4. Информационно-аналитический портал, посвящённый отечественным телекоммуникациям в целом, интернет-провайдингу, строительству сетей, передаче и хранению данных. [Электронный ресурс]. - Режим доступа: URL: <https://nag.ru/go/text/101183/>
5. Независимое российское онлайн-издание, посвященное цифровым технологиям. [Электронный ресурс]. - Режим доступа: URL: <https://3dnews.ru/570434>
6. Крупнейшая в Рунете площадка для предпринимателей. [Электронный ресурс]. - Режим доступа: URL: <https://vc.ru/finance/67047-chto-nam-stoit-mvno-postroit>
7. MCN Telecom - первый мобильный виртуальный оператор (MVNO) для бизнеса. [Электронный ресурс]. - Режим доступа: URL: <https://telcojournal.mcn.ru/interview/full-light-mvno-tekhnologiya-multi-sim-perspektiv>

Дахкильгова К.Б., Идигова А.А.

Проблемы пространственного поиска и обнаружения в системах квантовой криптографии

*ФГБОУ ВО Чеченский государственный университет
(Россия, Грозный)*

doi: 10.18411/lj-10-2020-55

idsp: ljjournal-10-2020-55

Аннотация

В статье рассматриваются проблемы поиска, приёма, обнаружения и обработки оптических сигналов, которые важны в системах квантовой криптографии, интенсивно развивающихся в настоящее время.

Ключевые слова: фотоны, однофотонный импульс, пространственный поиск, одноканальная регистрация, защита информации, квантовая криптография.

Abstract

The article discusses the problems of searching, receiving, detecting and processing optical signals, which are important in quantum cryptography systems, which are currently intensively developing.

Keywords: photon, single photon pulse, existential search, the single-channel registration, cybersecurity, quantum cryptography.

Проблема поиска, приёма, обнаружения и обработки оптических сигналов важна в системах квантовой криптографии, которые интенсивно развиваются в настоящее время.

Привлекательность идеи квантовой криптографии состоит в том, что предложен новый метод создания случайного секретного ключа между пользователями квантовой линии связи. Его абсолютная секретность и невозможность незаметного прослушивания посторонним лицом основана на законах квантовой физики в противоположность используемым сейчас методам криптографии, которые основаны на математических закономерностях и, в принципе, поддаются расшифровке.

При переходе от сигналов, где информация кодируется импульсами, содержащими тысячи фотонов, к сигналам, где среднее число фотонов, приходящихся на один импульс, много меньше единицы (порядка 0,1), вступают в действие законы квантовой физики. Именно на использовании этих законов в сочетании с процедурами классической криптографии основана природа секретности, обеспечиваемая квантовой криптографией. Здесь применим принцип неопределённости Гейзенберга, согласно которому попытка произвести измерения в квантовой системе вносит в неё нарушения, и полученная в результате такого измерения информация квалифицируется принимаемой стороной как дезинформация.

Интенсивные работы проводятся по созданию атмосферных и спутниковых систем КРК. Действительно, создание глобальной телекоммуникационной сети

невозможно с использованием ВОЛС. Пока предел коммерческих волоконно-оптических систем КРК оценивается в сотни километров. Надо ещё учесть, что из-за затухания в оптическом волокне через каждые 100 км необходимо ставить секретные промежуточные пункты, которые гораздо более доступны для разведки, чем спутник. Спутниковые системы КРК представляются на современном этапе развития технологии единственным направлением для преодоления этого предела.

Группа учёных национальной лаборатории из Лос-Аламоса под руководством Ричарда Хьюгса (Richard Hughes) занимается разработками спутниковых систем КРК. Для предотвращения поглощения исследователи выбрали длину волны в 770 нм, соответствующую минимальному поглощению излучения молекулами атмосферы. Сигнал с большей длиной волны также слабо поглощается, но более подвержен турбулентности, которая вызывает изменение локального показателя преломления воздушной среды и, ввиду этого, изменение поляризации фотонов.

Позднее группой R. Hughes передан квантовый ключ на расстояние 2 км через воздушную среду. При испытаниях сигналы передавались горизонтально, вблизи поверхности Земли, где плотность воздуха и флуктуации мощности максимальны. Поэтому расстояние в 2 км вблизи поверхности Земли эквивалентно 300 км между низкоорбитальным искусственным спутником Земли и наземным центром.

Британские физики из коммерческого подразделения QinetiQ Британской оборонной исследовательской лаборатории и немецкие физики из Мюнхенского университета Людвиг-Максимилиана впервые осуществили передачу ключа на расстояние 23,4 км непосредственно через воздушное пространство между двумя горными вершинами в Южных Альпах без использования оптического волокна. В эксперименте для кодирования информации использовалась поляризация фотонов – одна для передачи значения бита «0» и ортогональная для значения бита «1». Слабый импульсный сигнал посылался ночью с одной вершины (2 950 м) на другую (2 244 м), где находился счётчик фотонов.

Руководителем проекта John Rarity из QinetiQ отмечено, что для атмосферных систем КРК необходимо улучшить устойчивость системы к неизбежной потере фотонов при их посылке на расстояния в тысячи километров.

Группа ученых из Италии и Австрии провела первый в мире успешный эксперимент по устойчивой передаче и идентификации фотонных импульсов между Землей и высокоорбитальным ИСЗ. Эксперимент доказывает возможность защиты средствами квантовой криптографии каналов спутниковой связи, телеметрической и разведывательной информации, передаваемой даже на высокоорбитальные ИСЗ.

Исследовательская группа под руководством Anton Zeilinger и Cesare Barbieri для проведения эксперимента использовала стандартное оборудование лазерной станции Matera Laser Ranging Observatory Итальянского космического агентства и геодезический ИСЗ Ajisai японского космического агентства JAXA с перигеем 1485 км. Спутник Ajisai предназначен для прецизионного изучения изменения параметров его орбиты со временем и представляет собой покрытую уголковыми отражателями сферу. Мониторинг орбиты спутника осуществляется методами лазерной локации с помощью телескопа станции Matera апертурой 1,5 м (рис. 1).

Помимо спутника Ajisai, аналогичные эксперименты проведены также с геодезическими спутниками Lageos II (перигей 5625 км), Torex-Poseidon (1350 км) и Beacon-C (927 км), также оснащёнными уголковыми отражателями, однако с менее впечатляющими результатами.

Использованные лазеры излучают импульсы на длине волны 532 нм длительностью 700 пс и частотой следования 17 кГц с энергией 490 нДж. Последовательность импульсов посылается к спутнику через телескоп MLRO, первичное зеркало которого имеет диаметр 1,5 м (рис. 2).

Рис. 1. Схема однофотонной локации спутника LAGEOS

Поток фотонов, несущих полезную информацию на обратном пути из космоса, собирается телескопом и через узкополосный светофильтр направляется на кремниевый ЛФД. Поляризационное разделение в прямом и обратном направлении передачи информации из космоса достигается в поляризационном светоделителе и четвертьволновой пластине. Все события во временной области (например, запуск лазера, опрос фотоприёмников и импульсы управления) синхронизированы от атомных часов обсерватории MLRO и привязаны к среднему времени по Гринвичу.

Эксперимент показал возможность осуществления закрытой передачи данных с ИСЗ и на ИСЗ с использованием существующих средств лазерной спутниковой связи.

Демонстрация устойчивого приёма фотонных импульсов по каналу прямой лазерной связи между ИСЗ и самолетом указывает на перспективу появления принципиально перехватываемых и неидентифицируемых противником спутниковых каналов передачи информации.

Начиная с 1998 г, дальность связи через атмосферу постоянно увеличивается: 1998 г. – 1 км, 2000 г. – 1,6 км, 2002 г. – 10 км, 2005 г. – 13 км, 2007 г. – 144 км.

Рис. 2. Экспериментальная установка для передачи и идентификации фотонных импульсов между Землей и высокоорбитальным ИСЗ

Однако увеличение дальности связи через атмосферу для имитации спутниковой связи проблематично вследствие того, что дальнему распространению оптического излучения препятствуют атмосферные и географические препятствия. Во-первых, это искажение фронта импульса из-за атмосферной бури, нестабильность оптических систем при экологических колебаниях и качество оптики для формирования

дифракционного пятна малого размера. Ограничения накладывает география Земли (искривление, орография, препятствия, и т.д.) и поглощение радиации в приземных слоях атмосферы.

Учёным при создании атмосферных и спутниковых систем КРК приходится решать побочные задачи. Спутник, наряду с фотонами, несущими сообщение, может принимать и фотоны фонового излучения, исходящего как от Солнца, так и отражённого Землей или Луной. Поэтому применяется оптический приёмник со сверхузкой направленностью оптической антенной, а также светофильтр для приёма фотонов только определённой длины волны. Кроме того, для ослабления влияния турбулентности атмосферы фотоприёмник чувствителен к приёму фотонов в течение всего 5 нс периодически с интервалом в 1 мкс. С этой целью работа фотоприёмника должна быть жёстко синхронизирована с оптическим передатчиком.

Даже при сохранении поляризации, вследствие турбулентности, может измениться время распространения фотонов, приводя к фазовому дрожанию. С целью компенсации фазового дрожания впереди каждого фотона высылаются оптический импульс. Этот синхронизирующий импульс, подвергается такому же, как следующий за ним фотон, влиянию атмосферы. Поэтому независимо от момента получения импульса оптический приёмник искусственного спутника Земли знает, что через 100 нс нужно быть готовым к приёму информационного фотона.

Изменение показателя преломления атмосферы вследствие турбулентности вызывает отклонение луча от оптической оси приёмной антенны. Поэтому для излучения фотонов в заданном направлении приёмопередающий комплекс отслеживает слабое отражение оптических синхроимпульсов. Основное препятствие представляли атмосферные искажения, приводящие к искажению волнового фронта, поглощение в атмосфере, нестабильность наземного лазерного локатора вследствие сейсмических колебаний.

Следовательно, требование применения оптических приёмопередатчиков со сверхузкой направленностью оптических антенн в атмосферных и спутниковых системах КРК предполагает пространственный поиск источника оптического излучения. Требование же использования оптических импульсов длительностью в сотни и тысячи пикосекунд, а также жёсткой временной синхронизации предусматривает элементы временного поиска. Организация секретности не только при квантовом распределении, но и при вхождении в связь разнесённых объектов предполагает однофотонную регистрацию.

Таким образом, приём и обработка оптических сигналов в квантовой криптографии требует организации пространственно-временного поиска с целью обнаружения и выделения момента появления оптического импульса в режиме однофотонной регистрации для вхождения в связь и синхронизм приёмно-передающего комплекса в атмосферных и спутниковых системах КРК.

1. Румянцев К.Е. Системы квантового распределения ключа: Монография. – Таганрог: Изд-во ТТИ ЮФУ, 2011. – 264 с.
2. Rumyantsev K.E., Golubchikov D.M. Modeling of quantum key distribution system for secure information transfer // Chapter in the book «Integrated Models for Information Communication Systems and Networks: Design and Development» - IGI Global, 2012.
3. Котенко В.В., Румянцев К.Е. Теория информации и защита телекоммуникаций: Монография. – Ростов н/Д: Изд-во ЮФУ, 2009. – 369 с.
4. Алфёров А.П., Зубов А.Ю., Кузьмин А.С., Черёмушкин А.В. Основы криптографии. - М.: Гелиос АРВ, 2005. – 480 с.
5. Конахович Г. Ф., Климчик В. П., Паук С. М., Потапов В. Г. Защита информации в телекоммуникационных системах. - Киев: Изд-во «МК-Пресс», 2005. – 288 с.
6. Hughes R.J., Buttler W.T., Kwiat P.G., Lamoreaux S.K., Mookgarn G.L., Nordholt J.E., Peterson C.G. Quantum cryptography for secure satellite communications // Proceedings of IEEE Aerospace Conference. – 2000. – Vol. 1. – P. 191–200.
7. Бычков С.И., Румянцев К.Е. Поиск и обнаружение оптических сигналов: Монография / Под ред. К.Е.Румянцева. – М.: Радио и связь. Таганрог: Изд-во ТРТУ, 2000. – 282 с.