2016. **24**, N 3. P. 2619–2633.

Поступила в редакцию 30 марта 2016 г.