УДК 535.14

Квантовая криптография как перспективный метод абсолютно защищённой передачи данных для новых поколений РЛС

И.И. Рябцев [1, 2, 3], В.Л. Курочкин [1, 2, 3], А.В. Зверев [1], Д.Б. Третьяков [1], В.М. Энтин [1], А.Г. Черевко [3], И.Г. Неизвестный [1, 3]

[1] Институт физики полупроводников им. А. В. Ржанова СО РАН

[2] Новосибирский государственный университет

[3] Сибирский государственный университет телекоммуникаций и информатики

В статье представлен краткий обзор экспериментальных исследований в области квантовой криптографии и передачи данных одиночными фотонами. Приводится описание двух экспериментальных установок, предназначенных для генерации однофотонного квантового ключа в атмосферном и оптоволоконном квантовых каналах связи, а также результаты экспериментов по генерации квантового ключа.

Ключевые слова: квантовая криптография, одиночные фотоны, передача данных.

1. Введение

Основной задачей квантовой криптографии является поиск эффективных алгоритмов и разработка схем практической реализации передачи секретной информации с использованием квантовых объектов – одиночных фотонов [1, 2]. Современная система кодирования данных в телекоммуникациях (классическая криптография) основана на использовании шифров (ключей), для расшифровки которых необходимо уметь факторизовать (раскладывать на простые множители) большие числа. Так как быстрые алгоритмы факторизации больших чисел для современных компьютеров отсутствуют (хотя уже разработаны для квантовых компьютеров), это позволяет обеспечивать секретность. Однако можно ожидать, что в недалеком будущем такие алгоритмы будут найдены, и вся система безопасности может быть разрушена.

Поэтому для полной защищённости передаваемых данных в качестве ключей нужно использовать абсолютно случайные последовательности чисел (используемые только один раз, для передачи одного сообщения от отправителя *Алисы* к получателю *Бобу*), которые при этом не могут быть достоверно определены шпионом *Евой*. В соответствии с математически доказанным утверждением Шеннона [3], передача данных не поддается расшифровке, если сообщение зашифровано одноразовым случайным ключом, длина ключа равна длине сообщения и этот ключ известен только легитимным пользователям. Основная задача при реализации такого метода состоит в передаче секретного ключа между пространственно удалёнными пользователями. Для этого квантовая криптография предлагает использовать специфические свойства одиночных квантовых объектов – фотонов.

Один из основных постулатов квантовой механики состоит в том, что всякое измерение приводит к изменению состояния квантового объекта [4]. Это означает, что всякая попытка

со стороны *Евы* получить ключ, который передаётся с помощью одиночных фотонов по квантовому каналу (например, волоконному световоду) от *Алисы* к *Бобу*, приведёт к тому, что *Боб* получит ключ изменённым и не сможет прочитать послание от *Алисы*, которое нужно расшифровать с помощью этого ключа. Отсюда он сделает вывод, что канал подслушивают, и передача данных будет прекращена. Если к квантовому каналу подключилась шпион *Ева*, желающая перехватить ключ, ей придётся регистрировать квантовое состояние каждого фотона, а затем воспроизвести такой же фотон и послать его *Бобу* (осуществить так называемое «клонирование» фотона). Однако, согласно теореме о невозможности идеального клонирования квантового состояния [5], такой процесс будет содержать большой процент ошибок. Поэтому *Боб* получит неработоспособный ключ, о чём он сообщит *Алисе*. Далее они могут решить прекратить передачу ключа, или повторить её заново. Поскольку квантовые базисы для передачи и приёма фотонов выбираются случайным образом, у *Евы* нет возможности подобрать алгоритм для расшифровки ключа.

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 применяют фазовое кодирование фотонов с помощью фазовых модуляторов, а декодирование осуществляют с помощью управляемых оптических интерферометров. Для атмосферного канала применяется поляризационное кодирование и декодирование с помощью поляризационно-чувствительных элементов (призмы Глана или Волластона).

Для детектирования одиночных фотонов используют лавинные фотодиоды (ЛФД), включённые в режиме Гейгера [1]. В таком ЛФД для регистрации фотона на короткое время прикладывают обратное напряжение смещения, превышающее напряжение пробоя. Пришедший фотон с некоторой вероятностью, зависящей от квантовой эффективности, может вызвать лавинный пробой ЛФД, что порождает импульс тока на его выходе. После срабатывания ЛФД лавину необходимо быстро остановить, чтобы он был готов к приёму следующего фотона. Это делается с помощью активного или пассивного гашения лавины.

Источник одиночных фотонов должен выдавать короткие импульсы света, которые затем необходимо ослабить до уровня одного фотона. Поскольку необходима быстрая модуляция, подходящими являются только полупроводниковые лазеры. При этом желательно использовать лазеры, длина волны которых стабильна при модуляции (лазеры с распределённой обратной связью или с вертикальным резонатором). Импульсы полупроводникового лазера ослабляются с помощью ослабителей до такой степени, чтобы частота появления сигнала на выходах фотодиодов была много меньше частоты следования лазерных импульсов. Тогда, согласно статистике Пуассона, вероятность генерации двух и более фотонов будет практически равна нулю. Основным недостатком этого метода является то, что большинство лазерных импульсов вообще не содержит фотонов, поэтому скорость передачи данных существенно понижается.

В 1984 г. был предложен первый протокол BB84, а в 1992 г. осуществлена экспериментальная демонстрация генерации квантового ключа с помощью передачи одиночных, поляризованных в двух неортогональных базисах, фотонов по открытой линии связи [6, 7]. В дальнейшем фундаментальные научные исследования в этой области постепенно перешли к проблеме создания практических квантовых систем связи и появлению первых коммерческих устройств. Как и в классических видах оптической связи, представляет интерес развитие методов передачи квантового ключа по открытому пространству и оптоволокну.

2. 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 [8], причём в перспективе рассматривается возможность связи с орбитальными спутниками [9]. 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 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 расстояние между передатчиком и приёмником (длина квантового канала) было 30 см [7], то в дальнейшем наблюдался быстрый прогресс в сторону увеличения дальности связи. Так, в 2001 г. был поставлен эксперимент по организации передачи на 1.9 км [10]. Передача ключа на расстояния свыше эффективной толщины атмосферы была продемонстрирована в работе [11] на 10 км, [8] на 23 км на основе протокола BB84, и, используя перепутанные состояния [12], на 13 км [13]. Рекорд на данный момент принадлежит работе [14] – 144 км. В 2008 г. был проведён эксперимент со спутником и зарегистрирован отражённый однофотонный сигнал от лазерного импульса, посланного с Земли [15]. Для подавления фоновых засветок от солнечного или лунного света необходимо применять спектральные, пространственные и временны́е фильтры.

Нами в Институте физики полупроводников им. А. В. Ржанова СО РАН в 2003 г. была создана экспериментальная установка для исследования генерации квантового ключа через открытое пространство [16, 17]. 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. Длина волны генерации 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 разделялись на два луча светоделительным 50% зеркалом. Анализ поляризации фотонов производился с помощью двух призм Глана и четырёх однофотонных детекторов.

В качестве однофотонных детекторов применялись специально отобранные лавинные фотодиоды (ЛФД) C30902S производства фирмы EG&G (Канада) – одни из наиболее чувствительных для диапазона 0.8 мкм. Они работали в гейгеровском режиме с пассивным гашением лавины. Импульсы с фотодетекторов регистрировались компьютером только во время подачи стробирующего импульса длительностью 10 нс. Это позволяло избавиться от большей части собственных шумовых импульсов ЛФД, которые уменьшались также за счёт их охлаждения до температуры -30°C.

Скорость генерации квантового ключа зависит от тактовой частоты повторения лазерных импульсов, среднего количества фотонов в импульсе μ и частотных характеристик ЛФД. В нашем эксперименте тактовая частота составляла 100 кГц и ограничивалась темпом обмена данными между компьютером и приёмо-передающими узлами. В табл. 1 приведены полученные экспериментальные результаты [18] по скорости генерации квантового ключа и количеству ошибок в ключе в зависимости от квантовой эффективности детекторов и среднего числа фотонов в лазерном импульсе. Эти результаты согласуются с теоретическими расчётами и свидетельствуют о возможности генерации ключа с килобитной скоростью при достаточно малом количестве ошибок (предельное количество ошибок для протокола BB84 не должно превышать 11%). В дальнейшем увеличение тактовой частоты до 100

МГц может позволить увеличить скорость генерации ключа до мегабит в секунду, что представляет интерес для практического применения атмосферных и спутниковых квантовых линий связи.

Таблица 1. Результаты, полученные на атмосферной экспериментальной установке для скорости генерации квантового ключа, и количество ошибок в ключе в зависимости от квантовой эффективности детекторов и среднего числа фотонов в лазерном импульсе

Квантовая эффективность	0.3			0.4	
Число фотонов в импульсе	0.1	0.2	0.4	0.2	0.4
Скорость генерации ключа (бит/с)	1246	2534	4488	2897	4448
Количество ошибок в ключе (%)	2.0	1.3	0.9	1.4	1.0

На этой же установке нами была смоделирована ситуация несанкционированного перехвата *Евой* всех фотонов своими детекторами и попытка передачи перехваченных данных *Бобу*. При сравнении полученного квантового ключа в этом случае по открытому каналу сразу же выяснилось, что процент ошибок в коде увеличился до 25% и факт присутствия *Евы* в квантовой линии связи был выявлен.

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 схемы с телескопическим расширением лазерного пучка. Для уменьшения потерь квантового канала связи, связанных с дифракционной расходимостью лазерного луча на больших расстояниях, применены расширители пучка на основе телескопов ТАЛ-2 диаметром 150 мм. Фотоны, испускаемые передатчиком, направляются в телескоп с помощью оптоволокна. Из приёмного телескопа фотоны поступают в приёмник также с помощью оптоволоконного ввода. Генерация квантового ключа осуществляется с использованием поляризационного кодирования по протоколу BB84. Внешний вид модернизированной экспериментальной установки показан на рис. 1.

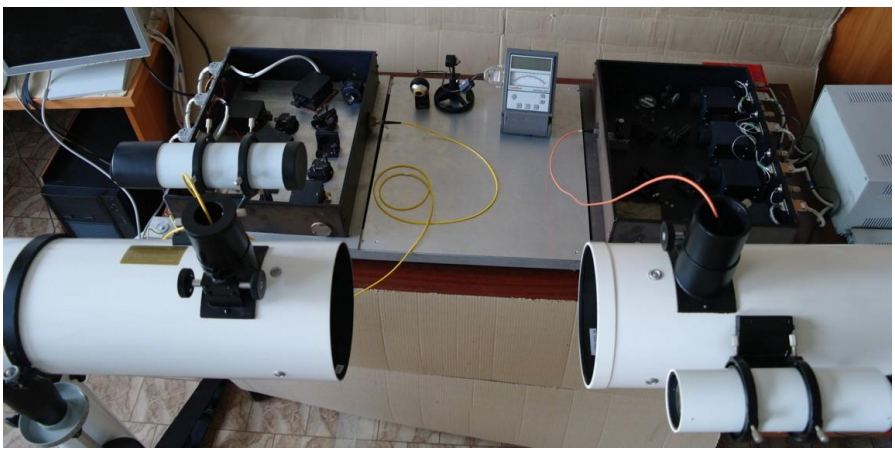

Рис. 1. Внешний вид модернизированной экспериментальной установки для генерации квантового ключа в атмосферном квантовом канале с добавленными телескопами для расширения лучей. Справа – модуль передатчика (*Алиса*), слева – модуль приёмника (*Боб*)

3. Генерация квантового ключа в оптоволоконных линиях связи

Первая работа по генерации квантового ключа в оптоволоконном квантовом канале появилась в 1993 г. [19]. Для квантовой криптографии используется стандартное одномодовое оптоволокно. Передача данных ведётся обычно на телекоммуникационной длине волны 1550 нм, которая соответствует наименьшему затуханию (0.2 дБ/км) и малой дисперсии в волокне.

На сегодняшний день наилучшими однофотонными детекторами в этой спектральной области для практического использования являются лавинные фотодиоды InGaAs/InP [20]. По сравнению с кремниевыми фотодиодами они обладают меньшей квантовой эффективностью, обычно на уровне 10 – 20%, и большими шумами. Охлаждение ЛФД до -40°...-70°С с помощью микрохолодильников на основе элементов Пельтье даёт заметное уменьшение темновых шумов. Для снижения вероятности появления послеимпульсов применяют метод активного гашения лавины или работают в режиме с импульсным питанием [21 – 23].

Для оптоволоконных линий связи применяются различные способы кодирования квантовых состояний фотонов [1]. Например, одни из первых криптосистем работали на основе поляризационного кодирования [19, 24]. В последующих работах была продемонстрирована дальность связи свыше 100 км [25]. Частотно-фазовое кодирование использовалось в [26], а временно́й способ был предложен и реализован авторами [27]. Наиболее широкое применение нашло фазовое кодирование с использованием интерферометров Маха-Цендера [1]. Продемонстрирована генерация квантового ключа на расстояния свыше 100 км с полупроводниковыми детекторами одиночных фотонов [28] и свыше 200 км – со сверхпроводниковыми детекторами [29].

Отдельно стоит отметить появление двухпроходной автокомпесационной оптической схемы для фазового кодирования [30], которая отличается устойчивой работоспособностью при изменяющихся внешних условиях и на основе которой построены коммерческие квантовые оптоволоконные криптосистемы. Такая оптическая схема была использована и в экспериментальной установке, созданной нами в Институте физики полупроводников им. А. В. Ржанова СО РАН [31]. Эта установка может служить прототипом для создания практической квантовой криптосистемы.

Она состоит из передатчика *Алиса* и приёмника *Боб* (рис. 2), которые соединены 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 СД50/50. Далее одна часть импульса поступает на вход поляризационного светоделителя ПСД по короткому плечу оптоволоконного интерферометра Маха – Цендера МЦ. Вторая часть импульса приходит на ПСД, пройдя длинное плечо, образованное линией задержки 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 импульса вышли через выход ПСД и направились от *Боба* к *Алисе* по протяжённому одномодовому оптоволокну (квантовому каналу связи).

После прохождения квантового канала лазерный импульс поступает на вход *Алисы*, проходит через накопительную линию НЛ длиной 25 км, фазовый модулятор ФМ, и отражается от фарадеевского зеркала ФЗ, которое поворачивает поляризацию излучения на 90° для автокомпенсации поляризационных искажений оптоволокна. На обратном пути, на выходе из *Алисы* лазерный импульс ослабляется перестраиваемым аттенюатором ПА 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 поляризационным светоделителем ПСД они направляются в другое плечо интерферометра МЦ, после прохождения которого соединяются на выходе СД50/50, где они интерферируют. Результат интерференции регистрируется лавинным фотодиодом ЛФД2 в одном плече, либо, после прохождения циркулятора Ц, – на ЛФД1 в другом плече. Поскольку эти две части импульса проходят одинаковый путь, причём в обратном порядке внутри *Боба*, этот интерферометр автоматически скомпенсирован. Это большое достоинство интерферометра такого типа и, например, коммерческие системы построены именно на таком принципе.

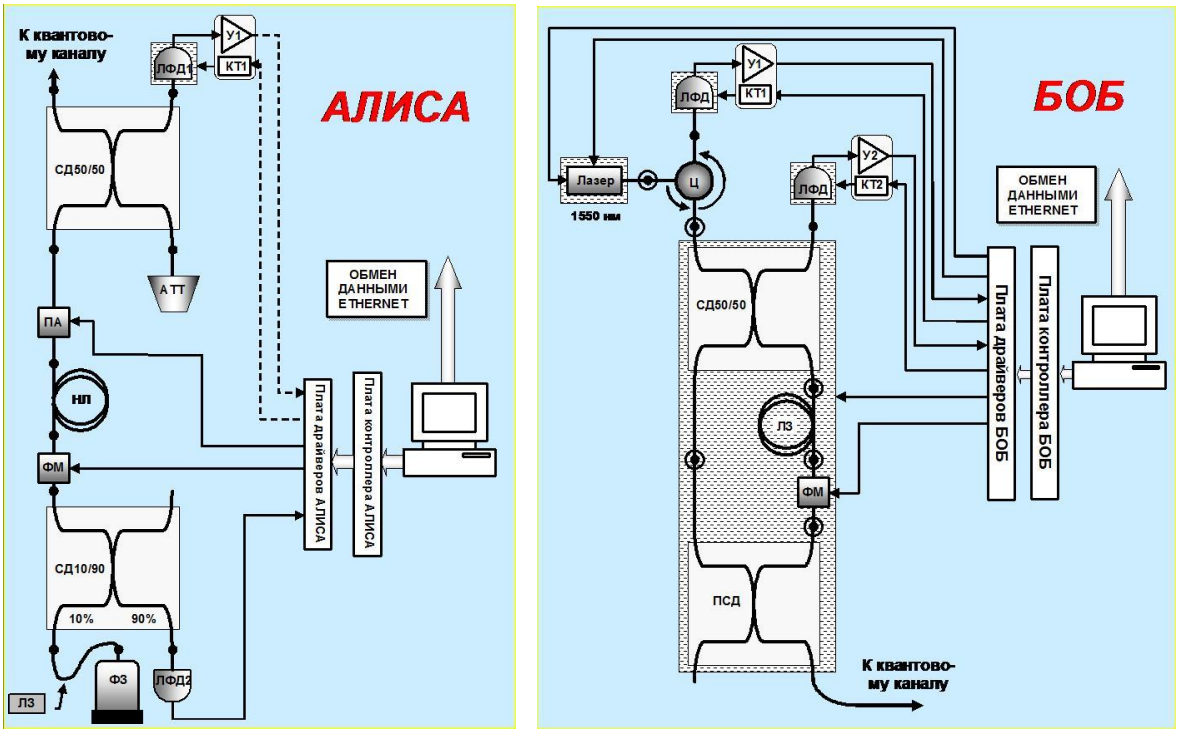

Рис. 2. Слева – схема передающего узла *Алиса* оптоволоконной экспериментальной установки. Справа – схема приёмного узла *Боб* оптоволоконной экспериментальной установки

На описанной экспериментальной установке нами были проведены тестовые эксперименты по генерации квантового ключа в оптоволоконной линии связи между *Алисой* и *Бобом* длиной 25 км. В экспериментах с однофотонными детекторами ETX40 (квантовая эффективность 15%) при тактовой частоте 1 МГц была получена генерация квантового ключа со скоростью 450 бит/с, при этом общее количество ошибок в ключе не превышало 3.7%. В экспериментах с детекторами на основе ERM547 (квантовая эффективность 5%) при тактовой частоте 5 МГц была получена генерация квантового ключа со скоростью 3100 бит/с при общем количестве ошибок в ключе не более 8.1%. Учитывая, что максимальная допустимая ошибка в квантовой передаче для протокола BB84 не должна превышать 11%, полученный результат можно считать удовлетворительным для экспериментальной генерации квантового ключа. Дальнейшее улучшение параметров может быть достигнуто применением более чувствительных однофотонных детекторов и более высокими тактовыми частотами передачи.

4. Заключение

Экспериментальные исследования в области квантовой криптографии ведутся несколькими исследовательскими группами и компаниями. Начиная с первой экспериментальной

работы, где расстояние между передатчиком и приёмником было 30 см, пройден большой путь развития. Передача ключа по открытому пространству продемонстрирована на 144 км. В оптоволоконных квантовых каналах достигнута дальность свыше 200 км. 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. Это позволит поднять скорость генерации квантового ключа до уровня, удовлетворяющего стандартным требованиям к телекоммуникационным системам связи, и при этом обеспечить абсолютную защищённость передаваемых данных.

Работа поддержана грантом РФФИ №14-07-00809, программами РАН и Минобрнауки.

Литература

1. *Gisin N., Ribordy G., Titlel W. et al.* Quantum cryptography // Rev. Mod. Phys. 2002. V. 74. P. 145.
2. *И.И.Рябцев, И.И.Бетеров, Д.Б.Третьяков, В.М.Энтин, В.Л.Курочкин, А.В.Зверев, И.Г.Неизвестный* Экспериментальная квантовая информатика с одиночными атомами и фотонами // Вестник РАН. 2013. Т. 83. №7. С. 606.
3. *Shannon C.E.* Communication Theory of Secret Systems // Bell Syst. Tech. Jour. 1949. V. 28. P. 658.
4. *Bennet C.H.* Quantum Cryptography Using any Two Nonorthogonal States // Phys. Rev. Lett. 1992. V.68. P. 3121.
5. *Wooters W.K., Zurek W.H.* A single quantum cannot be cloned // Nature. 1982. V. 299. P. 802.
6. *Bennet C.H. Brassard G.* Quantum cryptography: public key distribution and coin tossing // Proc. of IEEE Inter. Conf. on Comput. Sys. and Sign. Proces. Bangalore. India. December 1984. P. 175.
7. *Bennet C.H. Bessette F. Brassard G. et.al.* Experimental quantum cryptography // J. Cryptology. 1992. V. 5. P. 3.
8. *Kurtsiefer C., Zarda P., Halder M. et.al.* Quantum cryptography: A step towards global key distribution // Nature. 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. Phys. 2002. V. 4. P. 82.
10. *Rarity J.G., Tapster P.R., Gorman P.M.* Secure free-space key exchange to 1.9 km and beyond // J. Mod. Opt. 2001.V. 48. P. 1887.
11. *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. Phys. 2002. V. 4. P. 43.
12. *Ekert A.K.* Quantum Cryptography Based on Bell's Theorem // Phys. Rev. Lett. 1991. V. 67. P. 661.
13. *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.
14. *Ursin R., Tiefenbacher F., Schmitt-Manderbach T. et al.* Entanglement based quantum communication over 144 km // Nature Physics. 2007. V. 3. P. 481.
15. *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. P. 033038.
16. *Курочкин В.Л., Рябцев И.И., Неизвестный И.Г.* Генерация квантового ключа на основе кодирования поляризационных состояний фотонов // Оптика и спектроскопия. 2004. Т. 96. С. 772.

17. *Курочкин ВЛ., Рябцев И.И., Неизвестный И.Г.* Квантовая криптография и генерация квантового ключа с использованием одиночных фотонов // Микроэлектроника. 2006. Т. 35. С. 41.
18. *A.V.Kolyako, I.G.Neizvestny and V.L.Kurochkin* Investigation the bit rate of quantum key using Si single photon detectors // Journal of Physics: Conference Series. 2014. V. 541. P. 012046.
19. *Muller A., Breguet J., and Gisin N.* Experimental demonstration of quantum cryptography using polarized photons in optical fibre over more than 1 km // Europhys. Lett. 1993. V. 23. N. 6. P. 383.
20. *Trifonov A., Subacius D., Berzanskis A., Zavriev A.* Single photon counting at telecom wavelength and quantum key distribution // J. Mod. Opt. 2004. V. 51. P. 1399.
21. *Курочкин В.Л., Зверев А.В., Курочкин Ю.В., Рябцев И.И., Неизвестный И.Г.* Применение детекторов одиночных фотонов для генерации квантового ключа в экспериментальной оптоволоконной системе связи // Автометрия. 2009. Т. 45. С. 110.
22. *Ю.В.Курочкин, В.Л.Курочкин* Детекторы одиночных фотонов на основе лавинных фотодиодов // Известия вузов: Физика. 2011. Т. 54. № 2. С. 202.
23. *G.K.Krivyakin, A.S.Pleshkov, A.V.Zverev, I.I.Ryabtsev and V.L.Kurochkin* Noise reduction methods of single photon detector based on InGaAs/InP avalanche photodiodes // Journal of Physics: Conference Series. 2014. V. 541. P. 012050.
24. *Muller A., Zbinden H., Gisin N.* Quantum cryptography over 23 km in installed under-lake telecom fibre // Europhys. Lett. 1996.V. 33. P.335.
25. *Peng C., Zhang Jun, Yang Dong et al.* Experimental Long-Distance Decoy-State Quantum Key Distribution Based on Polarization Encoding // Phys. Rev. Lett. 2007. V. 98. P.010505.
26. *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.
27. *Boucher W., Debuisschert T.* Experimental implementation of time-coding quantum key distribution // Phys. Rev. A. 2005. V. 72. P. 062325.
28. *Kosaka H., Tomita A., Nambu Y. et.al.* Single-photon interference experiment over 100 km for quantum cryptography system using balanced gated-mode photon detector // Electron. Lett. 2003. V. 39. P. 1119.
29. *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.
30. *Stucki D., Gisin N., Guinnard O., Ribordy G., and Zbinden H.* Quantum key distribution over 67 km with a plug&play system // New J. Phys. 2002. V. 4. P. 41.
31. *Курочкин В.Л., Зверев А.В., Курочкин Ю.В., Рябцев И.И., Неизвестный И.Г.* Экспериментальные исследования в области квантовой криптографии // Микроэлектроника. 2011. Т. 40. С. 264.

Статья поступила в редакцию 04.04.2015

Рябцев, Игорь Ильич
д.ф.-м.н., заведующий лабораторией ИФП СО РАН имени А.В. Ржанова. (630090, Новосибирск, пр. академика Лаврентьева, 13), тел. 8(383) 3-332-408, e-mail: yabtsev@isp.nsc.ru

Зверев, Алексей Викторович
к.ф.-м.н., н.с. ИФП СО РАН имени А.В. Ржанова.

Курочкин, Владимир Леонидович
к.ф.-м.н., с.н.с. ИФП СО РАН имени А.В. Ржанова.

Неизвестный Игорь Георгиевич
чл.-корр. РАН, д.ф.-м.н., профессор, советник РАН (630090, Новосибирск, пр. академика Лаврентьева, 13), тел. 8(383) 3-306-631, e-mail: neizv@ isp.nsc.ru

Третьяков, Денис Борисович
к.ф.-м.н., н.с. ИФП СО РАН имени А.В. Ржанова.

Черевко, Александр Григорьевич
к.ф.-м.н., доцент, профессор-заведующий кафедрой физики, заведующий лабораторией физических основ телекоммуникаций СибГУТИ (630125, Новосибирск, ул. Кирова, 86), тел. 8 913 9806071, e-mail: cherevko@mail.ru

Энтин, Василий Матвеевич
к.ф.-м.н., с.н.с. ИФП СО РАН имени А.В. Ржанова.

Quantum cryptography as the promising method data transmission absolutely secure for new generations radars

Igor I. Ryabtsev, Vladimir L. Kurochkin, Aleksey V. Zverev, Denis B. Tretyakov, Vasiliy M. Entin, Alexander G. Cherevko, Igor G. Neizvestny

This paper presents a brief review of experimental studies in the field of quantum cryptography and data transmission by single photons. A description of two experimental setups intended for quantum key distribution in atmospheric and fiber-optic quantum channels as well as for the experimental results on quantum key distribution is considered.

Keywords: quantum cryptography, single photons, data transmission.