DOI 10.35264/1996-2274-2020-1-27-33

ПРОБЛЕМЫ И ПЕРСПЕКТИВЫ СОЗДАНИЯ КВАНТОВЫХ СИСТЕМ СВЯЗИ

И.И. Рябцев, зав. лаб., Институт физики полупроводников СО РАН, д-р физ.-мат. наук, чл.-корр. РАН, *ryabtsev@isp.nsc.ru*
С.П. Юркевичюс, нач. отд. ФГБНУ НИИ РИНКЦЭ, канд. техн. наук, доц., *jurkst@yandex.ru*
А.Е. Гриценко, зам. нач. отд. ФГБНУ НИИ РИНКЦЭ, канд. техн. наук, *gritsae@mail.ru*
Рецензент: В.А. Жмудь

Изложены научно-технические проблемы и перспективы создания квантовых систем связи. Проведен краткий анализ состояния научных исследований в этой области за рубежом. Отражены сильные и слабые стороны реализации технологии квантовой обработки информации.

Ключевые слова: квантовые системы связи, фотон, квантовые коммуникации, технологии квантовой обработки информации.

PROBLEMS AND PROSPECTS OF CREATION OF QUANTUM COMMUNICATION SYSTEMS

I.I. Ryabtsev, Head of Laboratory, Institute of Semiconductor Physics SB RAS, Ph. D., Correspondent Member of RAS, *ryabtsev@isp.nsc.ru*
S.P. Yurkevichyus, Head of Department, SRI FRCEC, Doctor of Engineering, Associate Professor, *jurkst@yandex.ru*
A.E. Gritsenko, Deputy Head of Department, Federal State Budgetary Scientific Institution Scientific Research Institute FRCEC, Doctor of Engineering, *gritsae@mail.ru*

Scientific and technological problems and prospects for creating quantum communication systems are herein outlined. A brief analysis of the state of scientific research in this area abroad is carried out. The strengths and weaknesses of the implementation of quantum information processing technology are reflected.

Keywords: quantum communication systems, photon, quantum communications, technologies of quantum information processing.

Введение

Основными задачами квантовых коммуникаций являются поиск эффективных алгоритмов и разработка схем практической реализации защищенной передачи секретной информации с использованием квантовых объектов – одиночных фотонов [1]. 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.

Для полной защищенности 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 [2] 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 удаленными пользователями. Для этого квантовая криптография предлагает использовать статистические свойства одиночных квантовых объектов, а именно – одиночных фотонов.

Один из основных постулатов квантовой механики состоит в том, что всякое измерение приводит к изменению состояния квантового объекта [3]. Это означает, что всякая попытка со стороны Евы получить ключ, который передается с помощью одиночных фотонов по квантовому каналу (например, волоконному световоду) от Алисы к Бобу, приведет к тому, что Боб получит ключ измененным 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 придется 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 [4] такой процесс будет содержать большой процент ошибок. Поэтому Боб получит неработоспособный ключ, о чем он сообщит Алисе. Далее они могут решить прекратить передачу ключа или повторить ее заново. Поскольку квантовые базисы для передачи и приема 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 наиболее широко применяют фазовое кодирование фотонов с помощью фазовых модуляторов, а декодирование осуществляют с помощью управляемых оптических интерферометров. Для атмосферного канала применяются поляризационное кодирование и декодирование с помощью поляризационно-чувствительных элементов.

Развитие направления совершенствования квантовых систем связи в мире

За рубежом имеется множество научных групп и компаний, занимающихся созданием и совершенствованием систем квантовых коммуникаций. В настоящее время наиболее активные исследования ведут следующие группы (табл. 1):

– Gisin N., Zbinden H., компания id Quantique, Geneva University, Switzerland, коммерческие оптоволоконные системы квантовой связи (статусы С4, С5, С6, С7);

– MagiQ, USA, коммерческие оптоволоконные системы квантовой связи (статусы Д4, Д5, Д6, Д7);

– Toshiba Cambridge Research Laboratory, UK, коммерческие оптоволоконные системы квантовой связи (статусы С4, С5, С6, С7);

– Tokyo QKD network, Japan, японская оптоволоконная сеть на основе квантовой связи (статусы Д4, Д5, Д6, Д7);

– Boyd R.W., University of Rochester, USA, многоразмерная квантовая криптография с закрученным светом (статус Л1);

– Tittel W., Calgary University, Canada, разработка оптоволоконных систем квантовой связи, не зависящих от метода регистрации фотонов (статус Д1);

– University of Science and Technology of China, Hefei, China, разработка оптоволоконных систем квантовой связи, не зависящих от метода регистрации фотонов (статус Д1);

– von der Weid J.P., Brasil, Pontifical Catholic University, Rio de Janeiro, Brazil, разработка оптоволоконных систем квантовой связи, не зависящих от метода регистрации фотонов (статус С1).

Таблица 1

Статусы создания квантовых систем связи

№ п/п	Стадия развития	Дистанции			
		Лабораторные (менее 200 м)	Короткие (менее 2 км)	Средние (менее 70 км)	Дальние (более 70 км)
Код		Л	К	С	Д
1	Реализация физических принципов	Л1	К1	С1	Д1
2	Реализация полной процедуры связи	Л2	К2	С2	Д2
3	Надежность компонент и устойчивость работы	Л3	К3	С3	Д3
4	Практическая реализация защищенной связи	Л4	К4	С4	Д4
5	Возможность передачи ключей шифрования[1]	Л5	К5	С5	Д5
6	Возможность организации сетевой архитектуры	Л6	К6	С6	Д6
7	Использование для шифрования данных[2]	Л7	К7	С7	Д7

[1] Практическая демонстрация скорости обмена – более 100 бит/с.
[2] Практическая демонстрация скорости обмена – более 1 Мбит/с.

Перечень достижений по стадиям развития квантовых систем связи

В 1984 г. был предложен первый протокол BB84 [5], а в 1992 г. осуществлена экспериментальная демонстрация генерации квантового ключа с помощью передачи поляризованных в двух неортогональных базисах одиночных фотонов по открытой линии связи [6]. 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 связи, представляет интерес развитие методов передачи квантового ключа по открытому пространству и оптоволокну.

При распространении излучения через атмосферу поляризация излучения подвергается незначительным изменениям, поэтому для организации квантовых каналов через открытое пространство используется поляризационный метод кодирования [7], причем в перспективе рассматривается возможность связи с орбитальными спутниками [8]. 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 приемниками также представляет значительный интерес.

Если в первой атмосферной экспериментальной установке [9] расстояние между передатчиком и приемником (длина квантового канала) было 30 см, 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 [11] – на 10 км, [12] – на 23 км

на основе протокола BB84, [13] – с использованием перепутанных состояний, на 13 км. Рекорд на данный момент принадлежит работе [14] (144 км). В 2008 г. был проведен эксперимент со спутником и зарегистрирован отраженный однофотонный сигнал от лазерного импульса, посланного с Земли [15]. Для подавления фоновых засветок от солнечного или лунного света необходимо применять спектральные, пространственные и временные фильтры.

Первая работа по генерации квантового ключа в оптоволоконном квантовом канале появилась уже в 1993 г. [16]. Для квантовой криптографии используется стандартное одномодовое оптоволокно. Передача данных ведется обычно на телекоммуникационной длине волны 1550 нм, которая соответствует наименьшему затуханию (0,2 дБ/км) и малой дисперсии в волокне.

Для оптоволоконных линий связи применяются различные способы кодирования квантовых состояний фотонов. Например, одни из первых криптосистем работали на основе поляризационного кодирования [17]. В последующих работах была продемонстрирована дальность связи свыше 100 км [18]. Частотно-фазовое кодирование использовалось в [19], а временной способ был предложен и реализован авторами [20]. Наиболее широкое применение нашло фазовое кодирование с использованием интерферометров Маха – Цендера. Продемонстрирована генерация квантового ключа на расстояния свыше 100 км с полупроводниковыми детекторами одиночных фотонов [21] и свыше 200 км со сверхпроводниковыми детекторами [22].

Отдельно стоит отметить появление двухпроходной автокомпенсационной оптической схемы для фазового кодирования [23], которая отличается устойчивой работоспособностью при изменяющихся внешних условиях и на основе которой построены коммерческие квантовые оптоволоконные криптосистемы.

Преимущества и недостатки квантовой коммуникации

Обычные оптические линии связи не могут обеспечить полную секретность передачи данных, поскольку в них применяются лазерные импульсы, содержащие большое число фотонов, а часть этих фотонов может быть перехвачена несанкционированным пользователем. В квантовой криптографии для передачи информации используются одиночные фотоны, которые не могут быть перехвачены и измерены с абсолютной достоверностью, что является основой для создания абсолютно защищенных линий связи. Наибольшая потребность в квантово-криптографических системах связи ожидается в секторе специальных применений, для которых абсолютная секретность передачи информации обладает бóльшим приоритетом, чем скорость передачи данных.

Абсолютная секретность квантовой криптографии основана на использовании одиночных фотонов, которые в квантовой теории соответствуют так называемым состояниям Фока для одной моды электромагнитного поля. Чистые однофотонные фоковские состояния очень сложно реализовать. Для их практической реализации, как правило, используют либо очень слабые лазерные импульсы, либо пары фотонов в перепутанном квантовом состоянии, которые в обоих случаях описываются статистикой Пуассона. Однако для таких источников фотонов всегда есть ненулевая вероятность испустить не один, а два и более фотона, что представляет потенциальную угрозу с точки зрения подслушивания. Поэтому для полной реализации идей квантовой криптографии необходимо разработать и создать детерминированные генераторы одиночных фотонов. В идеале источником одиночного фотона может служить любая одиночная квантовая частица – атом, молекула, ион, квантовая точка и т. д., способная поглощать и излучать фотоны в узкой полосе оптических частот. Основной проблемой на этом пути является повышение эффективности сбора однофотонного излучения, поскольку оно равновероятно распределено по всем направлениям, а также разработка простых методов электрического управления испусканием одиночного фотона.

Необходимо также создать более эффективные детекторы одиночных фотонов. В настоящее время в системах квантовой криптографии применяются Si и InGaAs/InP – лавинные

фотодиоды. Если Si-фотодиоды, работающие в атмосферных системах, обеспечивают квантовую эффективность до 90 % при уровне темновых шумов менее 1 кГц, то фотодиоды InGaAs/InP, предназначенные для оптоволоконных систем, имеют квантовую эффективность не более 20 % при уровне шумов более 10 кГц. Низкая квантовая эффективность и большой уровень шумов ограничивают максимальную дальность и скорость генерации квантового ключа в оптоволоконных системах связи.

Наконец, скорость генерации квантового ключа ограничена также максимальной частотной полосой работы элементов квантово-криптографических систем. Несмотря на то что в современных системах тактовая частота может достигать 1 ГГц, предельное быстродействие генераторов и детекторов одиночных фотонов, а также физических генераторов случайных чисел остается на более низком уровне. Поэтому необходимо совершенствовать генераторы и детекторы одиночных фотонов и генераторы случайных чисел на предмет увеличения рабочей полосы частот до 1 ГГц, а в перспективе – и до 10–100 ГГц.

Перспективы развития квантовых систем связи

Наибольшая потребность в квантово-криптографических системах связи ожидается в секторе специальных применений, для которых абсолютная секретность передачи информации обладает бóльшим приоритетом, чем скорость передачи данных (в современных системах квантовой криптографии скорость ограничена значениями порядка 0,01–1,0 Мбит/с в зависимости от длины оптической линии). Такие системы должны обеспечивать полную защищенность от несанкционированного прослушивания с помощью современных и будущих технических средств. Создание квантовых систем связи имеет критическое значение для обеспечения безопасности страны, так как средства прослушивания непрерывно совершенствуются. Предполагаемые потребители – ведомства, организации и предприятия, в работе которых необходимо использовать атмосферные или оптоволоконные каналы связи повышенной защищенности: министерство обороны, космическая связь, МВД, агентства правительственной связи, службы безопасности, телекоммуникационные компании и т. д.

В ближайшие пять лет необходимо создать российские коммерческие квантовые системы связи, предназначенные для внедрения как в секторе специальных применений, так и в других организациях, заинтересованных в передаче конфиденциальной информации. Должны быть созданы как оптоволоконные системы, совместимые со стандартными оптоволоконными линиями связи, так и атмосферные системы, предназначенные для оптической связи в пределах видимости и космической связи со спутниками.

Разработанные системы должны обеспечивать для оптоволоконных и атмосферных систем связи максимальную дальность генерации квантового ключа до 100 км при скорости генерации до 10–100 Мбит/с. Системы должны быть полностью сертифицированы соответствующими службами и ведомствами, пройти аккредитацию в Минсвязи России и доказать свою совместимость с современными системами телекоммуникаций. После этого должно быть проведено масштабное внедрение разработанных российских систем квантовой связи.

В ближайшие десять лет должны быть выполнены научно-исследовательские и опытно-конструкторские работы (НИОКР), направленные на увеличение дальности и скорости генерации квантового ключа в квантовых системах связи. Для этого необходимо разработать и создать быстродействующие, высокоэффективные, электрически управляемые генераторы одиночных фотонов на заданные длины волн и внедрить их в квантовые системы связи. Должны быть рассмотрены и изучены новые варианты кодирования одиночных фотонов, например в многобазисных закрученных состояниях света [24]. Должны быть разработаны детекторы одиночных фотонов с увеличенной квантовой эффективностью и быстродействием. Также следует выполнить поисковые исследования по проверке идей увеличения секретности квантовой криптографии за счет применения недавно предложенной квантовой связи, не зависящей от метода регистрации фотонов, когда передатчик и приемник посылают

одиночные фотоны в интерферометр с однофотонными детекторами, установленными посередине квантового канала [25].

Поскольку для развития квантовых систем связи в России необходимо разработать и создать отечественную элементную базу, требуется развитие всех сопутствующих технологий. Для разработки генераторов одиночных фотонов необходимо выполнить исследования квантовых точек в полупроводниках и создать полупроводниковые структуры, обеспечивающие токовую накачку и направленность однофотонного излучения. Для разработки полупроводниковых детекторов одиночных фотонов необходимо создать полупроводниковые структуры, обеспечивающие как эффективную регистрацию фотона, так и внутреннее усиление за счет лавинного размножения электронов. Для разработки оптоэлектронных компонентов необходимо развить производство и изготовление элементов интегральной оптики и фотоники. Наконец, теоретические исследования в области квантовой криптографии могут предложить новые протоколы генерации квантового ключа, способные увеличить скорость и дальность генерации ключа.

Создание элементной базы квантовой криптографии в России может послужить толчком к развитию и других квантовых технологий, например квантовых компьютеров и сенсоров. В этих технологиях зачастую требуется эффективно регистрировать одиночные фотоны или управлять их параметрами с помощью оптоэлектронных устройств. Быстродействующие электрически управляемые модули систем квантовой криптографии могут быть напрямую использованы как в квантовых компьютерах, так и в квантовых сенсорах.

Примерный временной план работ по созданию российских квантовых систем связи можно представить следующим образом:

– создание российской элементной базы для квантовых систем связи (однофотонные детекторы и оптоэлектронные компоненты) – 2 года;

– создание прототипов коммерческой оптоволоконной и атмосферной систем квантовой связи – 2 года;

– проведение испытаний, доводка и сертификация прототипов квантовых систем связи – 2 года;

– внедрение наземных квантовых систем связи – 3 года;

– внедрение спутниковых квантовых систем связи – 5 лет.

Заключение

Дальнейшее развитие квантовых систем связи требует увеличения дальности и скорости генерации квантового ключа, а также степени их защищенности. Для этого необходимо выполнять новые теоретические исследования для разработки новых идей по методам и протоколам генерации квантового ключа, организации наземных и космических сетей связи. Например, недавно теоретиками была выдвинута идея увеличения секретности за счет применения квантовой связи, не зависящей от метода регистрации фотонов, когда передатчик и приемник посылают одиночные фотоны в интерферометр с однофотонными детекторами, установленными посредине квантового канала. Также можно рассматривать предложенные теоретиками многобазисные протоколы генерации квантового ключа, обеспечивающие повышенный уровень секретности, и состояния света высокой размерности, обеспечивающие увеличение скорости генерации ключа.

***Список литературы* (*References*)**

1. Gisin N., Ribordy G., Tittel W. et al. (2002) Reviews of Modern Physics. Issue 74. P. 145.

2. Shannon C.E. (1949) Bell System Technical Journal. Issue 28. P. 658.

3. Bennet C.H. (1992) Physical Review Letters. Issue 68. P. 3121.

4. Wooters W.K. Zurek W.H. (1982) Nature. Vol. 299. P. 802.

5. Bennet C.H. Brassard G. (1984) Proc. of IEEE Int. Conf. on Comput. Sys. and Sign. Proces. P. 175.

6. Bennet C.H. et al. (1992) Cryptology. Vol. 5.
7. Kurtsiefer C. et al. (2002) Nature. Vol. 419. P. 450.
8. Rarity J.G. et al. (2002) New Journal of Physics. Issue 82.
9. Bennet C.H.et.al. (1992) Cryptology. Vol. 5.
10. Rarity J.G. et al. (2001) Journal of Modern Optics. 48. Issue 1887.
11. Hugheset R.J. et al. (2002) New Journal of Physics. Issue 43.
12. Kurtsiefer C. et al. (2002) Nature. Vol. 419. P. 450.
13. Peng C. et al. (2005) Physical Review Letters. Issue 94.
14. Ursin R. et al. (2007) Nature Physics. Issue 3. P. 481.
15. Villoresi P. et al. (2008) New Journal of Physics. Issue 10.
16. Muller A. et al. (1993) Europhysics Letters. Issue 23, P. 383.
17. Muller A. et al. (1996) Europhysics Letters. Issue 233. P. 335.
18. Peng C. et al. (2007) Physical Review Letters. Issue 98.
19. Merolla J.-M. et al. (1999) Physical Review Letters. Issue 82. P. 1656.
20. Boucher W., Debuisschert T. (2005) Physical Review A. Issue 72.
21. Kosaka H. et.al. (2003) Electron. Lett. Issue 39. P. 1119.
22. Takesue H. et al. (2007) Nature Photonics. Issue 1. P. 343.
23. Stucki D. et al. (2002) New Journal of Physics. Issue 4. P. 41.
24. Mirhosseini M. et al. (2015) New Journal of Physics. Issue 17. P. 330.
25. Valivarthi R. et al. (2015) ArXiv:1501.07307v1.