

На правах рукописи



Кравцов Константин Сергеевич

**Управление оптическими полями
для задач связи и защиты информации**

Специальность 01.04.21 — лазерная физика

АВТОРЕФЕРАТ
диссертации на соискание ученой степени
доктора физико-математических наук

Научный консультант:
д.ф.-м.н. Кулик С. П.

МОСКВА — 2022 г.

Работа выполнена на физическом факультете Московского государственного университета имени М.В. Ломоносова.

Научный консультант:

Кулик Сергей Павлович

доктор физико-математических наук, профессор, Центр квантовых технологий при физическом факультете Московского государственного университета имени М.В. Ломоносова, научный руководитель

Официальные оппоненты:

Калачёв Алексей Алексеевич

доктор физико-математических наук, профессор РАН, Федеральное государственное бюджетное учреждение науки «Федеральный исследовательский центр «Казанский научный центр Российской академии наук», директор

Бутов Олег Владиславович

доктор физико-математических наук, Федеральное государственное бюджетное учреждение науки «Институт радиотехники и электроники им. В.А. Котельникова Российской академии наук», заместитель директора по научной работе

Фельдман Эдуард Беньяминович

доктор физико-математических наук, профессор, Федеральное государственное бюджетное учреждение науки «Институт проблем химической физики Российской академии наук», главный научный сотрудник

Ведущая организация:

Федеральное государственное унитарное предприятие «Всероссийский научно-исследовательский институт автоматики им. Н.Л. Духова» (ФГУП «ВНИИА»).

Защита состоится [REDACTED] на заседании диссертационного совета Д 002.063.02 при Институте общей физики им. А. М. Прохорова РАН по адресу: г. Москва, ул. Вавилова, д. 38, корп. 1, конференц-зал.

С диссертацией можно ознакомиться в библиотеке и на сайте Института общей физики им. А. М. Прохорова РАН, <http://diss.gpi.ru>

Автореферат разослан «___» _____ 2022 г.

Ученый секретарь
диссертационного совета



Ушаков Александр Александрович

Общая характеристика работы

Актуальность темы исследования

Последняя четверть XX столетия и начало XXI являются эпохой становления и развития информационных технологий, которые за эти десятилетия из высокой науки и достижений ведущих университетов стали одним из фундаментов для дальнейшего развития цивилизации. Успех информационных технологий в первую очередь связан с двумя достижениями человечества: развитием электроники, которая способна обрабатывать информацию, и развитием технологий глобальной связи, за счет которой эта информация приобретает цену и смысл. Глобальная связь в мировом масштабе немыслима без представления информации в виде оптических сигналов. Именно разнообразию представления информации в виде фотонов, ее обработке и защите посвящена настоящая диссертационная работа.

Важность разработки фундаментально новых подходов к представлению, обработке, передаче и защите информации в виде оптических сигналов обусловлена широкими перспективами применения таких решений в будущих информационных технологиях. Подобно тому, как изобретение транзистора впоследствии привело к взрывному росту в области электронных вычислительных систем, появление новых оптических средств обработки, защиты и передачи информации обладает колоссальными перспективами развития.

Логика развития систем оптической связи однозначно свидетельствует о востребованности оптических информационных систем все более мелкого масштаба: с годами основной тренд развития смещается от магистральных оптических линий к локальным сетям и соединениям между модулями информационного оборудования. В настоящее время крайне актуальным выглядит развитие технологий оптических систем связи между вычислительными ядрами внутри процессоров и создание гибридных электронно-оптических чипов.

Развитие *квантовых* технологий также остро нуждается в переосмыслении оптических информационных технологий, являющихся основой для систем квантовой криптографии и линейно-оптических квантовых вычислений. Помимо квантовых вычислений, возможность использования оптики для решения традиционных прикладных вычислительных задач становится все более привлекательной и экономически обоснованной.

Естественным способом представления битов информации с помощью оптических сигналов является принцип телеграфа — либо лазер включен либо выключен, что соответствует передаваемым единицам и нулям. Однако, такой способ далеко не самый эффективный с точки зрения соотношения передаваемой информации и занятой частотной полосы канала. В начале эпохи оптической коммуникации казалось, что ресурс световода для передачи информации, то есть доступная частотная полоса, настолько велика, что исчерпать её полностью практически невозможно. Однако, с развитием доступных интернет-сервисов, возможно-

сти оптоволоконного канала связи перестали выглядеть как что-то бесконечное, и появились осязаемые ограничения, например, на число доступных частотных каналов. В результате, вопрос повышения эффективности модуляции стал одним из центральных направлений развития.

Необходимость развития таких вычислительно-сложных операций, как распознавание голоса и изображений, перевод текста с языка на язык и других аналогичных задач, привела к экспоненциальному росту технологий искусственного интеллекта и нейроморфной обработки сигналов, которая также в перспективе может быть реализована путем оптического представления информации.

Помимо обеспечения самого по себе обмена и обработки информации, важным вопросом является защита ее от прослушивания недоверенными лицами. Несмотря на принципиальную нерешаемость задачи достижения безусловной защиты в рамках классической физики, практически реализуемые методы защиты информации на физическом уровне остаются актуальными и востребованными.

Кроме классических технологий оптической связи, в XXI веке стали активно развиваться технологии квантовой связи. По сути, произошло качественное переосмысление возможностей квантового мира, иногда называемое второй квантовой революцией: одиночные квантовые объекты позволили качественно перешагнуть через границы дозволенного классической физикой. И если попытки создания квантовых вычислителей пока не позволяют решать сложные задачи, непосильные для современных вычислительных систем, то системы квантовой криптографии успешно решают задачу безусловной защиты информации.

Для решения многих практических задач требуется квантовое распределение ключей по открытому пространству — то есть буквально в пределах прямой видимости. Это позволяет организовать обмен секретными ключами с движущимися объектами, например, автомобилями, поездами и летательными аппаратами.

Бурный рост квантовой криптографии и тесное сотрудничество с промышленными компаниями для создания систем криптографической защиты информации на базе квантового распределения ключей, позволяют быстро пройти путь от идеи до промышленных образцов. Некоторые задачи квантовой метрологии также тесно связаны с квантовой криптографией. Так, томография квантовых состояний, то есть способ определения квантового состояния системы путем проведения измерений над многими ее копиями, необходима для контроля и отладки систем квантовой коммуникации. В квантовой механике томография — это единственный способ определения квантовых состояний, так как нахождение неизвестного квантового состояния лишь по одному экземпляру системы принципиально невозможно.

Степень разработанности темы исследования

В работе исследованы новые подходы к представлению информации в виде оптических сигналов, а также её обработке, передаче и защите. В каждой из глав поставлены конкретные исследовательские задачи и предложены законченные под-

ходы к их решению. В некоторых случаях предложенные методы могут быть расширены и усовершенствованы, что отдельно обсуждается в соответствующих разделах. Во многих случаях были разработаны экспериментальные демонстраторы работоспособности предложенных решений, которые на эксперименте доказывают состоятельность выбранных подходов.

Большинство исследованных задач представляют собой междисциплинарные темы на стыках оптики, квантовой физики, теории информации и прикладных интегрально-оптических технологий. Как известно, многие перспективные научные направления возникли именно на стыке разных тематик, так появилась квантовая криптография, квантовые вычисления, искусственный интеллект и другие активно развивающиеся направления. В настоящей работе в полной мере рассмотрены фундаментальные принципы представления информации в виде оптических полей, а также перспективные варианты ее обработки в таком виде.

Для задач связи был разработан подход, позволяющий выполнять необходимую операцию — дискретное преобразование Фурье — с помощью известного класса интегрально-оптических устройств. Для оптических интерконнектов на чипе — предложен новый класс устройств, которые с одной стороны просты в изготовлении, а с другой — позволяют реализовывать разнообразный функционал. Для задач защиты информации рассмотрено как фундаментальное решение, позволяющее организовать безусловно-защищенный обмен ключами — квантовое распределение ключей, — так и простое техническое решение для повышения защищенности передаваемой информации.

Таким образом, соединение подходов из разных дисциплин — это та задача, которая в полной мере была выполнена в рамках настоящей работы.

Цели и задачи диссертационной работы

Цель диссертационной работы состоит в разработке новых подходов к представлению информации в виде оптических сигналов, ее обработка, передача и защита, в том числе, развитие направления квантовой информации и методов квантового распределения ключей.

На пути к достижению поставленной цели были исследованы и решены следующие фундаментальные и прикладные задачи:

1. Разработка оптической платформы для модулирования сигналов в формате OFDM;
2. Разработка голографических методов управления оптическими полями в устройствах интегральной оптики;
3. Разработка сверхбыстрого оптического варианта нейроморфного вычислителя;
4. Поиск асимметричного метода для классического распределения условно секретных ключей;

5. Изучение турбулентных свойств оптических каналов связи по атмосфере для задач квантовой коммуникации с использованием пространственной степени свободы;
6. Поиск нового подхода к томографии пространственных квантовых состояний света, позволяющего проводить измерения быстрее, чем с помощью жидкокристаллических приборов;
7. Разработка простого и надежного устройства для генерации последовательности истинно случайных чисел;
8. Экспериментальная реализация релятивистского протокола квантовой криптографии;
9. Усовершенствование стандартного протокола квантовой криптографии BB84 с состояниями-ловушками с целью повысить защищенность базового протокола от ряда атак, включая измерения с определенным исходом.

Научная новизна

1. В работе впервые предложено универсальное полностью оптическое устройство для реализации прямого и обратного преобразования Фурье, на базе которого экспериментально продемонстрирована система связи с ортогональным частотным разделением OFDM.
2. Впервые предложена идея оптического нейроморфного устройства на базе полупроводникового оптического усилителя, позволяющая реализовать сверхбыстрые оптические нейронные сети, а также продемонстрирована его полноценная реализация.
3. Впервые разработана модель турбулентного канала по открытому пространству, позволяющая непосредственно предсказывать затухание для конкретных пространственных мод и амплитуды соответствующих перекрестных помех.
4. Впервые предложен и экспериментально продемонстрирован новый подход к томографии пространственных квантовых состояний света на базе микро-электромеханического деформируемого зеркала.
5. Впервые экспериментально реализован релятивистский протокол квантовой криптографии.
6. Впервые приведено доказательство и анализ секретности для протокола квантового распределения ключей на базе геометрически-однородных квантовых состояний света общего вида.

Научная новизна предложенных подходов подтверждена выходом публикаций про соответствующие достижения в профильных рецензируемых периодических изданиях в основном первого квартала. Все задачи, сформулированные в предыдущем пункте, были решены путем использования новых научных подходов.

Теоретическая и практическая значимость

Предложенные и изученные в работе подходы к представлению, обработке и защите информации в виде оптических сигналов имеют фундаментальное значение для развития оптических информационных технологий, чей серьезный рост имеет прямое влияние на различные сферы деятельности человека.

Теоретическая значимость работы заключается в развитии новых теоретических моделей, в первую очередь, для турбулентных оптических каналов связи по открытому пространству и для анализа секретности протокола квантовой криптографии на геометрически-однородных квантовых состояниях. Полезные теоретические модели разработаны также для планарных волноводных решеток, томографии пространственных квантовых состояний света и для экстракции случайных чисел из сырой случайной последовательности.

Помимо теоретической и фундаментальной значимости предложенных методов и подходов можно выделить следующие направления, которые представляют собой прямой практический интерес.

Для задач классической связи представляет интерес голографическая интегрально-оптическая платформа для создания оптических устройств на чипе, в том числе для решения задачи интерконнекта между вычислительными ядрами. Концепция, называемая цифровой планарной голографией, позволяет решать огромное количество задач управления оптическим полем, частично рассмотренных в настоящей работе.

Для задач квантовой коммуникации был предложен ряд новых подходов, которые находят применение в практических системах квантовой криптографии. Это в первую очередь квантовый генератор случайных чисел, обеспечивающий предельно простое и эффективное решение задачи экстракции случайных чисел. Идеи, развитые в настоящей работе, были впоследствии оптимизированы под кремниевые фотоумножители (SiPM) с большим количеством пикселей и используются в коммерческих устройствах квантовой криптографии.

Предложенный и разработанный протокол квантовой криптографии на геометрически однородных квантовых состояниях также внедряется в устройства квантовой криптографии. На конечной стадии практической реализации находятся две системы, использующие разработанный протокол.

Еще одной практически значимой задачей является исследование турбулентных свойств атмосферных линий связи. Несмотря на то, что в данный момент в мире есть лишь единичные демонстрации систем квантовой коммуникации, использующих пространственную степень свободы, дальнейшее развитие квантовых технологий может потребовать передавать многомерные квантовые состоя-

ния света через атмосферу. В этом случае понимание процесса передачи и полученные количественные соотношения позволяют прогнозировать перспективность атмосферных каналов связи для таких задач.

Методология и методы исследования

В работе используется широкий спектр научных методов, как теоретических, так и экспериментальных. Теоретическая часть применялась для нахождения ключевых зависимостей в разработанных физических моделях.

Для исследований планарных волноводных решеток, атмосферных каналов связи и анализа секретности протокола квантовой криптографии на геометрически-однородных квантовых состояниях света использовались аналитические методы, позволившие получить конечные выражения для искомым параметров. Такой подход наиболее наглядно позволил показать связь между различными конфигурационными характеристиками и искомым ответом, в связи с чем ему отдавалось предпочтение в теоретических исследованиях.

В случаях, когда аналитические методы оказывались неприменимыми или необоснованно сложными, использовалось численное моделирование, позволившее определить, например, статистические свойства атмосферных каналов связи в квадратичном приближении. Моделирование устройств на базе цифровой планарной голографии производилось путем многомерного численного интегрирования в специально разработанной программной среде.

Экспериментальная часть исследований осуществлялась на различных экспериментальных установках в лабораториях МГУ им. М. В. Ломоносова и Принстонского университета. В экспериментах использовались преимущественно оптические схемы на базе оптоволоконных компонентов. Подробно детали экспериментов и используемые методы представлены в соответствующих главах диссертации.

Сбор основных экспериментальных данных осуществлялся с помощью электронных средств, позволяющих переводить значения наблюдаемых параметров в цифровую форму. В некоторых установках полученные аналоговые сигналы оцифровывались в реальном времени, а обработка полученных данных проводилась позднее. Таким образом были выполнены исследования по классическому методу распределения ключей и исследования турбулентности в атмосферном канале связи. В других же установках, в первую очередь относящихся к квантовой генерации случайных чисел и квантовой криптографии, обработка проходила в реальном времени с помощью специализированной электроники на базе ПЛИС.

Положения, выносимые на защиту

1. Операции прямого и обратного дискретного преобразования Фурье могут быть реализованы с использованием планарных волноводных решеток. Данное решение принципиально важно для обработки оптических сигналов, в

частности, для систем передачи данных с модуляцией на ортогональных поднесущих (OFDM).

2. Скоростные уравнения для полупроводникового оптического усилителя соответствуют уравнениям для модели биологического нейрона типа «интегрировать-и-сработать» с утечками. Это позволило реализовать оптическую модель нейрона с субнаносекундным быстродействием.
3. Турбулентные искажения небольшой силы в атмосферных оптических каналах связи являются фазовыми искажениями, представимыми в виде ряда Тейлора по пространственным координатам, что позволяет получить аналитические выражения для коэффициентов пропускания и перекрестных помех пространственно-одномодовых каналов связи для возмущения первого порядка, а также относительно просто вычислить те же коэффициенты для возмущений второго и высших порядков.
4. Томография пространственных квантовых состояний света деформируемым зеркалом позволяет существенно (как минимум на порядок) повысить быстродействие метода по сравнению с традиционными жидкокристаллическими пространственными фазовыми модуляторами.
5. Релятивистский протокол квантовой криптографии может быть экспериментально реализован в однопроходной схеме с использованием постоянного лазера в качестве источника сигнала.
6. Протокол квантовой криптографии на геометрически-однородных квантовых состояниях с состояниями-ловушками обеспечивает безусловную секретность генерируемых ключей при использовании когерентных состояний в качестве носителей информации.

Достоверность полученных результатов и их апробация

Достоверность полученных результатов обеспечивается использованием современного научного оборудования, сопоставлением результатов теоретических предсказаний с полученными экспериментальными данными, созданием работоспособных экспериментальных демонстраций и устройств, а также успешным применением предложенных и разработанных принципов в более поздних экспериментальных исследованиях в том числе других научных коллективов.

Материалы, включенные в диссертацию, докладывались на семинарах Принстонского университета (США, Нью Джерси, г. Принстон, 2010), Физического факультета МГУ им. М.В. Ломоносова, ИОФ РАН, Массачусетского Технологического Института (США, Массачусетс, г. Кэмбридж, январь 2016), ИСАН (ноябрь 2018), университет Йоханеса Кеплера в Линце (Австрия, г. Линц, октябрь 2018), INRiM (Италия, г. Турин, декабрь 2019) а также в выступлениях на следующих конференциях: IEEE Photonics Society Avionics, Fiber Optics

and Photonics Technology Conference (AVFOP 2010, Denver, Colorado, 2010); 9th International Conference on Optical Communications and Networks (ICOCON 2010, Nanjing, China, 2010); ICO International Conference on Information Photonics (IP 2011, Ottawa, ON, 2011); IEEE Conference on Lasers and Electro-Optics (CLEO 2012, San Jose, California, 2012); 2nd International School on Surface Science - technologies and measurements on atomic scale (SSS-TMAS 2012, Khosta (Sochi), Russia, 2012); International Laser Physics Workshop (LPhys 2013, Prague, Czech Republic, 2013); 3rd international conference on quantum cryptography (QCrypt 2013, Waterloo, Canada, 2013); 3rd International School on Surface Science - technologies and measurements on atomic scale (SSS-TMAS 2013, Khosta (Sochi), Russia, 2013); 5th International Conference on Quantum Cryptography (QCrypt 2015, Tokyo, Japan, 2015); 26th International Laser Physics Workshop (LPhys 2017, Kazan, Russia, 2017); 7th International Conference on Quantum Cryptography (QCrypt 2017, Cambridge, UK, 2017); 1st Russian quantum technology school (QTS 2018, Rosa Khutor (Sochi), Russia, 2018); 27th International Laser Physics Workshop (LPhys 2018, Nottingham, UK, 2018); Quantum Photonics Technologies for Space (QTSPACE 2018, Bern, Switzerland, 2018); 9th International Conference on Quantum Cryptography (QCrypt 2019, Montreal, Canada, 2019); 18 Международная научная конференция-школа «материалы нано-, микро-, оптоэлектроники и волоконной оптики: физические свойства и применение (МНКШ 2020, Саранск / online, 2020); 4th International School on Quantum Technologies (QTS 2021, Voronovo, Moscow, Russia, 2021).

Публикации

По основному материалу диссертации опубликовано 20 статей в ведущих журналах, рекомендованных ВАК Российской Федерации, и зарегистрировано 5 патентов: четыре в США и один в Российской Федерации.

Структура и объем диссертации

Диссертация состоит из введения, шести глав, заключения и библиографии, а также списка использованных сокращений, списка опубликованных статей и списка зарегистрированных патентов. Общий объем диссертации 199 страниц включая 94 рисунка. Библиография включает 218 наименований на 17 страницах.

Содержание работы

Представление и передача информации в виде оптических сигналов — фундаментальная задача, решение которой примитивными методами известно уже давно. Однако, с повышением нагрузки на оптические сети передачи данных, такие вопросы, как модуляция оптических сигналов, позволяющая передавать больше бит информации в секунду в заданном частотном диапазоне, стали обладать крайней значимостью.

В первой Главе впервые предложены два новых решения для представления и передачи информации в виде оптических сигналов. Первое посвящено оптическим системам на ортогональных подчастотах OFDM, а именно, полностью оптической реализации дискретного преобразования Фурье, которое реализуется в определенном типе планарных волноводных решеток. Второе основано на технологии так называемой *цифровой планарной голографии* — интегрально-оптической технологии, позволяющей изготавливать широкий класс оптических приборов на чипе.

Оптическое мультиплексирование с ортогональным частотным разделением каналов (OFDM) обеспечивает многообещающее решение для будущей высокоскоростной передачи данных на большие расстояния [1, 2] из-за его прогрессивных и доказанных характеристик, таких как устойчивость к хроматической и поляризационной модовой дисперсии [2, 3] а также его высокая спектральная эффективность. Как и в традиционном беспроводном OFDM, основным принципом оптического OFDM является генерация аналоговых протяженных по времени символов, спектральные компоненты которых представляют собой несколько поднесущих, модулируемых независимыми потоками данных с относительно медленными скоростями. Все поднесущие попарно ортогональны и могут использовать разные форматы модуляции, такие как амплитудное включение-выключение, фазовая модуляция и квадратурная амплитудная модуляция (QAM). При этом поднесущие обладают достаточно большим перекрытием спектра, что обеспечивает высокую спектральную эффективность всей системы в целом. В приемнике информация с каждой поднесущей может быть извлечена без перекрестных помех из-за ортогональности поднесущих. Таким образом, оптический OFDM обеспечивает гибкую и эффективную платформу передачи для высокоскоростной оптической связи.

Процессы генерации и приема сигналов OFDM представляют собой, по сути, обратное дискретное преобразование Фурье (ОДПФ) в передатчике и дискретное преобразование Фурье (ДПФ) в приемнике, соответственно. Большинство современных систем реализуют оптический OFDM путем электронной цифровой обработки сигналов на основе ДПФ/ОДПФ. **В разделе 1.1** предложен полностью оптический метод вычисления дискретного преобразования Фурье на базе планарных волноводных решеток AWG. Типичная структура AWG показана на Рисунке 1(a). AWG состоит из входных и выходных волноводов, двух областей свободного распространения и массива волноводов между ними с постоянным шагом длины оптического пути между каналами, равным ΔL . Детальная схема области свободного распространения показана на Рисунке 1(b). Обычно две области свободного распространения идентичны между собой. В работе показано, что *циклическая AWG*, то есть такая, в которой произведение числа каналов на частотный шаг между каналами в точности равно свободному частотному диапазону, в определенные моменты времени выдает результат ДПФ/ОДПФ, что можно использовать в прикладных целях. На Рисунке 2 показана схема прохождения сигналов через циклическую AWG.

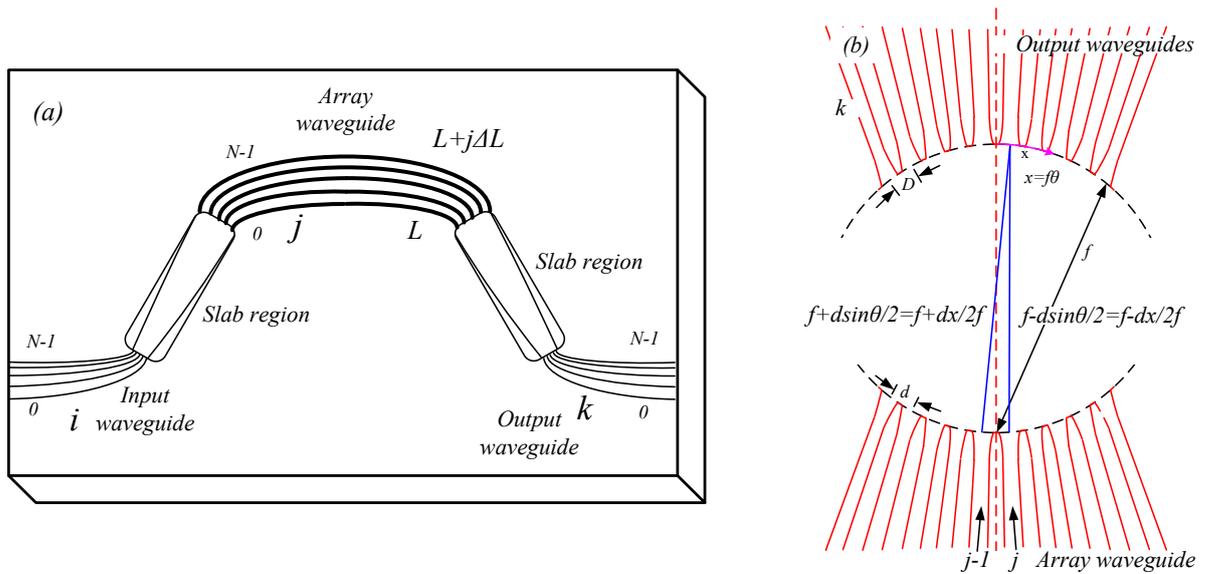


Рисунок 1: Структура планарной волноводной решетки: (а) структура полностью (b) увеличенная схема области свободного распространения (из работы [4].)

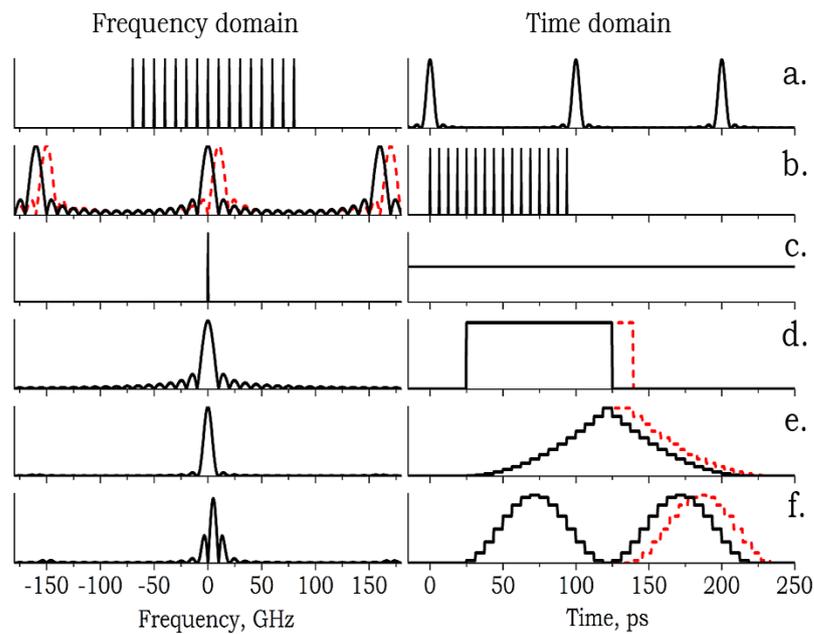


Рисунок 2: Временное и частотное представление сигналов в ключевых точках предлагаемой схемы OFDM: а. сигнал лазера; б. импульсный отклик для одного из каналов AWG; в. отфильтрованный сигнал лазера (поднесущая OFDM); д. окно модуляции; е. корректно декодированный сигнал; ф. некорректно декодированный сигнал (соседняя поднесущая). Красные пунктирные линии показывают соседний частотный канал AWG для спектрального представления и модуляцию на частоте $7/8$ от разности частот между поднесущими для временного представления. В частотном представлении показана амплитуда спектра $|f(\nu)|$, а во временном — интенсивность $|f(t)|^2$.

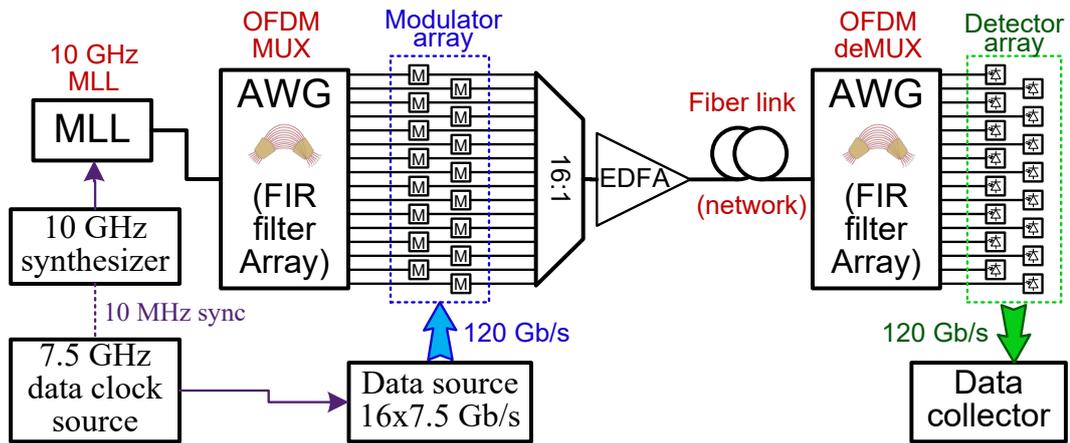


Рисунок 3: Предлагаемая экспериментальная установка для реализации 120 Гбит/с оптической линии связи на базе мультиплексирования OFDM с использованием AWG в качестве мультиплексоров-демультиплексоров.

Была предложена экспериментальная установка для демонстрации оптической линии связи на базе OFDM с пропускной способностью 16×7.5 Гбит/с = 120 Гбит/с, показанная на Рисунке 3. На практике была продемонстрирована урезанная версия такой системы, показавшая определенный потенциал использования AWG в качестве преобразователя ОДПФ.

Было продемонстрировано, что планарные волноводные решетки AWG могут полностью оптически выполнять функцию дискретного преобразования Фурье без всяких активных элементов. Это достигается при использовании именно циклической конфигурации AWG. Таким образом, AWG можно использовать для реализации полностью оптических систем OFDM, обеспечивающих высокую пропускную способность, прозрачную для модуляции. При таком подходе для реализации технологии OFDM могут быть использованы все предыдущие наработки по реализации устройств AWG. Простая волноводная структура AWG делает возможным их использование для ДПФ/ОДПФ с большим числом точек N . Выполненная экспериментальная демонстрация подтверждает состоятельность полностью оптической системы OFDM на базе AWG, и демонстрирует возможность достижения общей пропускной способности в 120 Гбит/с. Такая система может быть масштабирована до большого числа поднесущих, может быть сконфигурирована с использованием защитных интервалов между символами и обеспечивает гибкость в плане использования различной модуляции сигналов на разных поднесущих. Таким образом, продемонстрированная полностью оптическая система OFDM может быть перспективным решением для будущих оптических линий связи.

В разделе 1.2 рассмотрена так называемая „цифровая планарная голография“. Цифровая планарная голография — общее название технологии создания искусственно синтезированных голограмм, которые изготавливаются в планарном волноводе с помощью литографии. В отличие от традиционных аналоговых фазовых голограмм, модуляция показателя преломления в них не непрерывная, а бинар-

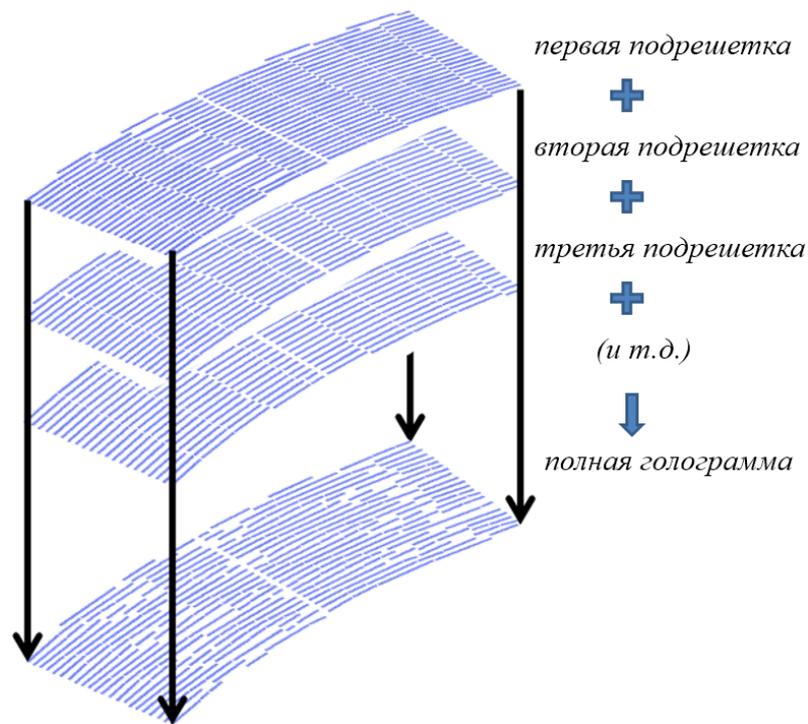


Рисунок 4: Синтез голограммы как суперпозиция разных подрешеток.

ная, откуда и название „цифровая“. Это позволяет изготавливать такие структуры с помощью одного цикла травления. Весь цикл производства таких устройств на базе кремниевых чипов воспроизводит упрощенную версию изготовления микросхем, а значит может быть масштабирован для производства дешевых чипов в больших количествах.

Фазовая голограмма — это по сути решетка изменения показателя преломления, обеспечивающая связь между произвольными волновыми фронтами. Более того, такая связь специфична для длины волны, по аналогии с Брэгговскими решетками в световодах или диэлектрическими спектральными фильтрами. В результате, с помощью планарной голограммы можно реализовать большое количество оптических приборов: начиная от разделения излучения по длинам волн и заканчивая перспективной платформой для реализации оптических интерконнектов на чипе.

Пример синтеза голограммы для реализации спектрометра высокого разрешения на чипе показан на Рисунке 4. Вся голограмма — это суперпозиция подрешеток, каждая из которых связывает два волновых фронта, входной и выходной, между собой. Чтобы реализовать спектрометр, делается по одной подрешетке для каждой длины волны. Каждая подрешетка по сути является фокусирующим распределенным зеркалом, которое фокусирует расходящийся планарный пучок из входного световода в соответствующую фокальную точку. Если точки фокусировки для разных длин волн разнести в пространстве, то разные длины волн будут фокусироваться в геометрически различных точках. Их можно совместить, например, с пикселями светочувствительной линейки, с помощью которой осуществляется прием и оцифровка полученных спектров.

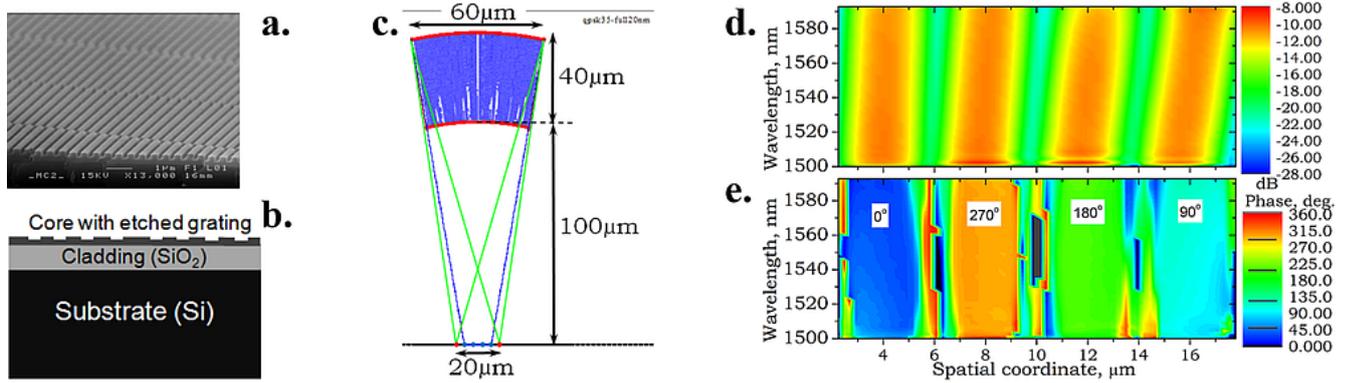


Рисунок 5: Голографический демодулятор QPSK. **a.** пример изготовленной голограммы; **b.** поперечная структура голограммы на базе платформы SOI; **c.** схема синтезированного дизайна и его размеры; **d.** зависимость интенсивности выходного сигнала от длины волны и координаты в выходной плоскости; **e.** выходная фаза в зависимости от длины волны и координаты.

В разделе предложен и смоделирован, например, демодулятор для квадратурной фазовой модуляции QPSK на базе данной технологии, который показан на Рисунке 5.

Кроме того, рассмотрены применения для так называемого „оптического интерконнекта“ на чипе — оптической подсистемы для обмена данными непосредственно внутри вычислительного чипа. Предложены и смоделированы компактные устройства для спектрального уплотнения каналов, оптические переключатели с чувствительностью к длине волны и некоторые другие устройства. Подобные голографические устройства обеспечивают эффективное повторное использование занимаемой площади на чипе, масштабируемы и устойчивы к производственным ошибкам. В силу данных свойств, цифровая планарная голография представляет собой перспективную платформу для оптических устройств на чипе.

Обработка информации, представленной в виде оптических сигналов, играет важнейшую роль наравне с уже рассмотренными задачами представления и передачи информации. Идея о полностью оптических вычислительных устройствах обсуждается уже не один десяток лет из-за того, что некоторые задачи, такие как умножение вектора на матрицу и, как частный случай, вычисление преобразования Фурье, могут быть решены оптической схемой „мгновенно“.

Во второй Главе предложен и разработан оптический метод обработки информации, основанный на нейроморфных вычислениях. Создан ключевой элемент такой системы обработки информации — оптическая импульсная модель биологического нейрона. Были экспериментально продемонстрированы два вида фотонных нейронов типа «интегрировать и сработать» с утечками. Поскольку уравнения для стандартной модели такого нейрона совпадают с уравнениями для динамики усиления в полупроводниковом оптическом усилителе (SOA), являющегося обрабатывающим ядром в его фотонной реализации, наблюдаемое экспериментально поведение предложенной модели корректно. Аналоговые свойства

продемонстрированного нейрона делают его хорошо подходящим для эффективной обработки сигналов, а его цифровые свойства позволяют выполнять сложные вычисления без накопления шума. Продемонстрированная петля обратной связи с нейроном имитирует поведение нейрона в протяженной оптической нейронной сети.

Раздел 2.1 является введением в данное направление исследований. Стандартная модель нейрона типа «интегрировать и сбросить» с утечками описывается следующими характеристиками (**раздел 2.2**) [5]:

1. В нейрон поступают N входных сигналов $\sigma_i(t)$, которые представляют собой наведенную проводимость во входных синапсах; у нейрона есть внутренний потенциал активации $V_m(t)$; нейрон формирует выходной сигнал $O(t)$. В состоянии покоя внутренний потенциал активации поддерживается на уровне V_{rest} .
2. Входные сигналы $\sigma_i(t)$ — это непрерывные временные последовательности, состоящие или из импульсов или из постоянных аналоговых сигналов.
3. Входным сигналам присваиваются веса w_i и они задерживаются на величину δ_i , в результате, получаются сигналы типа $w_i\sigma_i(t - \delta_i)$. Так как веса w_i могут быть как положительными, так и отрицательными, в нейроне могут быть реализованы как функции возбуждения, так и функции торможения.
4. Из полученных сигналов путем их сложения формируется общий эффективный входной сигнал $\sum_{i=1}^N w_i\sigma_i(t - \delta_i)$.
5. Внутренний потенциал активации $V_m(t)$ представляет собой экспоненциально взвешенный интеграл по времени от индуцированных входных токов, деленный на ёмкость нейрона, $V_m(t) = V_{\text{rest}} - \frac{1}{C_m} \int_{-\infty}^t I(t') e^{-\frac{t-t'}{\tau_m}} dt'$, где τ_m — постоянная времени интегрирования, $I(t) = C_m \sum_{i=1}^N w_i\sigma_i(t + \delta_i)$ — электрический ток, индуцированный общим входным сигналом, а C_m — ёмкость нейрона.
6. В момент когда значение проинтегрированного по времени сигнала опускается ниже порога, нейрон испускает выходной импульс $O(t) = 1$ если $|V_m(t)| < |V_{\text{thresh}}|$.
7. После испускания импульса у нейрона есть небольшой промежуток времени, так называемый рефрактерный период, в течение которого никакие другие импульсы не могут быть испущены: если $O(t) = 1$ то $O(t - \Delta t) = 0$, $\Delta t \leq T_{\text{refract}}$.
8. Выход нейрона состоит из последовательности импульсов с непрерывным временем

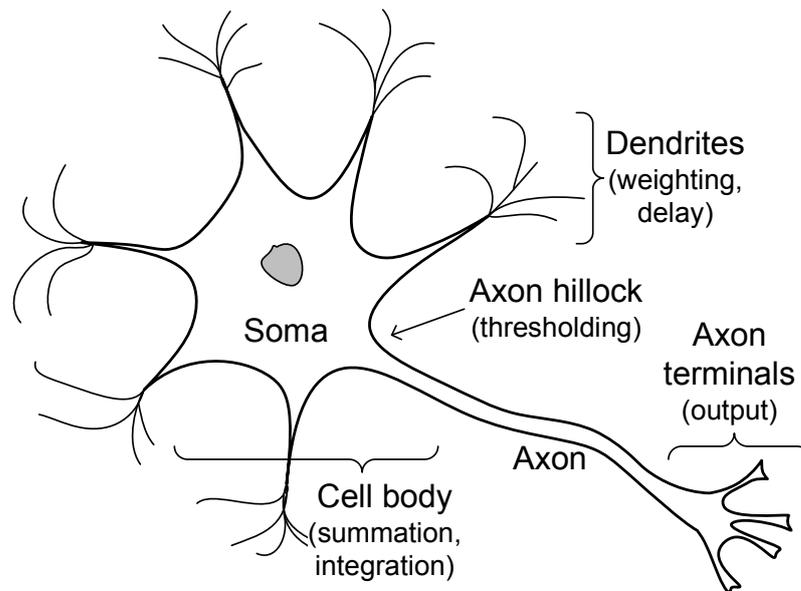


Рисунок 6: Схематическое изображение биологического нейрона.

Таким образом, параметрами, определяющими поведение устройства являются: w_i , δ_i , V_{thresh} , V_{rest} , T_{refract} , и постоянная времени интегрирования τ_m .

Представленная модель основана на исследованиях морфологии и физиологии биологических нейронов. Типичная упрощенная картинка нейрона схематически показана на Рисунке 6. Он состоит из дерева дендритов, которое представляет собой набор входов, собирающих, взвешивающих и задерживающих сигналы от других нейронов; сома, где все входные сигналы объединяются и интегрируются по времени; и аксон, в котором формируются выходные импульсы или потенциалы действия при условии, что совокупный входной сигнал превышает пороговое значение.

Динамика электрического потенциала нейрона типа «интегрировать и сработать» с утечками описывается уравнением (1.1). В качестве первичной переменной, определяющей его внутреннее состояние, выступает мембранный потенциал V_m , то есть напряжение между телом нейрона и внешней средой. Электрические свойства сомы, окруженной мембраной, можно смоделировать как RC цепь, где R связано с сопротивлением мембраны, а C — с емкостью, вызванной наличием мембраны. То есть сома, по сути, представляет собой фильтр низких частот первого порядка или, другими словами, интегратор с утечками, характеризующийся постоянной времени $\tau_m = R_m C_m$. Ток утечки через R_m уменьшает напряжение на мембране V_m до 0, но активный ток накачки мембраны противодействует ему и поддерживает напряжение покоя мембраны на уровне $V_m = V_{\text{rest}}$.

Потенциал	Активная накачка	Утечка	Входной сигнал	
$\frac{dV_m(t)}{dt}$	$\frac{V_{rest}}{\tau_m}$	$-\frac{V_m(t)}{\tau_m}$	$-\frac{1}{C_m}V_m(t)\sigma(t)$	(1.1)

$\frac{dN'(t)}{dt}$	$\frac{N'_{rest}}{\tau_e}$	$-\frac{N'(t)}{\tau_e}$	$-\frac{\Gamma a}{E_p}N'(t)I(t)$	(1.2)
---------------------	----------------------------	-------------------------	----------------------------------	-------

Точно так же динамика усиления короткого SOA регулируется уравнением (1.2) [6]. Его внутренняя переменная состояния — это плотность носителей выше уровня просветления $N'(t) = N(t) - N_0$, где $N(t)$ — фактическая плотность носителей, а N_0 — плотность носителей для достижения полного просветления. Опять же, существует три фактора, способствующих изменению $N'(t)$: пассивная утечка из-за спонтанного излучения света, приводящая к распаду носителей заряда; активная накачка, обеспечиваемая управляющим током SOA; и стимулированное излучение света вызванное излучением на входе нейрона, которое также „разряжает“ нейрон, уменьшая его переменную состояния $N'(t)$. Примечательно, что электрическая модель мембранного напряжения практически идентична оптической модели концентрации носителей в SOA. Константа интегрирования фотонного нейрона, τ_e , равна времени жизни носителей, в то время как слагаемое, соответствующее стимулированному излучению, зависит от полной интенсивности входного сигнала $I(t)$, коэффициента локализованности моды Γ , дифференциального коэффициента усиления a и энергии фотона E_p .

Разделы 2.3 и 2.4 посвящены экспериментальной реализации оптической модели нейрона. В то время как биологические нейроны работают с характерными временами не менее миллисекунд, экспериментально продемонстрированная оптическая модель нейрона работает с импульсами пикосекундной ширины и имеет постоянную времени интегрирования порядка 100 пс, что по крайней мере в 10^8 раз быстрее. Реконфигурация параметров устройства потенциально позволяет ему выполнять широкий спектр операций по обработке сигналов и формированию решений на основании входной информации.

Для использования в нейроне согласно представленной концепции, SOA работает в режиме кросс-модуляции усиления, его выход всегда инвертируется по отношению к его входу. Выполнение двух последовательных инверсий может восстановить исходный сигнал, сохранив все остальные свойства такими же. Таким образом получается «симметричная» модель нейрона. На Рисунке 7 схематично показан такой симметричный нейрон с возбуждающими и тормозящими входами.

В разделе 2.5 экспериментально демонстрируется режим работы оптического нейрона с обратной связью, что принципиально подтверждает возможность использования длинных цепочек из подобных оптических устройств без существенного накопления шума.

На базе предложенного решения в будущем возможно создавать более сложные устройства, имитирующие нейронные сети и позволяющие производить

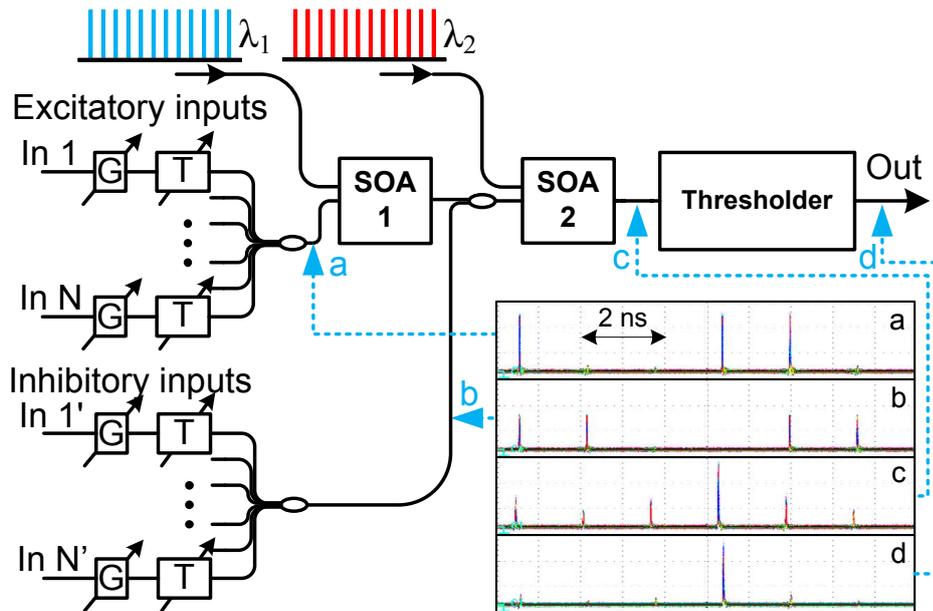


Рисунок 7: Схема симметричного фотонного нейрона с возбуждающими и тормозящими входами. Установка состоит из двух идентичных этапов интегрирования в SOA с соответствующими пассивными входными цепями и одного порогового элемента. G — переменное усиление/ослабление; T — переменная линия задержки. На вставке показан пример распространения сигнала через нейрон. Каждая диаграмма соответствует определенной точке в установке: **a** и **b** — возбуждающие и тормозящие входы соответственно, **c** — выходной сигнал после второго этапа интегрирования, **d** — выход нейрона, то есть сигнал **c**, прошедший через пороговый элемент.

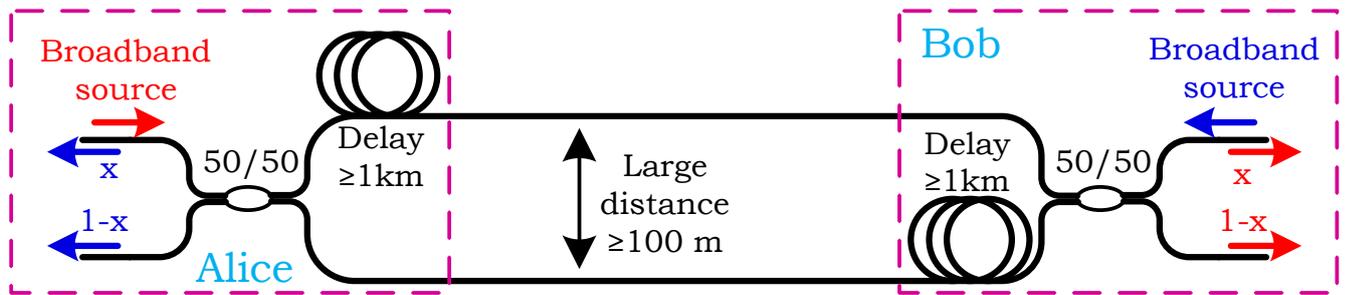


Рисунок 8: Система распределения условно-секретных ключей на базе протяженного интерферометра типа Маха-Цандера с добавленными линиями задержки, а также с физически разнесенными плечами интерферометра.

сверхбыструю обработку сигналов. Многие элементы представленной архитектуры могут быть выполнены в интегральном исполнении, таким образом существенно уменьшая геометрические размеры устройства. После этих пионерских исследований были созданы более совершенные и компактные реализации оптических нейронов, основанных на все том же принципе — сходстве скоростных уравнений для лазерной среды и уравнений, описывающих потоки зарядов в биологических нейронах.

Третьей ключевой задачей оптических информационных систем является обеспечение защиты информации от несанкционированного доступа. Наиболее перспективным способом защиты информации является ее шифрование симметричными шифрами, которые требуют предварительного защищенного распределения ключей шифрования.

В третьей Главе предложен и экспериментально продемонстрирован метод распределения секретных ключей, основанный на физических свойствах волоконно-оптических линий связи. **В разделе 3.1** показано, что в отличие от большинства других подходов к обеспечению безопасности в волоконно-оптических сетях на физическом уровне, наш метод не требует какой-либо предварительной секретной информации и работает в предположении, что злоумышленник имеет исчерпывающие знания о системе. Защищенность ключей основана на практической невозможности измерения оптической разности фаз между двумя некогерентными широкополосными оптическими сигналами.

Случайные флуктуации оптической фазы в волоконно-оптических линиях исследованы в **разделе 3.2**.

Продemonстрированный метод распределения ключей использует крупномасштабный интерферометр Маха-Цандера, покрывающий все расстояние между взаимодействующими сторонами. Предлагаемая в **разделе 3.3** схема такого интерферометра показана на Рисунке 8. Случайные изменения оптической фазы в плечах интерферометра вызывают коррелированные флуктуации интенсивности, которые, в свою очередь, наблюдаются сторонами. Секретный ключ формируется из получаемых флуктуаций интенсивности, которые одинаковы на обоих выходах интерферометра. Одним из необходимых требований для обеспечения безопасно-

го распределения ключей с помощью этого метода является наличие аутентифицированного классического канала связи между пользователями. Это позволяет избежать атаки типа «человек посередине».

Представленная в **разделе 3.4** лабораторная демонстрация, количественно очень похожая на коммерчески установленные линии связи, показала скорость генерации ключей 160 бит/с на линии длиной 26 км со средней долей битовых ошибок менее 4%. Ожидается, что использование более эффективных алгоритмов экстракции приведет к более высокой скорости генерации ключей. В целом, как скорость генерации ключей, так и максимальная дальность распределения ключей сопоставимы с характеристиками коммерческих систем квантового распределения ключей. Более того, использование двунаправленных эрбиевых оптических усилителей может помочь существенно превзойти квантовое распределение ключей с точки зрения дальности распределения ключей.

Наравне с уже рассмотренными классическими оптическими решениями для представления информации в виде оптических сигналов, её обработки, передачи и защиты, интерес представляет более наукоемкая и технически продвинутая область *квантовых* коммуникаций. Перед тем как обратиться к методам квантового распределения ключей, будут исследованы вопросы передачи (квантовых) оптических сигналов по открытому пространству и вопросы измерения квантовых состояний света — квантовой томографии.

Здесь следует отметить, что передача оптических сигналов по одномодовым световодам, как это делается в классических коммуникациях, сужает доступные степени свободы фотона до следующих трех: временного (в т.ч. фазового), частотного и поляризационного распределений сигнала. Поляризация является очень удобной степенью свободы, однако, она соответствует лишь двумерному гильбертову пространству. Остальные две степени свободы непрерывные. Использование же линий связи по открытому пространству позволяет еще в полной мере использовать пространственную степень свободы. В частном случае, можно рассмотреть конечный набор поперечных мод, соответствующий гильбертову пространству произвольной размерности. Это потенциально позволяет улучшить свойства квантового распределения ключей и передавать многомерные квантовые состояния света. Следующие две главы посвящены изучению такого подхода с каналами связи по открытому пространству.

В четвертой Главе изучены ключевые инструменты, как экспериментальные, так и теоретические, необходимые для работы с турбулентными каналами связи, в частности, для понимания процесса передачи пространственных квантовых состояний через турбулентную среду. **В разделе 4.1** разработана и реализована турбулентная камера с контролируемыми параметрами турбулентности, были проведены экспериментальные измерения ее основных параметров. **В разделе 4.2** разработано необходимое теоретическое описание каналов связи для передачи пространственных квантовых состояний, которое показало хорошее качественное сходство с результатами прямых измерений.

Турбулентные явления в атмосфере были впервые описаны Колмогоровым [7]

в 1941 году, когда он предсказал масштабирование структурной функции, пропорциональное $r^{2/3}$. Поскольку мы имеем дело с интегральным влиянием турбулентности на весь канал связи и не интересуемся локальными турбулентными свойствами атмосферы, будет использоваться хорошо известный результат для протяженного атмосферного канала и модель фон Кармана, которая предсказывает следующий спектр мощности фазовых флуктуаций [8, 9]

$$W_\varphi(f) = \vartheta r_0^{-5/3} (f^2 + L_0^{-2})^{-11/6} \exp(-l_0^2 f^2), \quad (2)$$

где

$$\vartheta = \frac{2\sqrt{2}\Gamma^2(11/6)}{\pi^{11/3}} \left[\frac{3}{5}\Gamma(6/5) \right]^{5/6} \approx 0.0229. \quad (3)$$

Это выражение показывает спектральную плотность флуктуаций оптической фазы φ в зависимости от пространственной частоты f . Модель фон Кармана представляет собой эмпирическую экстраполяцию результатов Колмогорова для всего диапазона пространственных частот, поскольку исходная теория была применима только для диапазона частот между внутренним масштабом l_0 и внешним масштабом L_0 . Параметр r_0 — это параметр турбулентности Фрида, который показывает, насколько сильна турбулентность. Можно считать, что это приблизительно диаметр телескопа, дифракционный предел которого равен пределу разрешения, вызванному турбулентностью [9].

В работе предложено рассматривать получаемые фазовые искажения как ряд Тейлора, при этом наиболее сильные фазовые искажения соответствуют минимальным степеням членов ряда.

$$\varphi(x, y) = \varphi_0 + ax + by + g\frac{x^2}{2} + h\frac{y^2}{2} + sxy + \dots, \quad (4)$$

где a и b — возмущения первого порядка, а g , h , и s — второго. Их можно найти как

$$\begin{aligned} a &= \frac{\partial \varphi}{\partial x} & b &= \frac{\partial \varphi}{\partial y} \\ g &= \frac{\partial^2 \varphi}{\partial x^2} & h &= \frac{\partial^2 \varphi}{\partial y^2} & s &= \frac{\partial^2 \varphi}{\partial x \partial y}. \end{aligned} \quad (5)$$

Поскольку фазовое искажение — это случайная функция, в силу очевидной симметрии задачи все упомянутые параметры возмущения являются случайными переменными с нулевым средним.

Показано, что в рамках линейного приближения модовое распределение мощности при возбуждении канала фундаментальной модой на передающей стороне описывается аналитически как

$$\begin{aligned} T_0 &= T_{00 \rightarrow 00} = e^{-\xi} \\ T_1 &= T_{00 \rightarrow 10,01} = \xi e^{-\xi} \\ T_2 &= T_{00 \rightarrow 20,11,02} = \frac{\xi^2}{2} e^{-\xi} \\ T_3 &= T_{00 \rightarrow 30,21,12,03} = \frac{\xi^3}{6} e^{-\xi} \\ T_N &= T_{00 \rightarrow mn:m+n=N} = \frac{\xi^N}{N!} e^{-\xi}, \end{aligned} \quad (6)$$

где нижние индексы соответствуют номерам мод Эрмита-Гаусса. Легко можно видеть, что полная мощность сохраняется, так как полученный ряд суммируется в единицу. В этих обозначениях $\xi = \frac{w^2}{4}(a^2 + b^2)$ — безразмерный параметр возмущения. Он имеет распределение

$$p(\xi) = \frac{2}{w^2 C_a} \exp\left(-\frac{2\xi}{w^2 C_a}\right), \quad (7)$$

где w — ширина Гауссова пучка, а C_a — параметр, зависящий от силы турбулентности.

Также получено решение для такого практического параметра канала как коэффициент пропускания для фундаментальной моды. Плотность вероятности для коэффициента пропускания задается выражением

$$p(T) = \frac{2}{w^2 C_a} T^{w^2 C_a - 1}. \quad (8)$$

Видно, что в первом приближении полученная плотность вероятности является степенной функцией коэффициента пропускания T , и следовательно чем выше турбулентность, тем меньше ожидаемая мощность. Для сравнения прогнозируемых плотностей вероятности с экспериментом мы провели серию измерений с одномодовым оптическим каналом, проходящим через турбулентную камеру, описанную выше. Измеренные распределения вероятностей вместе с подобранными теоретическими предсказаниями показаны на Рисунке 9. Эксперимент и теория хорошо согласуются, за исключением высоких значений коэффициента пропускания, когда приближение первого порядка не работает из-за фазовых искажений более высоких порядков.

Представление квантовой информации в виде оптических сигналов и её передача требует наличия соответствующих метрологических инструментов, которые в квантовом случае принципиально отличаются от классических решений. Известно, что измерение неизвестного квантового состояния по единственному экземпляру квантовой системы принципиально невозможно. Также невозможно создание копии неизвестного квантового состояния. Метод измерения квантового состояния по ансамблю квантовых систем в идентичных квантовых состояниях называется квантовой томографией или томографией квантовых состояний.

Томография квантовых состояний — важный экспериментальный инструмент для тестирования устройств, относящихся к квантовым технологиям. Поперечные пространственные квантовые состояния света играют ключевую роль во многих экспериментах в области квантовой информации, а также в оптических коммуникациях по открытому пространству.

В пятой Главе продемонстрировано использование деформируемого зеркала для томографии пространственных квантовых состояний света. В проведенных экспериментах продемонстрирована квантовая томография в четырехмерном гильбертовом пространстве путем проведения измерений во взаимно несмещенных базисах. Достигнуто среднее значение меры соответствия (fidelity), равное

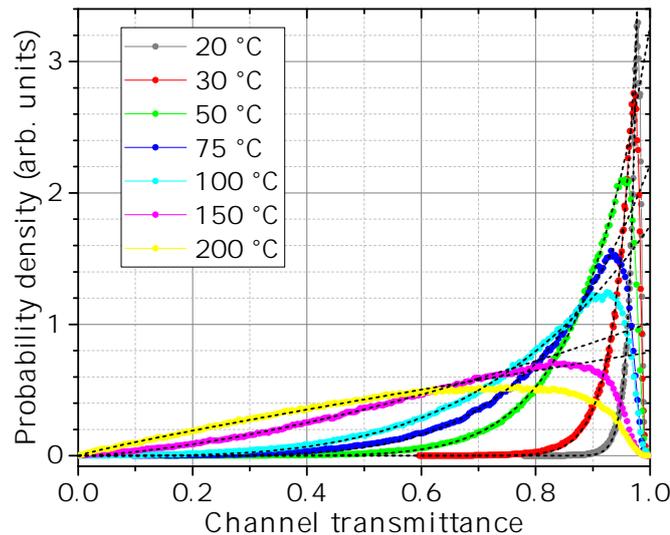


Рисунок 9: Распределение плотности вероятности для коэффициента пропускания канала, измеренного экспериментально, и теоретические предсказания в первом порядке теории возмущения (черные пунктирные линии). Экспериментальным параметром, определяющим силу турбулентности, является разница температур воздушных потоков, указанная в легенде. Обратите внимание, что для лучшего представления данных, распределения вероятностей не отнормированы должным образом.

0.95. Предложенный новый подход позволяет выполнять томографию на порядки быстрее и с меньшими потерями излучения, чем при традиционном подходе на основе пространственных фазовых модуляторов. Метод также позволяет реализовать полностью поляризационно нечувствительное восстановление квантовых состояний.

Раздел 5.1 посвящен введению в вопросы томографии пространственных квантовых состояний.

Экспериментальная установка, собранная для демонстрации метода, показана на Рисунке 10 (**раздел 5.2**). Для приготовления пространственных квантовых состояний используется пространственный фазовый модулятор (SLM), а для их измерения — деформируемое зеркало (DM). Измерения проводились путем проекции неизвестного квантового состояния на элементы взаимно-несмещенных базисов размерности 4, т.е. всего на 20 различных состояний.

Результаты калибровки системы показаны на Рисунке 11. Если бы система позволяла реализовывать идеальные проекторы на элементы взаимно-несмещенных базисов, калибровка бы соответствовала диаграмме (a). Идеальное деформируемое зеркало с бесконечным разрешением соответствует диаграмме (b). На третьем же графике показан результат калибровки реальной системы. Несмотря на то, что картина существенно отличается от идеальной, это не является существенным препятствием для проведения томографии квантовых состояний, так как полученная калибровочная матрица содержит полную информацию о реализуемых проекторах, а значит, позволяет в теории проводить безошибочное восстановление

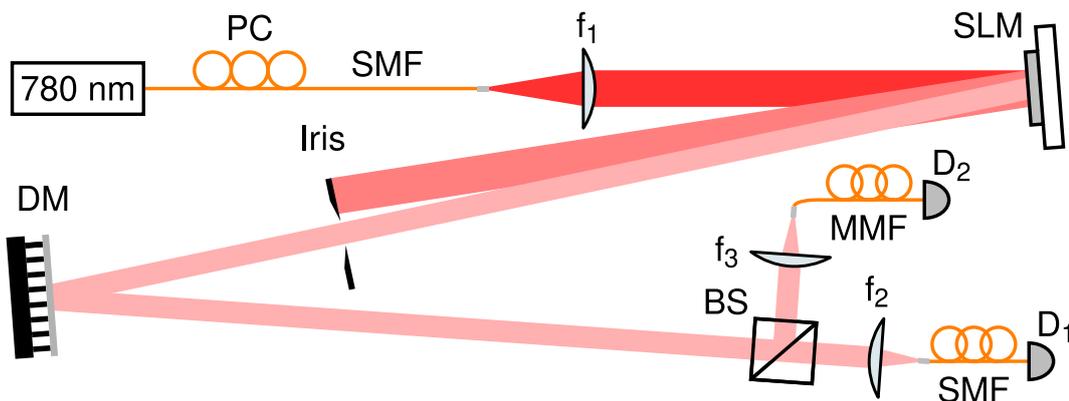


Рисунок 10: Экспериментальная установка. PC — контроллер поляризации, SMF — одномодовый световод, SLM — пространственный фазовый модулятор, DM — деформируемое зеркало, BS — симметричный светоделитель, MMF — многомодовый световод; $D_{1,2}$ — однофотонные лавинные фотодетекторы.

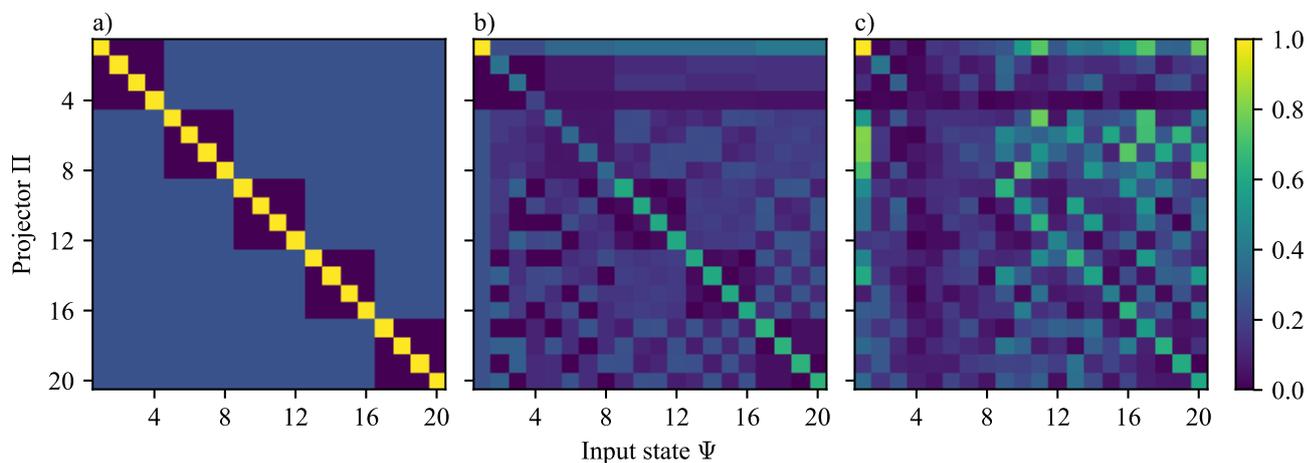


Рисунок 11: Матрица результатов измерения для протокола на взаимно-несмещенных базисах в гильбертовом пространстве размерности 4: вероятность прохождения состояния Φ_i через проектор Π_j а) идеальные проекторы на элементы ВНБ Φ_j ; б) идеальное деформируемое зеркало с бесконечным размером и пространственным разрешением; в) экспериментально измеренные результаты.

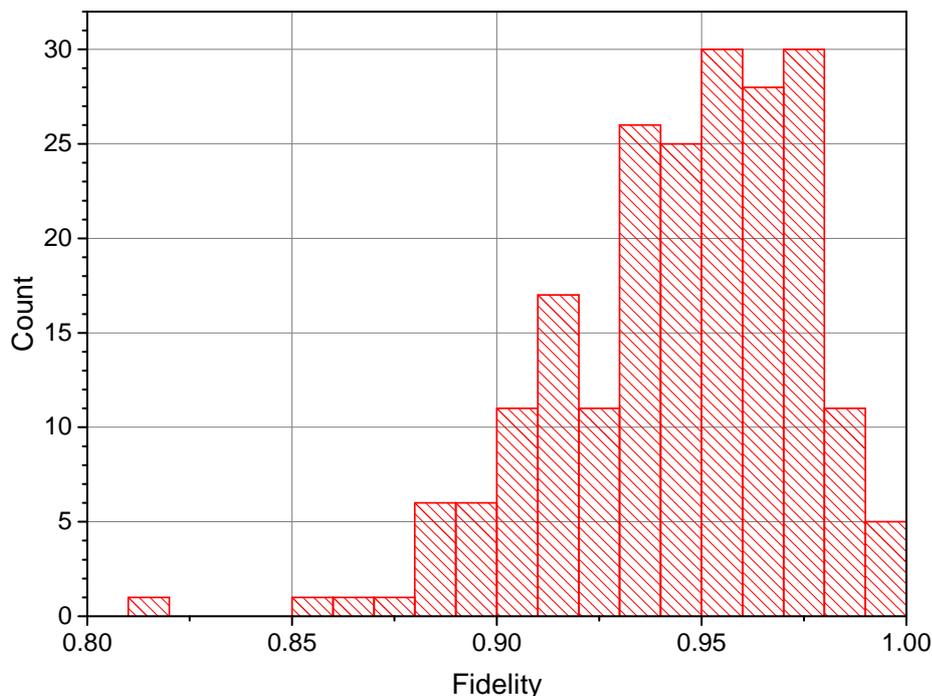


Рисунок 12: Гистограмма распределения значений меры соответствия для 210 случайных чистых квантовых состояний.

ние измеряемых квантовых состояний.

Прежде всего, была выполнена томография 20 состояний-проекторов, которая показала среднюю меру соответствия (fidelity) с реальными состояниями 0.977, а худшую — 0.940. Затем были сгенерированы случайные чистые состояния и восстановлены их матрицы плотности с использованием томографической процедуры. На Рисунке 12 показана гистограмма значений меры соответствия для измеренных 210 случайных квантовых состояний. Полученные значения не особенно высоки и не могут считаться лучшими среди аналогичных экспериментов, однако они вполне типичны для томографии пространственных состояний в гильбертовом пространстве размерности 4.

Известно, что методы защиты информации на физическом уровне в рамках классической физики не могут гарантировать полную защиту от подслушивания. Однако, в рамках квантовой физики, известно безусловно защищенное решение, называемое *квантовой криптографией*. Квантовая криптография позволяет организовать обмен секретными ключами с доказуемой секретностью. История такого подхода началась в 1984 году с публикации первого протокола [10], позже названного BB84. Несмотря на состоятельность этого, самого первого протокола квантовой криптографии, четкие доказательства его секретности появились сильно позже [11]. Разработка протоколов квантовой криптографии продолжается и по сей день. В первую очередь это связано с неидеальностью используемых на практике физических устройств. В частности, вместо одиночных фотонов, которые чрезвычайно дорого и не слишком удобно использовать в системах квантовой криптографии, используются ослабленные когерентные состояния, которые обла-

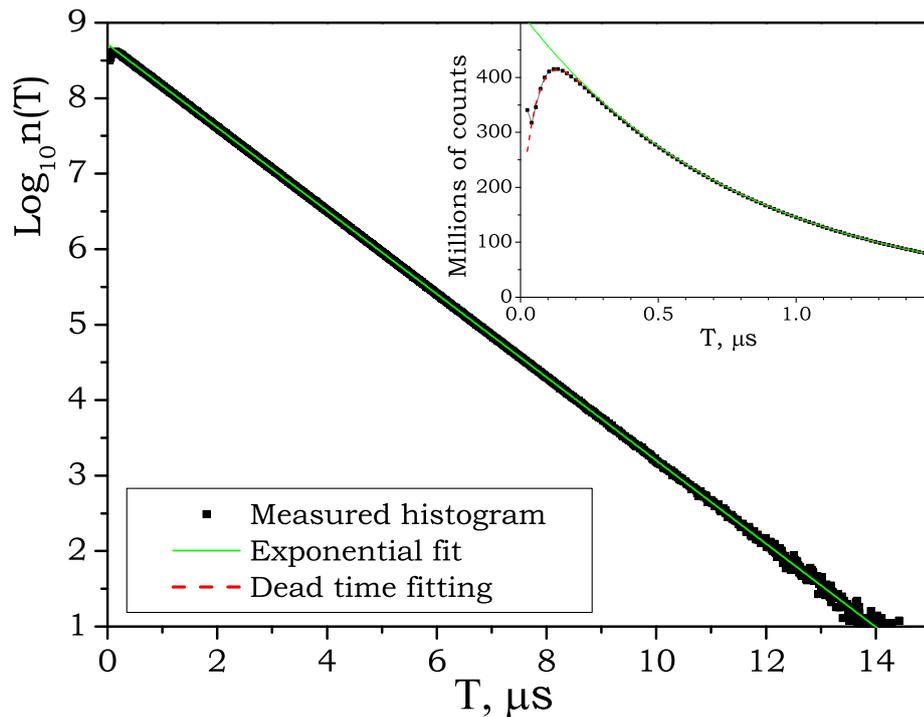


Рисунок 13: Измеренная гистограмма для времени ожидания между срабатываниями ОФД при средней частоте отсчетов 1.2 МГц. Сильное отклонение от ожидаемого экспоненциального поведения наблюдается при $T \lesssim 150$ нс.

дают совершенно другими физическими свойствами.

В шестой Главе рассмотрены методы квантового распределения ключей и получен ряд новых результатов. Предложен вариант квантового генератора случайных чисел с детерминистическим экстрактором случайности на базе измерения временных интервалов между срабатываниями однофотонного детектора. В экспериментальной реализации получены потоки случайных бит более 1 Мбит/с.

Генератор случайных чисел, предложенный **в разделе 6.1**, основан на измерении временных интервалов между срабатываниями однофотонного детектора (ОФД), при его освещении непрерывным по времени слабым оптическим сигналом. Исследование реального процесса детектирования было выполнено при той же средней скорости отсчетов, что и в конечном устройстве, а именно 1.2 МГц. На Рисунке 13 показана гистограмма частоты отсчетов как функция задержки между последовательными срабатываниями. Она идеально соответствует ожидаемому экспоненциальному распределению, за исключением интервалов короче 150 нс.

Обсуждаемые принципы и идеи были реализованы в экспериментальной реализации, показанной на Рисунке 14. Установка основана на кремниевом ОФД с тонким обедненным слоем и чувствительной областью диаметром $\varnothing 30$ мкм. Вся цифровая обработка выполняется в реальном времени в ПЛИС с подключенной микросхемой флэш-памяти объемом 2 МБ. В качестве источника излучения используется красный светодиод ($\lambda \approx 627$ нм, спектральная ширина $\Delta\lambda \approx 45$ нм), накачиваемый током ≈ 10 мкА.

В конечном устройстве применен детерминистический экстрактор случайно-

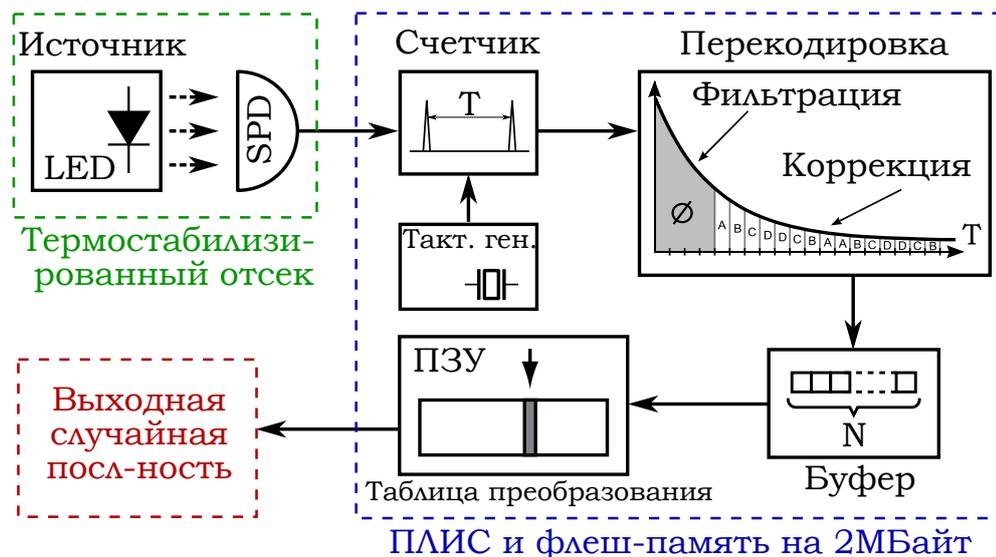


Рисунок 14: Блок-схема экспериментальной установки.

сти, основанный на предположении о стационарности случайного процесса фоторегистрации. Несмотря на различные вероятности появления определенных символов (см. диаграмму «перекодировка») в исходной последовательности, вероятности появления их комбинаций, отличающихся лишь перестановкой символов, равны. Исходя из этого предположения можно выполнить экстракцию случайных бит, о которой подробнее сказано в тексте диссертации.

В результате такой экстракции, которая выполняется в реальном времени в ПЛИС, получается случайная последовательность высокого качества, проходящая набор статистических тестов NIST [12].

В разделе 6.2 продемонстрированы две реализации релятивистского протокола квантового распределения ключей: более простая двухпроходная схема и более совершенная и технически сложная — однопроходная. В последней также была реализована система активного трекинга в канале связи по открытому пространству, которая позволяет существенно смягчить требования на установку терминалов канала связи, а также делающая возможной приемлемую работу системы в условиях атмосферной турбулентности.

Суть протокола релятивистской квантовой криптографии схематично показана на Рисунке 15 в виде пространственно-временной диаграммы. Его ключевой элемент - это передача квантовых состояний со скоростью света в двух временных окнах, разделенным измеримым временным интервалом ΔT . При этом, сама механика генерации ключей практически идентична протоколу B92 [13].

Напомним, что согласно общепринятой терминологии в области квантовой криптографии, передающую станцию называют *Алиса*, приемную — *Боб*, а условного противника — *Ева*. Чтобы получить один бит секретного ключа, Алиса и Боб случайным образом выбирают по одному биту информации, b_A и b_B соответственно, где $b \in \{0, 1\}$. Алиса передает два импульса: опорное слабое когерентное состояние $|\alpha\rangle$ в первом временном окне и сигнальное состояние $|e^{ib_A\varphi}\alpha\rangle$ во вто-

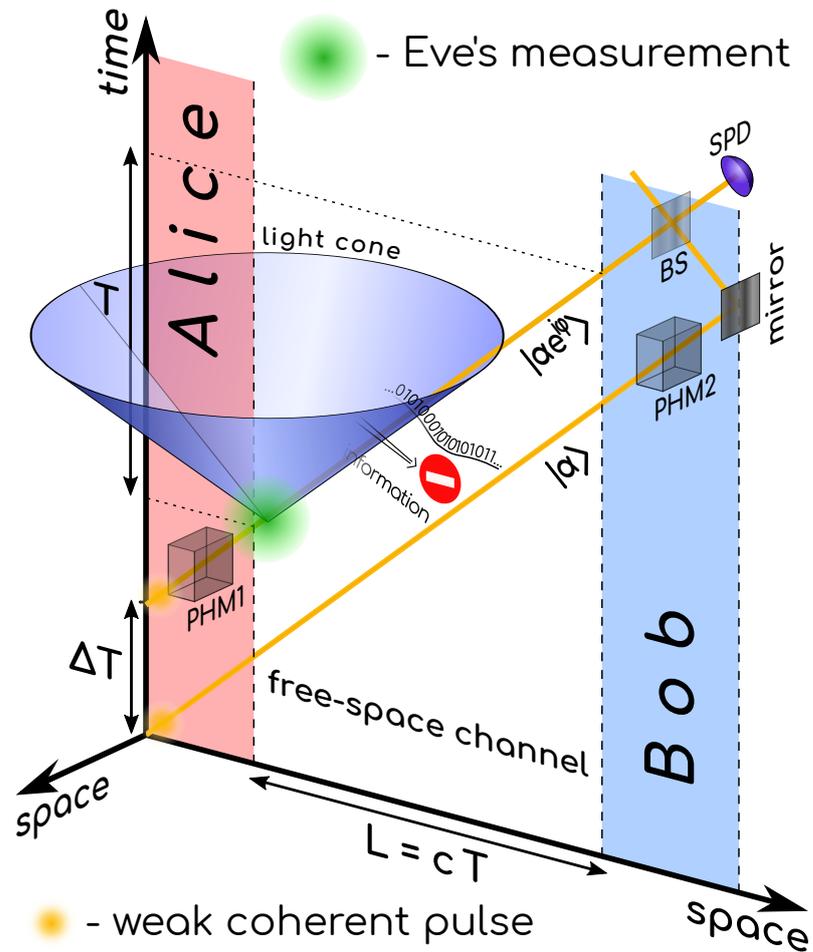


Рисунок 15: Пространственно-временная диаграмма релятивистского протокола квантового распределения ключей. Два импульса распространяются со скоростью света, тем самым исключая возможность злоумышленника воздействовать на первый импульс в зависимости от результата измерения второго, модулированного импульса. PHM – фазовый модулятор, BS – симметричный светоделитель, SPD – однофотонный детектор.

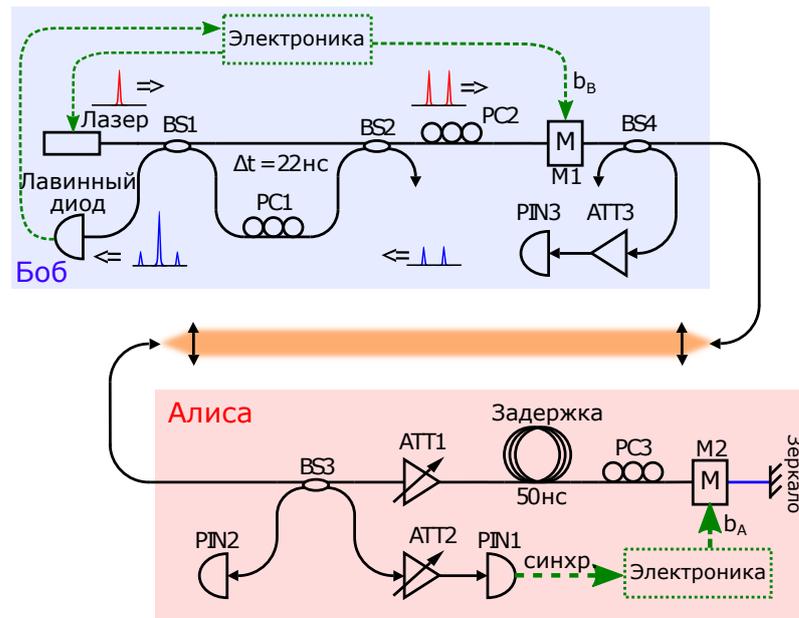


Рисунок 16: Экспериментальная установка для двухпроходного протокола релятивистской квантовой криптографии. BS – светоделитель, PC – контроллер поляризации, M – фазовый модулятор, PIN – PIN фотодиод, АТТ - аттенюатор.

ром. Боб делает дополнительный фазовый сдвиг $b_B \varphi$ во втором временном окне и измеряет результат интерференции двух получившихся импульсов. В результате, зарегистрировать ненулевой результат интерференции Боб может только если $b_A \neq b_B$. В противном случае, между двумя импульсами происходит деструктивная интерференция и в детекторе оказывается вакуумное состояние. Таким образом, при каждом срабатывании детектора Боба, он сообщает о факте срабатывания детектора Алисе, и они получают новый бит сырого ключа.

Схема реализованной экспериментальной установки для двухпроходного варианта протокола показана на Рисунке 16. Это оптоволоконная система, работающая на длине волны 850 нм. Канал связи по открытому пространству состоит из пары коллиматоров с выходной апертурой 23 мм, размещенных на штативах; потери в канале оцениваются в 3 дБ. Установка на другой стороне канала связи (Алиса) состоит из таких же компонентов и работает в ведомом режиме. Сигнал от фотоприемника PIN1 активирует установку, которая выборочно модулирует фазу второго оптического импульса после его отражения от зеркала.

Более эффективная экспериментальная реализация может быть выполнена на базе однопроходной схемы. Созданная экспериментальная установка представлена на Рисунке 17.

Переход к однопроходной конфигурации квантового канала делает систему более защищенной от действий Евы по сравнению с двухпроходной, так как в двухпроходной схеме Ева может управлять классическими импульсами, идущими от Боба к Алисе. Такой тип атаки называется по-разному, это и активное зондирование установки Алисы, и, в англоязычной литературе, атака типа Троянского коня. В любом случае, это достаточно опасная конфигурация, потенциально

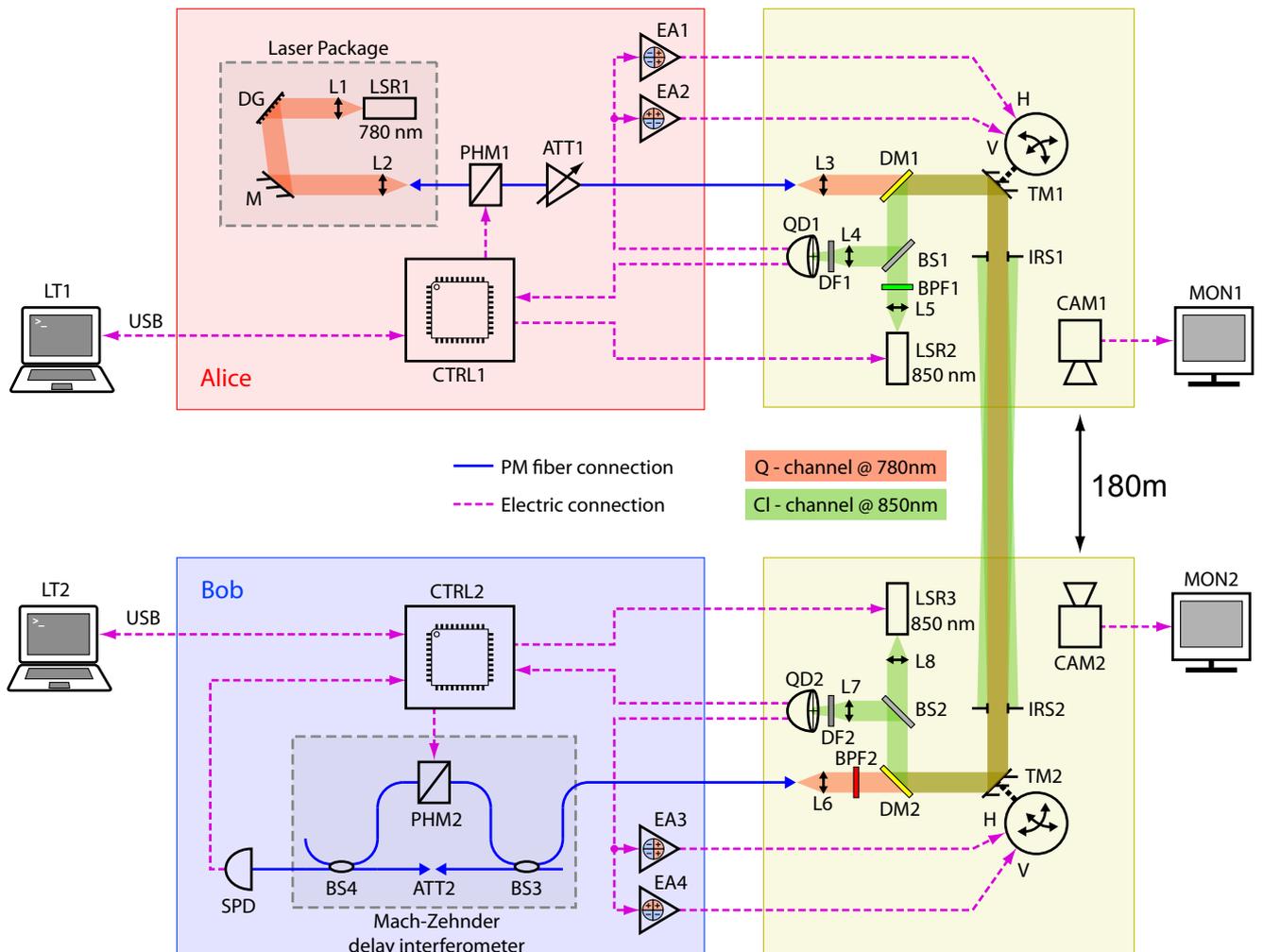


Рисунок 17: Схема экспериментальной установки. LT – абонентский терминал на базе ноутбука; DG – дифракционная решетка в схеме Литтроу; L – линза; M – зеркало; PHM – электрооптический фазовый модулятор с оптоволоконными выходами с частотной полосой 150 МГц; ATT – переменный оптический attenuator; CTRL – управляющая электроника; EA – электронный усилитель ошибки в системе обратной связи трекинга; DM – дихроичное зеркало; TM – управляемое качающееся зеркало с пьезоприводом; QD – квадрантный фотодетектор; DF – матовое стекло; BS – симметричный светоделитель; IRS – переменная диафрагма; BPF – многослойный полосовой фильтр; CAM – камера грубого прицеливания; MON – монитор пользователя для камеры; SPD – однофотонный детектор на базе кремниевого лавинного фотодиода.

позволяющая Еве манипулировать квантовыми состояниями, которые испускает Алиса. Кроме очевидного преимущества в защищенности системы, однопроходная схема также позволяет существенно повысить частоту посылок в системе, так как нет необходимости ждать пока вернется предыдущий импульс, чтобы отправлять новый.

Поскольку, как уже говорилось, безопасность релятивистского протокола зависит от точного контроля времени пролета, в любых его реализациях синхронизация станций играет критически важную роль в протоколе. Внесение ошибок в синхронизацию станций может легко подорвать основы безопасности протокола, открывая лазейку для подслушивания. Решение проблемы синхронизации реализовано аналогично двухпроходному протоколу, в котором требовался обратный классический канал связи, в котором информация также распространяется со скоростью света.

Чтобы инициировать квантовую передачу, Боб генерирует случайную последовательность битов и отправляет ее Алисе по классическому каналу с той же частотой, которую Алиса использует для квантового распределения ключей. Алиса сохраняет каждый принятый бит в своей локальной памяти и в ответ передает одно слабое когерентное состояние в квантовый канал. После того, как передача всего пакета завершена, Алиса и Боб сравнивают свои последовательности синхронизации. Если последовательности совпадают, Алиса может гарантировать, что она получила каждый бит не раньше, чем Боб ожидал это от нее. В противном случае была бы продемонстрирована классическая передача данных между Бобом и Алисой со сверхсветовой скоростью, что напрямую противоречит теории относительности, а значит никак не может быть реализовано Евой. Это в свою очередь означает, что Алиса никогда не отправляла квантовое состояние в канал ранее, чем Боб ожидал этого от неё. С другой стороны, это единственный вариант, как Ева может выиграть дополнительное время для реализации действия после получения результата своего измерения квантового состояния Алисы не вызывая ошибок в канале Алиса-Боб. Если бы она могла заставить Алису передавать данные раньше, чем думает Боб, протокол был бы нарушен. Если же, наоборот, Алиса пошлет свои импульсы позже, Боб просто не получит никаких отсчетов, коррелированных с сырым ключом Алисы, поэтому пакет будет отброшен как не содержащий никакой секретной информации. Если в результате сравнения окажется, что последовательность синхронизации, полученная Алисой, отличается от последовательности синхронизации Боба, это будет являться потенциальным признаком атаки на синхронизацию станций, и весь пакет должен быть отброшен как ненадежный.

Обратный классический канал связи, необходимый для синхронизации, реализуется через систему трекинга, которая также служит для передачи данных и управляющих сообщений в обоих направлениях между сторонами. Помимо передачи данных, система трекинга необходима для поддержания квантового канала в рабочем состоянии, поскольку, в отличие от большинства систем квантового распределения ключей в открытом пространстве, в данной демонстрации требуется

одномодовый приемник, который совместим с волоконным интерферометром задержки. Без активной подстройки канала такая система была крайне нестабильной и не могла надежно работать даже в течение нескольких минут. С реализацией системы активного трекинга, квантовый канал стал стабильным на протяжении нескольких часов работы. Стабильность канала на больших промежутках времени не проверялась.

Для демонстрации реального распределения сырых ключей использовались предварительно сохраненные данные из квантового генератора случайных чисел. В нашей экспериментальной демонстрации принципов релятивистской квантовой криптографии мы не реализовывали алгоритмы усиления секретности и исправления ошибок. Это относительно хорошо изученный вопрос, который потребовал бы слишком много времени для своей реализации. Поэтому все оценки производятся с использованием найденного выше асимптотического соотношения и полученных сырых ключей. На рисунке 18 показаны экспериментально измеренные данные — длина сырого ключа и доля ошибок в сыром ключе, — а также асимптотически оцененное число секретных бит. Каждая точка данных показывает результат конкретного обмена 1.68×10^7 ослабленных классических импульсов между Алисой и Бобом. Наиболее эффективная генерация секретного ключа наблюдалась при среднем числе фотонов в импульсе $\mu = 0.116$, где скорость генерации сырого ключа (внутри пакета) равна 2170 бит/сек, а асимптотическая скорость генерации секретного ключа оценивается как 660 бит/сек.

Наконец, в разделе 6.3 разработан протокол квантовой криптографии на геометрически-однородных квантовых состояниях (ГОКС) с состояниями-ловушками. Данный протокол основан на более совершенном протоколе распределения ключей по сравнению с традиционным протоколом BB84. Приведены доказательства секретности предлагаемого протокола и моделирование эффективности его работы при различных условиях передачи.

Ключевая идея данного протокола заключается в повышении числа информационных квантовых состояний до 8 и их логическая группировка в неортогональные пары. Информационные состояния и их сравнение с классическими конфигурациями, такими как B92 [13], BB84 [10] и SARG04 [14] показаны на Рисунке 19.

В результате проведенного анализа секретности получено следующее выражение для асимптотической длины секретного ключа

$$R'(\mu) = 2\mu e^{-2\mu} \bar{P}_1 [1 - \chi_1(\bar{Q}_1)] - \bar{P}(\mu) h(\bar{Q}(\mu)), \quad (9)$$

где μ — среднее число фотонов в информационном импульсе, $\bar{P}(\mu)$ — вероятность регистрации импульса, \bar{Q} — общий наблюдаемый уровень ошибок. Те же величины с индексом 1 относятся соответственно к вероятности регистрации однофотонной компоненты и доли ошибок, ассоциированной с ней. Они определяются путем использования состояний-ловушек, т.е. когерентных состояний с меньшей амплитудой, которые необходимы для оценки соответствующих однофотонных величин.

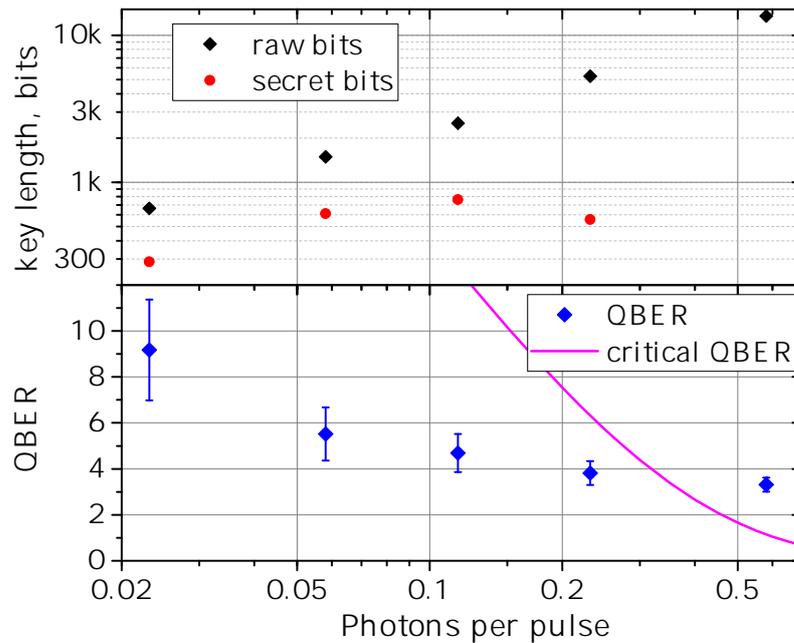


Рисунок 18: Длины полученных ключей и доля ошибок в сыром ключе (QBER) в зависимости от среднего числа фотонов для квантового распределения ключей со случайными данными из квантового генератора случайных чисел. Каждая точка является результатом распределения ключей с входным буфером размером 16 Мбит, т.е. для 256 переданных пакетов.

Таким образом, видно, что выражение для длины секретного ключа зависит лишь от измеряемых параметров α , следовательно, может быть использовано в реальных системах для оценки доли секретной информации.

В целом, направление, исследованное в Главе №6, как теоретически, так и экспериментально, привело к существенному развитию технологии квантового распределения ключей в первую очередь по открытому пространству. В настоящее время, многие идеи и технологические решения, представленные в этой главе находят применение в более совершенных экспериментальных системах квантового распределения ключей по открытому пространству, над которыми работает автор диссертации совместно с группой ученых и инженеров.

Заключение

В диссертации, в соответствии с её целью, предложены фундаментально новые подходы к представлению информации в виде оптических сигналов, её обработке, передаче и защите от несанкционированного доступа. Разработаны соответствующие методы управления классическими и квантовыми оптическими полями.

Основные результаты работы заключаются в следующем:

1. Предложены интегрально-оптические варианты реализации устройств для оптической связи. На базе планарных волноводных решеток эксперимен-

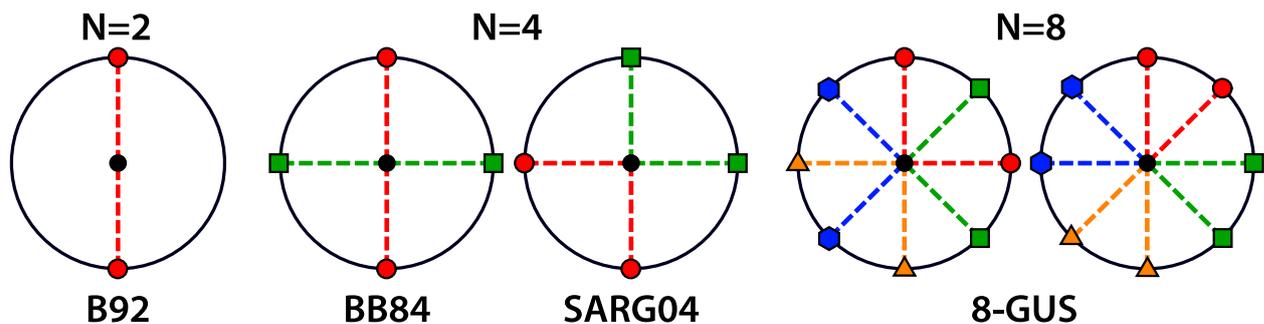


Рисунок 19: Информационные состояния и логические базисы в различных ГОКС протоколах, показанные на фазовой плоскости. Логические базисы показаны различными цветами и формой отметок. Для протоколов 8-ГОКС существует два удобных выбора базисов: с углом между состояниями $\Delta\varphi = \pi/2$ и $\Delta\varphi = \pi/4$, как показано на последних двух диаграммах.

тально продемонстрирована технология передачи на ортогональных поднесущих OFDM. При этом, решетки выполняют ключевую функцию — дискретное преобразование Фурье. Также предложена голографическая технология изготовления оптических чипов. На ее основе разработан ряд оптических приборов как для традиционной оптической связи, так и для оптических интерконнектов на чипе. В частности, предложены решения для фазового декодирования в когерентной связи, для оптических сетей CDMA и для спектрального мультиплексирования.

2. Предложено полностью оптическое решение для реализации модели биологического нейрона. Разработанное устройство основано на оптических свойствах полупроводниковых оптических усилителей, которые практически точно повторяют электрическую модель биологических нейронов. Экспериментально показаны некоторые режимы работы, в частности, функционирование возбуждающих и тормозящих входов, интегрирующие свойства нейрона, а также режим работы с обратной связью.
3. Предложен классический способ распределения условно секретных ключей. Несмотря на невозможность доказательства защищенности такого метода от взлома, он, тем не менее, обладает существенно асимметричными свойствами, т.е. взлом системы по технической сложности кардинально превышает ее использование легитимными пользователями.
4. Проанализированы турбулентные искажения в оптических каналах связи по открытому пространству. Исследована задача распространения отдельных поперечных мод по таким каналам. Для экспериментальной проверки разработанной теории создана турбулентная камера. Результаты измерений подтверждают выведенные аналитические выражения для потерь и перекрестных помех в канале.

5. Экспериментально продемонстрирована томография поперечных пространственных квантовых состояний света с помощью микроэлектромеханического деформируемого зеркала. Выбранный подход позволяет проводить томографию существенно быстрее, чем в традиционном варианте с жидкокристаллическим пространственным фазовым модулятором.
6. Предложено несколько решений для квантового распределения ключей, а также экспериментально продемонстрирован релятивистский протокол квантовой криптографии. Разработан квантовый генератор случайных чисел, обладающий большой надежностью за счет использования простого детерминистического экстрактора случайности. Предложен и проанализирован протокол квантовой криптографии на геометрически-однородных квантовых состояниях, обладающий рядом преимуществ по сравнению с традиционным протоколом квантовой криптографии BB84.

Список опубликованных статей

- [A1] Kravtsov Konstantin, Prucnal P. R., Bubnov M. M. Simple nonlinear interferometer-based all-optical thresholder and its applications for optical CDMA // *Opt. Express.* — 2007. — Vol. 15, no. 20. — P. 13114–13122.
- [A2] Suarez John, Kravtsov Konstantin, Prucnal Paul R. Incoherent Method of Optical Interference Cancellation for Radio-Frequency Communications // *IEEE J. Quant. Electron.* — 2009. — Vol. 45, no. 4. — P. 402–408.
- [A3] Rosenbluth D., Kravtsov K., Fok M. P., Prucnal P. R. A high performance photonic pulse processing device // *Opt. Express.* — 2009. — Vol. 17, no. 25. — P. 22767–22772.
- [A4] Fok M. P., Rosenbluth D., Kravtsov K., Prucnal P.R. Lightwave Neuromorphic Signal Processing // *IEEE Signal Process. Mag.* — 2010. — Vol. 27, no. 6. — P. 160,157–158.
- [A5] Suarez J., Kravtsov K., Prucnal P. R. Methods of Feedback Control for Adaptive Counter-Phase Optical Interference Cancellation // *IEEE Trans. Instrum. Meas.* — 2011. — Vol. 60, no. 2. — P. 598–607.
- [A6] Wang Z, Kravtsov K. S., Huang Y.-K., Prucnal P. R. Optical FFT/IFFT circuit realization using arrayed waveguide gratings and the applications in all-optical OFDM system // *Opt. Express.* — 2011. — Vol. 19, no. 5. — P. 4501–4512.
- [A7] Kravtsov K., Fok M. P., Prucnal P. R., Rosenbluth D. Ultrafast all-optical implementation of a leaky integrate-and-fire neuron // *Opt. Express.* — 2011. — Vol. 19, no. 3. — P. 2133–2147.
- [A8] Bogdanov Yu. I., Gavrichenko A. K., Kravtsov K. S. et al. Statistical reconstruction of mixed states of polarization qubits // *J. Exp. Theor. Phys.* — 2011. — Vol. 113, no. 2. — P. 192–201.
- [A9] Bogdanov Yu. I., Brida G., Bukeev I. D. et al. Statistical estimation of the quality of quantum-tomography protocols // *Phys. Rev. A.* — 2011. — Vol. 84, no. 4. — P. 042108.

- [A10] Fok Mable P., Deng Yanhua, Kravtsov Konstantin, Prucnal Paul R. Signal beating elimination using single-mode fiber to multimode fiber coupling // *Opt. Lett.* — 2011. — Vol. 36, no. 23. — P. 4578–4580.
- [A11] Rafidi N. S., Kravtsov K. S., Tian Yue et al. Power Transfer Function Tailoring in a Highly Ge-Doped Nonlinear Interferometer-Based All-Optical Thresholder Using Offset-Spectral Filtering // *IEEE Photonics Journal.* — 2012. — Vol. 4, no. 2. — P. 528–534.
- [A12] Pina-Hernandez Carlos, Lacatena Valeria, Calafiore Giuseppe et al. A route for fabricating printable photonic devices with sub-10 nm resolution // *Nanotechnology.* — 2013. — Vol. 24, no. 6. — P. 065301.
- [A13] Kravtsov Konstantin, Wang Zhenxing, Trappe Wade, Prucnal Paul R. Physical layer secret key generation for fiber-optical networks // *Opt. Express.* — 2013. — Vol. 21, no. 20. — P. 23756–23771.
- [A14] Radchenko I. V., Kravtsov K. S., Kulik S. P., Molotkov S. N. Relativistic quantum cryptography // *Laser Phys. Lett.* — 2014. — Vol. 11, no. 6. — P. 065203.
- [A15] Kravtsov K. S., Radchenko I. V., Kulik S. P., Molotkov S. N. Minimalist design of a robust real-time quantum random number generator // *J. Opt. Soc. Am. B.* — 2015. — Vol. 32, no. 8. — P. 1743–1747.
- [A16] Kravtsov K. S., Radchenko I. V., Kulik S. P., Molotkov S. N. Relativistic quantum key distribution system with one-way quantum communication // *Scientific Reports.* — 2018. — Vol. 8. — P. 6102.
- [A17] Kravtsov K. S., Zhutov A. K., Radchenko I. V., Kulik S. P. Turbulence-induced optical loss and cross-talk in spatial-mode multiplexed or single-mode free-space communication channels // *Phys. Rev. A.* — 2018. — Vol. 98, no. 6. — P. 063831.
- [A18] Kravtsov K. S., Molotkov S. N. Practical quantum key distribution with geometrically uniform states // *Phys. Rev. A.* — 2019. — Vol. 100, no. 4. — P. 042329.
- [A19] Kravtsov K. S., Zhutov A. K., Kulik S. P. Spatial quantum state tomography with a deformable mirror // *Phys. Rev. A.* — 2020. — Vol. 102, no. 2. — P. 023706.
- [A20] Kravtsov K. S., Molotkov S. N. Reply to “Comment on ‘Practical quantum key distribution with geometrically uniform states’” // *Phys. Rev. A.* — 2021. — Vol. 104, no. 2. — P. 026402.

Список зарегистрированных патентов

- [P1] Suarez J., Kravtsov K., Prucnal P. R. Optical counter-phase system and method of RF interference cancellation. — US Patent 8,693,810 Issued: April 8, 2014. Appl. No.: 12/613,512 Priority: November 5, 2008. — Pub. No.: US 20120251031 A1 Pub. date: October 4, 2012.
- [P2] Rosenbluth D., Prucnal P. R., Kravtsov K. Optical integration system and method. — US Patent 8,749,874 Issued: June 10, 2014. Appl. No.: 13/255,803 Priority: March 10, 2009 PCT Appl. No.: PCT/US2010/026830 PCT Filed: March 10, 2010. — Pub. No.: US 20120057221 A1 Pub. Date: March 8, 2012 Pub. No.: WO 2010104954 A1 Pub. date: September 16, 2010.
- [P3] Yankov V., Kravtsov K., Velikov L. Method of optical interconnection of data-processing cores on a chip. — US Patent 9,036,994 Issued: May 19, 2015. Appl. No.: 13/650,092 Priority: October 11, 2012. — Pub. No.: US 20140105613 A1 Pub. Date: April 17, 2014.
- [P4] Yankov V., Kravtsov K., Velikov L. Multicore chip with holographic optical interconnects. — US Patent 9,143,235 September 22, 2015. Appl. No.: 13/651,442 Priority: October 14, 2012. — Pub. No.: US 20140105611 A1 Pub. Date: April 17, 2014.
- [P5] Кравцов К. С., Кулик С. П., Молотков С. Н. et al. Квантовый генератор случайных чисел. — Патент РФ RU 2,613,027 С1 выдан 14.03.2017. Номер заявки: 2015141963 Приоритет: 02.10.2015.

Список литературы

- [1] Sanjoh H., Yamada E., Yoshikuni Y. Optical orthogonal frequency division multiplexing using frequency/time domain filtering for high spectral efficiency up to 1 bit/s/Hz // Conference on Optical Fiber Communication, OFC. — paper ThD1. — Anaheim, CA, 2002. — P. 401–402.
- [2] Shieh W., Djordjevic I. OFDM for Optical Communications. — Academic Press, 2009.
- [3] Lowery Arthur James, Armstrong Jean. Orthogonal-frequency-division multiplexing for dispersion compensation of long-haul optical systems // Opt. Express. — 2006. — Mar. — Vol. 14, no. 6. — P. 2079–2084.
- [4] Doerr Christopher Richard, Okamoto Katsunari. Advances in Silica Planar Lightwave Circuits // J. Lightwav. Technol. — 2006. — Dec. — Vol. 24, no. 12. — P. 4763–4789.
- [5] Pulsed Neural Networks / Ed. by Wolfgang Maass, Christopher M. Bishop. — The MIT Press, 1999.
- [6] Premaratne M., Nešić D., Agrawal G. P. Pulse Amplification and Gain Recovery in Semiconductor Optical Amplifiers: A Systematic Analytical Approach // J. Lightwav. Technol. — 2008. — Vol. 26, no. 12. — P. 1653–1660.
- [7] Колмогоров А. Н. Рассеяние энергии при локально изотропной турбулентности // Докл. АН СССР. — 1941. — Vol. 32. — P. 19–21.
- [8] Avila Remy, Ziad Aziz, Borgnino Julien et al. Theoretical spatiotemporal analysis of angle of arrival induced by atmospheric turbulence as observed with the grating scale monitor experiment // J. Opt. Soc. Am. A. — 1997. — Vol. 14, no. 11. — P. 3070–3082.
- [9] Jolissaint Laurent. Optical Turbulence Generators for Testing Astronomical Adaptive Optics Systems: A Review and Designer Guide // PASP. — 2006. — Vol. 118, no. 847. — P. 1205–1224.

- [10] Bennett C. H., Brassard G. Quantum Cryptography: Public key distribution and coin tossing // Proceedings of the IEEE International Conference on Computers, Systems, and Signal Processing. — Bangalore, 1984. — P. 175–179.
- [11] Christandl Matthias, Renner Renato, Ekert Artur. A Generic Security Proof for Quantum Key Distribution // arXiv. — 2004. — arXiv:quant-ph/0402131.
- [12] NIST Statistical Test Suite. — <https://csrc.nist.gov/projects/random-bit-generation/documentation-and-software>. — 2010. — Accessed: 2022-02-20.
- [13] Bennett C. H. Quantum cryptography using any two nonorthogonal states // Phys. Rev. Lett. — 1992. — Vol. 68, no. 21. — P. 3121–3124.
- [14] Scarani Valerio, Acín Antonio, Ribordy Grégoire, Gisin Nicolas. Quantum Cryptography Protocols Robust against Photon Number Splitting Attacks for Weak Laser Pulse Implementations // Phys. Rev. Lett. — 2004. — Feb. — Vol. 92. — P. 057901.