ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ
ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
МОСКОВСКИЙ ФИЗИКО-ТЕХНИЧЕСКИЙ ИНСТИТУТ
(национальный исследовательский университет)

На правах рукописи

Дуплинский Александр Валерьевич

Квантовое распределение ключа с высокочастотным поляризационным кодированием

Специальность 01.04.21-
«Лазерная физика»

Автореферат диссертации на соискание ученой степени
кандидата физико-математических наук

Научный руководитель:
к.ф.-м.н.
Курочкин Юрий Владимирович

Москва – 2019

Работа прошла апробацию на кафедре квантовой радиофизики Федерального государственного автономного образовательного учреждения высшего образования «Московский физико-технический институт (национальный исследовательский университет)».

Научный руководитель: Курочкин Юрий Владимирович, к.ф.-м.н.

Ведущая организация: Федеральное государственное автономное образовательное учреждение высшего образования «Санкт-Петербургский политехнический университет Петра Великого».

Защита состоится 23.12.2019 в 10:00 на заседании диссертационного совета ЛФИ.01.04.21.001 по адресу: 141701, Московская область, г. Долгопрудный, Институтский переулок, д. 9.

С диссертацией можно ознакомиться в библиотеке и на сайте Московского физико-технического института (национального исследовательского университета) https://mipt.ru/education/post-graduate/soiskateli-fiziko-matematicheskie-nauki.php.

Работа представлена «14» октября 2019 г. в Аттестационную комиссию федерального государственного автономного образовательного учреждения высшего образования «Московский физико-технический институт (национальный исследовательский университет)» для рассмотрения советом по защите диссертаций на соискание ученой степени кандидата наук, доктора наук в соответствии с п.3.1 ст. 4 Федерального закона «О науке и государственной научно-технической политике».

Общая характеристика работы

Работа посвящена квантовому распределению ключей - технологии, позволяющей двум удалённым пользователям генерировать общий криптографический ключ, секретность которого обеспечивается законами квантовой физики.

Актуальность

На сегодняшний день квантовая теория информации является одной из наиболее динамично развивающихся областей науки. Исследования в этом направлении носят как фундаментальный, так и прикладной характер и имеют огромную перспективу развития. В данный момент наиболее развитой с точки зрения практического применения частью квантовой теории информации является квантовая коммуникация и ее подраздел - квантовая криптография, которая в большинстве случаев сводится к квантовому распределению ключа [1].

Квантовое распределения ключа позволяет двум удаленным пользователям, при помощи фотонов, передаваемых по оптоволокну или открытому пространству генерировать закрытый ключ с уровнем секретности, не зависящим от вычислительных возможностей потенциального перехватчика.

Динамичное развитие квантовой криптографии, находящейся на пересечении квантовой оптики и теории информации, требует постоянного совершенствования систем для качественного увеличения параметров квантовой генерации ключей: предельной дальности, скорости и стабильности, а также миниатюризации устройств. Это требует исследований как протоколов, так и оптических схем.

Оптическая схема является основой квантового распределения ключей, позволяющей реализовать на практике заложенные в протоколе правила приготовления и измерения квантовых состояний фотонов. В первую очередь она должна максимально соответствовать модели секретности протокола, основанной на универсальных измерениях, а существующие неидеальности составных частей должны поддаваться количественной оценке, позволяющей учесть их влияние. Кроме того, для максимизации скорости генерации ключа оптическая схема

должна позволять реализовывать высокую частоту приготовления квантовых состояний (более 1 ГГц), а также иметь низкие потери на стороне приёмника. Стабильность и компактность устройства также во многом зависят от оптической схемы.

Цель

Цель работы заключалась в исследовании и разработке методов приготовления и измерения поляризационных состояний света с последующим их применением при создании безопасной системы квантового распределения ключа.

В рамках этой цели были поставлены задачи:

1. Разработать методику обобщающей оценки различимости состояний света, нацеленную на определение уровня секретности квантового распределения ключа.
2. Создать высокочастотную волоконно-оптическую схему поляризационного кодирования для квантового распределения ключа с пониженными потерями.
3. Обеспечить автономность работы системы в изменяющихся внешних условиях путём построения модели оптической схемы квантового распределения ключа.
4. Создать устройство квантового распределения ключа и провести испытания в условиях действующих телекоммуникационных оптоволоконных линий связи.

Научная новизна

Создана новая оптическая схема поляризационного кодирования для протокола BB84, тактовая частота в которой ограничена только полосой пропускания электрооптического фазового модулятора (до 40 ГГц). При этом схема может использоваться на различных частотах без необходимости внесения каких-либо изменений в оптоволоконную конфигурацию.

В отличие от классических схем поляризационного кодирования, авторская схема использует только один лазерный источник, минимизируя возможные уязвимости

в дополнительных степенях свободы. Передатчик в такой схеме может применяться как в системах с оптоволоконным каналом связи, так и в открытом пространстве.

Преимущество системы стабилизации поляризации в разработанной схеме по сравнению с аналогами заключается в том, что калибровка происходит без использования дополнительных устройств и компонент.

Активный выбор базиса на стороне приёмника позволяет использовать два однофотонных детектора вместо четырёх, в большинстве схем поляризационного кодирования, что упрощает и миниатюризирует систему, одновременно уменьшая вероятность темновых срабатываний на один такт. При этом потери на стороне приёмника минимальны (2-3дБ) в сравнении с другими схемами активного выбора базиса.

Впервые предложен и теоретически обоснован метод, позволяющий сделать обобщающую оценку на побочную различимость импульсов, потенциально создающую утечки информации о ключе.

Практическая значимость

Разработанный метод модуляции оптических состояний, может применяться для широкого класса оптических (в том числе квантово-оптических) экспериментов.

Разработанная оптическая схема кодирования легла в основу промышленного устройства квантового распределения ключа. Разработанные алгоритмы калибровки и стабилизации позволяют системе функционировать автономно, что в совокупности с надежностью схемы, позволяет использовать систему на реальных линиях связи.

Устройство на базе авторской оптической схемы было протестировано на телекоммуникационных оптоволоконных линиях, связывающих отделения банков и узлы операторов связи. Испытания включали в себя в том числе сопряжение с коммерческим шифровальным оборудованием.

Предложенный метод оценки пассивной утечки информации о ключе особенно актуален для количественной оценки надежности систем квантовой

передачи ключа по открытому пространству, использующих несколько лазерных источников.

Положения, выносимые на защиту

1) Разработка методики обобщающей оценки различимости световых импульсов, нацеленной на определение уровня секретности квантового распределения ключа.
2) Создание новой высокочастотной оптической схемы квантового распределения ключа с поляризационным кодированием и пониженными потерями.
3) Результаты моделирования оптической схемы квантового распределения ключа с целью обеспечения автономной работы системы в изменяющихся внешних условиях.
4) Результаты испытания системы квантового распределения ключа в условиях действующих телекоммуникационных сетей.

Апробация работы

Основные результаты диссертационной работы были представлены автором лично на международных конференциях:

1. А. Дуплинский, А. Канапин, А. Лосев, А. Соколов, Е. Киктенко, А. Федоров. Разработка промышленного устройства для квантового распределения ключа. Международная конференция-конкурс молодых физиков, ФИАН, 2-е место, Москва, Россия, 2016.
2. A. Duplinskiy, V. Ustimchik, Y. Kurochkin. One-way quantum key distribution scheme. 17th International Conference Laser Optics, St. Petersburg, Russia, 2016.
3. A. Duplinskiy, V. Ustimchik, A. Kanapin, Y. Kurochkin. Fast polarization QKD scheme based on $LiNbO_3$ phase modulators. The International Conference “Micro- and Nanoelectronics – 2016”, Zvenigorod, Moscow Region, Russia, 2016.

4. A. Duplinskiy, V. Ustimchik, A. Kanapin, Y. Kurochkin. Experimental quantum key distribution using polarization encoding with active measurement basis selection. 4th International School and Conference Saint-Petersburg OPEN, St. Petersburg, Russia, 2017.
5. A. Duplinskiy, V. Ustimchik, A. Kanapin, Y. Kurochkin. The influence of urban line imperfections on QKD process. 25th Central European Workshop on Quantum Optics, Palma, Spain, 2018.
6. A. Duplinskiy, E. Kiktenko, N. Pozhar, V. Kurochkin, A. Fedorov, Y. Kurochkin. Industrial QKD with polarization states. 8th International Conference on Quantum Cryptography, Shanghai, China, 2018.
7. A. Duplinskiy, D. Sych. Evaluation of decoy state distinguishability via Hong-Ou-Mandel interference. 5th International Conference on Quantum Technologies, Moscow, 2019.
8. A. Duplinskiy, D. Sych. Bounding source side channels via Hong-Ou-Mandel interference. 9th International Conference on Quantum Cryptography, Montreal, Canada, 2019.

Личный вклад

Все результаты, вошедшие в диссертацию, были получены лично автором, либо при его непосредственном участии.

Публикации

Основные результаты по теме диссертации изложены в 9 печатных изданиях, в том числе 4 в рецензируемых научных журналах, индексируемых Web of Science и Scopus и 4 – в трудах конференций, оформлен патент на изобретение.

Содержание работы

Во введении обосновывается актуальность темы диссертационного исследования, формулируются цели и задачи, описываются научная новизна и практическая значимость работы. Проводится анализ изученности темы в предшествовавших исследованиях, приводятся данные об апробации работы. Описывается структура работы.

Первая глава посвящена исследованию влияния различных степеней свободы света на раскрытие информации о ключе и методу оценки их вклада в падение скорости генерации ключа на основе интерференции второго порядка.

В пункте 1.1 описывается проблема различимости и текущие методы количественных оценок.

Протоколы квантового распределения ключа предполагают, что за пределами операционного пространства, которое используется для кодирования, сигналы абсолютно одинаковы и неразличимы. Однако это предположение часто нарушается на практике. В этом контексте наиболее уязвимым типом установки является система с несколькими лазерными источниками. Поляризационное кодирование широко используется для квантового распределения ключа в свободном пространстве, поскольку атмосфера вызывает незначительные помехи для состояния поляризации света. Самый простой способ реализовать поляризационное кодирование на гигагерцовых частотах для протокола BB84 - четыре разных лазера, по одному для каждого типа состояния. Некоторые установки требуют еще четыре лазера для генерации обманных состояний [10].

Физические отличия в работе различных лазерных источников, влекут за собой отличия в излучаемых импульсах [11].

В пункте 1.2 описана классическая схема эксперимента Хонга-У-Манделя для одиночных фотонов. Величина видности, получаемая в этом опыте позволяет судить о степени различимости волновых функций и чистоте состояний.

В пункте 1.3 исследуется интерференция второго порядка для слабых когерентных состояний с рандомизированной фазой, которые используются в подавляющим большинстве систем квантового распределения ключа. В отличие от

экспериментов Хонга-У-Манделя [13] с однофотонными состояниями, для когерентных состояний не возможен провал статистики совпадений до нуля, однако для слабых когерентных состояний со случайной фазой наблюдается аналог эффекта Хонга-У-Манделя с провалом статистики двойных кликов до уровня 50% при полном наложении друг на друга двух неразличимых импульсов с произвольными фазами [14]. Поскольку количество двойных кликов непосредственно зависит от степени неразличимости состояний, этот параметр является естественной мерой оценки степени совпадения в диапазоне чувствительности однофотонных детекторов (рис.1).

В данном разделе приводятся аналитические оценки, а также результаты численного моделирования зависимости видности интерференции второго порядка от степени несовпадения двух состояний.

В пункте 1.4 описана связь между видностью отдельных интерференционных экспериментов, описанных в пункте 3.2 и величиной разбалансировки базисов протокола BB84, связанной напрямую со степенью совпадения двух базисов.

В пункте 1.5 полученные ранее соотношения используются для симуляции скорости генерации секретного ключа в зависимости от потерь в линии и видности интерференции второго порядка, характеризующей различимость состояний. Приводятся графики, иллюстрирующие полученные зависимости.

Полученные результаты соотносятся с реальными экспериментальными данными, для того чтобы оценить применимость метода на практике. Тема интерференции Хонга-У-Манделя для двух слабых когерентных фазово-рандомизированных состояний от различных источников получила широкое распространение в последние годы в связи с необходимостью таких измерений в независящем от измерительного оборудования квантовом распределении ключа (MDI QKD). Благодаря проведённым исследованиям, достигнутые результаты видности вплотную подходят к теоретическому пределу: 0,5 [14]. Главная проблема, с которой сталкиваются такие эксперименты - квантовые флуктуации времени излучения в лазере. Типичные значения для полупроводниковых лазеров с распределенной обратной связью на длине волны 1550 нм составляют порядка 10

пс. При ширине оптического импульса в 100 пс, и отличном от нуля факторе Генри в полупроводниковом лазере, этот эффект заметно ухудшает видность интерференционной картины. В лучших на сегодняшний день экспериментах его уменьшение достигается за счет внешней оптической инжекции в лазер [14].

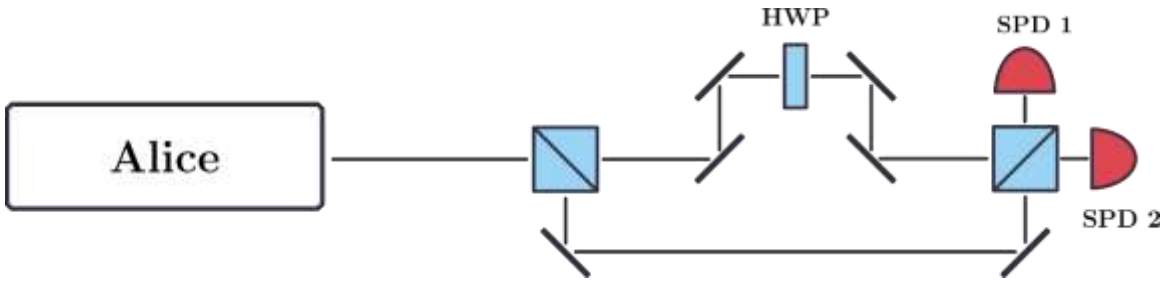

Рис. 1. Пример оптической схемы, необходимой для оценки различимости состояний при помощи интерференции второго порядка

Важно, что квантовые флуктуации времени излучения лазера ухудшают видность интерференции, но при этом не компрометируют систему, так как этот процесс носит истинно случайный характер и не увеличивает знание перехватчика о том, какой импульс был излучен. Таким образом предложенный метод ведет к переоценке степени различимости различных импульсов, а значит ухудшает скорость генерации ключа. Обсуждается возможность пост-селекции событий при измерении в определенном временном окне с целью выборки состояний с минимальным временным отклонением друг от друга, вызванным квантовыми флуктуациями в активной среде лазера.

Это позволяет заметно повысить прогноз на скорость генерации секретного ключа, тем самым позволяя сделать метод более прецизионным.

Вторая глава посвящена методам поляризационного кодирования в системах квантового распределения ключа. Рассмотрены классические схемы, применяемые на практике, исследуются их достоинства и недостатки. Акцент сделан на системах, использующих ячейки Поккельса.

Рассматривается возможность использования волоконного фазового модулятора на основе кристалла ниобата лития, в качестве ячейки Поккельса. Цель такого подхода – получить гигагерцовый активный переключатель поляризации с

низким (до 10 В) управляющим напряжением. Дополнительным преимуществом является стабильность и простота волоконных конфигураций. К сложностям этого метода можно отнести необходимость заведения излучения в модулятор в определенном состоянии поляризации, а также дисперсию поляризационных мод, возникающую в кристалле ниобата лития [5, 6].

В пункте 2.1 описаны наиболее распространенные методы модуляции состояний поляризации. Приведены основные характеристики различных конфигураций поляризационных контроллеров, а также ячеек Поккельса, в том числе в формате волоконно-оптического фазового модулятора.

В пункте 2.2 рассматривается действия модулятора на состояние поляризации проходящего излучения. Его можно проиллюстрировать унитарным преобразованием, описываемым матрицей Джонса. Устанавливается общий вид входных состояний поляризации, который позволяет обеспечить необходимый выходной набор для реализации квантового криптографического протокола BB84. В отличие от предшествующих работ [5, 6], акцент делается на возможности использования произвольных состояний поляризации, для которых выполняется условие равенства компонент поля вдоль обыкновенной и необыкновенной осей кристалла $LiNbO_3$, не ограничиваясь диагональным состоянием [7, 8].

Геометрическим местом точек, соответствующим таким состояниям поляризации является кольцо на сфере Пуанкаре, проходящее через диагональные и циркулярные состояния. Кроме того, на этой же окружности будут лежать любые состояния, получаемые на выходе из модулятора (рис.2).

В пункте 2.3 рассматриваются различные способы введения излучения в фазовый модулятор, позволяющие удовлетворить требованиям, описанным ранее. Так, наряду с использованием поляризационного контроллера, рассматривается возможность добавления в схему элементов объемной оптики или поворотных разъёмов. Важно, что такой подход позволяет применять стандартную конфигурацию модулятора, в которой оси поляризационно-поддерживающего волокна совмещены непосредственно с осями кристалла (поляризационная экстинкция около 20 дБ).

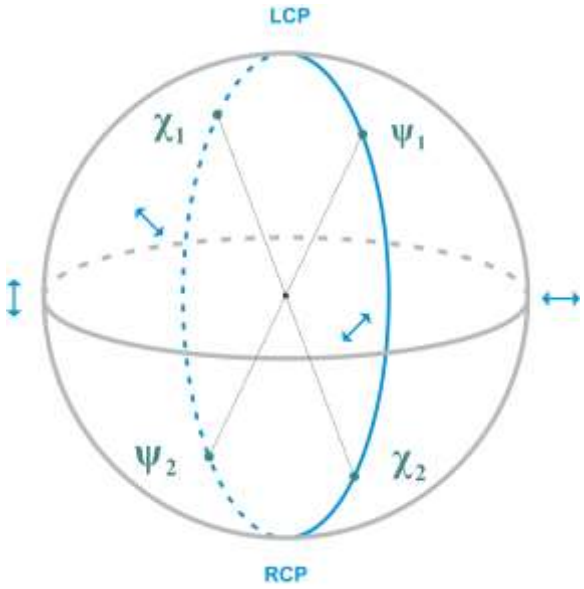

Рис. 2. Геометрическое место точек на сфере Пуанкаре, иллюстрирующее состояние поляризации импульсов на выходе из передатчика. В качестве примера точками отмечены 4 возможных состояния, используемые для протокола BB84.

В пункте 2.4 подробно рассматривается вопрос влияния дисперсии поляризационных мод, при прохождении фазового модулятора, на экстинкцию схемы.

Кристалл ниобата лития, используемый в фазовых модуляторах, имеет существенную разницу в показателях преломления для обыкновенной и необыкновенной осей. В результате, когда свет вводится в кристалл под углом к его осям, наблюдается существенное влияние дисперсии. Разница в оптических путях осей внутри модулятора составляет около 0,5 мм (менее 2 пс), поэтому для импульсов, длительностью более 1 нс, сама по себе поляризационная дисперсия не дает значительного ухудшения экстинкции. Однако прямая модуляция током полупроводникового лазерного диода, который используется для генерации импульсов, приводит к вариации фазы внутри одного импульса, то есть к так называемому, чирпированию этих импульсов. Этот эффект в сочетании со сдвигом между двумя ортогональными компонентами поляризации, вызванным дисперсией, приводит к значительному ухудшению степени поляризованности, так как состояние поляризации радикально изменяется внутри одного импульса. Это в свою очередь вызывает увеличение доли ошибок [5].

В работе изложен простой метод, позволяющий двум кристаллам, применяющимся в модуляторах схемы, компенсировать поляризационную дисперсию друг друга. Значительное снижение эффекта достигается при помощи того же поляризационного контроллера, который компенсирует преобразования поляризации в квантовом канале. Таким образом, решение не требует каких-либо физических изменений в схеме, что упрощает конструкцию и позволяет минимизировать потери на стороне приемника, что важно, для повышения скорости генерации ключа.

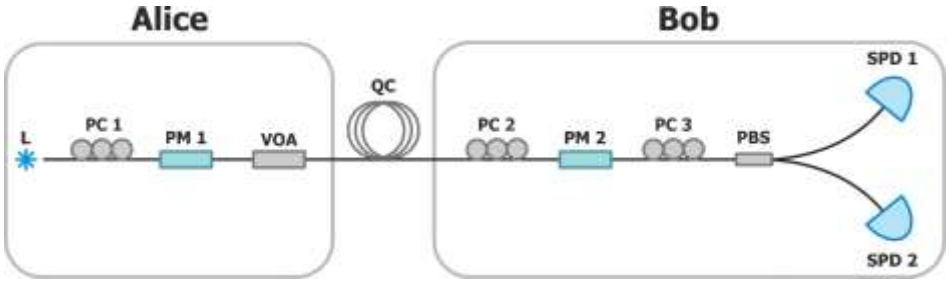

Рис. 3. Оптическая схема квантового распределения ключа для протокола BB84 с поляризационным кодированием. Лазерный источник (L) излучает поляризованные оптические импульсы на длине волны около 1550 нм. Контроллер поляризации (PC 1) преобразует состояние поляризации так, чтобы амплитуды вдоль осей кристалла фазового модулятора Алисы (PM 1) были равны друг другу. Это позволяет Алисе кодировать биты секретного ключа в состояниях поляризации с помощью модулятора. Для ослабления импульса используется переменный оптический аттенюатор (VOA). Интенсивность снижается до уровня калибровки или генерации ключа, в зависимости от режима работы. После квантового канала (QC) второй пьезо-управляемый контроллер поляризации (PC 2) компенсирует дрейф поляризации и вращает его так, что компоненты поляризации вдоль осей кристалла ниобата лития меняются местами, компенсируя двулучепреломление $LiNbO_3$. Модулятор Боба PM 2 используется для выбора базиса. Наконец, контроллер поляризации PC 3 преобразует состояние поляризации для поляризационного светоделителя (PBS) для различения состояний с помощью однофотонных детекторов (SPD1, SPD2). Для всех

элементов может применяться стандартное одномодовое волокно; однако в таком варианте схемы используются три поляризационных контроллера.

В пункте 2.5 представлены результаты эксперимента по проверке работоспособности предложенных методов кодирования в многофотонном режиме на оптическом столе. Было показано, что полученный уровень ошибки позволяет осуществлять квантовое распределение ключа.

В третьей главе рассматриваются вопросы автоматизации настройки и поддержания необходимых преобразований состояния поляризации в схеме. Для того, чтобы превратить лабораторную квантово-оптическую систему в устройство, способное надёжно функционировать на телекоммуникационных линиях связи, необходимо обеспечить автоматизированную настройку всех компонент системы и автономную непрерывную стабилизацию параметров, чувствительных к внешним условиям.

Для схем с поляризационным кодированием в оптоволокне наиболее нетривиально компенсировать все дрейфы преобразования поляризации в квантовом канале. Мониторинг преобразования поляризации в канале должен производиться непрерывно. В случае выхода наблюдаемых параметров за допустимый диапазон должна производиться повторная калибровка.

В пункте 3.1 описана постановка задачи калибровки для оптической схемы поляризационного кодирования. Сформулированы условия на состояния поляризации:

1) на входе в фазовый модулятор отправителя для кодирования состояния;

2) на входе в фазовый модулятор приёмника для выбора базиса;

3) на входе в поляризационный светоделитель для корректного измерения.

На основании этих условий сформулирована модель преобразования поляризации в терминах матриц Джонса, позволяющая как формализовать процедуру настройки, так и упростить некоторые участки схемы.

В пункте 3.2 представлена авторская оптическая схема квантового распределения ключа в рамках протокола BB84 с поляризационным кодированием. В основу схему заложены принципы, описанные ранее. На рис. 3 представлена вариация схемы с тремя поляризационными контроллерами.

Контроллеры поляризации PC 1 и PC 3 воздействуют только на оптоволокно внутри устройств передатчика и приёмника, поэтому их можно заменить пассивными оптическими компонентами и поддерживающим состояние поляризации волокном. Рассмотрены альтернативные конфигурации схемы, позволяющие сократить число активных элементов и значительно упростить процедуру настройки, описываются плюсы и минусы различных вариаций схемы.

В пункте 3.3 изложен принцип действия устройств и алгоритмов, позволяющих автоматически калибровать преобразование поляризации в системе при изменяющихся внешних условиях.

В качестве инструмента обратной связи используются пьезоэлектрические контроллеры поляризации. Калибровка выполняется автоматически. Входными данными для настройки является статистика счёта однофотонных детекторов. Чтобы увеличить количество срабатываний детектора и ускорить процесс, интенсивность света значительно увеличивается во время калибровки с помощью управляемого аттенюатора. Анализируя эти данные, программа корректирует напряжения контроллеров поляризации. В зависимости от номера поляризационного контроллера выбирается нужная конфигурация напряжений на фазовых модуляторах, позволяющая выделить нужный участок для настройки. На основании модели системы сформулированы параметры, минимизация которых соответствует настройки необходимых преобразований. Минимизация осуществляется последовательным градиентным спуском.

В четвёртой главе рассматриваются механизмы стабилизации и синхронизации системы квантового распределения ключа, необходимые для функционирования в составе устройства на телекоммуникационных линиях связи, а также результаты испытаний.

В пункте 4.1 описана система синхронизации, реализованная в схеме. Процедура синхронизации решает две задачи, необходимые для работы устройства:

1) выравнивание частот генераторов в устройствах приемника и передатчика;

2) синхронизация нумерации импульсов на обоих устройствах.

В качестве устройств синхронизации применяется пара синхролазер - синхродетектор, на приемнике и передатчике, соответственно (рис. 4). Лазер излучает последовательность импульсов длительностью каждый от 100 до 1600 пс в зависимости от длины линии. Классический детектор регистрирует данную последовательность и сравнивает полученный сигнал с частотой внутри своей платы, эффективно измеряя сдвиг фазы пришедших импульсов. Разработанный алгоритм синхронизации позволяет вырабатывать сигнал обратной связи в виде сдвига частоты на опорном генераторе на основе измеренного сдвига фаз.

В пункте 4.2 представлена модификация оптической схемы (рис. 3), позволяющая расширить возможности системы, дополнив протокол BB84 методом обманных состояний (decoy state) [9]. Для этого в систему добавляется высокоскоростной модулятор интенсивности на базе интерферометра Маха-Цанднера в кристалле ниобата лития. Особенностью этого устройства является нестабильность рабочей точки вследствие температурных эффектов и накопления заряда. Для корректировки рабочей точки в модуляторе предусмотрен низкочастотный электрический вход для подачи постоянного напряжения. Чтобы отследить отклонение характеристики, в схему добавлен измеритель оптической мощности с большим временем интегрирования (~1 секунды). Так как частота смены состояний на 8 порядков превосходит это время, доли всех типов импульсов достаточно усредняются и итоговое значение получается суммированием энергии импульсов каждого типа (сигнал, обманные) в пропорции частоты их использования. Можно подобрать значения напряжений так, чтобы смещение характеристики вызывало заметное отклонение интегральной интенсивности от целевого значения. Таким образом, сигнал обратной связи вырабатывается на основе показаний измерителя мощности и подается на низкочастотный вход

модулятора в виде постоянного смещения. Контроль и стабилизация характеристики модулятора достигается простыми средствами без необходимости измерения амплитуды каждого импульса в отдельности и дополнительных пауз в генерации ключа.

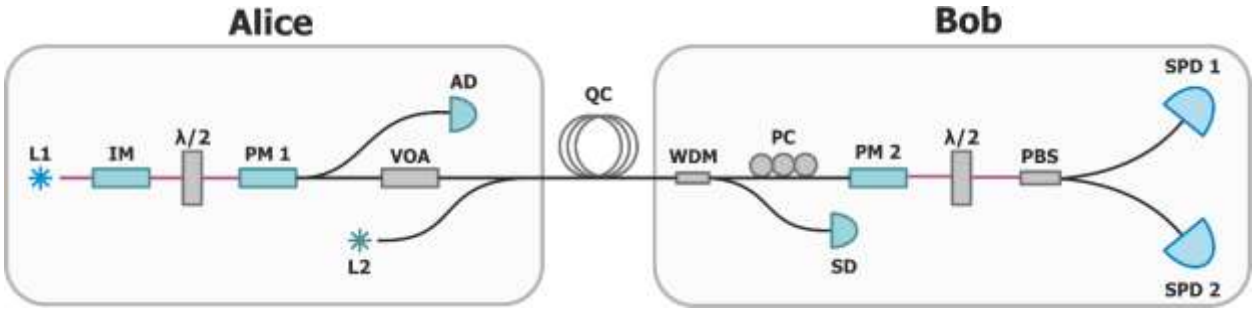

Рис. 4. Оптическая схема с добавлением модулятора интенсивности IM, анализируещего детектора AD, синхролазера L2 и синхродетектора SD.

В пункте 4.3 описано устройство квантового распределения ключа, построенное на базе изложенных ранее решений. Разработанное устройство значительно превосходит макетные образцы по целому ряду параметров. Так, частота приготовления квантовых состояний увеличена до 312,5 МГц, работа всех частей установки автоматизирована, добавлены модули, отвечающие за классическую пост-обработку сигнала.

В пункте 4.4 приводятся результаты испытаний установки. Наряду с лабораторными исследованиями установки КРК, созданные на базе авторской оптической схемы были успешно испытаны на телекоммуникационных оптоволоконных линиях связи. Макет установки, созданный для отработки алгоритмов компенсации поляризационных искажений, использовался для демонстрации сети квантового распределения ключа, состоящей из трёх узлов, на линиях связи, связывающих офисы банков. Другим связующим звеном сети являлась установка, использовавшая автокомпенсационную оптическую схему квантового распределения ключа с фазовым кодированием.

Следующие испытания схемы поляризационного кодирования проходили с макетом электроники для промышленного устройства. Были впервые испытаны

однофотонные детекторы собственного производства в условиях серверной комнаты. Соединение точка-точка было организовано между двумя офисами Сбербанка. Потери в оптоволоконном канале составили 14,05 дБ при длине 25 км (эквивалент 70 км стандартного волокна). Оптоволоконная линия связи состояла из 8 сваренных между собой сегментов.

Была использована версия оптической схемы с элементами объёмной оптики и полуволновыми пластинками, что позволило использовать упрощённую процедуру калибровки, однако потери на стороне Боба составили порядка 6 дБ. В схеме также использовались обманные состояния, сгенерированные при помощи модулятора интенсивности.

В заключении приводятся основные результаты работы:

1) Предложена новая методика, позволяющая дать обобщающую оценку различимости световых импульсов в побочных степенях свободы излучения, потенциально компрометирующих систему распределения ключа. Методика предполагает выполнение измерений с анализируемой системой по схеме опыта Хонга-У-Манделя. Использование получаемой оценки в модели секретности системы может гарантировать секретность генерации ключа для значений видности в схеме Хонга-У-Манделя вплоть до 0.47.
2) Создана новая оптическая схема квантового распределения ключа с поляризационным кодированием на основе волоконных фазовых модуляторов, отличающаяся от большинства схем поляризационного кодирования наличием только одного лазерного источника на стороне Алисы, а также только двух однофотонных детекторов на стороне Боба. По сравнению с ближайшими аналогами, реализующими активный выбор базиса в устройстве Боба, схема имеет низкие потери (2-3 дБ). Частота модуляции в предложенной схеме ограничена только полосой пропускания волоконного фазового модулятора, которая составляет более 40 ГГц.
3) Выполнено моделирование оптической схемы квантового распределения ключа на основе формализма матриц Джонса, позволившее разработать

механизмы обратной связи для настройки и поддержания необходимых преобразований состояния поляризации. Это обеспечило автономную работу системы в изменяющихся внешних условиях, без необходимости добавления в схему дополнительных элементов. Эмпирически измеренное среднее соотношение времени подстройки поляризации к времени генерации ключа составляет около 1:4.

4) С использованием реализованной оптической схемы квантового распределения ключа с поляризационным кодированием создано устройство, предназначенное работать со стандартными оптоволоконными линиями связи. Установка испытана в нескольких телекоммуникационных сетях между отделениями банков, в том числе в конфигурации квантовой сети и с подключением специализированного оборудования шифрования. Результирующая скорость генерации сырого ключа составила 2 кбит/с при потерях в линии более 14 дБ.

Публикации автора по теме диссертации

1. A. V. Duplinskiy, V. E. Ustimchik, Y. V. Kurochkin One-way quantum key distribution scheme // 2016 International Conference Laser Optics (LO). – IEEE, 2016. – C. R8-14-R8-14
2. Fast polarization QKD scheme based on $LiNbO_3$ phase modulators / A. Duplinskiy, V. Ustimchik, A. Kanapin, Y. Kurochkin // International Conference on Micro-and Nano-Electronics 2016. – International Society for Optics and Photonics, 2016. – Т. 10224. – С. 102242W.
3. Demonstration of a quantum key distribution network in urban fibre-optic communication lines / E. O. Kiktenko, N. O. Pozhar, A. V. Duplinskiy et al. // Quantum Electronics. – 2017. – Т. 47. – №. 9. – С. 798.
4. QKD using polarization encoding with active measurement basis selection / A. Duplinskiy, V. Ustimchik, A. Kanapin, Y. Kurochkin // Journal of Physics Conference Series. – 2017. – Т. 917. – №. 6.
5. Low loss QKD optical scheme for fast polarization encoding / A. Duplinskiy, V. Ustimchik, A. Kanapin et al. // Optics Express. – 2017. – Т. 25. – №. 23. – С. 28886-28897.
6. QKD optical scheme calibration system / A. Duplinskiy, V. Ustimchik, A. Kanapin et al. // Journal of Physics: Conference Series. – IOP Publishing, 2017. – Т. 936. – №. 1. – С. 012086.
7. Urban QKD test for phase and polarization encoding devices / A. Kanapin, A. Duplinskiy, A. Sokolov et al. // International Journal of Quantum Information. – 2017. – Т. 15. – №. 08. – С. 1740018.
8. Quantum-Secured Data Transmission in Urban Fiber-Optics Communication Lines / A. V. Duplinskiy, E. O. Kiktenko, N. O. Pozhar et al. // Journal of Russian Laser Research. – 2018. – Т. 39. – С. 113-119.
9. Пат. 15854298 США. High-speed autocompensation scheme of quantum key distribution / A. V. Duplinskiy, V. E. Ustimchik, Y. V. Kurochkin et al.

Список литературы

1. Quantum cryptography / N. Gisin, G. Ribordy, W. Tittel, H. Zbinden // Reviews of modern physics. – 2002. – Т. 74. – №. 1. – С. 145.
2. F. Xu, B. Qi, H. K. Lo Experimental demonstration of phase-remapping attack in a practical quantum key distribution system // New Journal of Physics. – 2010. – Т. 12. – №. 11. – С. 113026.
3. After-gate attack on a quantum cryptosystem / C. Wiechers, L. Lydersen, C. Wittmann et al. // New Journal of Physics. – 2011. – Т. 13. – №. 1. – С. 013043.
4. Full-field implementation of a perfect eavesdropper on a quantum cryptography system / I. Gerhardt, Q. Liu, A. Lamas-Linares et al. // Nature communications. – 2011. – Т. 2. – С. 349.
5. 100 MHz amplitude and polarization modulated optical source for free-space quantum key distribution at 850 nm / M. Jofre, A. Gardelein, G. Anzolin et al. //Journal of Lightwave Technology. – 2010. – Т. 28. – №. 17. – С. 2572-2578.
6. Proof-of-concept of real-world quantum key distribution with quantum frames / I. Lucio-Martinez, P. Chan, X. Mo et al. // New Journal of Physics. – 2009. – Т. 11. – №. 9. – С. 095001.
7. Fast polarization QKD scheme based on $LiNbO_3$ phase modulators / A. Duplinskiy, V. Ustimchik, A. Kanapin, Y. Kurochkin // International Conference on Micro-and Nano-Electronics 2016. – International Society for Optics and Photonics, 2016. – Т. 10224. – С. 102242W.
8. Low loss QKD optical scheme for fast polarization encoding / A. Duplinskiy, V. Ustimchik, A. Kanapin et al. // Optics Express. – 2017. – Т. 25. – №. 23. – С. 28886-28897.
9. Quantum-Secured Data Transmission in Urban Fiber-Optics Communication Lines / A. V. Duplinskiy, E. O. Kiktenko, N. O. Pozhar et al. // Journal of Russian Laser Research. – 2018. – Т. 39. – С. 113-119.
10. Decoy-state quantum key distribution with polarized photons over 200 km / Y. Liu, T. Y. Chen, J. Wang et al. // Optics express. – 2010. – Т. 18. – №. 8. – С. 8587-8594.

11. Free-space QKD system hacking by wavelength control using an external laser / MS Lee, MK Woo, J Jung et al. // Optics express. – 2017. – Т. 25. – №. 10. – С. 11124-11131.
12. Security of quantum key distribution with imperfect devices / D. Gottesman, H. K. Lo, N. Lutkenhaus, J. Preskill // International Symposium on Information Theory, 2004. ISIT 2004. Proceedings. – IEEE, 2004. – С. 136.
13. C. K. Hong, Z. Y. Ou, L. Mandel Measurement of subpicosecond time intervals between two photons by interference //Physical review letters. – 1987. – Т. 59. – №. 18. – С. 2044.
14. Near perfect mode overlap between independently seeded, gain-switched lasers / L. C. Comandar, M. Lucamarini, B. Fröhlich et al. //Optics express. – 2016. – Т. 24. – №. 16. – С. 17849-17859.