А. П. Плёнкин
К. Е. Румянцев

Однофотонные приёмники для систем квантового распределения ключей

учебное пособие

ЮЖНЫЙ ФЕДЕРАЛЬНЫЙ УНИВЕРСИТЕТ
ЮФУ
РОСТОВ-НА-ДОНУ·ТАГАНРОГ

УДК 621.391.64
ББК 32.875я73-5
Р865

Печатается по решению кафедры информационной безопасности телекоммуникационных систем Института компьютерных технологий и информационной безопасности Южного федерального университета (протокол № 13 от 12 февраля 2020 г.)

Рецензенты:

заместитель директора по научной работе Ростовского филиала Российской таможенной академии, заслуженный деятель науки РФ, доктор технических наук, профессор *Д. А. Безуглов*

профессор кафедры «Антенны и радиопередающие устройства» Южного федерального университета, заслуженный работник высшей школы РФ, доктор технических наук, профессор *В. А. Обуховец*

Румянцев, К. Е.

Р865 Однофотонные приёмники для систем квантового распределения ключей : учебное пособие / А. П. Плёнкин, К. Е. Румянцев ; Южный федеральный университет. – Ростов-на-Дону ; Таганрог : Издательство Южного федерального университета, 2020. – 117 с.

ISBN 978-5-9275-3491-3

Пособие содержит теоретические сведения о принципах работы однофотонных приёмников на основе лавинных фотодиодов, а также материалы лабораторно-практических занятий по разделу «Квантовые коммутации» дисциплины «Квантовая связь и криптография». Рассмотрены принципы работы, конструкции и основные параметры однофотонного детектора ID 201 фирмы idQuantique (Швейцария). Приведено описание принципа работы системы квантового распределения ключа на основе фазового кодирования состояний фотонов.

Учебное пособие предназначено для студентов специальности 10.05.02 «Информационная безопасность телекоммуникационных систем».

УДК 621.391.64
ББК 32.875я73-5

ISBN 978-5-9275-3491-3

1. РОЛЬ ОДНОФОТОННЫХ ДЕТЕКТОРОВ ДЛЯ РЕАЛИЗАЦИИ ПРЕДЕЛЬНЫХ ХАРАКТЕРИСТИК СИСТЕМ КВАНТОВОГО РАСПРЕДЕЛЕНИЯ КЛЮЧЕЙ

1.1. Проблемы при реализации систем квантовой криптографии

Работа «Сопряжённое кодирование» Стефана Визнера (Stephen Wiesner) из Колумбийского университета положила начало новому направлению в криптографии. В квантовой криптографии, благодаря законам квантовой механики, возможно распространение между двумя или более абонентами секретного ключа, удовлетворяющего всем требованиям, предъявляемым шифром Вернама, что означает абсолютную секретность передаваемой информации. В 1984 г. Чарльз Беннет (Charles Bennett) из фирмы IBM и Жиль Брассард (Gilles Brassard) из Монреальского университета запатентовали первый протокол обмена BB84 для квантово-криптографической системы. С этого момента одной из наиболее интересных стала идея использовать для целей защиты информации фотоны, поведение которых подчиняется законам квантовой механики.

Квантовая криптография уже заняла достойное место среди систем, обеспечивающих конфиденциальную передачу информации. От обсуждения достоинств и недостатков различных протоколов распределения ключа, научный мир перешёл к поиску наиболее удачных структурных и схемотехнических решений, обеспечивающих увеличение дальности связи, повышение скорости формирования ключа и снижение влияния дестабилизирующих факторов. Природа секретности квантового канала заключается в том, что при переходе от сигналов, где информация кодируется импульсами, содержащими тысячи фотонов, к сигналам, где среднее число фотонов, приходящихся на один импульс (фотонный или квантовый импульс), много меньше единицы (порядка 0,1), вступают в действие законы квантовой механики. Именно на использовании этих законов в сочетании с процедурами классической криптографии основана секретность квантово-криптографических систем.

В системах квантовой криптографии непосредственно применяется принцип неопределённости Гейзенберга:

Попытка произвести измерения в квантовой системе искажает её состояние, а полученная в результате такого измерения информация не полностью соответствует состоянию системы до начала измерений.

Попытка перехвата информации из квантового канала связи неизбежно приводит к внесению в него помех, обнаруживаемых легальными пользователями. Квантовая криптография использует этот факт для обеспечения возможности двум сторонам, которые ранее не встречались и предварительно не обменивались никакой секретной информацией, осуществлять между собой связь в обстановке полной секретности без боязни быть подслушанными.

Наибольшее практическое применение квантовая криптография находит в сфере защиты информации, передаваемой по волоконно-оптическим линиям связи (ВОЛС). Это объясняется тем, что оптические волокна позволяют обеспечить передачу фотонов на большие расстояния с минимальными искажениями. В качестве источников фотонов применяются лазерные диоды. Далее происходит существенное ослабление мощности светового сигнала до уровня, когда среднее число фотонов на один импульс становится много меньше единицы.

Системы передачи информации по ВОЛС, в приёмном модуле которых применяются лавинные фотодиоды (ЛФД) в режиме счёта фотонов, называются квантовыми оптическими каналами связи.

Исследования в области квантовой криптографии ведут несколько компаний, в том числе швейцарская компания IdQuantique, представившая коммерческую систему квантовой криптографии, и фирма MagiQ Technologies из Нью-Йорка, выпустившая прототип коммерческой квантовой криптотехнологии собственной разработки.

В разработке фирмы MagiQ система Navajo для распределения ключей способна в реальном времени генерировать и распространять ключи средствами квантовых технологий, обеспечивая защиту от внутренних и внешних злоумышленников.

Две швейцарские фирмы IdQuantique и WISeKey и одна интернациональная организация (OISTE) представили совместный проект по внедрению методов квантовой криптографии и развитию инфраструктуры квантовых ключей для правительственных структур, банковских и финансовых

институтов. Отметим, что компания IdQuantique приступила к выпуску коммерческой квантово-криптографической системы, обеспечивающей передачу информации через ВОЛС на расстояние до 150 км.

При создании коммерческих систем квантовой криптографии разработчики столкнулись со следующими проблемами:

– ограниченная дальность связи;

– низкая скорость формирования квантовых ключей;

– отсутствие промышленных образцов однофотонных источников для квантовой криптографии;

– несанкционированный съём информации (НСИ) злоумышленником (некогерентные или индивидуальные, когерентные или массовые атаки злоумышленника) на квантовый канал.

Проблема ограниченной дальности квантовой криптографии состоит в том, что сигнал в квантовом канале нельзя усилить без потери его квантовых свойств. Следовательно, из-за потерь при передаче квантовый канал имеет ограничения по дальности связи. Для всех существующих систем, основанных на фотонах в инфракрасном диапазоне длин волн в кварцевых оптических волокнах, минимальный уровень потерь составляет порядка 0,2 дБ/км. Так что построение систем квантовой коммуникации на расстояниях, превышающих 100 км (с потерями менее 20 дБ) проблематично. Следовательно, создание трансатлантической ВОЛС с системой секретности на основе квантовой криптографии пока не реализуемо.

Проблема низкой скорости передачи информации при квантовой криптографии связана с тем, что в принимаемом импульсе среднее число фотонов равно 0,1. Следовательно, только в одном принятом импульсе из 10 содержится фотон. Естественно, что это существенно ограничивает скорость передачи информации при распределении квантового ключа.

1.2. Укрупнённая архитектура системы квантового распределения ключей

Комплекс для передачи конфиденциальной информации с квантовым распределением ключа. Программно-аппаратный комплекс для передачи конфиденциальной информации с системами синхронизации и КРК представлен на рис. 1.1.

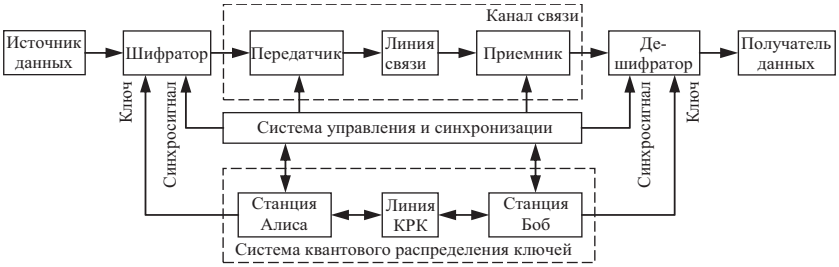

Рис. 1.1. Программно-аппаратный комплекс для передачи конфиденциальной информации с системами синхронизации и КРК

В приведенной схеме источник данных формирует цифровые сигналы, соответствующие определённому виду информации телекоммуникации (ГОСТ 22670-77). В шифраторе осуществляется криптографическая обработка (шифрование) параметров сигналов для защиты информации от несанкционированного доступа. Для дальнейшей передачи зашифрованных данных используется канал связи, представляющий совокупность технических средств (передатчика и приёмника) и линии связи (среды распространения). Канал связи формирует маршрут передачи данных от источника до получателя.

В симметричной криптосистеме отправитель и получатель данных используют один и тот же секретный ключ, который требует периодического обновления одновременно у отправителя и получателя. В комплексе (рис. 1.1) эту функцию выполняет система КРК, которая состоит из двух станций, названных Алиса (Alice) и Боб (Bob). Станции имеют управляющие входы для синхронизации работы и контроля параметров, и управления каналом связи.

Формирование секретных ключей происходит через линию связи, где передаются одиночные фотоны. В системах КРК применяют три вида кодирования квантовых состояний: поляризационное и фазовое кодирования, а также кодирование временными сдвигами. Линия КРК может представлять атмосферу или оптическое волокно (ОВ). Коммерческие системы КРК используют волоконно-оптическую линию связи.

Каждая из станций генерирует общий секретный ключ и распределяет его между законными пользователями. С помощью этого ключа производится как шифрование данных источника, так и дешифрование данных для получателя.

Система синхронизации обеспечивает синхронизацию разнесённых в пространстве оптического передатчика и оптического приёмника в канале связи, станций Алиса и Боб в системе КРК, а также шифратора и дешифратора. Точность прихода сигнала синхронизации колеблется в пределах десятков пикосекунд и сильно влияет на общие характеристики системы. Программное обеспечение системы управления и синхронизации формирует управляющие команды.

1.3. Коммерческие системы квантового распределения ключей

В мире существует четыре компании, которым удалось выйти на рынок с коммерческими системами КРК.

Одной из первых систему ID 500 Clavis начала предлагать компания IdQuantique (Щвейцария). Система состоит из двух станций, которыми управляют один или два компьютера. Программное обеспечение гарантирует квантовое распределение ключей в автоматическом режиме. Система поддерживает квантово-криптографические протоколы BB84 и SARG04. Формирование ключа возможно для квантовых каналов протяженностью до 100 км. Система использует встроенный протокол просеивания ключа, коррекции ошибок и усиления секретности. Заявленная производителем скорость формирования ключей составила до 1500 бит/с.

Позднее компанией IdQuantique выпущены усовершенствованные системы ID 3000 Clavis, ID 3100 Clavis2 и ID 5000 Vectis.

Компания MagiQ Technologies (США) предлагает системы QPN 5505 (2003), QPN 7505 (2005) и QPN 8505.

Компания SmartQuantum (Франция) предлагает линейку систем КРК. Отдельная система для распределения ключа носит название SQKeyGenerator (2005). Интегрированные системы называются SQBoxDefender и SQBoxFibreShield.

К трем компаниям, работающим на рынке систем КРК, в 2009 г. присоединилась компания Quintessenc Labs Pty Ltd (Австралия), предлагающая систему КРК для ВОЛС. Система располагается в стойке, которая легко вписывается в сетевую инфраструктуру.

В настоящее время коммерческие системы КРК в основном нацелены на правительственные организации и корпорации с повышенными

требованиями к безопасности. Однако уменьшение цены может сделать квантовую криптографию доступной для большого количества организаций в самое ближайшее время. Ожидается, что квантовая криптография может стать фактическим стандартом в межбанковской коммуникации уже через несколько лет.

1.4. Принципы квантового распределения ключей с фазовым кодированием состояний фотонов

Коммерческие системы КРК, производимые компаниями и работающие через ВОЛС, кодируют информацию о битах ключа в фазовых состояниях фотонов. Это связано с тем, что нестабильность поляризации сильно затрудняет применение поляризационного кодирования состояний фотона.

Рис. 1.2 иллюстрирует принцип фазового кодирования состояний фотона с помощью интерферометра.

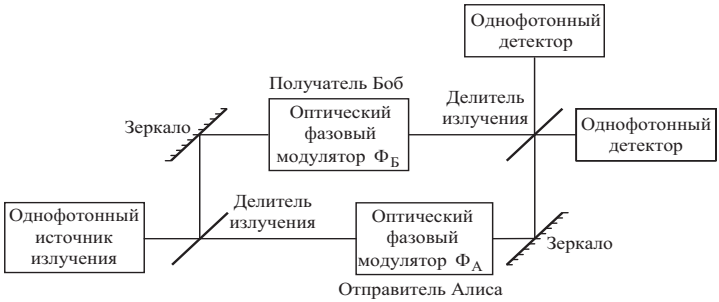

Рис. 1.2. Фазовое кодирование состояний фотона с помощью интерферометра

В протоколе BB84 приёмник и передатчик создают систему, базирующуюся на интерферометрах Маха–Цендера. Отправитель определяет углы фазового сдвига, соответствующие логическому нулю ($\Phi_A = 0$ или $\Phi_A = \pi/2$) и единице ($\Phi_A = \pi$ или $\Phi_A = 3\pi/2$). Приёмник задаёт фазовые сдвиги для эквивалента вертикального базиса $\Phi_Б = 0$ и эквивалента диагонального базиса $\Phi_Б = \pi/2$. В данном контексте изменение фазы на 2π с помощью оптического фазового модулятора соответствует изменению длины пути на одну длину волны используемого излучения.

Хотя фотоны ведут себя при фотодетектировании как частицы, они распространяются как волны.

Вероятность того, что фотон, посланный отправителем, будет принят получателем, равна

$$P_D = cos^2\left(\frac{\Phi_A - \Phi_Б}{2}\right).$$

Вероятность P_D определяется интерференцией волн, распространяющихся по верхнему и нижнему плечам интерферометра Маха–Цендера.

Вероятность регистрации будет меняться от единицы (при нулевой разности фаз) до нуля, при условии, что оптические фазовые модуляторы отправителя (Алиса) и получателя (Боб) используют фазовые сдвиги $\Phi_A = 0$ и $\Phi_Б = 3\pi/2$ для нулевых бит и $\Phi_A = \pi/2$ и $\Phi_Б = \pi$ для единичных бит.

Получение квантовых состояний и последующий их анализ производится с помощью интерферометра, который может быть реализован на одномодовых элементах волоконной оптики.

На рис. 1.3 показана волоконно-оптическая реализация интерферометра Маха–Цендера. Интерферометр состоит из направленного волоконно-оптического ответвителя (НВО) Y-типа, двух волоконно-оптических фазовых модуляторов (ВОФМ) и НВО X-типа. В каждое плечо интерферометра включено по одному ВОФМ. В интерферометр можно ввести однофотонное оптическое излучение и регистрировать фотоны на выходах 3 и 4 НВООХ-типа.

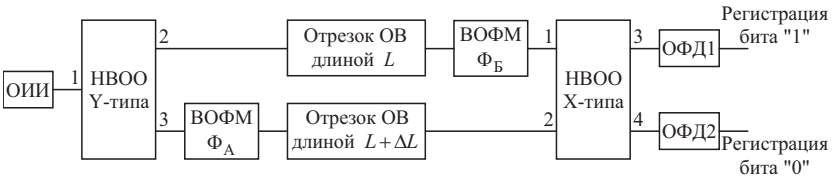

Рис. 1.3. Волоконно-оптическая реализация интерферометра Маха–Цендера

Волоконно-оптический фазовый модулятор выполнен на основе электрооптического кристалла ниобата лития. Принцип его действия основан на эффекте Керра. Модулятор позволяет внести фазовый сдвиг в сигнал.

Если длина когерентности однофотонного источника излучения (ОИИ) больше разности длин плеч интерферометра, то можно получить интерференционную картину.

СОДЕРЖАНИЕ