Федеральное государственное бюджетное учреждение науки
Федеральный исследовательский центр

Институт общей физики им. А.М. Прохорова Российской академии наук
(ИОФ РАН)

На правах рукописи

Кравцов Константин Сергеевич

Управление оптическими полями для задач связи и защиты информации

Специальность 01.04.21 — лазерная физика

ДИССЕРТАЦИЯ
на соискание ученой степени
доктора физико-математических наук

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

МОСКВА — 2022 г.

Оглавление

Введение

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, возможности оптоволоконного канала связи перестали выглядеть как что-то бесконечное, и появились ощутимые 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 подходы 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 микроэлектромеханического 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 квартиля. 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 состояния 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 искомых 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 быстро-

действием.

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 (ICOCN 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 наименование на 17 страницах.

Благодарности

Автор хочет высказать благодарность тем, без кого настоящая работа была бы немыслима. В первую очередь это касается научной поддержки, обсуждения новых идей, помощи в воплощении теоретических результатов в экспериментальной работе и конечно объективной (хотя и не всегда:) критики со стороны. В неменьшей степени это касается и организационной поддержки, в которой нуждается любой исследователь, особенно экспериментатор.

Хочется особо отметить вклад Сергея Павловича Кулика, Константина Николаевича Ельцова, Сергея Николаевича Молоткова, Владимира Янькова, Игоря Радченко и Пола Пруцнала (Paul R. Prucnal).

Автор благодарит Ирину Белякову, Ивана Боброва, Леонида Великова, Александра Гольцова, Ивана Дьяконова, Артёма Жутова, Михаила Исиченко, Александра Калинкина, Константина Катамадзе, Егора Ковлакова, Татьяну Кравцову, Ивана Погорелова, Юрия Полянского, Михаила Рослякова, Владимира Светикова, Станислава Страупе, Глеба Стручалина, Ирину Юдину, Mable Fok, Christophe Peroz, Zhenxing Wang.

Глава 1

Модуляция и мультиплексирование в классических линиях связи

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. Настоящая глава посвящена разработке нового подхода к модуляции и мультиплексированию оптических сигналов, а также разработке новой технологии для изготовления соответствующих интегральных оптических устройств.

1.1. Планарные волноводные решетки для технологии OFDM

Планарные волноводные решетки (arrayed waveguide gratings, AWG) в настоящее время широко используются в качестве спектральных мультиплексоров/демультиплексоров в линиях связи со спектральным уплотнением каналов. В этом разделе предлагается использование таких решеток в качестве интегрированного спектрального фильтра для реализации дискретного преобразования Фурье (ДПФ) и его инверсии — обратного дискретного преобразования Фурье (ОДПФ). Будет показано, что работа волноводной решетки в качестве спектрального фильтра одновременно позволяет выполнять функции ДПФ/ОДПФ. Следовательно, большой накопленный опыт по дизайну и изготовлению AWG теперь может быть применен для проектирования оптических схем с ДПФ/ОДПФ [A6]. При прохождении сигналов через это пассивное устройство автоматически выполняются операции ДПФ или ОДПФ, а результаты этих преобразований могут быть получены с помощью оцифровки выходного оптического сигнала в нужный момент времени. По сравнению с другими оптическими схемами, реализующими ДПФ/ОДПФ, AWG имеют существенно меньшую сложность, особенно для большого количества входов и выходов. В качестве важного приложения AWG могут использоваться для мультиплексирования на ортогональных подчастотах (orthogonal frequency division multiplexing, OFDM) и, что более важно, для демультиплексирования соответствующих поднесущих. Также экспериментально было продемонстрировано использование AWG

с 16 портами ввода/вывода и расстоянием между каналами в 10 ГГц в оптической системе OFDM со скоростью модуляции 7.5 Гбит/с, что подтверждает основные теоретические выводы. В целом, AWG представляет собой реальное решение для полностью оптических систем OFDM, особенно с большим количеством поднесущих.

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. На Рисунке 1.1 схематически показана принципиальная схема такой системы OFDM. После преобразования последовательного потока входных данных в параллельный и отображения символов на поднесущих, выполняется ОДПФ для генерации символов OFDM. Далее между символами OFDM обычно вставляются защитные интервалы или, так называемые, циклические префиксы, чтобы сохранить ортогональность поднесущих при наличии дисперсии и других искажений сигнала в канале. Сгенерированные цифровые выборки OFDM преобразуются в аналоговые сигналы через цифро-аналоговый преобразователь (ЦАП). Полученные аналоговые сигналы используются для модуляции оптической несущей. На стороне приемника оптический сигнал регистрируется фотодетектором и дискретизируется аналого-цифровым преобразователем (АЦП). Для демультиплексирования поднесущих выполняется ДПФ, после чего реализуются другие методы цифровой обработки для успешного извлечения исходных данных.

Реальная оптическая система OFDM, способная работать в реальном времени, устроенная таким образом, сильнейшим образом ограничена доступной полосой частот электронных устройств и возможностями обработки данных с высокой скоростью. В первую очередь, эти ограничения касаются АЦП, ЦАП и модулями ДПФ/ОДПФ. В настоящее время в оптических системах OFDM с электронной реализацией в реальном времени скорость передачи символов ограничена миллио-

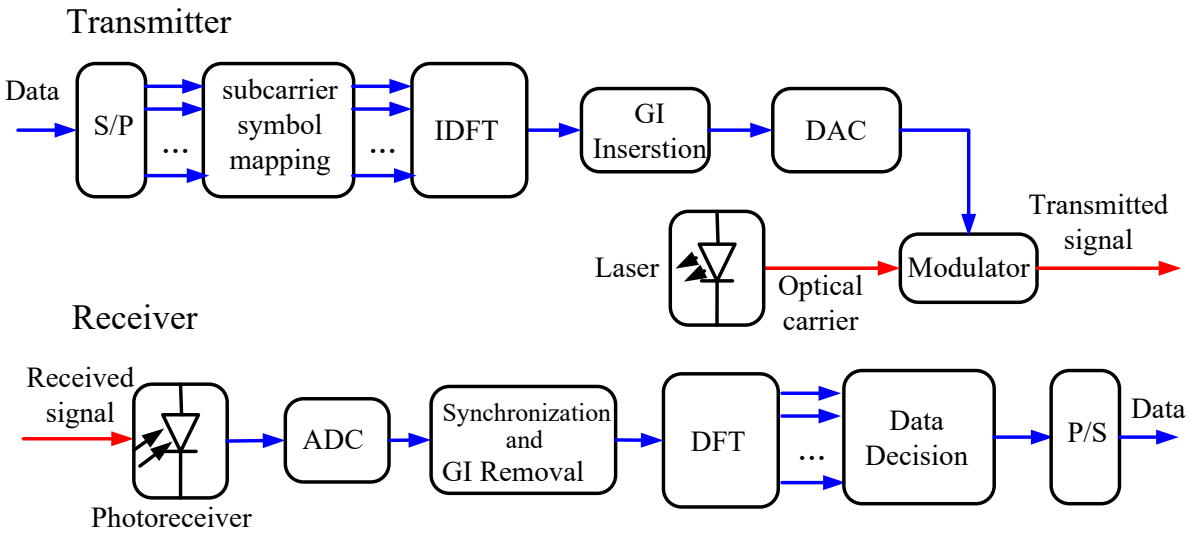

Рисунок 1.1: Схема системы оптической связи на базе OFDM. S/P – преобразование последовательного потока данных в параллельный; IDFT – ОДПФ; GI – защитный интервал; DAC – цифро-аналоговый преобразователь; ADC – аналогово-цифровой преобразователь; P/S –преобразование параллельного потока данных в последовательный

нами символов в секунду [4, 5, 6]. Совсем недавно была продемонстрирована оптическая система OFDM с пропускной способностью 110 Гбит/с в реальном времени [7], использующая оптическое мультиплексирование полосы. Приемная система обрабатывает получаемый сигнал только в полосе частот 2 ГГц. Чтобы преодолеть ограничение, связанное со скоростью электроники, ранее был предложен полностью оптический OFDM для реализации передатчика и приемника OFDM на базе исключительно оптических устройств, возможно, с небольшими исключениями [8, 9, 10]. Оптические схемы ДПФ/ОДПФ также были предложены [11] и экспериментально продемонстрированы [12, 13, 14]. Упомянутые схемы имитируют в оптическом домене алгоритмы прямого и обратного *быстрого преобразования Фурье (БПФ)*, что позволяет реализовать их в оптике без преобразования в электронные сигналы и обратно. Такие оптические схемы ДПФ/ОДПФ обычно реализуются в виде интегральной планарной оптической структуры с несколькими ступенями преобразования, на каждой из которых реализуются подобранные временны́е задержки и фазовые сдвиги. Многие такие оптические схемы имеют специальную конструкцию для упрощения их структуры [12, 14]. В [14] предложены каскадные интерферометры задержки для реализации функции БПФ, что значительно сокращает количество фазовращателей и линий задержки. Но для реализации полной матрицы ДПФ/ОДПФ размерности $N \times N$ все равно требуется достаточно большое количество модулей в схеме, особенно при увеличении числа поднесущих N. Насколько нам известно, существующие подходы позволили реализовали оптические схемы ДПФ/ОДПФ с максимальной числом входов и выходов $N = 8$ [12, 14].

В настоящей работе предлагается полностью оптическое решение задачи вычисления ДПФ/ОДПФ с помощью AWG. Такой подход обеспечивает полностью интегральную и масштабируемую оптическую реализацию ДПФ/ОДПФ на одном чипе, основанном на технологии, которая раз-

рабатывались десятилетиями. Подобная идея была независимо предложена ранее в работе [15], где AWG была предложена в качестве демультиплексора OFDM и были показаны некоторые результаты численного моделирования. В нашей работе мы сосредоточимся на конкретной конструкции AWG для обеспечения реализации условий ДПФ/ОДПФ, а также покажем, что конструкция AWG для ДПФ/ОДПФ имеет много общего с традиционными схемами AWG, работающих в качестве спектральных мультиплексоров.

Будут представлены также результаты экспериментальной демонстрации полностью оптической системы OFDM с частотой передачи символов 7.5 Гбит/с, с использованием AWG с 16 портами ввода/вывода и шагом по частоте 10 ГГц. Для иллюстрации возможностей данной технологии была использована как амплитудная, так и фазовая модуляция. Полученные экспериментальные результаты показывают, что коммерчески изготовленная AWG демонстрирует свойства ДПФ, отличные от простого частотного фильтра WDM. Поскольку современные технологии позволяют реализовывать AWG с большим количеством каналов, полученные результаты демонстрируют реальный способ создания полностью оптических систем OFDM с высокой пропускной способностью.

1.1.1. Принцип действия AWG в качестве фильтра ДПФ/ОДПФ и требования к её параметрам

AWG обычно предназначены для мультиплексирования и демультиплексирования сигналов в WDM системах. Такое устройство AWG подробно описано в [16, 17]. Использование AWG в качестве схемы ДПФ и демультиплексора OFDM было теоретически предложено в [15]. Оригинальность нашей работы заключается в том, что мы показали тесную связь между AWG выполняющими роль спектрального фильтра с устройствами для реализации оптического ДПФ/ОДПФ. Кроме того, помимо прямого преобразования, показана реализация ОДПФ с помощью AWG, что не обсуждалось в работе [15].

Типичная структура AWG показана на Рисунке 1.2(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 1.2(b). Обычно две области свободного распространения идентичны между собой. Обозначим расстояние между входными и выходными волноводами AWG как D, а шаг для массива волноводов как d (для входа) и d_1 (для выхода). Радиус кривизны равен f (для входа) и f_1 (для выхода). На рисунке и в дальнейшем подразумевается $d = d_1$ и $f = f_1$. Пусть число входных и выходных волноводов, а также число волноводов в массиве равно N.

Фильтрация по длине волны для конкретного выходного волновода (или, что то же самое для точки с координатой x) происходит в результате конструктивной интерференции лучей из массива

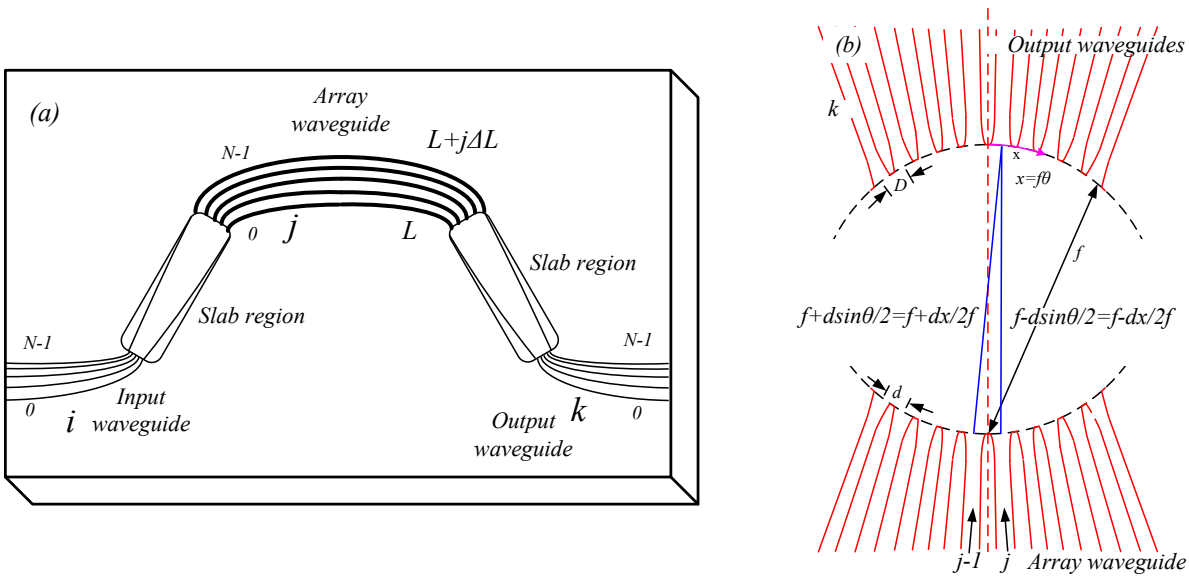

Рисунок 1.2: Структура планарной волноводной решетки: (a) структура полностью (b) увеличенная схема области свободного распространения (из работы [16].)

волноводов [16], т.е.

$$\frac{2\pi n_s(\lambda_0)}{\lambda_0}\left(f_1 - \frac{x_1 d_1}{2f_1}\right) + \frac{2\pi n_s(\lambda_0)}{\lambda_0}\left(f + \frac{xd}{2f}\right) = \frac{2\pi n_s(\lambda_0)}{\lambda_0}\left(f_1 + \frac{x_1 d_1}{2f_1}\right) + \frac{2\pi n_s(\lambda_0)}{\lambda_0}\left(f - \frac{xd}{2f}\right) + \frac{2\pi n_c(\lambda_0)}{\lambda_0}\Delta L + 2m\pi, \quad (1.1)$$

где m — целое число, λ_0 — центральная длина волны, а n_s и n_c — эффективные показатели преломления для зоны свободного распространения и для волноводов из массива соответственно.

Для симметричной решетки ($d = d_1$ и $f = f_1$) данное выражение сильно упрощается:

$$\frac{n_c(\lambda_0)}{\lambda_0}\Delta L + m = 0. \quad (1.2)$$

Получаем $\lambda_0 = n_c \Delta L / m$. Введем следующие величины

$$\Delta\lambda = \frac{n_s dD\lambda_0}{N_c f \Delta L}, \quad N_{\text{ch}} = \frac{\lambda_0 f}{n_s dD}, \quad (1.3)$$

где $\Delta\lambda$ — шаг по длине волны между каналами, а N_{ch} — число каналов внутри свободного спектрального диапазона. $N_c = n_c - \lambda dn_c/d\lambda$ — показатель преломления для групповой скорости в волноводах из массива.

Перейдем из пространства длин волн в пространство частот. Тогда шаг по частоте между каналами определяется как

$$\Delta f = \frac{c}{\lambda^2}\Delta\lambda = \frac{n_s dD}{f\lambda_0} \cdot \frac{c}{\Delta L N_c} = \frac{1}{N_{\text{ch}}} \cdot \frac{1}{\tau}, \quad (1.4)$$

где $\tau = \Delta L N_c / c$. Легко видеть, что τ — это задержка, реализующаяся между соседними волноводами в массиве, а $1/\tau$ — свободный спектральный диапазон в частотном пространстве.

Покажем теперь, что планарная волноводная решетка может осуществлять функцию ДПФ/ОДПФ. Рассмотрим всю решетку как спектральный фильтр. Основываясь на параметрах из Рисунка 1.2 и принимая за точку отсчета вертикальную ось симметрии на Рисунке 1.2(b), импульсный отклик между i-м входом и k-м выходом может быть записан как (формула аналогичная уравнению (1) из работы [18])

$$h_{ik}(t) = \sum_{m=0}^{N-1} \exp\left[-j\pi \frac{n_s d}{\lambda_0}(2m - N + 1)(\sin\theta_i + \sin\theta_o)\right] \cdot \delta\left(t - \frac{n_s f}{c} - N_c \frac{L + m\Delta L}{c}\right), \tag{1.5}$$

где j — мнимая единица, а индексы i и o соответствуют входу и выходу структуры. В этом выражении фазовые соотношения возникают из области свободного распространения, а задержки — как из нее, так и из области волоконной решетки. Слегка упрощая выражения, можно записать

$$\sin\theta_i \approx (2i - N + 1)\frac{D}{2f}, \qquad \sin\theta_o \approx (2k - N + 1)\frac{D}{2f}. \tag{1.6}$$

Положим теперь $N_{\text{ch}} = N$ и пренебрежем постоянной временно́й задержкой, так как она не влияет на окончательный вид передаточной функции. В результате, получаем упрощенное выражение

$$\begin{aligned} h_{ik}(t) &= \sum_{m=0}^{N-1} \exp\left[-j\pi \frac{n_s dD}{\lambda_0 f}(2m - N + 1)(i + k + 1)\right] \cdot \delta(t - m\tau) = \\ &= \sum_{m=0}^{N-1} \exp\left[-j\frac{\pi}{N_{\text{ch}}}(2m - N + 1)(i + k + 1)\right] \cdot \delta(t - m\tau) = \\ &= \sum_{m=0}^{N-1} \exp\left[-j\frac{\pi}{N}(2m - N + 1)(i + k + 1)\right] \cdot \delta(t - m\tau). \end{aligned} \tag{1.7}$$

Подчеркнем, что уравнение (1.7) получено с использованием уравнения (1.4), определяющего условие выбора длины волны. Условие $N_{\text{ch}} = N$ означает, что спектр передачи для планарной волноводной решетки повторяется с периодом $N\Delta\lambda$. Другими словами, свободный спектральный диапазон устройства $1/\tau$ в точности равен расстоянию между соседними частотными диапазонами, каждый из которых содержит N каналов. Такие планарные волноводные решетки называются *циклическими*. Полученное выражение можно интерпретировать следующим образом: N волноводов из области решетки обеспечивают временны́е задержки, а входная и выходная области свободного распространения отвечают за фазовые сдвиги. Если просто рассмотреть фазовые сдвиги в выходной области свободного распространения между l-тым световодом решетки и k-м выходом, получим

$$\theta_{l,k} = 2\pi \frac{n_s dD}{\lambda_0 f}\left(m - \frac{N+1}{2}\right)k. \tag{1.8}$$

Это выражение аналогично уравнению (5) из работы [15] только с другой точкой отсчета фазы.

Рассмотрение случая $N_{\text{ch}} = N$ уже демонстрирует некоторые ключевые отличительные черты функций ДПФ/ОДПФ. Чтобы из уравнения (1.7) получить формулу для ДПФ необходимо подставить номер входного канала $i = N - 1$. Для входного сигнала $s_i(t)$ период наблюдения равен $N\tau$. Сигнал на k-м выходе равен

$$S_k(t) = \int s_i(\tau)h(t - \tau)d\tau = \sum_{m=0}^{N-1} \exp\left[-j\frac{2\pi}{N}\left(m - \frac{N-1}{2}\right)k\right] \cdot s_i(t - m\tau) \tag{1.9}$$

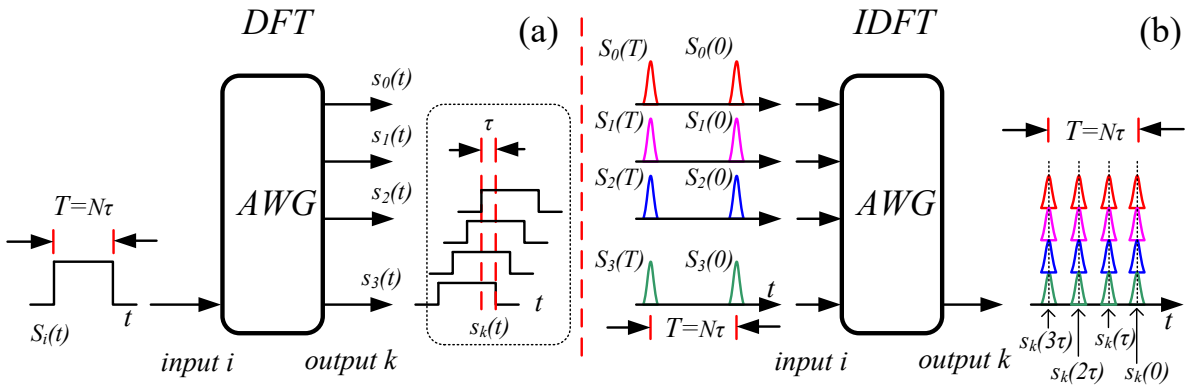

Рисунок 1.3: Конфигурация AWG для реализации (a) ДПФ и (b)ОДПФ

В момент оцифровки, равный $t = (N-1)\tau$, а также с использованием подстановки $n = N/2-m$, получаем

$$S_k[(N-1)\tau] = \sum_{m=0}^{N-1} \exp\left[-j\frac{2\pi}{N}\left(\frac{N-1}{2}-m\right)k\right]\cdot s_i(m\tau) =$$

$$= \sum_{n=0}^{N-1} s_i'\left[\left(\frac{N}{2}-n\right)\tau\right]\cdot \exp\left(-j\frac{2\pi nk}{N}\right)\cdot \exp\left(j\frac{\pi}{N}k\right) = \text{ДПФ}\left(s_i'\left[\left(\frac{N}{2}-n\right)\tau\right]\right)\cdot \exp\left(j\frac{\pi}{N}k\right). \quad (1.10)$$

Легко видеть, что $S_k[(N-1)\tau]$ является результатом ДПФ для серии $s_i'[(N/2-n)\tau]$, которая является циклическим сдвигом $s_i(m\tau)$ на $N/2$ внутри периода $N\tau$ в обратном порядке. Дополнительный множитель $\exp[j\pi k/N]$, просто обозначает дополнительный циклический сдвиг последовательности $s_i'[(n+N/2)\tau]$. И циклический сдвиг и дополнительный фазовый множитель могут быть устранены перенумерацией входов и выходов устройства и выбором другой опорной фазы. Следует обратить внимание, что уравнение (1.10) действительно только для случая, когда все N копий $s_i(t)$ накладываются с разными временны́ми сдвигами. Другими словами, если мы наблюдаем за значением $s_i(t)$ в промежутке $0 \le t < T = N\tau$, то есть лишь временно́е окно с шириной τ, внутри которого реализуется ДПФ, что показано на Рисунке 1.3(a). Таким образом, для считывания сигнала в этом временном окне обычно требуется какое-либо устройство стробирования.

Для получения обратного преобразования, т.е. ОДПФ, положим $k = N-1$. Передаточная функция для каждого из входов становится равной

$$h_i(\tau) = \sum_{m=0}^{N-1} \exp\left[-j\frac{2\pi}{N}\left(m-\frac{N-1}{2}\right)i\right]\cdot \delta(t-m\tau). \quad (1.11)$$

Предположим, что на вход подается множество сигналов $S_i(t)$, где $i \in \{0,1,\ldots,N-1\}$, причем, $S_i(t)$ — это один и тот же временной отсчет.

$$S_i(t) = \begin{cases} S_i(mT), & t = mT \\ 0, & \text{otherwise} \end{cases} \quad (1.12)$$

По-прежнему, рассматривая временной интервал $0 \le t < T = N\tau$, получаем, что имеет значение лишь $S_i(0)$, а выходной сигнал равен

$$s_{out}(t) = \sum_{i=0}^{N-1} \int S_i(\tau)h_i(t-\tau)\,d\tau. \quad (1.13)$$

Рассматривая значение $s_{out}(t)$ в моменты времени $t = m\tau$, где $m \in \{0, 1, \ldots, N-1\}$, получаем

$$s_{out}(m\tau) = \sum_{i=0}^{N-1} \exp\left[-j\frac{2\pi}{N}\left(m - \frac{N-1}{2}\right)i\right] \cdot S_i(0) = \sum_{i=0}^{N-1} S_i(0) \exp\left[-j\frac{2\pi}{N}\left(\frac{N-1}{2}\right)i\right] \cdot \exp\left[-j\frac{2\pi mi}{N}\right]. \tag{1.14}$$

Используя подстановку $n = -N/2 + m$, имеем

$$s'_{out}\left[\left(n + \frac{N}{2}\right)\tau\right] = \sum_{i=0}^{N-1} S_i(0) \exp\left[j\frac{\pi}{N}i\right] \cdot \exp\left[j\frac{2\pi ni}{N}\right] = \text{ОДПФ}\left(S_i(0) \exp\left[j\frac{\pi}{N}i\right]\right). \tag{1.15}$$

Здесь $s'_{out}[(n+N/2)\tau]$ — циклический сдвиг последовательности $s_{out}(m\tau)$ на $N/2$. Как и в предыдущий раз, фазовый множитель $\exp[j\pi i/N]$ лишь соответствует дополнительному циклическому сдвигу для последовательности $s_{out}(m\tau)$.

В конфигурации ОДПФ входной сигнал должен быть дискретным для каждой поднесущей, или по крайней мере с временны́м интервалом τ. В противном случае возникнут помехи от других символов в некоторых из N значений $s_{out}(m\tau)$ из-за задержек сигнала в волноводной решетке. На практике можно использовать N последовательностей данных $S_i(m)$, чтобы индивидуально модулировать N оптических последовательностей коротких импульсов с периодом повторения $T = N\tau$. Результаты ОДПФ получаются на одном из выходов устройства в моменты времени $t = m\tau$, где $m \in \{0, 1, \ldots, N-1\}$.

Приведенные выше рассуждения диктуют выбор важных параметров структуры AWG для реализации ДПФ/ОДПФ и её применения в системах оптического OFDM. Например, если требуется оптический OFDM с 16 поднесущими, разнесенными на 10 ГГц, прибор должен быть 16-портовой циклической планарной волноводной решеткой с шагом по частоте 10 ГГц. Свободный спектральный диапазон прибора, в этом случае составляет 160 ГГц, а следовательно задержка между волноводами решетки равна $\tau = 1/160\,\text{ГГц} = 6.25\,\text{пс}$. Шаг по длине волновода ΔL вычисляется исходя из этой величины задержки. Более того, полученные выражения показывают, что для реализации функционала ДПФ/ОДПФ достаточно конфигурации прибора $1 \times N$, т.е. один вход и N выходов. В дальнейшем, мы будем рассматривать только симметричные решетки $N \times N$ для большей гибкости в построении оптических схем и потенциала для других применений [18]. В то же время, такая расширенная конфигурация не приводит к существенному усложнению дизайна и изготовления прибора в силу его симметричности.

Рассмотрим теперь передаточную функцию AWG в спектральном представлении. Она соответствует преобразованию Фурье уравнения (1.7) и записывается как

$$H_{ik}(f) = \exp[-j\pi(N-1)f\tau] \cdot \sum_{m=0}^{N-1} \exp\left[-j\pi(2m+N-1)\left(\frac{i+k+1}{N} + f\tau\right)\right] = \\ = \exp[-j\pi(N-1)f\tau] \cdot \frac{\sin[\pi(i+k-1+Nf\tau)]}{\sin[\pi(i+k-1)/N + f\tau]} \tag{1.16}$$

Полученные соотношения легко вычисляются численно. На Рисунке 1.4 показаны теоретические спектры пропускания каналов устройства, а также измеренные спектры AWG, разработанной и приобретенной нами на коммерческой основе. Из графика теоретической зависимости видно,

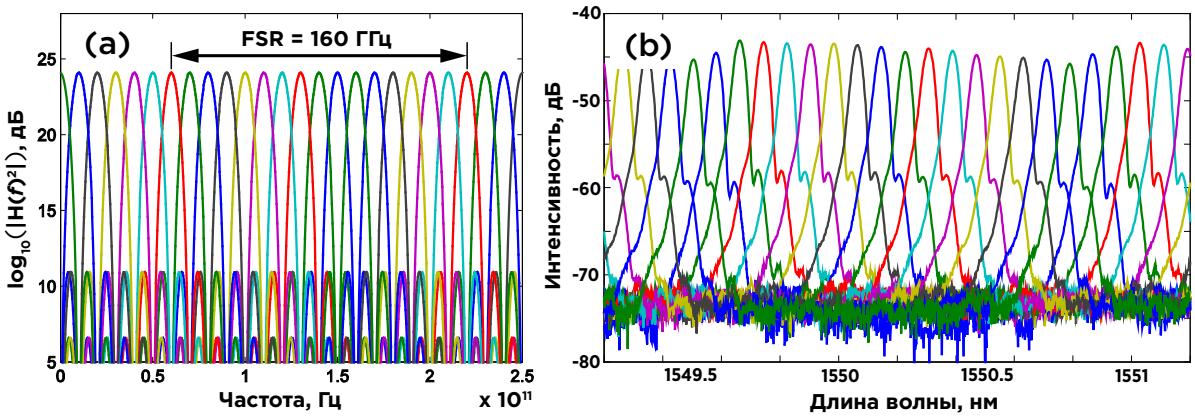

Рисунок 1.4: Теоретические (a) и экспериментально измеренные (b) спектры всех каналов AWG показанные на графике с логарифмической шкалой ординат. Спектры соответствуют решетке с шагом по частоте между каналами 10 ГГц и свободным спектральным диапазоном 160 ГГц.

что каждый канал имеет свободный спектральный диапазон, равный $1/\tau$, а также понятна его ортогональность всем остальным каналам, так как он зануляется на пиках всех других каналов. Типичный профиль спектра пропускания для каждого канала достаточно неплохо приближается гауссовой функцией. На экспериментально измеренных спектрах хорошо заметны искажения по сравнению с теорией, а также некоторая асимметрия. Перекрестные помехи с соседними каналами составляют около -18 дБ. Эти искажения и перекрестные помехи в каналах в основном связаны с фазовыми ошибками, возникшими при изготовлении устройства.

Несмотря на неидеальность полученного устройства, данный подход не является тупиковым, так как существуют методы компенсации фазовых ошибок, которые ранее применялись для исправления формы спектра и уменьшения перекрестных помех в каналах [16, 17]. Хороший экспериментальный результат из работы [16] для сравнения показан на Рисунке 1.5. Этот спектр соответствует 32-х канальному устройству с таким же шагом по частоте — 10 ГГц. Следует обратить внимание, что это устройство разрабатывалось в первую очередь как обычный частотный (де)мультиплексор. Спектральная форма каналов достаточно близка к теоретическим результатам на Рисунке 1.4(a), а перекрестные помехи с соседними каналами составляют около -30 дБ, даже без дополнительной коррекции фазовой ошибки после изготовления прибора.

На Рисунке 1.4(b), также видно отклонение в значении коэффициента пропускания в пределах свободного спектрального диапазона на ~3 дБ. Как поясняется в работе [16] в циклических планарных волноводных решетках обычно присутствует разница в мощности каналов порядка 2.5–3 дБ между центральными и периферийными портами. Влияние неоднородности отклика на функцию ДПФ анализировалось в работе [15] и может быть уменьшена с помощью предварительной коррекции мощности канала.

В результате, можно сделать заключение, что AWG вместе с подходящей системой стробирования, т.е. быстрого измерения амплитуды выходного сигнала, может выполнять функцию ДПФ и ОДПФ. Для соответствия такому преобразованию, решетка должна быть циклической. Преимущество такого использования заключается в том, что для дизайна и изготовления таких устройств

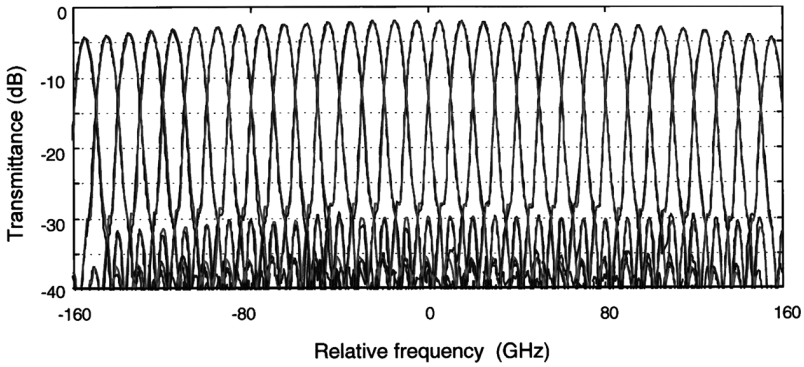

Рисунок 1.5: Спектры 32-х канальной планарной волноводной решетки с шагом по частоте 10 ГГц из работы [16].

применимы результаты многолетних исследований по общей конструкции решеточных фильтров включая методы компенсации фазовых ошибок для уменьшения перекрестных помех с соседними каналами.

Проведем также сравнение с другими схемами оптического ДПФ, предложенными ранее. В работе [12] была разработана оптическая схема, основанная на алгоритме быстрого преобразования Фурье (БПФ) «butterfly», которая реализует преобразование высокой размерности с помощью компоновки нескольких схем БПФ меньшей размерности. Однако, сложность такой схемы, по-прежнему, быстро увеличивается по мере увеличения N. В работе [14] конструкция существенно проще, она использует $N - 1$ последовательных интерферометров задержки для получения полнофункциональной схемы ДПФ/ОДПФ. Тем не менее, она содержит $N - 1$ ответвителей и $N - 1$ фазовых стабилизаторов. Подход с использованием волноводных решеток, требует всего лишь изготовить решетку волноводов и две области свободного распространения для произвольного N. Это намного проще и поэтому может рассматриваться как возможное практическое решение для интегральной оптической схемы ДПФ/ОДПФ с большим N. В настоящее время уже сообщается о волноводных решетках с количеством каналов 128 и 512 при частотном шаге 10 ГГц [19, 20]. Это подтверждает хорошую масштабируемость выбранного нами подхода.

1.1.2. Моделирование применения AWG для линий с OFDM

Для пояснения принципа действия AWG в качестве фильтра ДПФ/ОДПФ приведем результат соответствующего моделирования. Для более полного понимания рассмотрим трансформацию сигналов в системе оптического OFDM как во временном, так и в частотном пространстве. Источником широкополосного когерентного сигнала — гребёнки поднесущих — является лазер с синхронизацией мод. Его сигнал разделяется на поднесущие первой AWG, каждая из поднесущих модулируется и все сигналы складываются в общем канале. На приемной стороне располагается демультиплексор — вторая AWG.

Форма сигналов, проходящих через систему, во временно́м и частотном пространствах показана на Рисунке 1.6. Исходный сигнал, генерируемый лазером с синхронизацией мод, представ-

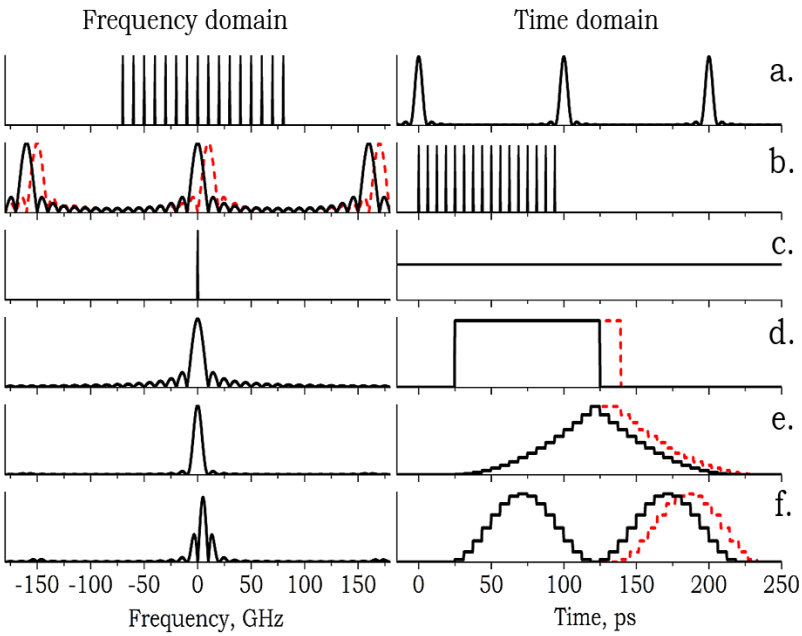

Рисунок 1.6: Временно́е и частотное представление сигналов в ключевых точках предлагаемой схемы OFDM: a. сигнал лазера; b. импульсный отклик для одного из каналов AWG; c. отфильтрованный сигнал лазера (поднесущая OFDM); d. окно модуляции; e. корректно декодированный сигнал; f. некорректно декодированный 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 временно́го представления. В частотном представлении показана амплитуда спектра $|f(\nu)|$, а во временно́м — интенсивность $|f(t)|^2$.

ляет собой последовательность импульсов с частотой повторения 10 ГГц. Для простоты мы предполагаем, что общая полоса генерации лазера составляет в точности один свободный частотный диапазон для AWG, то есть 160 ГГц. Позже в этом разделе будет обсуждаться и более реальная ситуация, в которой ширина линии лазера выходит за его пределы. Поскольку сигнал периодический, его спектр представляет собой набор дельта-функций, как показано на Рисунке 1.6a.

Первая AWG, подключенная к выходу лазера, используется для разделения спектральных линий, то есть для выделения поднесущих OFDM. Центры спектральных каналов AWG при этом должны совпадать со спектральными линиями лазера, поэтому все линии, кроме корректной для данного выхода AWG, блокируются нулями передаточной функции в частотной области. Во временном представлении передаточная функция AWG выглядит как набор из 16 (количество волноводов в решетке) дельта-функций с определенными циклическими фазовыми сдвигами между ними, которые зависят от номера канала N, как показано на Рисунке 1.6b. После прохождения AWG происходит свертка сигнала с передаточной функцией AWG, что эквивалентно умножению в частотном представлении, как показано на Рисунке 1.6c.

Модулятор формирует прямоугольное окно модуляции, показанное на Рисунке 1.6d. В общем случае, размер окна не обязан совпадать с интервалом между импульсами задающего лазера. Однако в классических схемах OFDM эти две величины практически одинаковы. На практике

часто используются несколько более длинные окна модуляции, где это избыточное время обычно называется циклическим префиксом. Для примера такой случай показан на рисунке красной пунктирной линией.

Прохождение сигнала через модулятор эквивалентно умножению во временно́й области. Затем на приемном конце этот сигнал проходит через идентичный AWG, и в зависимости от номера выходного порта он может быть либо корректно (Рисунок 1.6e), либо некорректно (Рисунок 1.6f) декодирован. Как можно видеть, существует определенное временное окно (последние 6.25 пс от символа длиной 100 пс), где корректно декодированный сигнал по существу равен единице, а некорректный — нулю. Легко показать, что все отличные от правильного выходные каналы имеют нули в этом временном окне, и, следовательно, обнаруживается ортогональность каналов. Аналогичная ситуация возникает, если используется более длинное окно модуляции, но в этом случае окно, в котором наблюдается ортогональность сигналов, соответственно растягивается.

В таком подходе принципиальным моментом является синхронность работы всех модуляторов: если окна модуляции для разных каналов будут сдвинуты во времени, окна ортогональности сигналов в разных каналах не будут перекрываться, что приведет к сильным перекрестным помехам. На важность синхронности модулирования и когерентности поднесущих также указывалось в работе [21], где было предложено название «когерентный WDM», а в качестве демультиплексора использовался обычный спектральный демультиплексор. Напротив, в рамках нашей работы предлагается использовать демультиплексор на основе ДПФ для того, чтобы в полной мере использовать истинную ортогональность каналов в определенном временном окне. Можно сказать, что граница между истинным OFDM и традиционным спектральным уплотнением WDM скорее плавная, чем резкая; чем больше растягивается окно модуляции по сравнению с разностью частот между поднесущими, тем уже спектр и, следовательно, тем меньше спектральное перекрытие с остальными каналами. В результате, с увеличением длины циклического префикса происходит плавный переход от OFDM к традиционному спектральному уплотнению.

Практические реализации такого полностью оптического демультиплексирования OFDM сильно страдают от ограниченной полосы пропускания оптических модуляторов и фотодетекторов. На Рисунках 1.7 и 1.8 показаны смоделированные глазковые диаграммы для идеальных устройств и аналогичных устройств с ограниченной полосой пропускания соответственно. Чтобы иметь возможность провести сравнение с нашими экспериментальными результатами, были смоделированы задетектированные сигналы для одного соседнего канала и четырех соседних каналов при частоте модуляции равной разности частот между поднесущими и для частоты 7/8 от этого.

1.1.3. Экспериментальная реализация и результаты

Одним из важных применений фильтра ДПФ/ОДПФ на основе AWG является оптическая передача данных с модуляцией OFDM. Схема демонстрации предлагаемой системы OFDM на базе AWG показана на Рисунке 1.9. Установка спроектирована как прототип полноценной оптической систе-

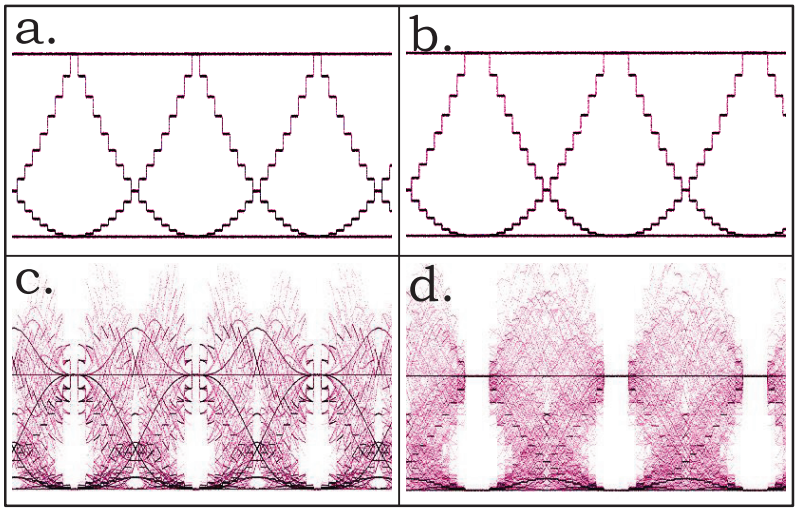

Рисунок 1.7: Смоделированные глазковые диаграммы декодированных сигналов OFDM для случая идеальной модуляции и детектирования без ограничений по полосе пропускания: a. одиночный канал на полной скорости R_0; b. одиночный канал на скорости $7/8R_0$; c. четыре соседних канала, скорость R_0; d. то же с частотой модуляции $7/8R_0$. При этом частота модуляции R_0 соответствует разности частот для соседних поднесущих.

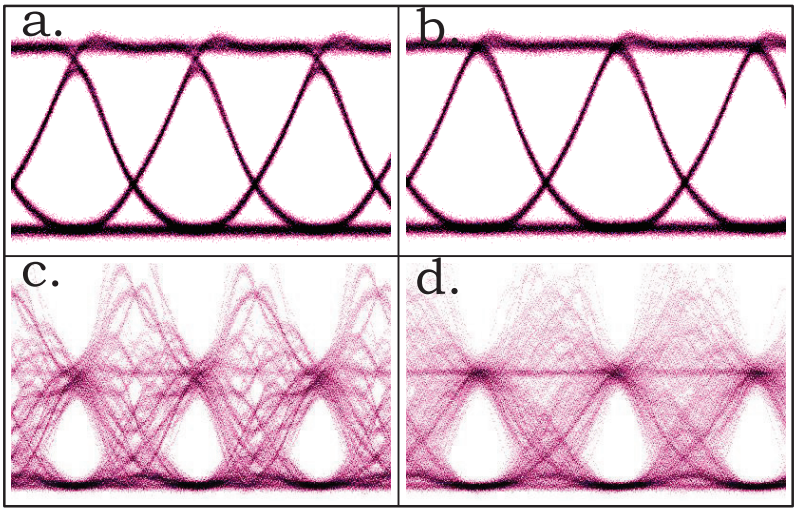

Рисунок 1.8: Те же глазковые диаграммы, что и на Рисунке 1.7, но с ограничением по полосе пропускания. Полоса пропускания модулятора составляет 15 ГГц, а фотодетектора – 30 ГГц, что соответствует компонентам, использованным в экспериментальной демонстрации. Оба устройства моделируются как низкочастотные фильтры Баттерворта 4-го порядка.

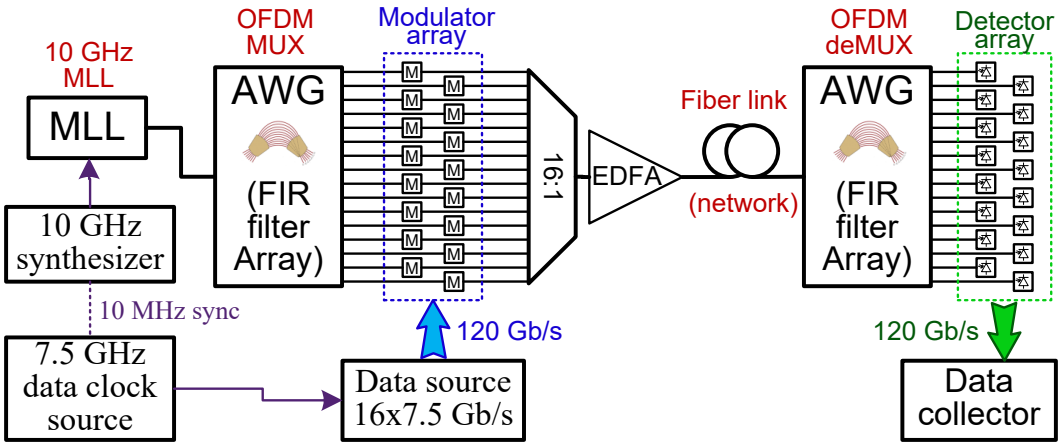

Рисунок 1.9: Предлагаемая экспериментальная установка для реализации 120 Гбит/с оптической линии связи на базе мультиплексирования OFDM с использованием AWG в качестве мультиплексоров-демультиплексоров.

мы OFDM. В качестве источника сигнала используется стабильный по частоте волоконный лазер с синхронизацией мод, который создает поток импульсов с частотой повторения 10 ГГц и длительностью около 2 пс. Таким образом, идеальная скорость передачи символов OFDM составляет 10 Гсимволов/с, а интервал каждого символа составляет 100 пс. В спектральной области поток импульсов соответствует частотной гребенке с центральной длиной волны 1550,84 и шириной полосы по уровню 3 дБ около 1.3 нм, включая 16 линий гребенки. Частотный интервал между соседними поднесущими составляет 10 ГГц (около 0.08 нм).

Выходной сигнал волоконного лазера проходит через AWG, где его спектральные линии разделяются, формируя поднесущие OFDM. Здесь мы используем AWG фактически как демультиплексор длин волн, что было предложено ранее [8, 10, 22]. В данной конфигурации AWG не используется как фильтр ОДПФ, поэтому AWG и разветвитель 16×1 установлены в обратном порядке. Это сделано по двум основным причинам. Во-первых, чтобы использовать AWG в качестве фильтра ОДПФ как показано на Рисунке 1.3, частота повторения входных импульсов должна быть такой же, что и спектральное расстояние между каналами. То есть в этом случае скорость передачи символов жестко фиксирована и равна 10 Гбит/с. В этом случае к сигналу невозможно добавить защитные интервалы между символами для повышения устойчивости системы к искажениям в канале. Во-вторых, использование AWG в качестве фильтра ОДПФ более восприимчиво к неидеальностям устройства, так как через AWG в этом случае проходят уже модулированные поднесущие, а не чистые сигналы из частотной гребенки лазера.

В идеале каждая поднесущая имеет одну единственную оптическую частоту. На практике амплитуда сигнала поднесущей имеет некоторые вариации амплитуды из-за перекрестных помех с соседними спектральными каналами, а также от других свободных частотных диапазонов (± 160 ГГц). Поэтому каждая поднесущая выглядит как практически постоянный сигнал с некоторыми колебаниями амплитуды, как показано на Рисунке 1.10(b). Данный сигнал был измерен стробируемым скоростным осциллографом с оптическим входом.

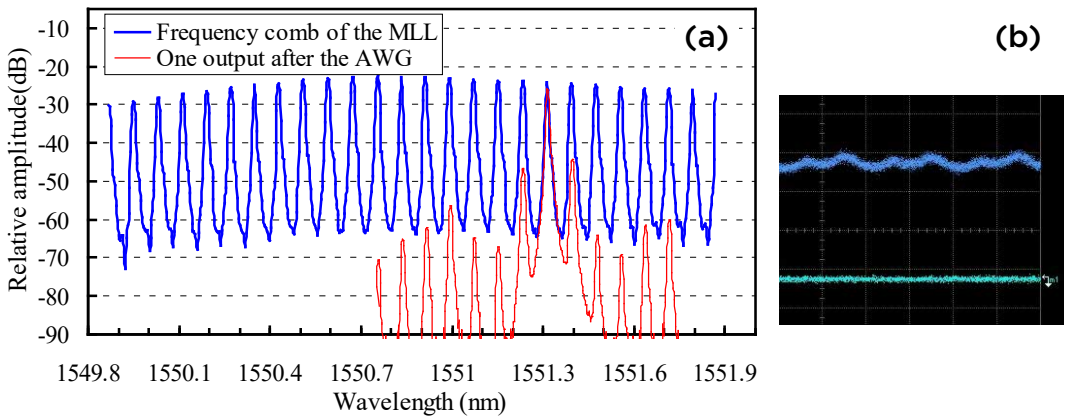

Рисунок 1.10: (a) Исходный спектр лазера с синхронизацией мод, а также его спектр после прохождения AWG в одном из каналов; (b) осциллограмма сигнала на выходе этого же спектрального канала AWG.

AWG, использованные в наших экспериментах, представляют собой две коммерческие циклические планарные волноводные решетки сохраняющих поляризацию, каждая из которых имеет 16 входов, 16 выходов и 16 волноводов в решетке. Спектральное расстояние между каналами составляет 10 ГГц, что соответствует величине шага групповой задержки в решетке волноводов τ = 100 пс/16 = 6.25 пс. Свободный спектральный диапазон составляет $1/\tau$ = 160 ГГц. Спектр пропускания устройства показан на Рисунке 1.4(b). Во всех экспериментах используется только одна поляризация. Тем не менее, в литературе есть сообщения о поляризационно-нечувствительных AWG [17, 20].

После разделения поднесущих каждая из них модулируется отдельным потоком данных, и все модулированные поднесущие смешиваются с другими поднесущими в оптоволоконном объединителе 16 × 1. Ключевым требованием для реализации OFDM является выравнивание модулированных символов на всех поднесущих по времени, что кардинальным образом отличает его от традиционного асинхронного спектрального разделения каналов. Формат модуляции для каждой поднесущей может выбираться независимо, однако все изменения фазы и амплитуды должны происходить одновременно во всех каналах, чтобы обеспечить ортогональность каналов, подразумеваемую в OFDM. Более того, в идеальном случае переходы между соседними символами модуляции для каждой из поднесущих должны происходить мгновенно [15], а в течение всей длительности каждого символа все фазы и амплитуды должны оставаться постоянными.

На принимающей стороне сигнал OFDM демультиплексируется через AWG и после этого детектируется. В нашей экспериментальной демонстрации фильтру на AWG требуется 93.75 пс (задержка между самым коротким и самым длинным волноводом решетки) для установления после изменения фазы и/или амплитуды. Следовательно, в течение длительности символа, равной 100 пс, остается лишь последнее временное окно в 6.25 пс для измерения значений амплитуды и фазы. Именно в течение этого временного окна все поднесущие полностью ортогональны между собой. При этом любая ошибка выравнивания символов на разных поднесущих по времени приводит к дополнительным перекрестным помехам между каналами в течение этого временного

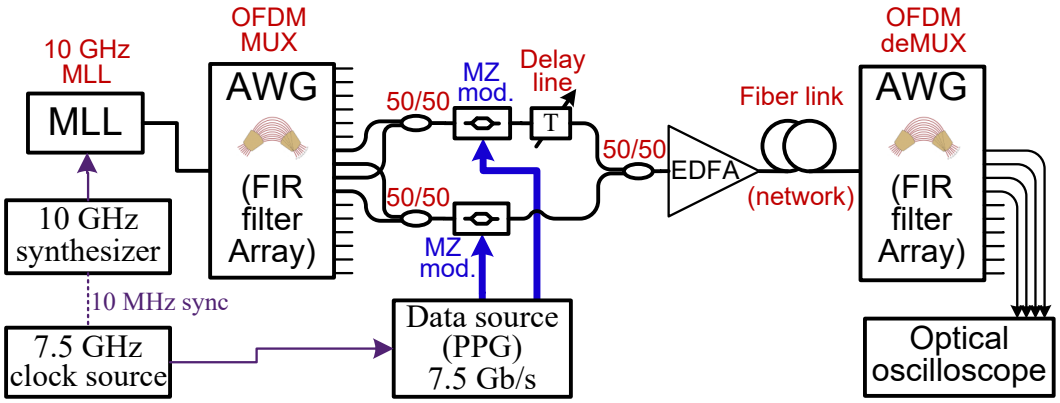

Рисунок 1.11: Продемонстрированная экспериментальная установка. MLL – лазер с синхронизацией мод, MZ mod. – интерферометр Маха-Цандера, EDFA – эрбиевый волоконный усилитель.

окна.

Такое короткое окно детектирования требует сверхбыстрых полностью оптических устройств стробирования для получения результата ОДПФ. Кроме того искажения сигнала из-за несовершенства используемых устройств а также в линии связи негативно влияют на принимаемый сигнал в этом временном окне. В экспериментальной реализации в поток символов модуляции вставляются защитные интервалы для компенсации эффекта конечного времени переключения модуляторов и для увеличения временного окна, доступного для считывания данных. Защитные интервалы могут легко регулироваться по длительности путем изменения частоты модуляции данных, поскольку все поднесущие после разделения в первой AWG являются непрерывными сигналами, а увеличение периода модуляции не сказывается на выполнении условий OFDM. Продемонстрированная экспериментально скорость передачи данных составляет 7.5 Гбит/с на каждую поднесущую, то есть длительность каждого символа составляет 133 пс. Ниже приводится дополнительная информация, которая иллюстрирует влияние изменения скорости модуляции на систему OFDM.

Из-за ограничений доступного оборудования экспериментально была продемонстрирована конфигурация, показанная на Рисунке 1.11, где используются только четыре соседних поднесущих. Мы считаем, что наличия четырех поднесущих достаточно для демонстрации принципов мультиплексирования OFDM, так как перекрестные помехи между соседними каналами намного сильнее, чем помехи от каналов с бóльшим спектральным разделением. Эти четыре канала разделены на две группы (нечетные и четные) и промодулированы разными потоками данных.

Сначала были изучены эффекты изменения скорости модуляции. Результаты измерений показаны на Рисунке 1.12. На нем показаны оптические спектры четырех последующих каналов OFDM, модулированных со скоростью 5, 7.5 и 10 Гбит/с. Как можно видеть, более высокие скорости модуляции приводят к большему спектральному перекрытию между каналами. При модуляции с низкой скоростью (< 5 Гбит/с) система ведет себя аналогично обычным системам спектрального уплотнения. Все каналы оказываются независимыми, поскольку спектры каналов заметно не перекрываются. Однако при более высокой скорости модуляции они начинают перекрываться, проявляя свойства присущие OFDM. Последний спектр на Рисунке 1.12 соответствует

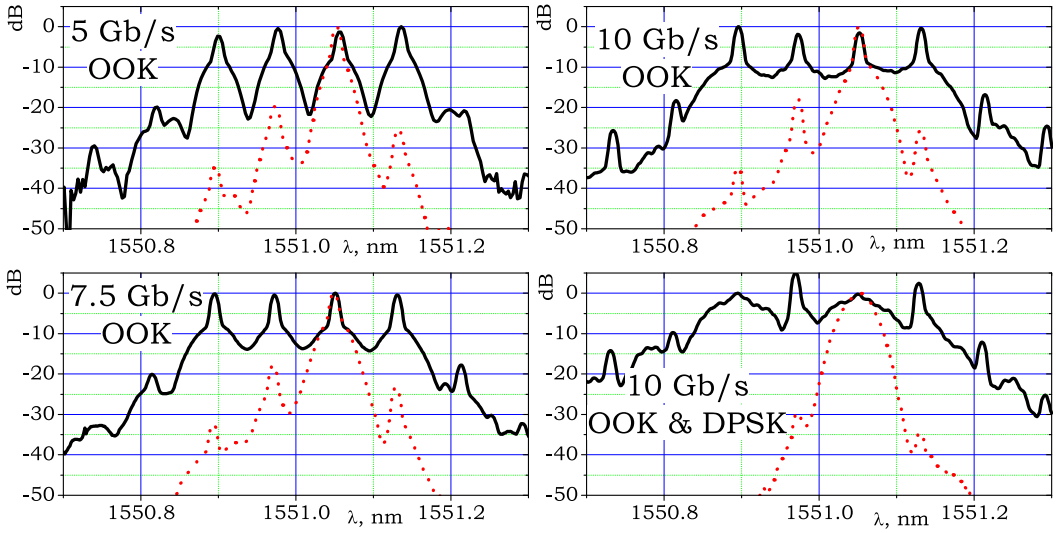

Рисунок 1.12: Измеренные спектры четырех модулированных и мультиплексированных OFDM каналов, а также результат демультиплексирования одного из них. Спектры показаны для разных скоростей модуляции (5, 7.5 и 10 Гбит/с) и разных типов модуляции (OOK – on/off keying – бинарная амплитудная модуляция, DPSK – differential phase shift keying – дифференциальная бинарная фазовая модуляция.)

случаю смешанной модуляции, где два канала модулируются по амплитуде, а два других используют дифференциальную бинарную фазовую модуляцию, которая подавляет несущую частоту. Пунктирные линии на всех спектрах показывают результат демультиплексирования каналов на второй AWG.

Результаты временны́х измерений представлены на Рисунке 1.13. Глазковые диаграммы (a) и (b) показывают демодуляцию одного канала OFDM при разных скоростях модуляции. При амплитудной модуляции со скоростью 7.5 Гбит/с на диаграмме наблюдается широкое раскрытие, в то время как при 10 Гбит/с качество сигнала существенно ухудшается. Это согласуется с теоретическим предсказанием размера окна выборки в 6.25 пс, что короче, чем время отклика нашей системы детектирования. Для сравнения, глазковая диаграмма на Рисунке 1.13(c), соответствующая фазовой модуляции со скоростью 10 Гбит/с, показывает более широкое раскрытие. Такая тенденция ранее наблюдалась в подобных экспериментах [23]. Это происходит из-за лучшей устойчивости бинарной фазовой модуляции к спектральной фильтрации по сравнению с бинарной амплитудной модуляцией. Из-за ограничений, связанных с оборудованием, фазовая модуляция не использовалась для дальнейших измерений. Следует отметить, что аналогичная система с квадратурной фазовой модуляцией была исследована с помощью моделирования [15], которое показало лучшую спектральную эффективность и бóльшую скорость передачи данных.

После тестирования одного канала была выполнена оценка работы системы для всех четырех активных каналов. Полученные глазковые диаграммы для одного из средних каналов представлены на Рисунке 1.14. В верхнем ряду показаны глазковые диаграммы демультиплексированного канала OFDM при скорости модуляции 5, 7.5 и 10 Гбит/с соответственно. Модуляция всех че-

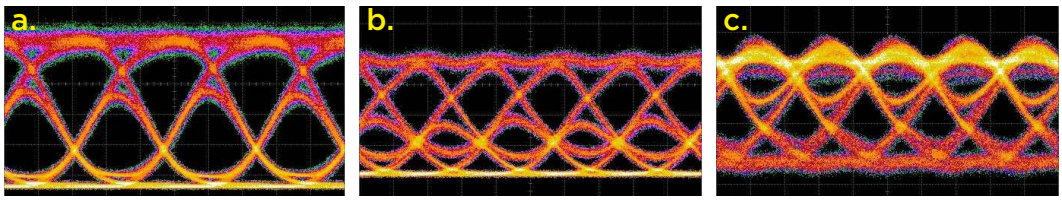

Рисунок 1.13: Глазковые диаграммы для одной поднесущей, прошедшей через мультиплексор и демультиплексор OFDM. (a) 7.5 Гбит/с бинарная амплитудная модуляция; (b) 10 Гбит/с бинарная амплитудная модуляция; (c) 10 Гбит/с дифференциальная бинарная фазовая модуляция

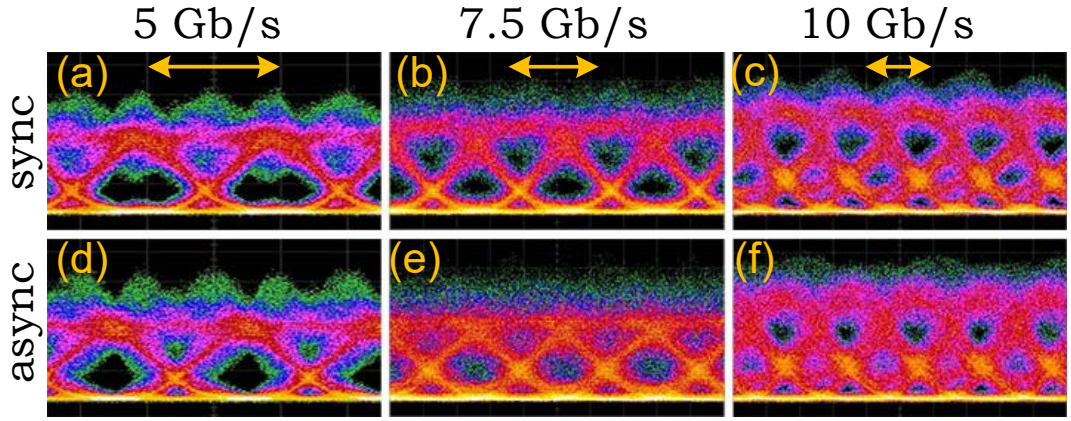

Рисунок 1.14: Измеренные глазковые диаграммы для передачи OFDM с четырьмя активными каналами. В разных колонках используется разные скорости модуляции, а в разные строчки соответствуют синхронной и асинхронной модуляции.

тырех каналов была полностью выровнена по времени, что достигалось регулировкой линии задержки между каналами. Теоретически, если применять быстрое временно́е стробирование, раскрытие глазковых диаграмм на разных скоростях должно быть одинаковым из-за ортогональности всех поднесущих. В нашем эксперименте с фотоприемником, ограниченным полосой пропускания 30 ГГц наблюдались чистые раскрытия диаграммы на скорости 5 Гбит/с с длительностью ~80 пс. При скорости модуляции 7.5 Гбит/с раскрытие становится короче по времени (~30 пс), но все равно остается чистым. Модуляция со скоростью 10 Гбит/с не позволяет детектировать переданную информацию без быстрого временно́го стробирования, что приводит к закрытию глазковой диаграммы при измерениях осциллографом.

Чтобы доказать важность выравнивания символов на всех поднесущих во времени и показать отличие нашей системы от традиционной системы со спектральным уплотнением, были изучены эффекты изменения относительной задержки между каналами. Результаты измерений показаны в нижнем ряду Рисунка 1.14. Изменение задержки при скорости модуляции 5 Гбит/с на ~80 пс приводит к значительному уменьшению раскрытия глазковой диаграммы, поскольку переходы в разных поднесущих появляются в разное время. Изменение задержки на ~70ps при скорости модуляции 7.5 Гбит/с приводит к полному закрытию диаграммы. Глазковая диаграмма со смещенной по времени модуляцией на скорости 10 Гбит/с демонстрирует дальнейшее ухудшение качества принятого сигнала.

Наблюдаемые свойства присущи лишь OFDM, который основан на *ортогональности* символов на соседних поднесущих. Таким образом, полученные результаты указывают на то, что наша демонстрация принципиально отличается от тривиального спектрального уплотнения. Сделанные измерения подтверждают успешность реализации OFDM с использованием AWG. Полученная глазковая диаграмма при скорости модуляции 7.5 Гбит/с показывает возможность эксплуатации такой системы с обеспечением передачи данных со скоростью 16×7.5 Гбит/с = 120 Гбит/с. Продемонстрированное сосуществование амплитудной и фазовой модуляции в системе показывает потенциал для решения OFDM, прозрачного по отношению к формату модуляции.

1.1.4. Выводы

Было продемонстрировано, что планарные волноводные решетки AWG могут полностью оптически выполнять функцию дискретного преобразования Фурье без всяких активных элементов. Это достигается при использовании так называемой 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.

1.2. 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 бинарная, 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

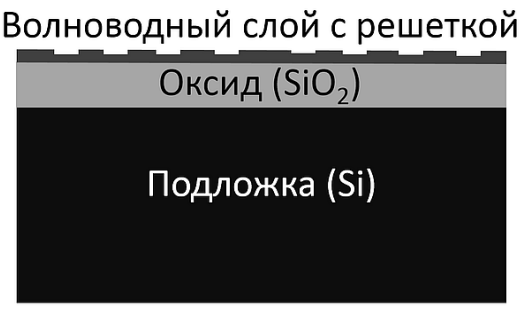

Рисунок 1.15: Структура поперечного сечения чипа для оптических устройств на базе цифровой планарной голографии.

спектральными фильтрами. В результате, с помощью планарной голограммы можно реализовать большое количество оптических приборов, примеры которых продемонстрированы в настоящем разделе: начиная от разделения излучения по длинам волн и заканчивая перспективной платформой для реализации оптических интерконнектов на чипе.

Простейшая структура такого чипа показана на Рисунке 1.15. На кремниевой подложке выращивается слой термального оксида, на который наносится волноводный слой с повышенным показателем преломления. Волноводный слой может быть как допированным оксидом, чаще всего Si_3N_4 или смешанным оксидом-нитридом, так и аморфным кремнием. Во втором случае такая платформа называется «silicon over insulator, SOI» и подходит только для длин волн более 1.3 мкм, соответствующих окну прозрачности кремния. Ключевым параметром волноводного слоя является контраст показателя преломления по сравнению с нижней „оболочкой“ из оксида. Чем выше разница показателей преломления, тем более компактные устройства можно изготавливать, так как становится возможным реализация изогнутых волноводов с меньшим радиусом поворота. Контраст показателя преломления максимален для структур типа SOI, поэтому они являются основными для устройств, работающих на телекоммуникационной длине волны 1.55 мкм.

Для реализации устройств на базе цифровой планарной голографии требуется одномодовый волноводный слой, т.е. такой, в котором есть лишь одна поддерживаемая пространственная конфигурация электромагнитного поля вдоль нормали к плоскости волновода. При этом возможны две поляризационные моды: TE, в которой электрическое поле лежит в плоскости волновода и TM, в которой так расположено магнитная составляющая поля. В соответствии с названием (transverse electric и transverse magnetic), соответствующее поле не имеет составляющей вдоль оси распространения. Типичная толщина волноводного слоя составляет 750 нм при контрасте показателя преломления 3%.

После формирования планарной волноводной структуры, на волноводе реализуется голограмма. Это делается методами литографии за один цикл травления. Обыкновенно, это нанесения резиста, его экспонирование либо фотошаблоном либо прорисовкой электронным пучком, и реактивное ионное травление (RIE). Обычно глубина травления составляет лишь долю толщины волноводного слоя, что приводит к небольшому локальному изменению показателя преломления, необходимому для получения голограммы. Полученную структуру можно закрыть верхним слоем

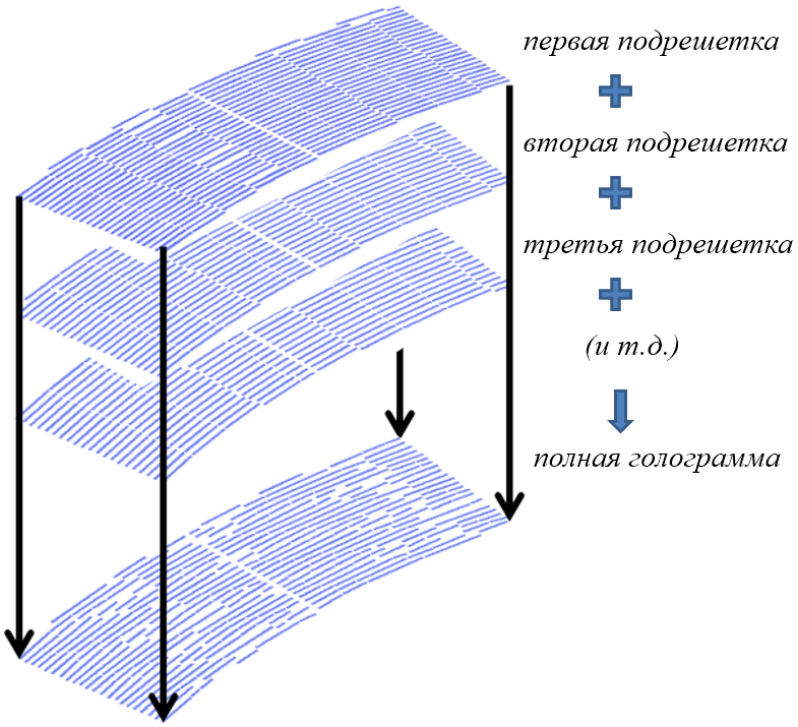

Рисунок 1.16: Синтез голограммы как суперпозиция разных подрешеток.

оксида, для защиты волноводного слоя от грязи и других воздействий окружающей среды. Также, возможно сформировать линейные волноводы с помощью второго цикла травления на бóльшую глубину. К таким волноводам, выходящим на торец чипа можно приклеить внешние световоды для ввода и вывода излучения.

Рассмотрим для примера синтез голограммы для реализации спектрометра высокого разрешения на чипе. Вся голограмма — это суперпозиция подрешеток, каждая из которых связывает два волновых фронта, входной и выходной, между собой, как показано на Рисунке 1.16. 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, см. Рисунок 1.17. Их можно совместить, например, с пикселями светочувствительной линейки, с помощью которой осуществляется прием и оцифровка полученных спектров. Изготовленное устройство, приклеенное к светочувствительной линейке показано на Рисунке 1.18.

Представленная технология цифровой планарной голографии является универсальной платформой для реализации оптических чипов с различной функциональностью. В процессе исследований, проведенных компанией Nanooptic Devices, LLC, были разработаны средства для синтеза, подготовки чертежей, а также для симуляции получаемых структур. Были изготовлены десятки работающих чипов, в частности, спектрометров [24], была достигнута поразительная согласованность результатов симуляции и фактических результатов измерений на изготовленных структу-

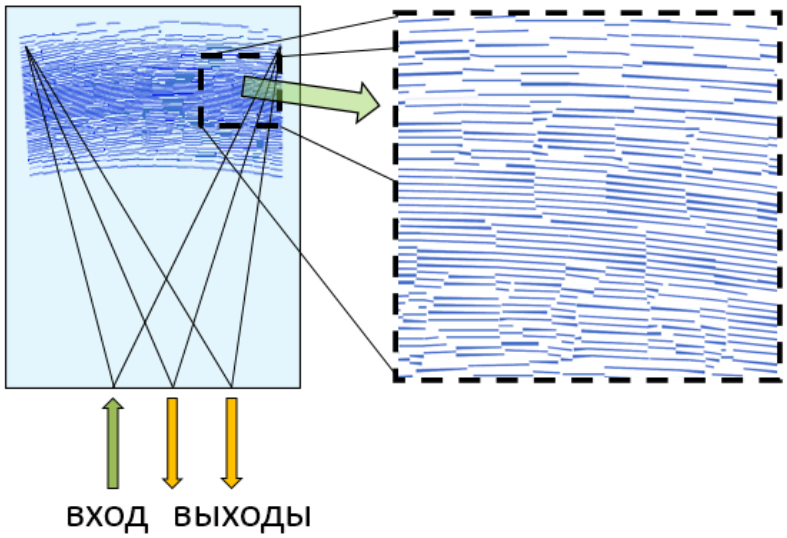

Рисунок 1.17: Принцип действия простейшего устройства на чипе, сформированного из фокусирующих Брэгговских отражателей.

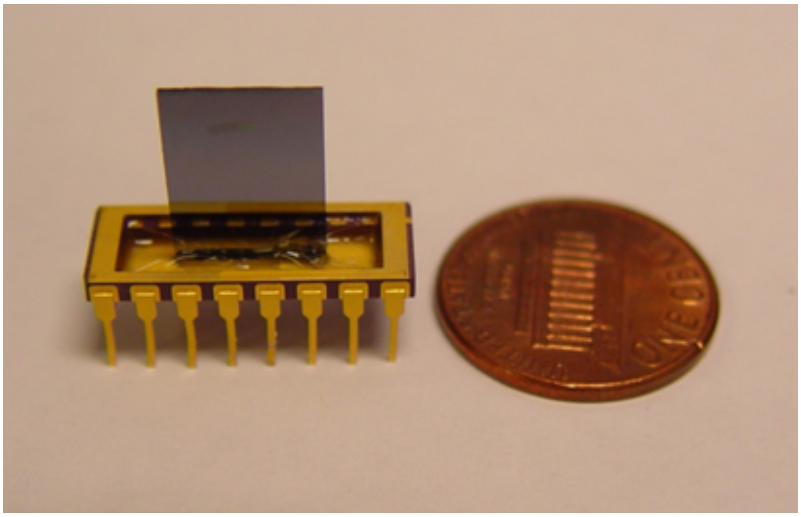

Рисунок 1.18: Пример изготовленного устройства с помощью цифровой планарной голографии — спектрометр на чипе со спектральным разрешением 0.2 нм, приклеенный к ПЗС линейке. Рабочий диапазон длин волн 475-567 нм.

рах.

В результате, возник вопрос о возможности использования данной технологии для реализации различных устройств, связанных с передачей и представлением информации. Мы на симуляциях исследовали возможности планарных голограмм и получили результаты, представленные в следующих двух разделах.

1.2.1. Применение методов цифровой планарной голографии для реализации устройств модуляции/демодуляции

С ростом спроса на высокоскоростную волоконно-оптическую связь в ней стали находить применение прогрессивные методы мультиплексирования и модуляции, заимствованные из беспроводной связи. Некоторые из них, такие как квадратурная фазовая модуляция (QPSK), активно выходят на рынок. Другие, такие как оптический множественный доступ с кодовым разделением каналов (CDMA), предлагается использовать в будущих пассивных оптических сетях (PON). Очевидно, все упомянутые технологии для своего практического применения требуют соответствующих кодеров/декодеров с высоким уровнем интеграции. В этом разделе будут представлены такие устройства в полностью интегральном исполнении, основанные на цифровой планарной голографии. Это оптические демодуляторы QPSK (так называемый, 90-degree optical hybrid), демодуляторы QPSK с одновременным демультиплексированием WDM, а также спектрально-фазовые кодеры/декодеры для когерентного оптического CDMA [25], реализующие весь кодовый набор на одном чипе.

Чипы изготавливаются по технологии цифровой планарной голографии [24], которая подразумевает нанесение на поверхность волноводного слоя чипа специальной синтезированной оптической голограммы, что реализуется с помощью простой одноступенчатой литографии. Голограмма предназначена для отражения определенных диапазонов длин волн входящего сигнала в несколько выходных фокальных точек, обеспечивая требуемые спектральные фазовые соотношения между ними. В отличие от традиционных устройств на базе одномерных волноводов на чипе, таких как волноводные решетки (AWG), голограмма потенциально более многофункциональна, так как позволяет в более полной мере использовать преимущества всего двухмерного пространства волновода и, таким образом, реализовать более широкий спектр возможностей.

Изначально цифровая планарная голография была разработана для оптических спектрометров высокого разрешения на чипе. Однако, она оказалась чрезвычайно эффективной с точки зрения размера устройства и простоты его изготовления [26]. Множество итераций по синтезу, изготовлению и оптимизации дизайна голограммы по результатам экспериментальных измерений помогли создать программную среду для проектирования и моделирования, которая обеспечивает хорошее согласие с экспериментами и позволяет расширить спектр функций, которые может выполнять голограмма. Здесь представлены новые концепции разработанных спектрально-фазовых устройств на чипе, реализованных по данной технологии.

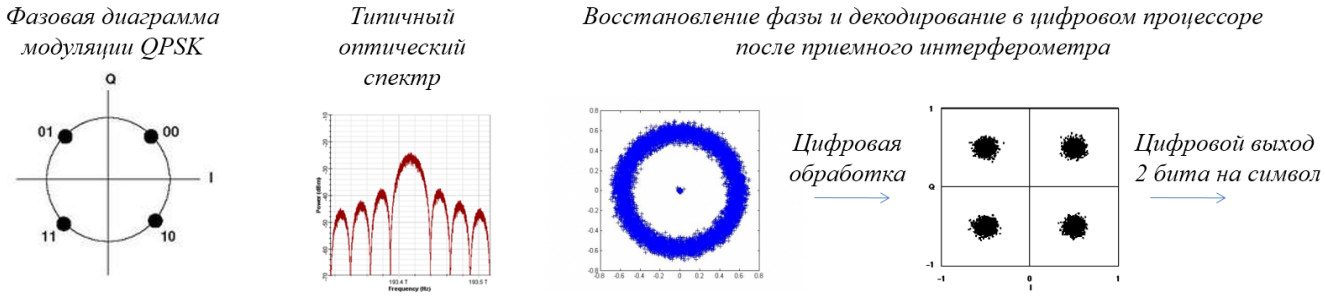

Рисунок 1.19: Квадратурная фазовая модуляция — принципы кодирования и декодирования.

Демодуляторы QPSK

Квадратурная фазовая модуляция используется для представления информации в виде потока оптического излучения. При этом, информация представляется в виде фазы оптического сигнала, которая выбирается в виде одного из четырех определенных значений — квадратурных состояний, как показано на Рисунке 1.19. Таким образом, один символ представляет сразу два бита информации. За счет этого достигается большая спектральная эффективность, чем при амплитудной модуляции. Кроме того, такая модуляция является модуляцией с подавлением несущей, т.е. на спектре сигнала отсутствует яркая спектральная линия на нулевой частоте модуляции (см. Рисунок 1.19). В результате, вся передаваемая мощность переносит информацию, повышается эффективность использования оптической мощности. Кодирование происходит с помощью амплитудной модуляции прямого и квадратурного каналов, т.е. самой несущей и ее копией, сдвинутой по фазе на $\pi/2$. Декодирование осуществляется с помощью сбивания принятого сигнала с сигналом локального осциллятора (гомодина), причем также в двух вариантах: без дополнительного фазового сдвига и со сдвигом на $\pi/2$. В результате, восстанавливается как нормальная, так и квадратурная составляющая, обычно называемые I и Q соответственно. Техническая сложность демодуляции также заключается в том, что локальный осциллятор всегда немного отстроен по частоте от передающего лазера. Из-за этого фазовое „созвездие“ постоянно вращается по фазе с неопределенной скоростью, что условно показано на том же рисунке. Коррекция такого фазового вращения производится специализированным цифровым процессором, который в реальном времени отслеживает разность фаз между передатчиком и гомодином приемника. Вычитая найденное вращение из принятого сигнала, в процессоре вычисляются стационарные I и Q компоненты, по которым восстанавливаются переданные биты.

Для реализации квадратурной фазовой модуляции (QPSK) необходим оптический демодулятор, с помощью которого происходит декодирование информации. Дизайн соответствующей голограммы очень прост: это устройство с двумя входами и четырьмя выходами. От каждого из входов свет отражается на все четыре выхода параболическими отражателями в виде брэгговских решеток, расположенных таким образом, что достигаются требуемые фазовые сдвиги, как показано на Рисунке 1.20. Другими словами, голограмма представляет собой наложение 8 таких отражателей, каждый из которых занимает всю площадь чипа. Посредством разработанных методов аппроксимации и дискретизации, получаемая суперпозиция преобразуется в бинарную маску,

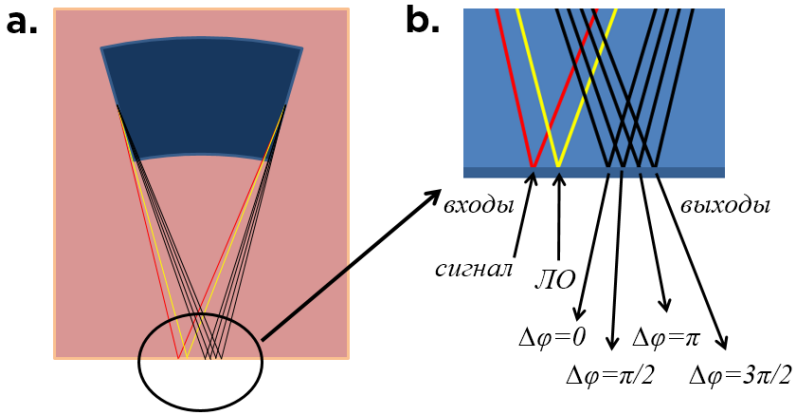

Рисунок 1.20: Принцип действия голографического демодулятора QPSK.

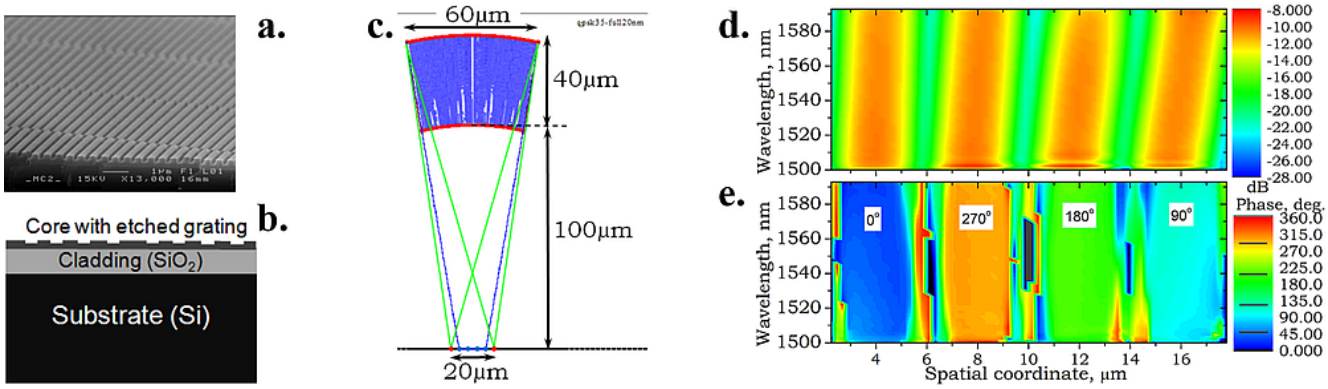

Рисунок 1.21: Голографический демодулятор QPSK. **a.** пример изготовленной голограммы; **b.** поперечная структура голограммы на базе платформы SOI; **c.** схема синтезированного дизайна и его размеры; **d.** зависимость интенсивности выходного сигнала от длины волны и координаты в выходной плоскости; **e.** выходная фаза в зависимости от длины волны и координаты.

представляющую протравленные и непротравленные области соответственно. На Рисунке 1.21 показана соответствующая голограмма, спроектированная для платформы SOI, т.е. кремниевого планарного световода на слое оксида.

На синтезированной структуре, схожей с показанной на Рисунке 1.21a изготовленной голограммой, ширина вытравленных штрихов составляет четверть эффективной длины волны ($\lambda/4$) в волноводе. Для платформы SOI и диапазона длин волн 1550 нм она составляет около 120 нм, что относительно легкодоступно для современных литографических технологий изготовления как с помощью фотомасок, так и путем наноимпринта [27]. На схеме на Рисунке 1.21c показаны два входа (две красные точки внизу) и четыре выхода (синие точки), расположенных с шагом 4 мкм. Голограмма, расположенная наверху, собирает излучение со входов и доставляет его на выходы.

Работа устройства моделировалась с помощью численного решения двумерного уравнения Гельмгольца [26]. Результаты моделирования, показывающие разность фаз и интенсивность отраженного света в зависимости от длины волны и пространственной координаты, показаны на Рисунке 1.21d,e. Видна хорошая однородность по длине волны в диапазоне 1510-1580 нм. Избыточные световые потери в устройстве оцениваются в 2 дБ (помимо коэффициента разделения в

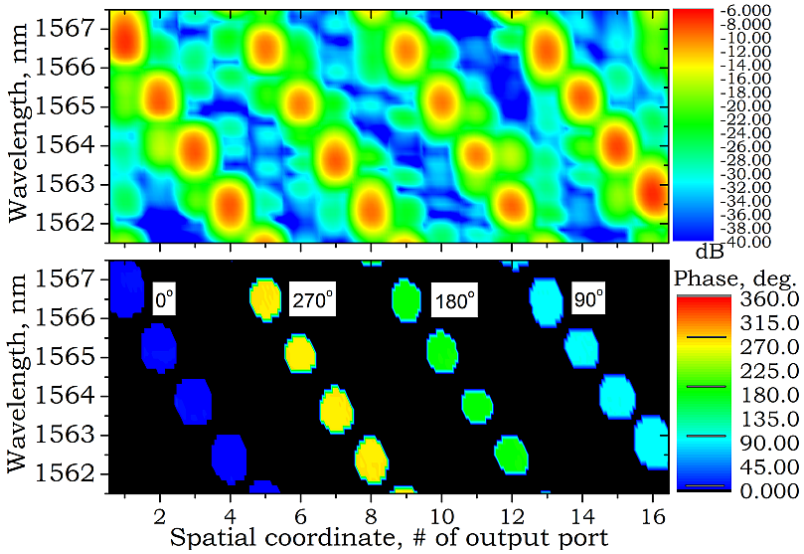

Рисунок 1.22: Результаты моделирования для голограммы демультиплексора WDM, объединенного с демодулятором QPSK. На графиках показана зависимость интенсивности (вверху) и фазы от длины волны и пространственной координаты.

6 дБ), а фазовая погрешность составляет менее 10°.

В реальных высокоскоростных волоконно-оптических линиях связи QPSK-модуляция может использоваться совместно со спектральным уплотнением (WDM). В этом случае, приемник должен реализовывать как демультиплексирование WDM, так и демодуляцию QPSK. Типовое решение заключается в использовании двух различных устройств для решения двух этих задач. Однако, для повышения уровня интеграции, снижения общей стоимости и уменьшения оптических потерь, возможно совмещение двух этих функций на одном чипе.

На Рисунке 1.22 показан дизайн голограммы одновременно реализующей демодуляцию QPSK для различных WDM каналов. Устройство рассчитано на четыре длины волны с интервалом 160 ГГц (около 1,29 нм) между каналами. Длина голограммы L, удовлетворяет условию $\Delta\lambda/\lambda \approx \lambda/L$ и составляет около 0,6 мм. Устройство имеет четыре выхода на каждую из длин волн, а его голограмма представляет собой суперпозицию 32 отражающих решеток, которые доставляют излучение с двух входов на 16 выходов с определенными фазовыми соотношениями.

Кодер/декодер для спектрально-фазового когерентного оптического CDMA

CDMA или множественный доступ с кодовым разделением — технология широкополосного мультиплексирования каналов, разработанная в первую очередь для военных применений. Позже, эта технология мультиплексирования активно использовалась в сотовых сетях второго поколения, в том числе в Российской Федерации (сотовая сеть «CONET»/ОАО «Персональные коммуникации», 1995-2004). Его преимущества заключаются как в масштабируемом, за счет использования динамически присваиваемых кодов, пространстве мультиплексирования, так и в повышенной защищенности от прослушивания на физическом уровне.

Спектрально-фазовый когерентный оптический CDMA — это одна из возможных оптических

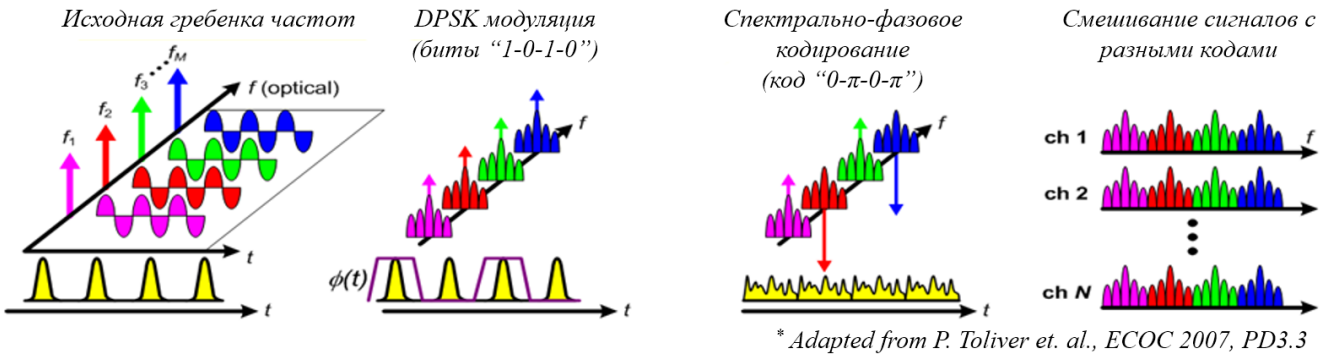

Рисунок 1.23: Схема формирования сигналов в спектрально-фазовом оптическом CDMA. Широкополосный когерентный сигнал, например, частотная гребенка из импульсного лазера с синхронизацией мод, модулируется данными, например с помощью дифференциально-фазового кодирования, расщепляется по спектру на частотные компоненты к которым добавляются определенные фазовые сдвиги для формирования кода. При этом во временно́м представлении, короткие импульсы превращаются в хаотичные сигналы, которые можно смешивать с сигналами других передатчиков оптического CDMA.

реализаций технологии CDMA. Такой способ мультиплексирования обладает преимуществом высокой спектральной эффективности и повышенной конфиденциальности данных [28]. Соответствующие спектрально-фазовые коды синтезируются путем добавления фазовых сдвигов, равных 0 или π, к различным частотным компонентам когерентного широкополосного оптического источника, обычно, импульсного лазера с синхронизацией мод, используемого в передатчике, как показано на Рисунке 1.23. Сигналы, закодированные разными кодами, могут быть смешаны в общей среде распространения, а на приемной стороне могут быть разделены из-за взаимной ортогональности используемых кодов. Схематично, процесс декодирования показан на Рисунке 1.24. Современные интегрально-оптические технологии спектрально-фазового кодирования/декодирования реализуют только один код в каждом устройстве, как в случае кодера на основе кольцевых резонаторов [29] так и для кодеров на основе волоконной брэгговской решетки [30].

В настоящей работе были спроектированы интегральные голографические спектрально-фазовые кодеры/декодеры, способные обрабатывать полный набор возможных кодов на одном чипе. Для примера было разработано устройство на базе планарного волновода из допированного кварцевого стекла с контрастом показателя преломления 3%. Кодер реализует полный набор из четырех кодов Уолша-Адамара с четырьмя длинами волн, разнесенными на 40 ГГц. Общая ширина спектра составляет 160 ГГц с центральной длиной волны 1556 нм. Устройство занимает площадь 7x5 мм на кристалле, имеет один вход и четыре выхода, соответствующие четырем кодам. На Рисунке 1.25 показаны фазовые профили для четырех выходов в зависимости от длины волны. Четыре кода описываются фазовыми диаграммами $(0,0,0,0)$, $(0,\pi,0,\pi)$, $(0,0,\pi,\pi)$ и $(0,\pi,\pi,0)$, которые составляют полный набор ортогональных спектрально-фазовых кодов Уолша-Адамара размерности 4. Также там показаны амплитудно-частотные характеристики четырех получаемых кодов.

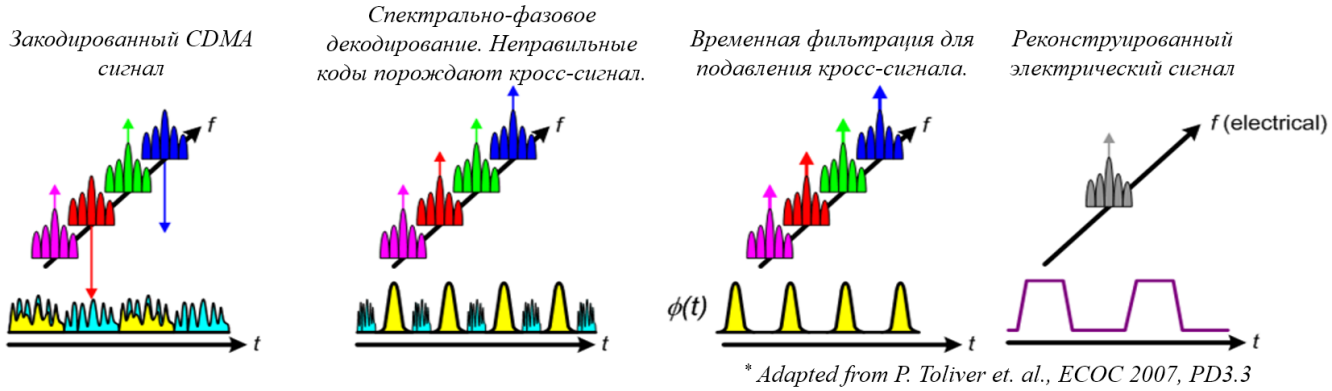

Рисунок 1.24: Схема декодирования сигналов в спектрально-фазовом оптическом CDMA. Входящий сигнал расщепляется на спектральные компоненты, после чего на них накладываются фазовые сдвиги, соответствующие конкретному коду. Далее все спектральные компоненты объединяются. Сигнал, соответствующий выбранному коду, преобразуется в исходные лазерные импульсы — так называемые автокорреляционные пики. Излучение от других кодов остается хаотичным и обычно называется кросс-сигналом или кросс-корреляцией. Такой смешанный сигнал фильтруется по времени для отделения автокорреляционных пиков от кросс-сигналов, после чего происходит демодуляция полученного сигнала и его детектирование.

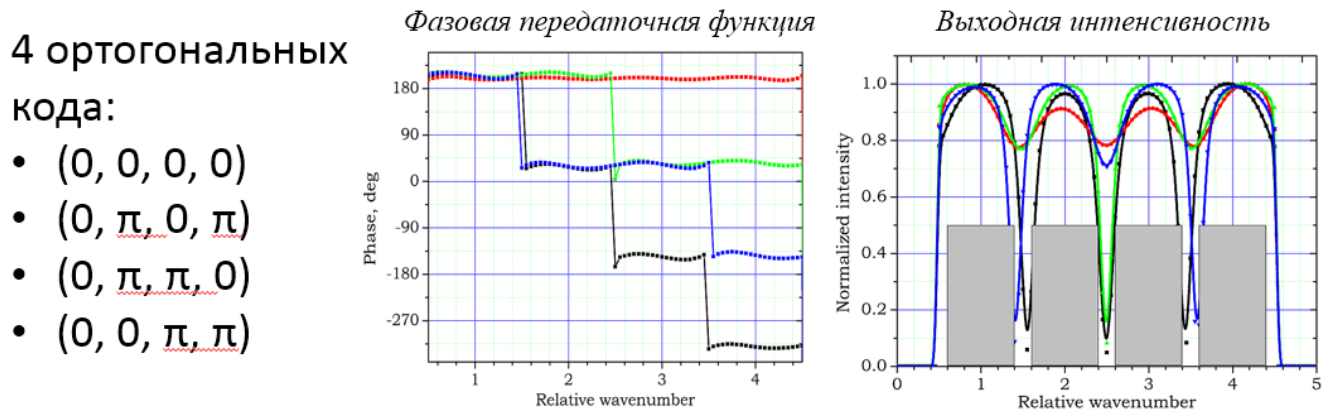

Рисунок 1.25: Результаты моделирования кодера для спектрально-фазового когерентного оптического CDMA.

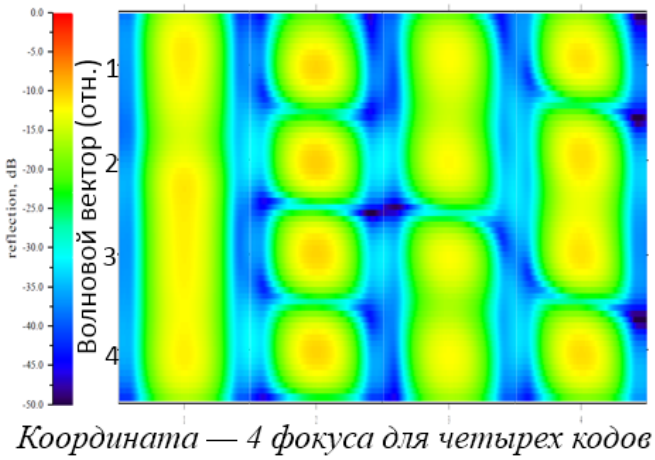

Рисунок 1.26: Зависимость отраженной интенсивности от длины волны (волнового числа) и пространственной координаты в выходной плоскости для спектрально-фазового кодера/декодера CDMA с шагом по частоте в 40 ГГц.

На Рисунке 1.26 показана зависимость выходной мощности от длины волны и пространственной координаты. Как следует из рисунка, сдвиги фазы в кодах создают выемки в профиле интенсивности, поэтому все коды четко видны на этом графике интенсивности. Длина голограммы составляет 5 мм, а общая длина чипа — 7 мм. Общий уровень потерь — около 4 дБ, полная ширина спектральных линий по уровню -3 дБ около 25 ГГц. Фазовая ошибка составляет не более 20°.

Для практического использования желательно иметь более узкое спектральное разделение и большее пространство кода. Наше текущее моделирование показывает возможность производства кодеров с разнесением каналов 10 ГГц и как минимум с восемью длинами волн. Результаты моделирования соответствующего устройства показаны на Рисунке 1.27.

1.2.2. Применение цифровой планарной голографии для оптических интерконнектов на чипе

Оптические интерконнекты на чипе — важное направление исследований в последние два десятилетия. Эта технология предполагает замену электрических соединений между различными частями микросхемы на оптические. Задача интерконнекта — осуществлять обмен информацией между ядрами процессора, а также между ядрами и кэшем различных уровней или памятью. С ростом производительности процессоров, а также необходимостью распараллеливать вычисления между ядрами на кристалле, площадь, занимаемая интерконнектом на кристалле постоянно увеличивается. По сути, интерконнект является одним из наиболее значимых „бутылочных горлышек“ на пути дальнейшего развития высокопроизводительных процессоров. Внедрение оптики на чип может решить проблему интерконнекта, также как появление оптических линий связи решило проблему передачи информации по медным проводам. Оптика позволяет передавать информацию без жестких ограничений на частоту модуляции, без необходимости экранировать проводники друг от друга, а также без существенных ограничений на дальность передачи. По-

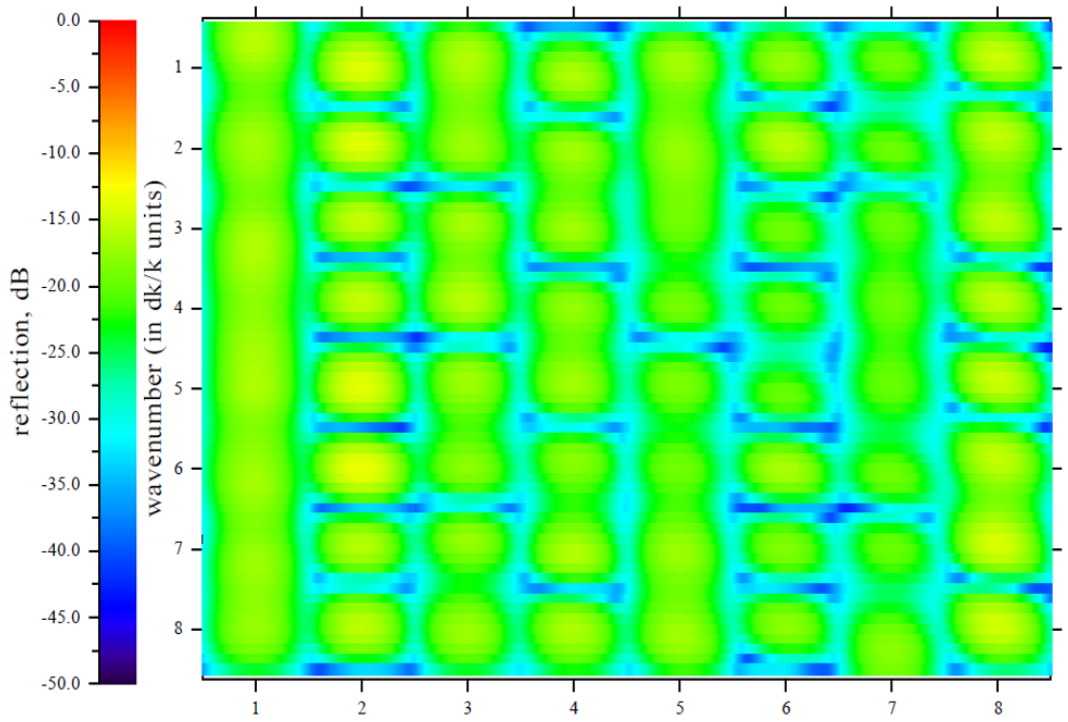

Рисунок 1.27: Зависимость отраженной интенсивности от длины волны (волнового числа) и пространственной координаты в выходной плоскости для спектрально-фазового кодера/декодера CDMA с шагом по частоте в 10 ГГц и 8 частотными каналами.

тенциально, реализация оптического интерконнекта может снизить как физическую площадь на чипе, занимаемую интерконнектом, так и его энергопотребление. В первом случае это снижает цену каждого чипа, а во втором — снижает издержки на эксплуатацию.

Реализация оптического интерконнекта на чипе традиционно предполагает использование планарной волноводной структуры, с помощью которой можно различными способами реализовать передачу, маршрутизацию и доставку оптических сигналов между разными узлами на кристалле. Однако, несмотря на огромную свободу организации оптических соединений в двумерном волноводном пространстве, большинство заявленных устройств основано на псевдоодномерных структурах — так называемых гребенчатых волноводах (ridge waveguides) [31]. Глобально, типичные спектрально-чувствительные и/или активные элементы, такие как мультиплексоры/демультиплексоры WDM, а также оптические переключатели и модуляторы, бывают двух основных типов: волноводные решетки (AWG) и кольцевые резонаторы. В настоящей работе предлагается новый тип оптических спектральных элементов на кристалле, основанный на цифровой планарной голографии [P3, P4]. В отличие от традиционных спектральных элементов, основанных на одномерных волноводах, планарные голограммы используют весь двумерный объем и, таким образом, могут обладать более широким набором функций, которые могут быть реализованы на одной и той же площади. Более того, они обеспечивают простую масштабируемость и повторное использование занимаемой площади за счет возможности реализовывать суперпозиции разных голограмм, например, для отличающихся длин волн или различных топологий. В общем случае такая голограмма может реализовать произвольную карту соединений для различных длин волны

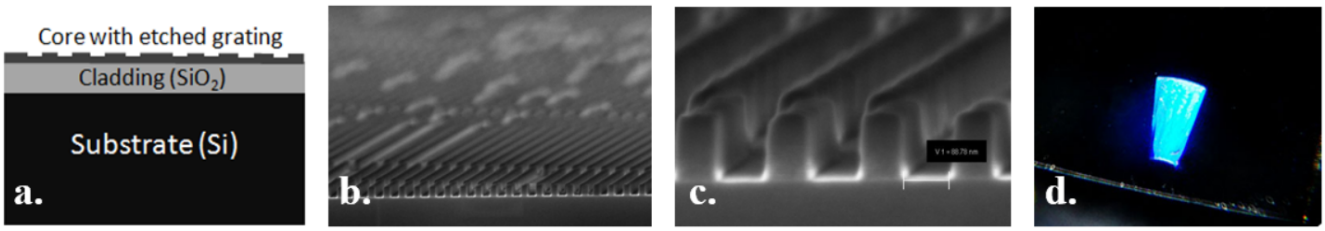

Рисунок 1.28: Изготовленный голографический мультиплексор/демультиплексор для видимого спектра: a. Используемая планарная структура; b. и c. СЭМ-изображения изготовленной структуры, разрезанной поперек голограммы; d. Вид устройства в оптический микроскоп.

между разными входными и выходными модами, например между модами традиционных гребенчатых волноводов.

Еще одна особенность голографических устройств на кристалле — их устойчивость к локальным ошибкам изготовления. В то время как традиционное псевдо-одномерное устройство, например AWG, кольцевой резонатор или даже светоделитель могут оказаться неработоспособными из-за наличия небольшого дефекта при изготовления гребенчатого волновода, голографическое устройство из-за своей двумерной структуры обладает принципиально большей устойчивостью к локальным дефектам структуры. Точечная ошибка проявляется просто как наличие (или отсутствие) дополнительного центра рассеяния, что приводит к относительно небольшому ухудшению качества всей структуры. То же самое относится и к точности изготовления: AWG или кольцевой резонатор требуют точного оптического контроля фазы в гребенчатом волноводе, что, в свою очередь, можно достичь только соблюдая геометрические размеры с огромной точностью. Напротив, когерентность в голографических устройствах должна сохраняться только вдоль распространения волны в двумерном планарном волноводе, который зависит лишь от среднего показателя преломления, который не сильно изменяется при небольших отклонениях геометрических размеров отдельных элементов.

Мультиплексор/демультиплексор для линий связи со спектральным уплотнением (WDM)

Из-за экспериментальных ограничений прототип (де)мультиплексора был разработан для планарного волновода на основе плавленого кварца для работы в видимом спектральном диапазоне. Волновод имеет сердцевину из легированного диоксида кремния толщиной 750 нм с контрастом показателя преломления 3% поверх слоя из диоксида кремния толщиной 14 мкм на кремниевой подложке. Рассчитанная цифровая голограмма была изготовлена электронным пучком в процессе одностадийной литографии с глубиной травления 140 нм. Изготовленное устройство представлено на Рисунке 1.28.

Подобные голографические устройства, продемонстрированные ранее, использовались для реализации оптических спектрометров на чипе [24]. Синтез таких голографических структур начинается с расчета интерференционной картины, которая соответствует обычной голограмме, соединяющей входной и выходной волновые фронты. Этот шаблон представляет собой аналоговую

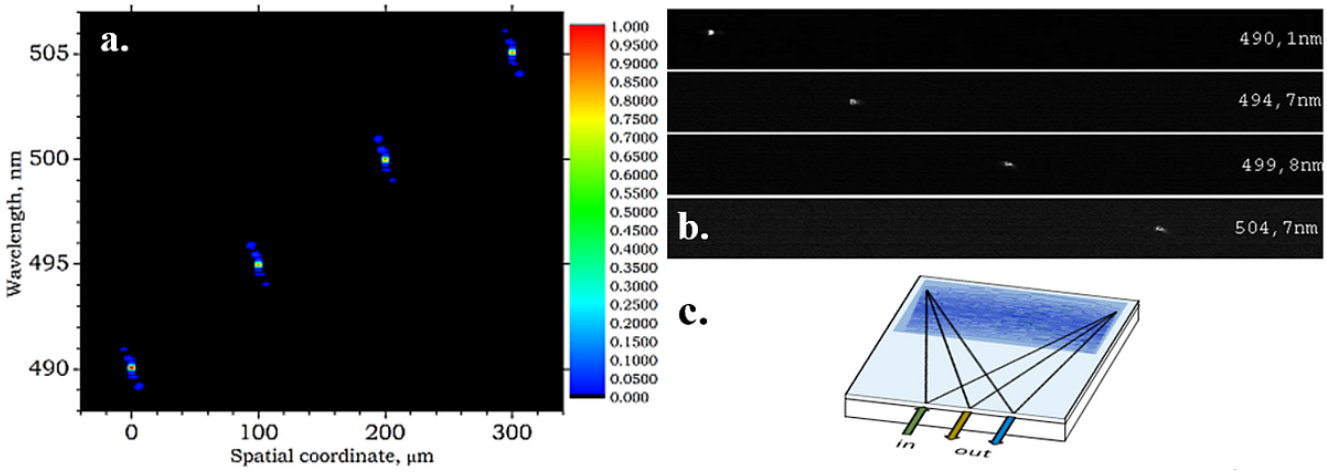

Рисунок 1.29: a. Результаты симуляции: выходная интенсивность (нормализованная) в зависимости от длины волны и пространственной координаты; b. Фотографии выходной грани устройства на четырех разных длинах волн, соответствующих четырем каналам мультиплексирования; c. Схема эксперимента.

двумерную функцию, поэтому его необходимо преобразовать в цифровой шаблон, который можно использовать для литографии. Его также необходимо оптимизировать для того, чтобы компенсировать изменение среднего показателя преломления из-за травления. Другие модификации рисунка, такие как корректировка геометрии и аподизация, еще больше улучшают его свойства. Конструкция этого конкретного устройства не была оптимизирована для того, чтобы иметь небольшую площадь, а была взята из спектрометра с гораздо более высоким спектральным разрешением.

Изготовленный демультиплексор [A12] разделяет четыре длины волны 490, 495, 500 и 505 нм и перенаправляет их на соответствующие выходы. Для каждой длины волны голограмма действует как эллиптическое зеркало, фокусирующее свет из входной точки в соответствующий выход. Следует отметить, что из-за высокого спектрального разрешения (большого размера голограммы) спектральная ширина каждого канала составляет всего около 0,3 нм, то есть устройство игнорирует все длины волн, которые не относятся ни к одному из каналов. Работа устройства моделировалась путем численного решения двумерного уравнения Гельмгольца с использованием специально разработанного быстрого собственного кода. Данный метод учитывает многократные отражения от всех вытравленных деталей на волноводе, и показывает, хорошее согласование с экспериментом [27]. Результаты моделирования показаны на Рисунке 1.29a.

Экспериментально измеренные выходные распределения на четырех длинах волн, соответствующих спектральным каналам устройства, показаны на Рисунке 1.29b. На длинах волн, отличных от спектральных каналов устройства, выход был полностью темным. Те же инструменты могут использоваться для (де)мультиплексирования длин волн в оптических интерконнектах, что далее показано с помощью моделирования.

Более реалистичный пример спектрального демультиплексора был исследован путем моделирования. Это 12-канальный демультиплексор стандартной ITU решетки частот WDM с шагом по частоте в 100 ГГц. Прибор сконструирован для планарных волноводом на базе плавленого

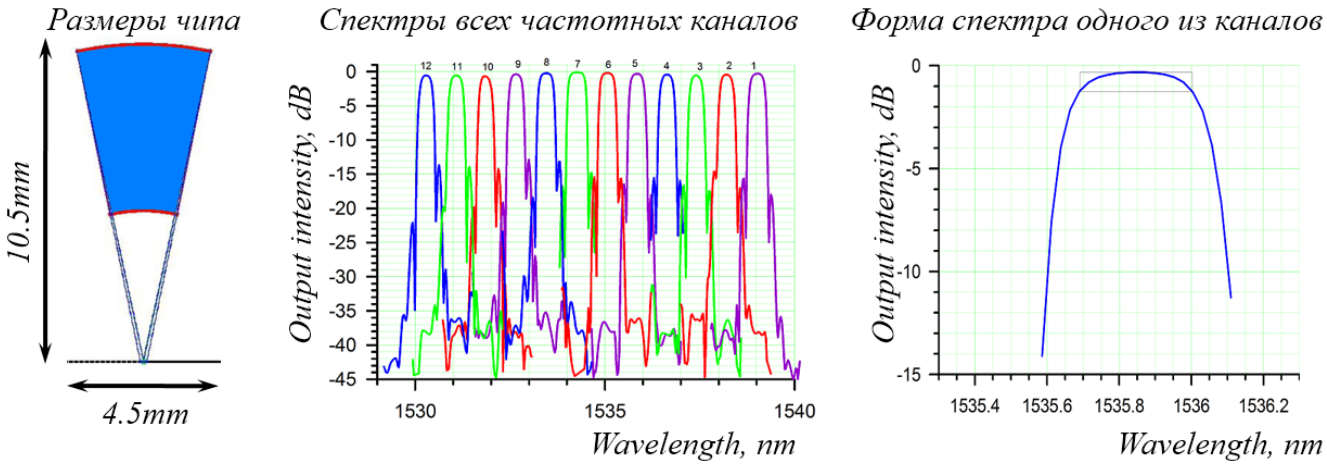

Рисунок 1.30: Размеры чипа 12-канального 100 ГГц WDM демультиплексора и результаты симуляции его работы.

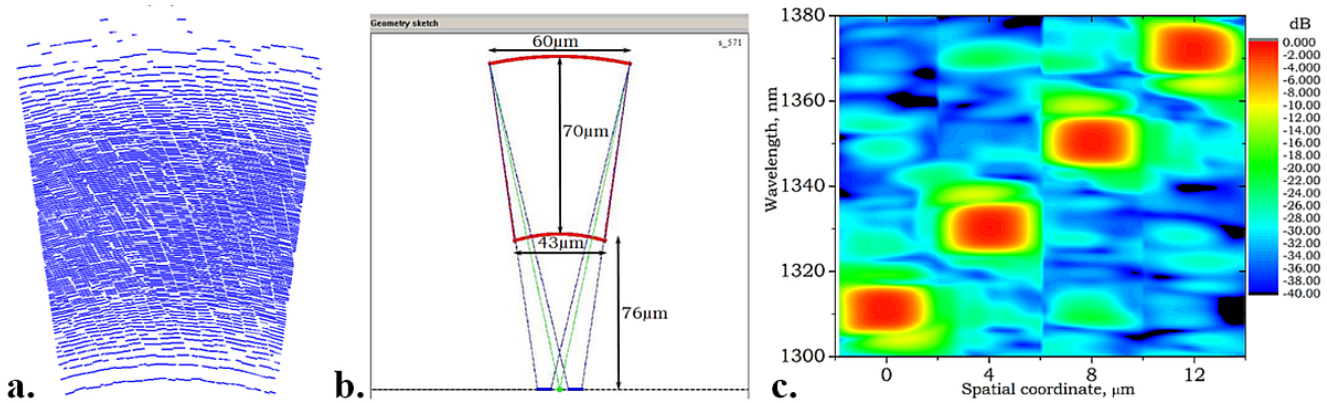

Рисунок 1.31: a. Полный чертеж голографической структуры для 4-канального WDM мультиплексора/демультиплексора с использованием платформы SOI; b. Схема устройства и его размеры; c. Передаточная характеристика устройства в дБ относительно входа в зависимости от длины волны и пространственной координаты.

кварца с контрастом показателя преломления 1.5%. Спектральный диапазон составляет 1530.33 – 1538.98 нм. Ширина полосы канала по уровню -1 дБ от максимума равна 40% от шага по частоте между соседними каналами. Размер чипа приблизительно 11×5 мм^2. Спектральные характеристики и геометрия чипа показаны на Рисунке 1.2.2.

Среди предложенных оптических платформ наиболее популярной структурой для фотонных интерконнектов является одномодовый планарный волновод на основе кремния на изоляторе (SOI). В этой работе был разработан подходящий для этой платформы WDM мультиплексор/демультиплексор с четырьмя спектральными каналами, разнесенными на 20 нм при длине волны около 1300 нм. Размер голограммы был выбран так, чтобы минимизировать спектральные перекрестные помехи, сохраняя при этом спектральную ширину каждого канала как можно большей. На Рисунке 1.31 показан полный чертеж голограммы (a.), схема устройства и размеры (b.), а также результаты моделирования его рабочих характеристик (c.).

Согласно результатам моделирования, уровень перекрестных помех для данного устройства

составляет менее -20 дБ, в то время как полезная полоса пропускания каждого канала превышает 6 нм. Поскольку конкретная конструкция имеет только четыре спектральных канала, занимаемую ей площадь на чипе можно использовать повторно, добавляя дополнительные каналы по мере необходимости, как обсуждалось ранее. Добавление большего количества каналов приводит только к постепенному увеличению перекрестных помех между каналами из-за растущего нерезонансного рассеяния излучения от результирующей голограммы. Помимо увеличения количества спектральных каналов, голограмма также может выполнять разделение каналов на разные выходы: каждая длина волны может быть направлена на два или более выходных порта вместо одного, опять же повторно используя площадь уже занимаемую голограммой.

Многочастотный и селективный по длине волны переключатель

Другая функция, которая может быть реализована с использованием технологии цифровой планарной голографии, - это селективное по длине волны переключение каналов. Поскольку обычные переключающие устройства на основе кольцевых резонаторов могут эффективно работать только для одной длины волны [32] или, в некоторых случаях, для регулярной гребенки длин волн [33], предлагаемый голографический переключатель может быть разработан для одновременного переключения любого количества длин волн, которое требуется. Работа переключателя аналогична традиционному подходу, в котором используется изменение показателя преломления волновода для сдвига резонансной частоты структуры. Такое изменение может быть обеспечено с использованием различных методов, включая тепловое переключение [34], инжекцию носителей заряда [32], использование жидких кристаллов [35] или электрооптических материалов и сегнетоэлектриков [36].

Принцип работы для переключения одной длины волны показан на Рисунке 1.32a. Более сложная структура, разработанная в настоящей работе, показана на Рисунке 1.32b, где 16-канальная голограмма действует как 8-канальный коммутатор, который переключает WDM трафик на 8 длинах волн между двумя выходами. Результаты моделирования свидетельствуют о низком уровне перекрестных помех и широкой (0.25 нм) полосе пропускания каждого канала. Изменение показателя преломления, необходимое для переключения, зависит от относительного разнесения длин волн между двумя выходами, которое можно сделать примерно таким же, как ширина полосы коммутируемых каналов. Для созданной голограммы требуемый для переключения сдвиг показателя преломления составляет всего $\Delta n/n = \Delta\lambda/\lambda = 0.5/1310 = 3,8 \times 10^{-4}$.

Правильное проектирования голограммы под конкретную задачу может позволить реализовать гораздо более сложные схемы переключения. Например, подобный голографический переключатель может иметь более одного входа и, таким образом, более одной пары выходов, переключение может происходить, например, в разных направлениях для разных длин волн.

В данном разделе были предложены, промоделированы и частично исследованы экспериментально устройства для схем оптических интерконнектов на чипе, таких как оптический (де)-мультиплексор и переключатель. Подобные голографические устройства обеспечивают эффективное повторное использование занимаемой площади на чипе, масштабируемы и устойчивы к

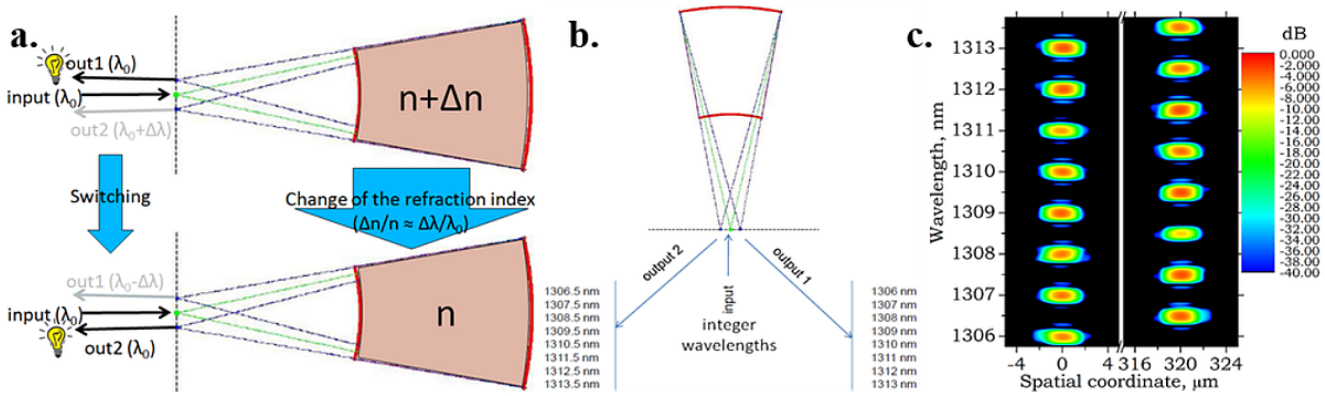

Рисунок 1.32: a. Принцип действия переключателя для одной длины волны. Изменение показателя преломления сдвигает резонансную длину волны голограммы и, таким образом, переключает входную длину волны между выходами; b. Схема сконструированного переключателя для 8 длин волн. В норме все каналы с целочисленной длиной волны направляются на выход output1. При изменении показателя преломления на $\approx$ 0.04% все сигналы направляются на выход output2; c. Результат симуляции для выходной интенсивности в дБ относительно входной мощности в зависимости от длины волны и пространственной координаты.

производственным ошибкам. В силу данных свойств, цифровая планарная голография представляет собой перспективную платформу для оптических устройств на чипе.

1.3. Заключение к Главе 1

В этой главе 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.

Реализация дискретного преобразования Фурье (ДПФ) в волноводной решетке была изучена теоретически, было проведено соответствующее численное моделирование, а также была продемонстрирована экспериментальная установка тестовой системы связи с оптическим OFDM, потенциально позволяющая достигать общей пропускной способности в 120 Гбит/с. Полученные результаты доказывают выдвинутую гипотезу о возможности реализации ДПФ в хорошо изученном интегрально-оптическом устройстве, а также открывают возможности практической реализации оптических линий связи с таким, проявившим себя в беспроводных применениях, типом мультиплексирования каналов.

Применения цифровой планарной голографии для оптической связи и интерконнектов на чипе были изучены, в первую очередь, с помощью моделирования на проприетарном программном обеспечении, зарекомендовавшем себя на других задачах и дающем высокое соответствие изго-

товленным приборам. Был предложен ряд устройств, связанных с фазовым модулированием, системами оптического множественного доступа с кодовым разделением CDMA, а также организацией оптической сети обмена данными на чипе — интерконнекта.

Глава 2

Нейроморфная обработка сигналов

Обработка информации, представленной в виде оптических сигналов, играет важнейшую роль наравне с задачами представления и передачи информации, которым была посвящена предыдущая глава. 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“. В этой главе предложен подход к реализации оптических нейронных сетей.

Использование нейронных сетей для некоторых сложных задач, таких как распознавание изображений, перевод текстов с языка на язык и многих других, является перспективной технологией, позволяющей совершенствовать системы искусственного интеллекта. В результате, все больше и больше вычислительных мощностей в мире занято симуляцией работы нейронных сетей. Очевидно, что создание специализированных вычислительных устройств для решения данной задачи является многообещающим подходом для усовершенствования этой технологии.

Полностью оптический вариант решения такой задачи потенциально позволяет использовать намного больший чем в электронных чипах частотный диапазон. Использование оптики позволяет переходить в гигагерцовый режим работы нейронов, что существенно повышает быстродействие системы по сравнению с типичными вычислительными моделями.

В этой главе продемонстрирован полнофункциональный сверхбыстрый оптический нейрон с импульсным режимом работы [A3, A4, A7], [P2]. Используемая экспериментальная установка представляет собой полностью оптическую реализацию нейрона типа «интегрировать и сработать» с утечками. Такой тип нейрона может являться базой для аналогово-оптических вычислений общего назначения. В отличие от чисто аналоговых вычислительных моделей, приближение к биологическим нейронам, использующее импульсный режим работы, исключает накопление шума и приводит к надежной и эффективной обработке сигналов. Продемонстрированный нейрон обеспечивает полный функционал, необходимый для модели нейронов с импульсами, и при этом работает на гигагерцовых скоростях, что соответствует ускорению по крайней мере на 10^8 по сравнению с настоящими биологическими нейронами.

2.1. Введение

Нейроморфная обработка данных представляет собой эффективную альтернативу традиционной цифровой модели вычислений. Она оказалась полезной как с точки зрения разработки алгоритмов, так и с точки зрения аппаратной реализации обработки сигналов с сенсоров. Значительные усилия были направлены на *оптическую* реализацию нейронов. Оптический подход позволяет использовать преимущества огромной частотной полосы пропускания, которая позволяет обеспечить сверхбыструю модуляцию и, следовательно, скорость обработки по сравнению с электронными подходами. С начала 90-х годов сообщалось о нескольких типах оптических нейронов или нейроноподобных устройств [37, 38, 39, 40, 41, 42, 43]. Большое внимание в современной теоретической нейробиологии уделяется значительным вычислительным возможностям импульсной модели нейронов, в которой точное время возникновения пиков или потенциалов действия используется как для кодирования, так и для обработки информации. Оптическая реализация прототипа вычислительного примитива для этой нейронной модели третьего поколения, так называемого нейрона типа «интегрировать и сработать» с утечками, требует разработки нового оптического принципа работы.

Как и в случае с предыдущими нейронными моделями, оптическая реализация импульсного нейрона представляет особый интерес из-за его способности работать с чрезвычайно высокой скоростью. Недавний прогресс в электронной реализации нейронов с использованием современных СБИС [44, 45] обеспечил более конкурентоспособную производительность по сравнению с возможными оптическими реализациями. Среди оптических реализаций импульсных нейронов и подобных им устройств, о которых сообщалось ранее [46, 47, 48, 49], самая короткая длительность импульса составляла около 0.1 мкс, в то время как в других работах она достигает нескольких мс. Эта относительно большая длительность импульсов ограничивает максимальную скорость обработки данных до нескольких МГц, что не превосходит показателей достигнутых на СБИС [44].

В рамках настоящей работы было показано [А3], что существует новая концепция импульсных оптических нейронов, которая обрабатывает сигналы с гигагерцовой частотой и выше, что значительно превосходит по скорости электронные аналоги. Далее проводятся результаты, позволяющие создавать сверхбыстрые оптические нейроны с импульсами, а также представлена полностью оптическая реализация, в которой присутствуют как возбуждающие, так и тормозящие оптические входы.

Устройства обработки оптических сигналов, представленные в этой главе, обеспечивают скорость обработки в терагерцовом диапазоне с высоким уровнем параллелизма, типичным для нейронных сетей. Будучи примерно в 10^8 раз быстрее, чем биологические нейроны, они также значительно превосходят нейроны на основе схем СБИС [44] и могут использоваться в относительно простых нейронных сетях, где высокая скорость обработки и передачи информации является критическим фактором.

2.2. Модель импульсного нейрона

Нейрон типа «интегрировать и сработать» — одна из наиболее широко используемых моделей биологических нейронов в современной теоретической нейробиологии [50]. Несмотря на сведение биологических нейронов в небольшой набор основных операций (задержка, умножение на веса, суммирование, временна́я интеграция и пороговое срабатывание), поведение сетей этих элементов сохраняет бóльшую часть разнообразия, присущего биологическим нейронным сетям. Интерес к нейронам как эффективным вычислительным устройствам постоянно растет и за пределами теоретического сообщества нейробиологов [51].

Импульсный режим работы нейронов — это естественный гибрид аналоговой и цифровой обработки в том смысле, что выходной сигнал нейрона является бинарным по амплитуде, в то время как прохождение сигналов в самом нейроне является аналоговым: в нем происходит взвешенное суммирование и/или вычитание входных сигналов. Такой тип обработки, по-видимому, развился в биологических (нервных) системах , чтобы преодолеть проблему накопления шума, присущую чисто аналоговым вычислениям [52]. Вся информация, передаваемая следующему нейрону в сети, содержится только в наличии или отсутствии импульсов, но не в их форме или амплитуде. Таким образом, средством для кодирования информации и обработки импульсов является лишь взаимное расположении импульсов во времени. Алгоритмы обработки импульсов хорошо изучены в ряде важных биологических систем обработки сенсорных данных, а также находят все более широкое применение в прикладных задачах обработки сигналов [51]. С точки зрения теории сложности вычислений нейроны типа «интегрировать и сработать» представляют собой полноценные вычислительные примитивы, способные моделировать как машины Тьюринга, так и традиционные нейронные сети [51]. Еще одним важным преимуществом вычислительной модели импульсных нейронов является ее способность естественным образом включать обучение и адаптацию с помощью механизмов пластичности на базе времени прихода импульса (spike time dependent plasticity, STDP).

Стандартная модель нейрона типа «интегрировать и сработать» с утечками описывается следующими характеристиками [51]:

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.

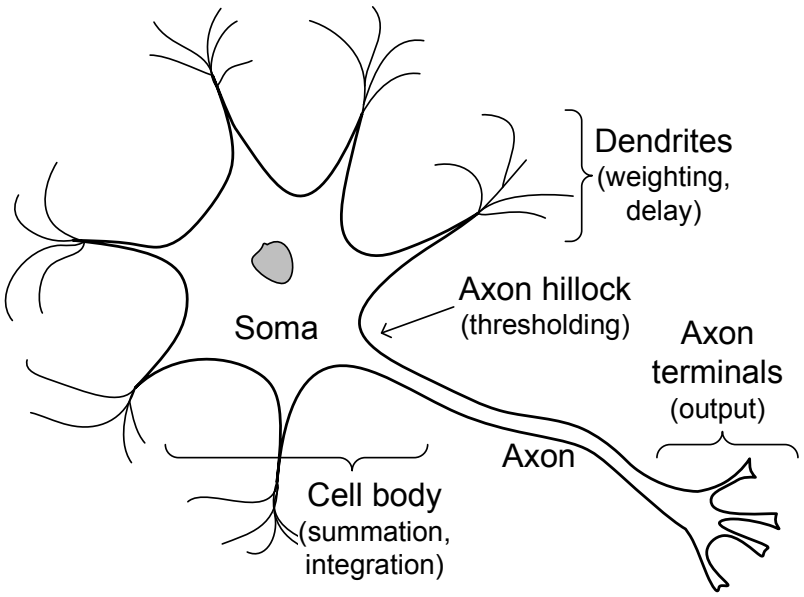

Рисунок 2.1: Схематическое изображение биологического нейрона.

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, $I(t) = V_m(t) \sum_{i=1}^{N} w_i \sigma_i(t + \delta_i)$ — 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

Таким образом, параметрами, определяющими поведение устройства являются: $w_i, \delta_i, V_{\text{thresh}}, V_{\text{rest}}$, 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 2.1. 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.

Оптоволоконная реализация дерева дендритов достаточно проста, так как сигналы можно суммировать с нужными весами используя оптоволоконные светоделители, аттенюаторы/модуляторы и линии задержки. Однако, такой тривиальный подход возможен лишь при условии, что все входные сигналы обладают разными длинами волн. Именно этот вариант был отдельно исследован в серии работ [A2, A5], [P1], где он применялся для операций сложения и вычитания радиочастотных сигналов в оптическом представлении. В работе [A10] исследовался альтернативный вариант сложения сигналов, который позволяет суммировать сигналы в том числе на одной и той же длине волны за счет использования различных пространственных мод. Оптический пороговый элемент был продемонстрирован нами ранее в работах [A1, A11]. Таким образом, единственной отсутствующей функциональной частью оптической модели нейрона остается механизм интегрирования с утечкой. Такой функционал был впервые продемонстрирован нами в работе [A3].

Чтобы раскрыть связь между биологическими нейронами и предложенным оптическим подходом, рассмотрим сначала механизм интегрирования с утечками, который используется в данной работе. В [A3] было обнаружено прямое соответствие между уравнениями, определяющими временное интегрирование в стандартном нейроне типа «интегрировать и сработать» с утечками, и уравнениями, определяющими концентрацию носителей в полупроводниковом оптическом усилителе (SOA). Согласно стандартной модели для такого нейрона, нейроны рассматриваются как электрические устройства, у которых 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 $V_m = V_{\text{rest}}$. Следовательно, на V_m оказывают влияние три фактора: пассивная утечка тока через мембрану, активный ток накачки и внешние входы, генерирующие изменяющиеся во времени значения проводимости мембраны $\sigma(t)$, которые помогают „разрядить“ нейрон. Эти три фактора представляют собой три члена, входящие в дифференциальное уравнение, описывающее V_m в уравнении 2.1 (1).

$$\begin{array}{lcccccl} \text{Потенциал} & & \text{Активная накачка} & & \text{Утечка} & \text{Входной сигнал} & \\ \dfrac{dV_m(t)}{dt} & = & \dfrac{V_{\text{rest}}}{\tau_m} & - & \dfrac{V_m(t)}{\tau_m} - \dfrac{1}{C_m} V_m(t)\sigma(t) & & (1) \\ \dfrac{dN'(t)}{dt} & = & \dfrac{N'_{\text{rest}}}{\tau_e} & - & \dfrac{N'(t)}{\tau_e} - \dfrac{\Gamma a}{E_p} N'(t) I(t) & & (2) \end{array} \tag{2.1}$$

Точно так же динамика усиления короткого SOA регулируется уравнением 2.1 (2) [53]. Его внутренняя переменная состояния — это плотность носителей выше уровня просветления $N'(t)$ =

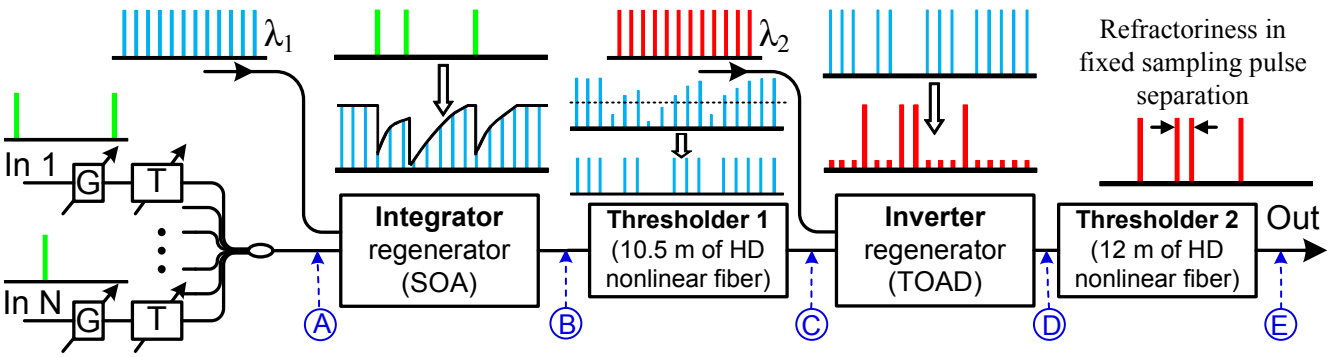

Рисунок 2.2: Блочная диаграмма фотонного нейрона. G — переменный аттенюатор, T — переменная линия задержки, SOA — полупроводниковый оптический усилитель, HD fiber — нелинейный световод, сильно допированный GeO_2, TOAD — terahertz optical asymmetric demultiplexer [54].

$N(t) - N_0$, 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.

Поскольку время жизни носителей в современных SOA может составлять всего порядка 10 пс, фотонные нейроны, использующие этот метод интегрирования могут быть более чем в 10^8 раз быстрее, чем их биологические предшественники. В следующих двух разделах будут представлены две экспериментальные реализации таких нейронов: первая была предложена в [A3], но не была полностью реализована, а вторая представлена здесь впервые и имеет преимущество в виде наличия тормозящих входов.

2.3. Экспериментальная модель нейрона типа «интегрировать-и-сработать» с утечками

Следуя схеме нейрона, предложенной в [A3], была собрана экспериментальная установка, показанная на Рисунке 2.2, которая состоит из пяти блоков: пассивное взвешивание входов, задержка и суммирование входов; временно́е интегрирование; первый этап пороговой обработки; инвертирование и второй этап пороговой обработки. Первые три функции были предложены нами в работе [A3], где они достаточно подробно описаны. Инверсия и второй этап пороговой обработки заслуживают дополнительного внимания. Полностью оптическая инверсия, необходимая для

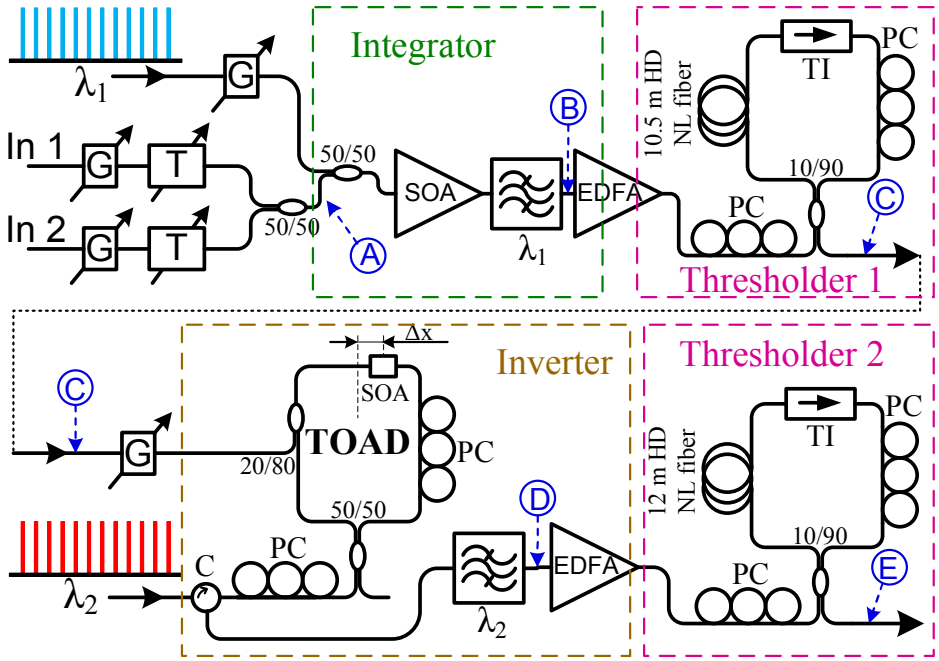

Рисунок 2.3: Экспериментальная установка. G — переменный аттенюатор, T — переменная линия задержки, PC — контроллер поляризации, TI — настраиваемый изолятор, EDFA — эрбиевый волоконный усилитель, C — циркулятор, HD NL fiber — нелинейный световод, сильно допированный GeO_2.

этой конструкции нейрона, обычно не может быть выполнена идеально: возникает ухудшение контраста между нулями и единицами. Такое ухудшение сигнала недопустимо на выходе нейрона, поскольку оно может привести к вычислительным ошибкам при дальнейшем распространении по нейронной сети. Второй этап пороговой обработки призван улучшить качество сигнала на выходе.

Полностью оптическая реализация законченного нейрона показана на Рисунке 2.3. Первые три блока построены согласно принципам, разобранным в [A3]. Вся установка основана на волоконно-оптических компонентах, работающих в телекоммуникационном диапазоне 1550 нм. В качестве источника задающих импульсов используется кольцевой волоконный лазер с синхронизацией мод и частотой повторения импульсов 1.25 ГГц. Чтобы реализовать последовательности импульсов на нескольких длинах волн, используется генератор суперконтинуума, который уширяет спектр импульсов более чем на 10 нм, и затем из него полосовыми фильтрами с шириной спектра 200 ГГц вырезаются сигналы с разными длинами волн. Длины волн 1551.6 и 1553.2 нм использовались в качестве входов нейрона, а длины волн $\lambda_1 = 1549.2$ нм и $\lambda_2 = 1544.8$ нм использовались для реализации зондирования и инверсии усиления, соответственно. Ширина оптических импульсов на полувысоте после полосовых фильтров составляет примерно 3 пс. Для создания различных последовательностей импульсов, необходимых для выполнения измерений, используются два электрооптических модулятора Маха-Цандера и генератор сигналов. Типичная энергия зондирующего импульса для измерения усиления SOA составляла от 0.02 до 0.1 энергии входных импульсов, или примерно 5-20 мкДж в абсолютных единицах.

Установка содержит два полностью оптических пороговых элемента, конструкция которых

аналогична описанной в [A1]. Такой пороговый элемент обеспечивает кубическую эффективную передаточную функцию и работает при относительно низком уровне мощности. Волокно с сильным допированием GeO_2 (HD), используемое в обоих пороговых устройствах, обеспечивает высокий нелинейный коэффициент и в то же время легко сваривается со стандартным одномодовым волокном. Параметры HD-волокна, измеренные при $\lambda = 1550$ нм, следующие: коэффициент нелинейности 35 $Вт^{-1}км^{-1}$, оптические потери 36 дБ/км, хроматическая дисперсия -70 пс/нм·км, разность показателей преломления $\Delta n = 0.11$ ([55], preform 311). Длина нелинейного световода у двух пороговых устройств немного отличается, но их характеристики очень похожи. Обе длины близки к оптимальным, а небольшие изменения длины слабо влияют на пороговый уровень мощности.

Инвертор построен на базе устройства TOAD [54], которое является переключателем с фиксированной длиной окна переключения. TOAD основан на интерферометре Саньяка, т.е. один из его выходов — отражение сигнала назад, а второй — отдельный световод. Импульсы из порогового устройства используются в качестве управляющего сигнала для TOAD; они создают окна переключения длительностью 40 пс. Пробные импульсы на длине волны λ_2 используются как входной сигнал TOAD, а порт отражения TOAD используется в качестве выхода инвертора с помощью оптического циркулятора. Оба потока импульсов, управляющих и пробных, должны быть синхронизированы для того, чтобы пробные импульсы попадали в окна переключения, создаваемое потоком управляющих импульсов. В нашей демонстрации оба потока импульсов были получены от одного и того же лазера с синхронизацией мод и поэтому были идеально синхронизированы. На выходе TOAD осуществляется спектральная фильтрация тонкопленочным фильтром с полосой пропускания 200 ГГц для удаления управляющего сигнала TOAD из его выходного сигнала. Получается, что это уже второе преобразование длины волны во всем устройстве. Этот инвертирующий элемент, во-первых, регенерирует оптические сигналы, а во-вторых, делает длину волны на выходе полностью независимой от длин волн на входе, что позволяет подавать выходной сигнал непосредственно на вход устройства для организации обратной связи.

Экспериментально измеренные сигналы на разных этапах их прохождения через оптический нейрон показаны на Рисунке 2.4. Коэффициент усиления SOA измеряется пробными импульсами, синхронными с импульсами входного сигнала, но импульсы дискретизации задерживаются примерно на 10 пс. Сигнал (A), то есть суммарный входной сигнал нейрона, представляет собой повторяющийся 10-битный шаблон 1110010100 с тактовой частотой 1.25 ГГц. Следует отметить, что расстояние между импульсами в этой экспериментальной установке (около 800 пс) намного больше, чем время восстановления SOA (около 180 пс), поэтому каждый импульс фактически обрабатывается независимо, потому что усиление SOA полностью восстанавливается после предыдущего импульса. Следовательно, в этом эксперименте SOA лишь реагирует на одиночные импульсы, а его интегрирующие по времени свойства не используются. После интегратора последовательность инвертируется (B), а контраст между нулями и единицами уменьшается из-за свойств интегратора SOA, заданных уравнением 2.1 (2). Сигнал (C) является результатом порогового детектирования сигнала (B), который снова становится бинарным по амплитуде. После прохождения

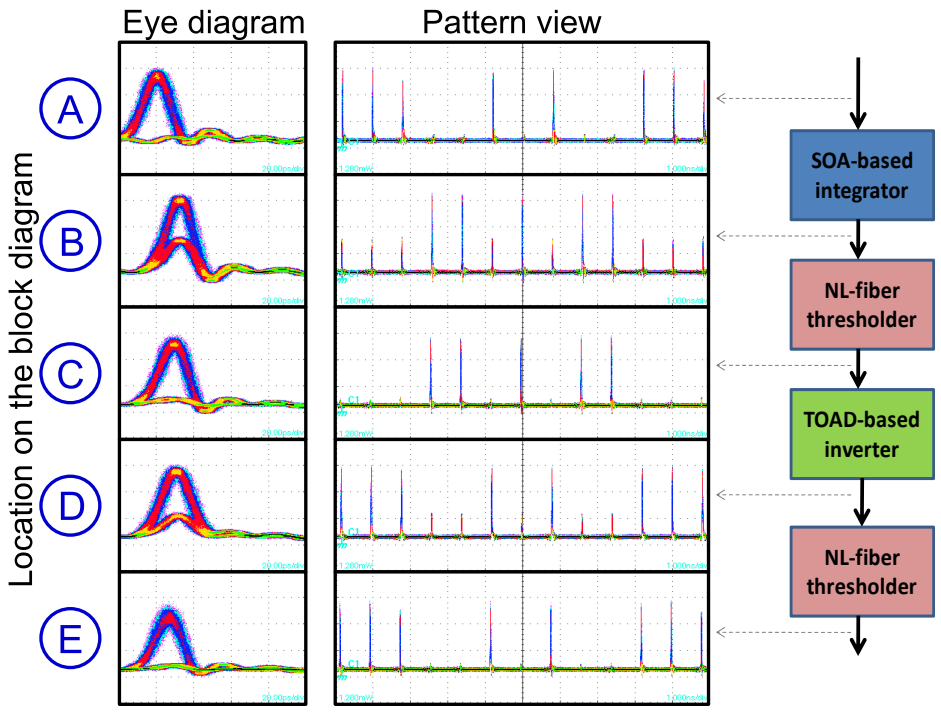

Рисунок 2.4: Прохождение сигналов через нейрон. (A) — входной сигнал, (B) — сигнал поле интегратора, (C) — сигнал после первого порогового элемента, (D) — инвертированная последовательность, (E) — выход нейрона.

инвертора сигнал переворачивается во второй раз (D) и становится похожим на исходную битовую последовательность (A). Второй пороговый элемент улучшает отношение амплитуд единиц и нулей на выходе нейрона и гарантирует, что выходной сигнал состоит из оптических импульсов примерно одинакового размера. Такая бинарная амплитуда требуется для предотвращения накопления амплитудного шума и, таким образом, значительно увеличивает масштабируемость системы.

Хотя выходной сигнал похож на входной, это всего лишь реконструкция того отпечатка, который входящий сигнал оставляет в SOA. Фактически, исходный сигнал дважды заменяется новым потоком импульсов при прохождении через нейрон. Помимо интегратора, который является „сердцем“ нейрона, остальная часть установки требуется для измерения текущего коэффициента усиления SOA, инвертирования результата этого измерения и реализации порогового преобразования.

Другой более сложный пример показывает возбуждение нейрона несколькими импульсами за время восстановления SOA. Измеренные сигналы показаны на Рисунке 2.5. Специально подготовленный входной сигнал состоит из шести потоков импульсов (поступающих на шесть входов нейрона) на трех длинах волн 1550.0, 1551.6 и 1553.2 нм, схематически показанных на Рисунке 2.5a разными цветами. Частота повторения для всех входов составляет 622 МГц. Все шесть входов нейрона разделены на две группы, так что каждая длина волны есть в каждой группе. В то время как импульсы в первой группе выровнены по времени в пределах нескольких пс, импульсы в другой группе имеют задержки между собой в 83 и 67 пс. Группы модулируются битовой после-

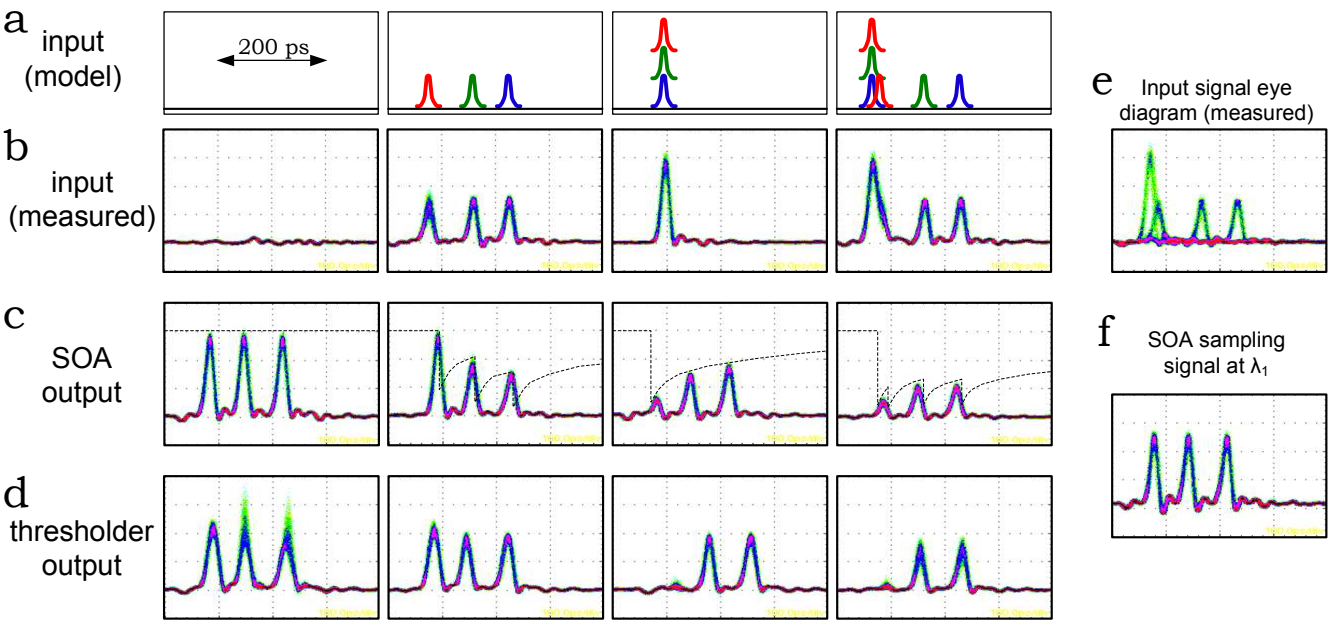

Рисунок 2.5: Возбуждение нейрона несколькими импульсами за время интегрирования. На графиках показана часть одного битового периода в последовательности с частотой повторения 622 МГц. Строки **a** и **b** показывают модель входного сигнала и соответствующую измеренную зависимость мощности входного сигнала от времени. **c** соответствует выходному сигналу каскада интегрирования нейрона, дискретизированному с помощью трех импульсов за битовый период, показанных на диаграмме **f**. Последняя строка (**d**) показывает измеренный выходной сигнал порогового элемента. В данном случае работа нейрона эквивалентна обнаружению выровненных по времени тройных импульсов: если они присутствуют, соответствующий выходной импульс пропадает. Часть **e** представляет собой измеренную глазковую диаграмму входного сигнала.

довательностью „0011“ с задержкой в один бит между ними, так что существует четыре разных типа битовых периодов: без импульсов (первый столбец на рисунке), с импульсами только из второй группы (2-й столбец), с импульсами только из первой группы (3-й столбец) и с импульсами из обеих групп вместе (4-й столбец). Замер усиления SOA в этой демонстрации также выполняется быстрее, чем время восстановления SOA. Используются три пробных импульса, разнесенные по времени на 64 и 72 пс в каждом битовом периоде. Измеренная последовательность пробных импульсов показана на Рисунке 2.5f с использованием той же шкалы времени. Поскольку битовый период достаточно велик для полного восстановления усиления SOA (1600 пс против времени восстановления 180 пс), каждый битовый период может считаться независимым, другими словами в SOA нет памяти между соседними битами последовательности.

Агрегированный входной сигнал, измеренный с помощью стробируемого осциллографа с полосой пропускания 30 ГГц, показан на Рисунке 2.5b. Легко видеть прямое соответствие между измеренными данными и моделью, описанной выше. На Рисунке 2.5e показана глазковая диаграмма такого входного сигнала. Как следует из диаграммы, расстояние между совмещенными импульсами первой группы и первым импульсом второй группы составляет около 16 пс. Пробные импульсы выровнены так, что первый импульс прибывает в пределах этих 16 пс.

На Рисунке 2.5c показана дискретизированная по времени динамика усиления SOA, измеренная на выходе интегратора. Для наглядности там же пунктирными линиями показана приблизительная зависимость коэффициента усиления SOA от времени, на который влияют входные импульсы. Как видно, при отсутствии входных импульсов коэффициент усиления постоянен и равен своему максимальному значению. Во втором столбце показано действие импульсов из второй группы. Каждый из них уменьшает усиление, но так как оно не может полностью восстановиться между импульсами, их воздействия накапливаются. В следующем столбце показана динамика усиления SOA после возбуждения тремя совмещенными импульсами первой группы. Это действие происходит почти мгновенно, после чего следует экспоненциальное восстановление усиления, дискретизированное по трем точкам. Последний столбец показывает действие всех шести импульсов. В этом случае коэффициент усиления SOA снова пропорционален экспоненциально взвешенной сумме всех импульсов.

Измеренный результат после первого порогового элемента показан на Рисунке 2.5d, где наблюдается различие результата между самыми маленькими входными импульсами и всеми остальными. Таким образом, нейрон настроен на обнаружение первой (выровненной) группы импульсов. Если она присутствует, нейрон срабатывает, если нет — то нет. Поскольку дальнейшая инверсия и второй пороговый элемент действуют тривиально, они не показаны на рисунке.

Как следует из описанного эксперимента, нейрон должным образом реагирует на множественные всплески входного сигнала, которые интегрируются, дискретизируются и проходят через пороговый элемент для создания осмысленной последовательности выходных импульсов.

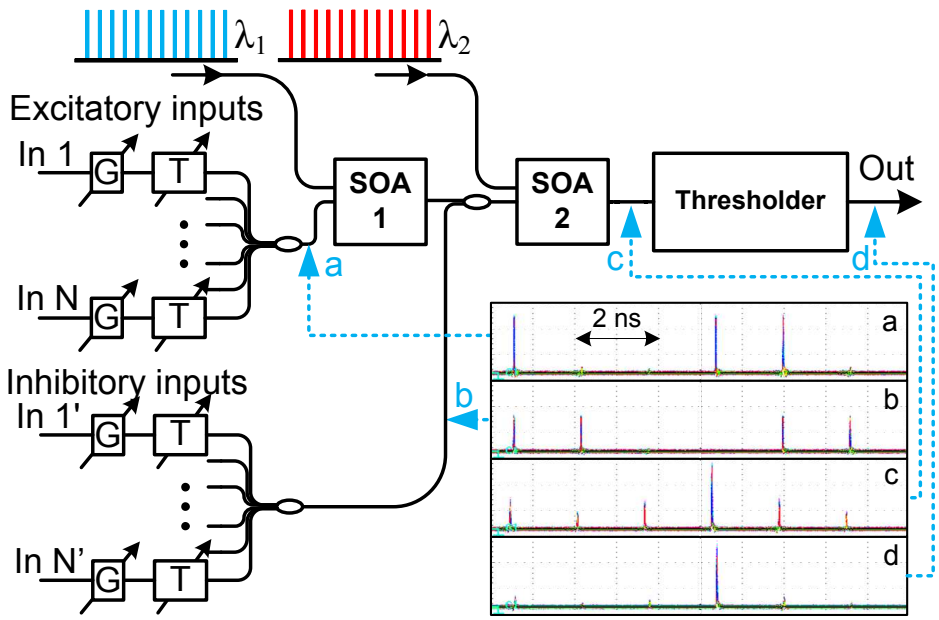

Рисунок 2.6: Схема симметричного фотонного нейрона с возбуждающими и тормозящими входами. Установка состоит из двух идентичных этапов интегрирования в SOA с соответствующими пассивными входными цепями и одного порогового элемента. G — переменное усиление/ослабление; T — переменная линия задержки. На 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.

2.4. Симметричный нейрон в возбуждающими и подавляющими входами

Роль торможения в нейронных цепях имеет большое значение и с вычислительной точки зрения, и с точки зрения возможности создания стабильных цепей и с точки зрения эмпирической нейробиологии, где важная роль торможения в нервной системе хорошо известна. Таким образом, реализация импульсного нейрона без возможности реализации торможения существенно ограничивает возможный диапазон применений. Кроме отсутствия функции торможения, ранее описанная архитектура нейрона неэффективна, поскольку в ней требуется использовать два пороговых элемента. Это было необходимо, так как второй пороговый элемент устранял недостатки инвертора. Однако, такая конфигурация чересчур сложна и дорога в реализации.

В этом разделе предлагается решение обеих задач. Поскольку SOA работает в режиме кроссмодуляции усиления, его выход всегда инвертируется по отношению к его входу. Выполнение двух последовательных инверсий может восстановить исходный сигнал, сохранив все остальные свойства такими же. На Рисунке 2.6 схематично показан такой симметричный нейрон с возбуждающими и тормозящими входами.

Такая конфигурация названа *симметричной*, поскольку она содержит два идентичных SOA,

которые обрабатывают возбуждающие (первый SOA) и тормозящие (второй SOA) входы одинаково, обеспечивая схожее интегрирование по времени и остальные свойства активации. Единственная разница, которая делает один из них возбуждающим, а другой тормозящим, заключается в том, что второй SOA не только принимает тормозящий сигнал, но и инвертирует выходной сигнал из первого SOA, который становится положительным, то есть работает как возбуждение. Таким образом, эта конструкция обеспечивает полную функциональность нейрона и в то же время существенно проще, чем описанная выше. В выходном каскаде по-прежнему используется пороговый элемент для декодирования и приведения выходных импульсов к одинаковой амплитуде.

Экспериментальная установка состоит из тех же блоков, которые использовались в предыдущей версии нейрона. SOA, используемые в установке, модели Kamelian SOA-NL-L1-C-FA; ток накачки составляет 200 мА, а соответствующее время восстановления составляет 110 пс. Длины волн пробных импульсов равны $\lambda_1 = 1544.3$ нм и $\lambda_2 = 1551.7$ нм, а входная длина волны была равна 1550.1 нм. Уровень мощности в последовательности пробных импульсов такой же, как и в предыдущих демонстрациях.

Для демонстрации работы такого *симметричного* нейрона были проведены несколько простых экспериментов. На вставке на Рисунке 2.6 показаны измеренные осциллограммы сигналов в различных точках установки. В этом эксперименте интервалы между импульсами (≈1.6 нс) намного больше, чем время восстановления SOA (≈0.1 нс), поэтому каждый битовый интервал можно считать полностью независимым. Каждый возбуждающий импульс (**a**) увеличивает потенциал нейрона к срабатыванию, что приводит к увеличению амплитуды соответствующего импульса в точке (**c**). Напротив, каждый тормозящий импульс (**b**) подавляет импульсы в (**c**), делая их меньше. Таким образом, самый большой импульс в (**c**) (4-й импульс) соответствует наличию импульса в (**a**) и отсутствию импульса в (**b**). Точно так же, наименьший импульс в (**c**) (2-й импульс) возникает из-за отсутствия импульса в (**a**) и наличия импульса в (**b**). Если присутствуют как возбуждающий, так и тормозящий импульсы или оба из них отсутствуют (1-й и 3-й битовые интервалы соответственно), результирующие импульсы в (**c**) имеют средний размер. Пороговое значение было настроено таким образом, что только самые высокие импульсы в (**c**) приводят к импульсам выходного сигнала (**d**). Этот пример демонстрирует, что тормозящие импульсы могут подавлять возбуждающие. Таким образом, нейрон срабатывает только в том случае, если возбуждающий импульс присутствует, а тормозящий — нет. Режим работы можно изменять, подстраивая входные веса или пороговый уровень.

Более подробная иллюстрация поведения нейрона показана на Рисунке 2.7. Для представления бинарных входных последовательностей, есть импульс/нет импульса, используются цифры 1 и 0 соответственно. В первой строке показан вход возбуждающего канала, а во второй - тормозящего. Третья и четвертая строки отображают измеренные сигналы на выходе первого и второго SOA соответственно.

Сигнал показанный в столбце **a**, когда на нейрон не посылаются тормозящие импульсы, позволяет увидеть двойную инверсию в SOA. Первый выход SOA является инвертированной версией возбуждающего входа, а второй SOA выполняет повторную инверсию, поэтому его выход является

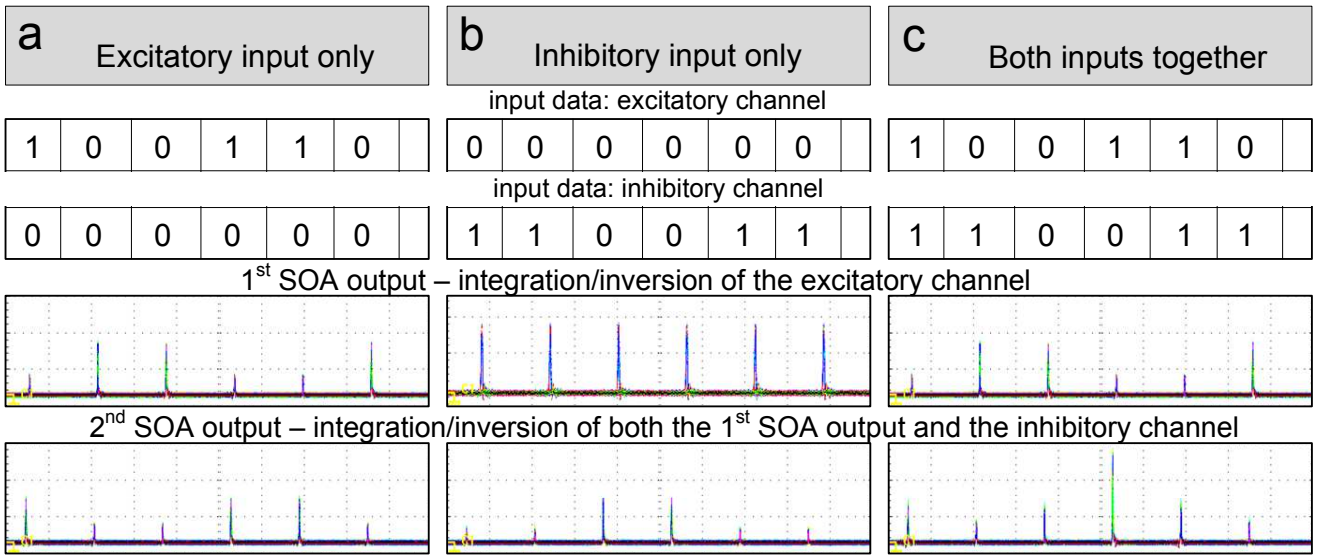

Рисунок 2.7: Измеренные сигналы на выходах двух каскадов нейрона, а также соответствующие входные сигналы. Столбец **a** — в нейрон подаются только возбуждающие импульсы; **b** — только тормозящие импульсы; **c** — подаются и возбуждающие и тормозящие импульсы.

положительным откликом на возбуждающие импульсы и соответствует входной последовательности возбуждения. Точно так же столбец **b** показывает действие только тормозящих импульсов. Поскольку первый выход SOA не зависит от тормозящего входа (см. Рисунок 2.6), он соответствует всем единицам — инверсии возбуждающего входа. Во второй SOA попадает как выход первого SOA, так и тормозящий сигнал, а на его выходе появляется, в свою очередь, их инвертированная версия. Поэтому, нижняя диаграмма в столбце **b** перевернута по отношению к тормозящему входу. В столбце **c** показаны как возбуждающие, так и тормозящие воздействия вместе, что аналогично уже рассмотренному случаю на вставке к Рисунку 2.6.

Важно отметить, что все интегрирующие свойства фотонного нейрона, продемонстрированные в предыдущем разделе, дублируются в настоящей установке как для возбуждающих, так и для тормозящих входов. Таким образом, реализованная модель импульсного нейрона полностью симметрична. Поскольку его интегрирующие и пороговые свойства определяются динамикой носителей в SOA и свойствами порогового элемента, которые полностью идентичны показанным ранее, мы ограничиваем описание этой конструкции предоставленными данными, касающимися взаимодействия между возбуждающими и тормозящими входами. Эта конструкция еще ближе к теоретической модели нейрона, но и она имеет некоторые недостатки, которые кратко изложены в разделе с обсуждением результатов ниже. В следующем разделе будет продемонстрирован другой режим работы нейрона, при котором выходной сигнал нейрона подается на его вход.

2.5. Режим работы с обратной связью

Как и в случае с тормозящими входами, возможность включения в архитектуру нейросети кольцевых цепей с обратной связью имеет большое значение с точки зрения возможности достижения

большой вычислительной мощности, с точки зрения инженерных затрат и эффективности системы, а также с точки зрения эмпирической нейробиологии. Важность роли петель обратной связи в нервной системе не вызывает сомнений и хорошо известна. Петли обратной связи в сочетании с возможностью реконфигурировать элементы обработки на лету обеспечивают естественные средства для повторного использования дорогостоящего оборудования посредством временно́го мультиплексирования и реализации длинных и сложных цепочек обработки сигналов. Здесь мы продемонстрируем модель цепочки оптических нейронов с помощью только одного экземпляра устройства. Его выход соединен с одним из его входов, так что сигнал проходит через одно и то же устройство много раз. Параметры нейрона потенциально могут изменяться от прохода к проходу, что позволяет имитировать различные нейроны в цепи. Такой компромисс между количеством необходимых нейронов и скоростью работы может помочь в разработке более сложных оптических нейронных сетей, используя всего несколько физических устройств. В данной работе демонстрируется простейший случай работы в режиме обратной связи, когда параметры нейрона остаются неизменными. Одним из примеров такой операции, реализованной в нашем исследовании, является буферизация оптического сигнала в контуре.

Работа нейронного буфера сигнала очень похожа на ранее продемонстрированную оптическую петлевую память [56, 57, 58, 59] с той лишь разницей, что в нашей демонстрации задействован фотонный нейрон. Хотя принцип запоминающего контура тривиален (импульсы циркулируют по кругу, а потери сигнала компенсируются усилителем), его практическая реализация требует наличия активной электроники, помогающей противодействовать искажению сигнала и усилению шума. Для этой цели используется несколько методов, которые служат двум целям: удержание импульсов в выделенных временных интервалах и поддержание их амплитуды на уровне «ноль» или «единица». Хотя последнее может быть реализовано прямо в оптике с помощью нелинейных эффектов (например, солитонное распространение [57] или нелинейное вращение поляризации [58, 59]), удержание импульсов в выделенных временных интервалах обычно требует использования электроники. Однако самый простой и понятный метод, который использовался в [56], — это опто-электронное преобразование, детектирование с помощью электронных средств и повторная передача сигналов, что мы и используем в этой демонстрации для контура обратной связи.

Принцип действия нейронной петли памяти показан на Рисунке 2.8. Чтобы сохранить повторяющуюся последовательность импульсов, она должна быть сначала передана в нейрон через один из его входов, при этом обратная связь отключена (**a**). Затем необходимо настроить внутреннюю задержку таким образом, чтобы последовательность в цепи обратной связи совпадала с внешним входом (**b**). Это достигается, если общая задержка в цикле (включая задержку внутри нейрона) кратна длине последовательности. Затем включается обратная связь и тогда можно отключить входной сигнал (**c**). Поскольку сигнал обратной связи теперь заменяет собой внешний сигнал, далее последовательность распространяется по петле без изменений.

Блок-схема экспериментальной установки показана на Рисунке 2.9. В этой установке используется преобразование оптического сигнала в электрическое с помощью фотодетектора и модуля восстановления тактовой частоты и данных (clock and data recovery, CDR). Остальная часть уста-

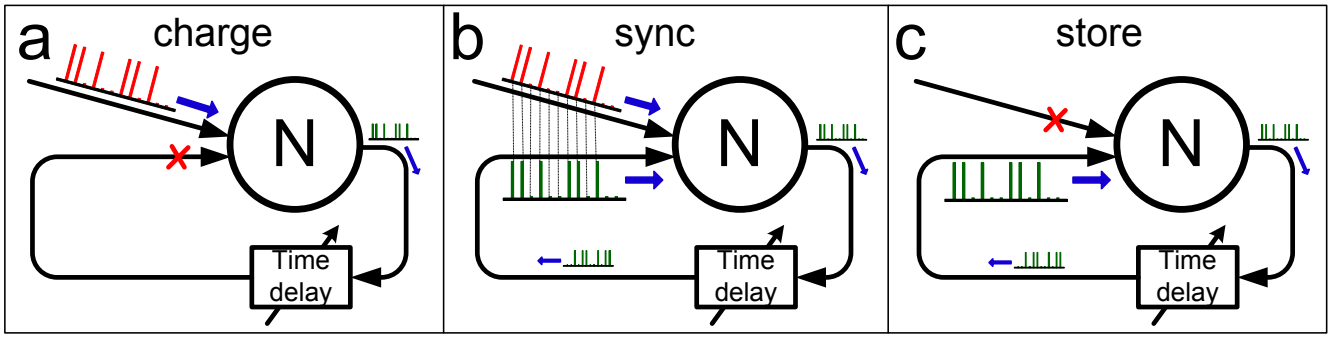

Рисунок 2.8: Принцип хранения информации в нейронной петле с положительной обратной связью. Показаны три стадии процесса.

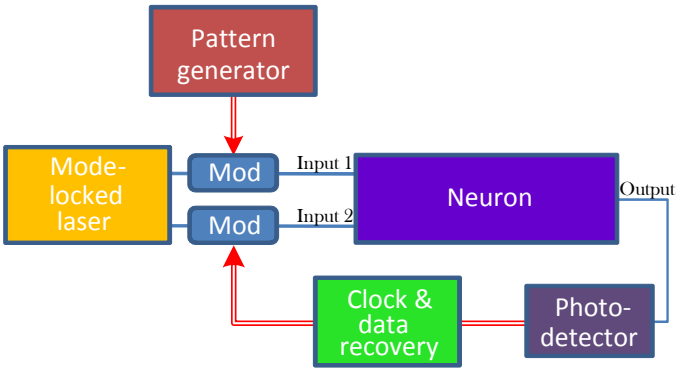

Рисунок 2.9: Схема работы нейрона в режиме обратной связи. Mod — электрооптический модулятор интенсивности типа.

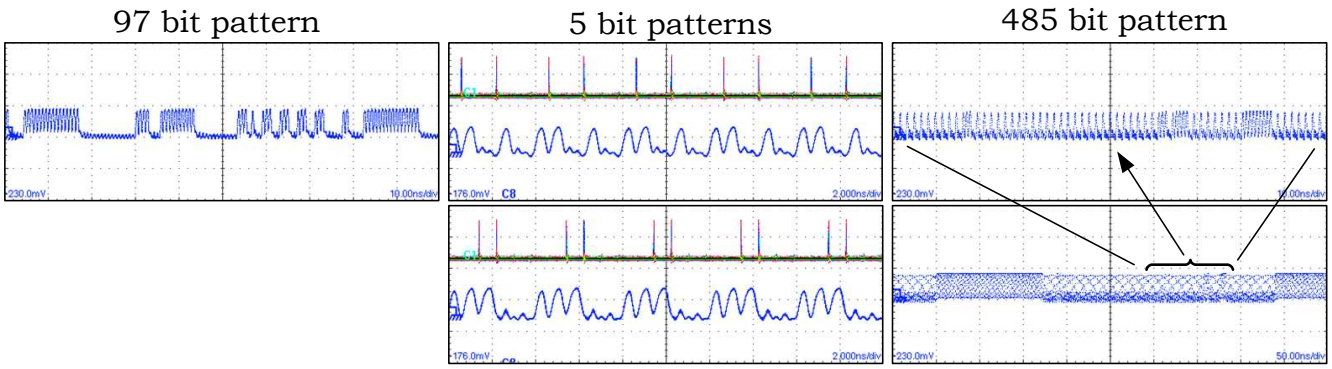

Рисунок 2.10: Примеры сохраненных битовых последовательностей в петле обратной связи с нейроном. Общее время обхода равно 485 битовых интервалов, поэтому в этой конфигурации могут храниться шаблоны длиной 5, 97 и 485 бит. На диаграмме показан один пример шаблона длиной 97 бит, два примера различных 5-битных последовательностей и в последнем столбце 485-битный шаблон. В последнем для наглядности показан увеличенный фрагмент.

новки построена для реализации функций, показанных на блок-схеме на Рисунке 2.8. Первый вход нейрона принимает последовательность импульсов от импульсного лазера с синхронизацией мод, модулированную данными из генератора последовательностей, а второй принимает импульсы, модулированные с использованием сигнала с выхода нейрона. Хотя нейрон всегда работает со новыми оптическими импульсами от лазера, *биты данных*, с помощью которых модулируются импульсы на втором входе, поступают с выхода нейрона, обеспечивая обратную связь. Длина сохраненного шаблона определяется общим временем прохода в цикле, которое составляет 0.39 мкс. При используемой частоте повторения 1.25 Гбит/с это составляет 485 битовых интервалов. Следовательно, битовая комбинация длиной 485 бит должна иметь возможность стабильно распространяться в полученном цикле без изменений при условии, что порог нейрона установлен на достаточно низкое значение, чтобы разрешить срабатывание, вызванное каналом обратной связи. Даже если внешний ввод с данными от генератора последовательностей после этого отключается, последовательность продолжает свое распространение в цикле. Таким образом, данные сохраняются в петле обратной связи с нейроном.

В эксперименте становится возможным „записать“ битовую последовательность в нейрон, посылая модулированную последовательность импульсов на первый вход, а затем наблюдать за распространением этой последовательности в цикле после отключения первого входа. Вместе с длиной шаблона 485 битов также можно хранить более короткие шаблоны, длина которых является делителем числе 485. Поскольку $485 = 5 \times 97$, также можно использовать длины последовательностей равные 5 и 97 бит. На Рисунке 2.10 показаны примеры сохранённых битовых комбинаций в цепи обратной связи с нейроном. Стабильность работы системы в режиме обратной связи такова, что один и тот же шаблон может распространяться в цикле в течение нескольких часов без искажений, что указывает на высокую надежность возможных нейронных цепей, в том числе линейных.

2.6. Обсуждение результатов

Две продемонстрированные конфигурации фотонного нейрона, а также схема с обратной связью, доказывают реализуемость подхода для реализации фотонных нейронных сетей на базе SOA. Однако есть несколько открытых вопросов, требующих отдельного внимания. Поскольку биологические нейроны являются очень гибкими и легко настраиваемыми элементами, возможный диапазон перестройки искусственных нейронов имеет большое значение. Наш подход позволяет широко варьировать многие параметры.

Входная цепь, которая контролирует задержки и веса входящих сигналов, может изменяться в очень широком диапазоне. Что касается весов, их можно очень быстро регулировать с помощью электрооптических амплитудных модуляторов из ниобата лития, которые могут иметь частотную полосу модуляции 40 ГГц и более. Амплитудный диапазон перестройки составляет не менее 20 дБ, и его можно расширить с помощью более медленных аттенюаторов. Задержки входных сигналов намного сложнее контролировать с такой же скоростью. Быстрый подход может заключаться в переключении входов по оптоволоконным путям разной длины, но для этого требуется несколько электрооптических переключателей, вызывающих ослабление сигнала. Механические переключатели или переключатели MEMS с низкими потерями работают намного медленнее, но могут использоваться для изменения задержки большими шагами. Также приемлемы относительно медленные линии задержки с непрерывной перестройкой, но они обычно имеют ограниченный диапазон перестройки, который определяется их физическими размерами.

В предлагаемой конструкции нейрона также возможна подстройка времени интегрирования и порогового уровня. Первый напрямую связан с типом используемого SOA и его током накачки. Чем он выше, тем быстрее восстанавливается коэффициент усиления, т.е. тем меньше время интегрирования. Два типа коммерчески доступных SOA, которые используются в наших демонстрациях, охватывают диапазон перестройки времени восстановления по крайней мере от 100 до примерно 500 пс. Переход к более коротким временам интегрирования также возможен, поскольку коммерчески доступны гораздо более быстрые SOA, время восстановления которых составляет всего 25 пс. Второй параметр, пороговый уровень, также настраивается. Хотя пороговый уровень самого порогового устройства определяется нелинейным элементом и поэтому является фиксированным, эффективный пороговый уровень регулируется путем изменения коэффициента усиления в эрбиевом усилителе, предшествующем пороговому элементу.

Другая проблема связана с представлением сигналов в нашей модели нейрона. Во-первых, поскольку вместо напряжения используется оптический сигнал, появляется дополнительная степень свободы в выборе рабочей длины волны. Чтобы предотвратить интерференцию сигналов и когерентные эффекты между разными входами нейронов, все они должны иметь разные длины волн. В то же время для замера коэффициента усиления SOA требуется еще одна длина волны для пробных импульсов, которая должна отличаться от всех входных длин волн. Хотя это накладывает ограничения на структуру сети, его влияние сводится к минимуму, поскольку длина волны на выходе каждого нейрона может быть выбрана независимо от длины волны на входе благода-

ря двойному преобразованию длины волны в предлагаемой установке. Помимо проблем с длиной волны, импульсный характер оптических сигналов несколько отличается от исходной модели нейрона с импульсами. Поскольку импульсы не производятся нашим нейроном самостоятельно, а фактически лишь модулируются им, они сохраняют синхронность с используемым источником импульсов. Таким образом, для правильной работы нейрона требуется, чтобы интервалы между импульсами были меньше, чем время восстановления SOA, поэтому каждое падение коэффициента усиления гарантированно будет зарегистрировано. Считается, что за счет увеличения частоты следования пробных импульсов можно устранить этот недостаток.

Последний вопрос, который следует рассмотреть, — это проблема уже на уровне нейронной сети. Как упоминалось в предыдущем разделе, в контуре обратной связи используется преобразование оптического сигнала в электрический. Это помогает предотвратить деградацию сигнала после миллионов прохождений через нейрон. Хотя предполагается, что эту работу должны выполнять полностью оптические пороговые устройства, до сих пор нам не удавалось добиться стабильной работы контура без помощи электроники. Эта деградация сигнала накладывает определенные ограничения на размер сети, то есть на количество последовательно соединенных нейронов. Оценка этого числа заслуживает дополнительного изучения, как и дальнейшее исследование возможности улучшения оптических пороговых элементов. Связанные с этим исследования контуров оптической памяти [58, 59] показывают, что как только проблема синхронизации решена, полностью оптического порогового элемента становится достаточно для достижения стабильности. Однако, может случиться так, что для реализации относительно большой фотонной нейронной сети необходимо будет включить в ее состав несколько электронных регенераторов сигнала для обеспечения стабильности. Несмотря на то, что электроника работает намного медленнее, чем используемые полностью оптические устройства, свойство рефрактерности нейрона гарантирует, что частота повторения импульсов на выходе нейрона намного меньше ожидаемой скорости на комбинированном входе. Проводя аналогию с биологическими системами, подобное поведение наблюдается в синапсах, связях между различными нейронами, где относительно медленная химическая реакция используется для передачи импульсов возбуждения от одного нейрона к другому. Несмотря на его медленную работу по сравнению с электрическими процессами *внутри* нейронов, он не ограничивает скорость нейронной сети, поскольку вся быстрая обработка выполняется в нейронах *перед тем*, как сигнал передается к следующему нейрону.

Другая проблема на уровне всей нейронной сети, которую мы до сих пор не рассматривали в нашем исследовании, - это механизмы обучения. Эта важнейшая функция потребует внешней электронной схемы, которая контролирует веса, задержки и другие параметры нейронов. Таким образом, реализация обучения нейронной сети — еще одно направление исследований на пути к реализации полностью оптической реализации нейронных сетей.

2.7. Заключение к Главе 2

В этой 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 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.

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.

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

Глава 3

Классические способы распределения ключей

Третьей ключевой задачей оптических информационных систем является обеспечение защиты информации от несанкционированного доступа. Две другие задачи, передача и обработка информации с помощью оптических инструментов, уже были нами разобраны в предыдущих главах. Первая из этих двух задач и так решается в основном с использованием оптических сигналов, а решение второй с помощью оптики, по-видимому, только пытается начать конкуренцию с электроникой. Задачам организации защиты информации фактически посвящена вся остальная часть диссертации. В этой главе предложен оптический способ обмена условно секретными ключами в рамках классической физики.

Задача распределения секретных ключей между абонентами всегда являлась актуальной прикладной задачей для систем связи. Поскольку с помощью таких ключей можно организовать зашифровку любой передаваемой информации, защищенные методы распределения ключей, по сути, глобально решают и задачу защищенного обмена любыми объемами информации. Для шифрования с помощью ранее распределенных ключей можно использовать стандартные блочные шифры, например, AES или ГОСТ Р 34.12-2018 „Кузнечик“.

Существуют различные способы организации распределения ключей. В рамках классической физики существуют два основных подхода: 1) использование представления и защиты информации на физическом уровне; 2) использование принципов стеганографии, т.е. сокрытия самого факта передачи информации. Настоящая работа посвящена распределению ключей на физическом уровне, т.е. первому из этих двух подходов. Будет предложен и экспериментально продемонстрирован метод генерации и распределения секретного ключа с использованием фазовых флуктуаций в волоконно-оптических линиях связи. Полученный ключ можно использовать для обеспечения защищенного обмена данными между абонентами. Безопасность нашего подхода основана на фундаментальной асимметрии, связанной с оптическим представлением информации на физическим уровнем: сложность и стоимость инструментов, необходимых подслушивающему злоумышленнику для взлома системы, значительно выше, чем эти же характеристики аппаратуры,

необходимой законным абонентам для распределения ключей. В этом смысле предлагаемый метод аналогичен классическим асимметричным алгоритмам шифрования (Диффи-Хеллмана, RSA и пр.) Основные результаты данного исследования опубликованы в статье [A13].

3.1. Введение

Распространение секретных ключей — сложная проблема, тесно связанная с обеспечением безопасности передаваемых данных. Сегодня наиболее распространенные методы распределения ключей основаны на асимметричной криптографии или криптографии с открытым ключом. Схемы формирования ключей, такие как алгоритм Диффи-Хеллмана, и алгоритмы с открытым ключом, такие как RSA, безопасны лишь в силу нашего понимания сложности задачи разложения чисел на множители или вычисления дискретного логарифма. На настоящее время не существует доказательств состоятельности и надежности таких схем. Более того, существование „односторонних“ функций, лежащих в основе подобных алгоритмов, остается открытым вопросом. Подтверждение факта их существования автоматически приведет к ответу на центральный вопрос теории алгоритмов, а именно, подтвердит, что $P \neq NP$. Более того, недавние достижения в области квантовых вычислений, а именно, демонстрация на эксперименте алгоритма Шора, а также квантового превосходства [60, 61, 62] угрожают серьезно подорвать будущую полезность этих схем с открытым ключом. Единственная действительно надежная альтернатива, известная сегодня, - это квантовая криптография, которая обеспечивает безусловную защищенность ключей. Однако в большинстве случаев это очень дорогое решение, подходящее только для наиболее критических приложений. Поэтому разработка простых, дешевых и эффективных методов распределения ключей также является приоритетной задачей. Методы квантовой криптографии также представлены в настоящей диссертации: им непосредственно посвящена Глава 6.

Одним из многообещающих подходов к распределению секретных ключей является использование базовых свойств оптических коммуникаций на физическом уровне для генерации распределенного секрета. Распределение секретных ключей на физическом уровне было успешно продемонстрировано в беспроводных системах связи [63, 64], где свойство взаимности беспроводного канала с замираниями являлось основой для создания пары ключей. Однако, эти подходы неприменимы к крупным городским и магистральным сетям, где средой передачи практически безальтернативно является оптическое волокно. Физический уровень, лежащий в основе оптической связи, кардинально отличается от беспроводной связи, и поэтому разработка системы распределения секретных ключей на физическом уровне для оптических сетей требует принципиально нового подхода.

История защищенной оптоволоконной связи на физическом уровне достаточно богата. Опубликованы десятки статей, посвященных этой теме с использованием разных подходов. Однако большинство из них, как будет обсуждаться позже, используют наивные предположения о том, что злоумышленник не знает секретный параметр или код, используемый легитимными пользователями; или даже предположение, что злоумышленник Ева не может реализовать „сложный“

метод извлечения данных, используемый в системе. Кроме того, эти методы не предполагают никакой асимметрии, связанной с самим каналом на физическом уровне.

В этом разделе представлена схема распределения секретного ключа для оптической связи, которая использует свойства оптического канала на физическом уровне. Предлагаемый подход основан на мониторинге фазовых флуктуаций в волоконно-оптической линии связи и работает в предположении, что злоумышленник знает всю возможную информацию о системе, даже во время ее работы. Подход является „асимметричным“, то есть реализация системы подслушивания (которая обсуждается далее в статье) значительно сложнее и дороже, чем построение самой системы распределения ключей. Объединение этих двух свойств в одной системе делает ее более выгодной по сравнению с предыдущими подходами, а также более эффективной с точки зрения объема работы, которую должны выполнить легитимные пользователи, чтобы создать серьезные сложности для подслушивающего противника.

3.1.1. Обзор метода

Предлагаемый метод распределения ключей основан на идее крупномасштабного интерферометра, обнаруживающего флуктуации фазы в волоконных линиях связи между абонентами. Простейшая реализация метода показана на Рисунке 3.1, где Алиса и Боб являются терминалами большого интерферометра Маха-Цандера. Наблюдаемый выходной сигнал является результатом интерференции двух оптических полей $\frac{1}{2}E_0e^{i(\omega t+\varphi_1)}$ и $\frac{1}{2}E_0e^{i(\omega t+\varphi_2)}$ приходящих из плеч интерферометра, где E_0 — амплитуда заведенного оптического поля, ω — круговая оптическая частота, а $\varphi_{1,2}$ — полный сдвиг фазы в двух плечах интерферометра. Эффективный коэффициент деления x определяется выражением

$$x = \frac{\left|\frac{1}{2}E_0e^{i\varphi_1} + \frac{1}{2}E_0e^{i\varphi_2}\right|^2}{E_0^2} = \frac{1+\cos(\varphi_1-\varphi_2)}{2} = \frac{1+\cos\Delta\varphi}{2}.$$

Он зависит только от относительного сдвига фазы $\Delta\varphi$ между плечами интерферометра и является одинаковым для обоих направлений распространения. Поскольку фаза в таком большом интерферометре постоянно флуктуирует, коэффициент x является функцией времени. Таким образом, измеряя идентичные функции $x(t)$, Алиса и Боб тем самым получают распределенную *общую случайность*, которую можно затем использовать для формирования идентичных секретных ключей.

В интерферометр с обеих сторон заводится излучение от широкополосного источника света для того, чтобы предотвратить прямое отслеживание фазы в обоих плечах злоумышленником Евой. Более того, поскольку флуктуации фазы распределены по всей длине обоих волокон, Ева не может заменить часть интерферометра своей собственной установкой. Вместо этого, чтобы провести атаку, ей потребуется знать полную характеристику всего интерферометра. Использование такой обширной хаотической системы, как оптоволоконная линия, накладывает множество ограничений на потенциальные стратегии, которые Ева может использовать для подслушивания, что будет подробно обсуждаться в разделе по анализу безопасности ниже.

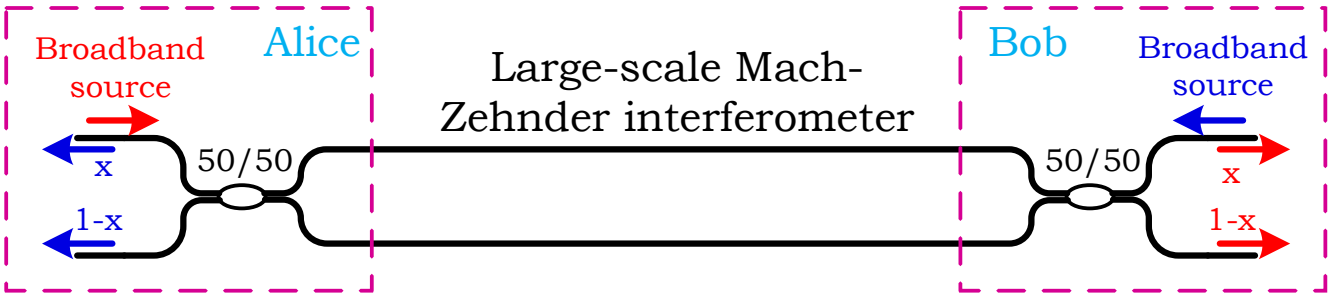

Рисунок 3.1: Схема предлагаемой системы распределения ключей.

3.1.2. Предыдущие подходы к защите классической оптической связи от подслушивания

Вопреки распространенному мнению, даже на заре оптической связи было ясно, что оптическое волокно не обеспечивает физической защиты от подслушивания. Несмотря на то, что несанкционированное подключение к оптоволоконному кабелю является более сложной задачей, чем подключение к электрическому проводу [65], существует множество способов сделать это. Это и утечка света при изгибе волокна, и создание направленного ответвителя путем сварки с другим оптоволокном, и травление оболочки световода для обнажения сердцевины и т. д. Следовательно, стандартное предположение для всех моделей безопасности оптической связи заключалось в том, что злоумышленник имеет доступ к передаваемым сигналам, и, таким образом, передача должна быть защищена средствами, отличными от простой физической изолированности среды от несанкционированного доступа.

Изначально были предприняты несколько попыток сделать передачу данных более защищенной, путем избегания простой амплитудной модуляции типа включения-выключения лазера, при которой все данные четко видны. Использование фазовой модуляции, скачкообразной перестройки несущей или других методов, при которых интенсивность несущей остается постоянной, также не обеспечивает дополнительной защиты, поскольку тот же тип демодулятора и детектора, который используется приемником, может также использоваться и противником. Это привело к существенному интересу к созданию специальных детекторов, параметризованных секретным кодом или функцией, для которых невозможно восстановить данные без этого кода.

Одна из первых реализаций такого метода [65, 66, 67, 68] использовала модулированный по фазе широкополосный сигнал с гомодинным детектированием. Не зная разности хода в используемом несимметричном интерферометре, восстановить данные невозможно. В более поздних подходах использовались более сложные модуляторы/демодуляторы, включая использование секретного оптического кода CDMA ([69] и ссылки в нем). Комбинация этого подхода с „секретным параметром“ со скрытой передачей сигнала на фоне обычного потока данных привела к ряду стеганографических методов, используемых для улучшения конфиденциальности данных на физическом уровне [70, 71]. Некоторые методы включают скремблер секретного канала [72] или кодовый скремблер [69], который делает передачу данных практически необнаружимой, в случае если не

используется соответствующий дескремблер.

Интересный подход был предложен в 2000 году [73], где утверждается, что если Боб и Ева имеют статистически независимый шум в своих измерениях, то можно организовать защищенную схему распределения ключей. Реализация этого протокола, обычно называемого Y-00, может обеспечить очень высокие скорости шифрования данных, вплоть до скоростей в гигабиты в секунду [74]. Однако для этого уже требуется наличие общего секретного ключа, который позже расширяется с помощью псевдослучайной генерации битов. Следовательно, этот метод относится к классу методов на базе „секретного кода“, которые применимы только в особых обстоятельствах, когда существуют предварительно распределенный секрет достаточной длины.

Однако любые методы на базе „секретного параметра“ или „секретного кода“ следует использовать с осторожностью, поскольку противник может узнать необходимые настройки декодера и использовать их для подслушивания. Проблема особенно серьезна, если „секретный код“ неизменен во времени: он в конечном итоге может быть угадан или определен злоумышленником, что было неоднократно показано. Однако, если коды меняются со временем, то возникает вопрос, как защищенным образом распределить коды между сторонами. Наиболее идеализированное решение такой задачи — это шифрование методом одноразового блокнота (см., например, [75]). Оно подразумевает шифрование каждого бита информации собственным битом ключа, но это лишь переводит исходную проблему в другую классическую проблему обеспечения безопасности данных — проблему распределения секретных ключей. Другими словами, для достижения безопасности такой схемы необходимо предполагать, что аналогичная предыдущая проблема безопасного распределения ключей уже решена. Более подробную информацию о некоторых упомянутых методах можно найти в исчерпывающих обзорах [69, 76].

Практически во всех перечисленных выше методах использовалось все более сложное конечное оборудование, в попытках предотвратить подслушивание данных злоумышленником. К сожалению, во всех описанных системах копия установки Алисы или Боба, попавшая в руки Евы, также будет работать и для нее, что делает такие системы абсолютно небезопасными.

Недавно были попытки использовать принципиально новые идеи, основанные на обширном статистическом анализе и шумоподобной передаче с обратной связью [77, 78], однако они не оправдались из-за ошибок в анализе безопасности [79] .

Интересная классическая система распределения ключей была предложена Шойером и Яривом [80], в которой линия связи превращается в гигантский волоконный лазер, а выбор различных оконечных зеркал позволяет получать антикоррелированные последовательности данных на концах линии. Этот метод был усовершенствован для повышения скорости генерации ключей [81, 82], однако до сих пор нет доказательств того, что система защищена от атаки, когда злоумышленник непосредственно измеряет спектр отражения используемого зеркала. Напротив, очевидно, что такая простая атака или ее модификация может разрушить предлагаемую дорогостоящую и технически продвинутую систему.

Последний метод, на котором хотелось бы остановиться, — это система связи на основе интерферометра Саньяка, предложенная в [83], а также в [84]. Это большая петля Саньяка

со смещенным от центра передающим фазовым модулятором и центрированным модулятором, генерирующим фазовый шум. Это единственная система, обеспечивающая асимметрию при подслушивании. Для Алисы и Боба это простая система передачи данных, в которой из-за используемого интерферометра, Боб видит простые модулированные по интенсивности данные, отправленные Алисой. Однако Еве восстановить эти данные относительно сложно. Возможная стратегия (которая стала возможной намного позже, чем был предложен метод) заключается в точном измерении фазовых сдвигов всей установки Алисы в обоих направлениях. Выполнение простых вычислений с двумя полученными функциями позволяет восстановить данные, но, как уже упоминалось, это пример сильно асимметричного метода.

Насколько нам известно, это завершает текущий список классических методов обеспечения безопасности на физическом уровне, применимых к волоконно-оптической связи. Конечно, существует множество методов квантового распределения ключей, некоторые из которых рассмотрены в Главе 6. Оставим их пока за рамками нашего рассмотрения. Подводя итог, можно сказать, что существует лишь несколько методов, которые можно использовать без каких-либо предварительно распределенных общих секретов, и эти методы уязвимы для определенных типов простых атак. Другие методы, которые требуют использования предварительно распределенного „кода“, также важны, но требуют первоначального распределенного секрета, что потребовало бы решения эквивалентной проблемы распределения ключей, прежде чем они могут быть использованы. Следовательно, практическая методика распределения секретных ключей на основе оптических сигналов, которая не полагается на ранее предложенные схемы, очень желательна, особенно если она гарантирует, что сложность потенциального подслушивания значительно больше, чем сложность организации такой связи легитимными пользователями.

3.1.3. Потенциальные сценарии использования

Предлагаемый метод позволяет генерировать идентичные случайные секретные ключи на двух концах длинного интерферометра. Поскольку в этом методе не используются какие-либо искусственные фазовые скремблеры или генераторы шума, которые может активно считывать Ева, а вместо этого используются случайные фазовые флуктуации по всей длине оптоволоконной линии, он обеспечивает естественную защиту от подслушивания. Более того, он не требует наличия какого-либо ранее существовавшего „секрета“ между Алисой и Бобом[1].

Как уже указывалось, данный подход не может гарантировать абсолютную защиту формируемых ключей. Он лишь создает очень серьезные технические проблемы для потенциального злоумышленника, который заинтересован в краже ключей. Таким образом, использование лишь одного данного метода может быть недостаточным для критических приложений. Однако, его можно использовать вместе с другими системами безопасности. Например, естественно представить, что наш метод используется для создания одной половины ключа для последующего шифрова-

[1]Строго говоря, для формирования защищенных ключей необходима аутентификация классического канала связи между Алисой и Бобом. В общем случае, она может требовать пред-распределенного ключа аутентификации.

ния AES, в то время как вторая половина этого же ключа формируется методами асимметричной криптографии. При этом под „половинами“ ключа может подразумеваться либо простая операция XOR между двумя ключами, либо специальные протоколы объединения ключей шифрования. Конечным результатом такой защиты будет ситуация, в которой Еве для взлома криптосистемы потребуются не только вычислительные мощности для взлома асимметричной криптографической части, намного превосходящие вычислительные мощности Алисы или Боба, но и гораздо более совершенные оптические технологии!

Некоторые проблемы в реальных приложениях нашего метода будут связаны с ограниченной скоростью генерации ключей. Как будет показано позже, скорость генерации ключей в типичных условиях составляет порядка 250 бит/с, что намного ниже, чем типичные скорости передачи данных в оптических сетях. Однако это не сильно отличается от ситуации с традиционной криптографией с открытым ключом, где сам асимметричный протокол используется для генерации сеансовых ключей, которые затем используются для гораздо более быстрого симметричного шифрования. Сгенерированный ключ может также стать начальным «кодом», необходимым для некоторых других схем безопасности на физическом уровне, которые допускают шифрование на линейных скоростях [69].

Еще одна практическая проблема — расширение потенциальной дальности распределения ключей. Без каких-либо модификаций метод работает до длины, ограниченной потерями в волокне. Используя чувствительные низкоскоростные фотодетекторы и относительно высокую входную мощность, можно легко справиться с затуханием в 40 дБ, что в идеальном случае составляет около 200 км, а на практике — около 100+ км. Для выхода за эти рамки требуются оптические усилители. Поскольку оба волокна, используемые в установке, переносят двунаправленный поток света, нужны двунаправленные эрбиевые волоконно-оптические усилители. Примеры их использования были успешно продемонстрированы в [85, 86], что дает некоторый оптимизм в отношении будущего масштабирования данного метода.

В следующем разделе мы приводим результаты исследования фазовых флуктуаций в волоконно-оптических линиях связи, которые служат основой предлагаемого метода. Далее мы обсуждаем вопросы, связанные с безопасностью, и формулируем несколько необходимых модификаций, которые делают систему защищенной от подслушивания. В разделе 3.4 предоставлена подробная информация об экспериментальной демонстрации и основных результатах, полученных в ходе экспериментов. Также анализируется достижимая скорость генерации ключей, и представлен простой алгоритм экстракции ключей. В заключение приводится краткое изложение полученных результатов и обсуждение будущей работы по практической реализации этого метода распределения секретных ключей.

3.2. Флуктуации фазы в волоконно-оптических линиях связи

До недавнего времени фазовые флуктуации в волоконно-оптических сетях в значительной степени игнорировались, поскольку все традиционные формы оптической связи были невосприимчивы

к подобным искажениям сигнала в линии. Лишь с развитием когерентной оптической передачи данных, задача компенсации фазовых и поляризационных флуктуаций в канале стала практически важной. Однако, они существенно маскируются флуктуациями между принимаемой несущей и используемым локальным осциллятором. Поскольку эффект от самой линии связи на порядки меньше, чем разница фазы между двумя различными лазерами, его практически невозможно выделить в чистом виде. Флуктуации поляризации обычно еще на несколько порядков медленнее, чем флуктуации фазы, потому что при нормальных условиях фазовые изменения обеих поляризаций практически идентичны.

Фазовые флуктуации становятся ограничивающим фактором, если рассматривать передачу оптических частот на большие расстояния, например для синхронизации оптических часов сверхвысокой точности [87, 88]. Как указано в серии публикаций [87, 89], бóльшая часть фазового шума попадает в килогерцовый спектральный диапазон и приводит к спектральному уширению сверхстабильных по частоте лазерных сигналов. Другие важные приложения, чувствительные к фазовым флуктуациям, включают крупномасштабные эксперименты по квантовой когерентности [90, 91] и квантовые коммуникации [92].

В отличие от вышеупомянутых приложений, наш подход к генерации секретных ключей основан на наличии фазовых флуктуаций в канале и использует их как источник случайности. Для более детального понимания всей физической картины была собрана некоторая информация о фазовых флуктуациях в волоконно-оптических линиях связи. Одно интересное исследование фазовых флуктуаций было опубликовано в [93], где использовались коммерчески установленные оптоволоконные линии связи. Для сравнения с этой работой и подтверждения нашей экспериментальной демонстрации была выполнена серия экспериментальных измерений в наших лабораторных условиях.

Ясно, что флуктуации фазы зависят от длины оптоволоконной линии и среды, в которой она расположена. В нашем исследовании мы измеряли фазовые флуктуации с помощью интерферометра Маха-Цандера, аналогичного тому, который используется в [93]. Для исследования дрожания фазы были выбраны три разных длины плеч интерферометра. Во всех экспериментах измерялась оптическая интенсивность на одном из выходов интерферометра, которая пропорциональна $1+\cos\Delta\varphi(t)$, где $\Delta\varphi(t)$ — разность фаз между двумя плечами. На Рисунках 3.2 и 3.3 показаны образцы измеренных форм сигналов и их спектры, рассчитанные с помощью преобразования Фурье длинной серии измерений.

Как и следовало ожидать, временной масштаб измеряемых флуктуаций напрямую зависит от длины плеч интерферометра. Для самого короткого интерферометра с длиной плеч 2 м фаза заметно изменяется за время порядка 10 секунд, а амплитуда фазовых изменений такова, что фазовый сдвиг никогда не превышает π в серии длиной в 1000 секунд. Преобразование Фурье такого сигнала показывает, что бóльшая часть мощности флуктуаций находится ниже 0,4 Гц. Интерферометр промежуточной длины (100 м) показывает гораздо более быстрые колебания с типичным временем изменения 0,1 с, в то время как большинство колебаний все еще относительно малы, достигая значения π только несколько раз за 10 с. Спектр мощности лежит ниже 60 Гц.

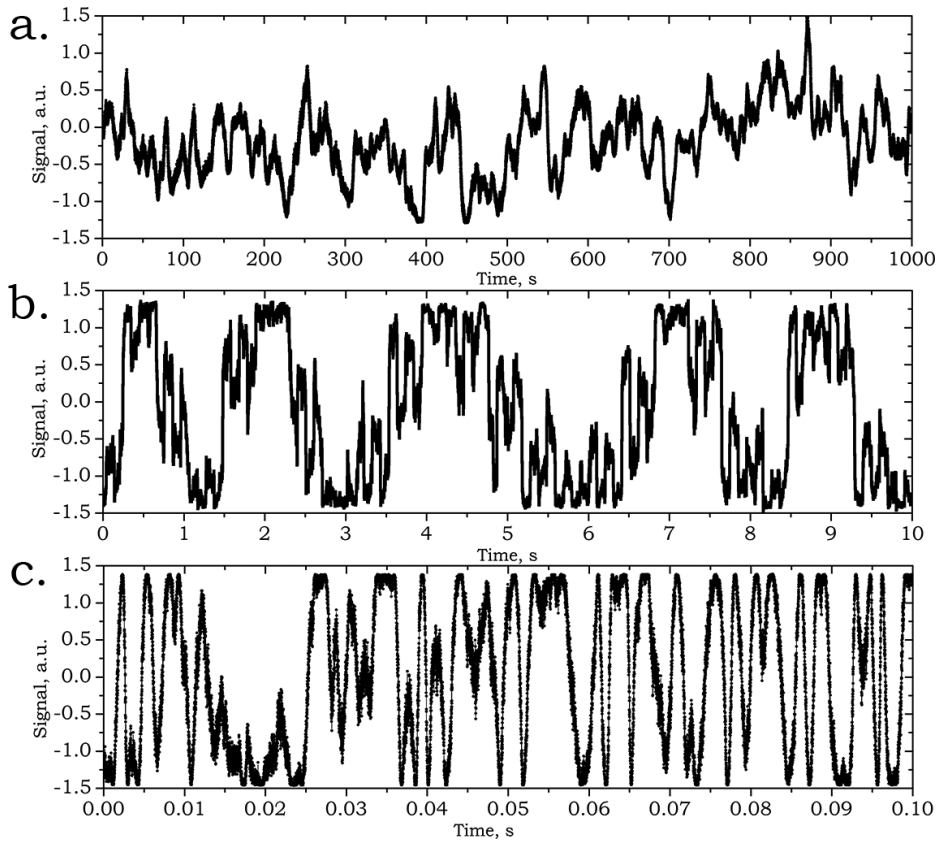

Рисунок 3.2: Флуктуации интенсивности, вызванные фазовыми флуктуациями в интерферометре Маха-Цандера с разной длиной плеч: a. 2 м; b. 100 м; c. 26 км. Кривые нормированы так, что при нулевой разности фаз ($\Delta\varphi = 0$) сигнал равен 1.4, а при противоположных фазах ($\Delta\varphi = \pi$) равен -1.4.

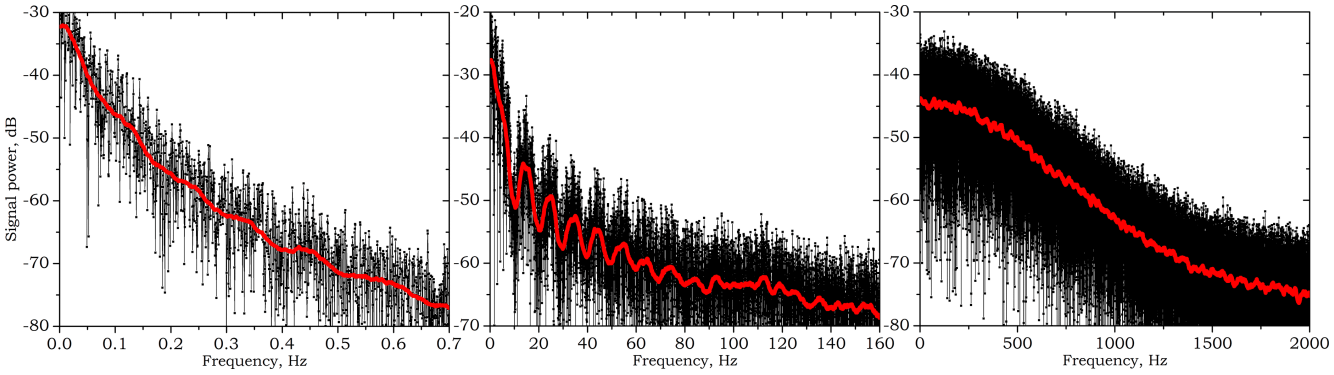

Рисунок 3.3: Фурье спектры фазовых флуктуаций в интерферометре Маха-Цандера: a. длина плеча 2 м; b. длина плеча 100 м; c. длина плеча 26 км.

Самый длинный интерферометр с плечами 26 км ведет себя качественно иначе. Большинство фазовых изменений существенно больше, чем π, поэтому бóльшую часть времени измеренная кривая идет непосредственно от максимума к минимуму и обратно. Временной масштаб таких изменений находится в миллисекундном диапазоне, в то время как ширина спектра мощности колебаний составляет около 1 кГц.

Наше исследование показало, что измеренные флуктуации фазы, особенно в длинном интерферометре, в основном связаны с наличием акустического шума в лабораторных условиях: такой интерферометр чрезвычайно чувствителен к звукам и к малейшим колебаниям. Более медленные эффекты, такие как изменение температуры, также способствуют флуктуациям: преднамеренное изменение температуры плеча интерферометра приводит к сильному фазовому дрейфу и, следовательно, к быстрым, почти периодическим колебаниям интенсивности.

Полученные нами результаты согласуются с экспериментом, проведенным в реальной телекоммуникационной сети [93], что позволяет нам обобщить наши дальнейшие лабораторные эксперименты на случай реальных линий связи.

3.3. Защищенность получаемых ключей от подслушивания

Реализация большинства алгоритмов обеспечения безопасности часто связана с операцией или функцией, которая может быть выполнена только при некоторых очень специфических условиях, доступных легитимным пользователям. В квантовой криптографии осмысленное измерение квантового состояния может быть выполнено только в том случае, если не было предыдущих попыток его измерения. В традиционной асимметричной криптографии факторизация большого числа возможна только при условии, что известен один из сомножителей. Генерация секретного ключа в беспроводных системах [94] возможна, потому что характеристики канала с замиранием уникальны для пары антенн и не могут быть измерены третьей стороной. В оптическом мире также есть операция, которая может быть выполнена только при соблюдении некоторых очень строгих условий - это измерение оптической фазы.

Сложность измерения фазы напрямую связана с невероятно высокой скоростью изменения фазы. На оптических частотах фаза вращается со скоростью порядка 10^{15} рад/с, что не может отслеживаться даже самыми сложными доступными инструментами. Единственный известный и потенциально достижимый метод измерения фазы — это интерференция двух оптических полей между собой. Лишь таким способом можно получить доступ к относительной фазе или разнице между двумя оптическими фазами.

Еще одним сильным ограничением является полоса пропускания доступных приборов: в большинстве ситуаций (обычно называемых некогерентным сложением света) даже характерная частота изменения разницы двух оптических фаз выходит далеко за пределы потенциально измеряемой полосы пропускания, которая ограничена сотнями гигагерц. Таким образом, значимая оценка фазы может быть сделана только в том случае, если разность фаз между двумя интерферирующими оптическими волнами имеет очень узкую (по оптической шкале) частотную полосу, доступную для электроники. Это справедливо только в двух случаях: (1) ширина полосы обоих оптических полей настолько узкая, что их разница также узкополосна; и (2) полоса пропускания полей велика, но фазы коррелированы так, что их разность колеблется намного медленнее и может быть измерена электроникой. Эти два случая обычно называют когерентным сложением света.

Очевидным требованием для успешного проведения такого измерения является то, что оба

оптических поля должны существовать в одной и той же точке пространства. Если это не так, и они разделены по крайней мере несколькими десятками метров, флуктуации фазы, связанные с переносом света через это расстояние, могут привести к значительным ошибкам измерения. Аналогичная проблема возникает, если поля являются широкополосными и коррелированными, но со значительным сдвигом во времени, т.е. одно из них должно быть задержано для выполнения условия (2). Единственный способ задержать оптические сигналы — позволить им распространиться на некоторое расстояние, но это, в свою очередь, приводит к дополнительным фазовым флуктуациям.

Предлагаемая нами схема распределения ключа, Рисунок 3.1, использует крупномасштабный волоконный интерферометр Маха-Цандера, который организуется между двумя сторонами: Алисой и Бобом. Интерферометр расположен так, что конечные светоделители размещены на территории Алисы и Боба в защищенных местах. Если длины плеч интерферометра равны, даже очень широкополосный оптический сигнал, используемый в качестве входа, будет удовлетворять условиям когерентности, а выходная мощность или коэффициент расщепления будут колебаться с относительно медленной частотой. Алиса и Боб могут отслеживать эти изменения и использовать получаемую функцию для генерации секретного ключа. Как упоминалось ранее, эти колебания мощности возникают из-за постоянно меняющейся длины оптического пути, что является результатом тепловых и механических эффектов в волокнах. Если расстояние между Алисой и Бобом относительно велико (несколько километров и более), флуктуации фазы в интерферометре достаточно велики, чтобы создать уникальную картину, которую могут измерить только Алиса и Боб, но не Ева. Его можно легко преобразовать в секретный ключ, который затем можно использовать для традиционной криптографии.

Ниже мы анализируем возможные уязвимости системы и формулируем модель противника, которую мы используем на протяжении всей этой работы. Мы также суммируем все необходимые меры предосторожности, которые следует предпринять для обеспечения надлежащей защиты системы от подслушивания.

3.3.1. Измерения фазы злоумышленником

Если в системе используется широкополосный источник света с частотной полосой, превышающей возможности электроники, предположения об измеримости интерференции оптических полей, изложенные выше, требуют, чтобы два альтернативных оптических пути к точке интерференции сигналов, осуществляемой Евой имеют одинаковую длину.

Возможная стратегия Евы показана на Рисунке 3.4. Она подключается к обоим волокнам, разделяя интерферометр на четыре сегмента: a, b, c и d. Если длина отрезка a равна длине c, Ева может наблюдать интерференцию между a и c, обнаруживая флуктуации фазы в левой части интерферометра. Похожим образом она может наблюдать флуктуации фазы в правой части интерферометра по сигналам из сегментов b и d.

С практической точки зрения, даже эта простая задача требует точной оптики, электрони-

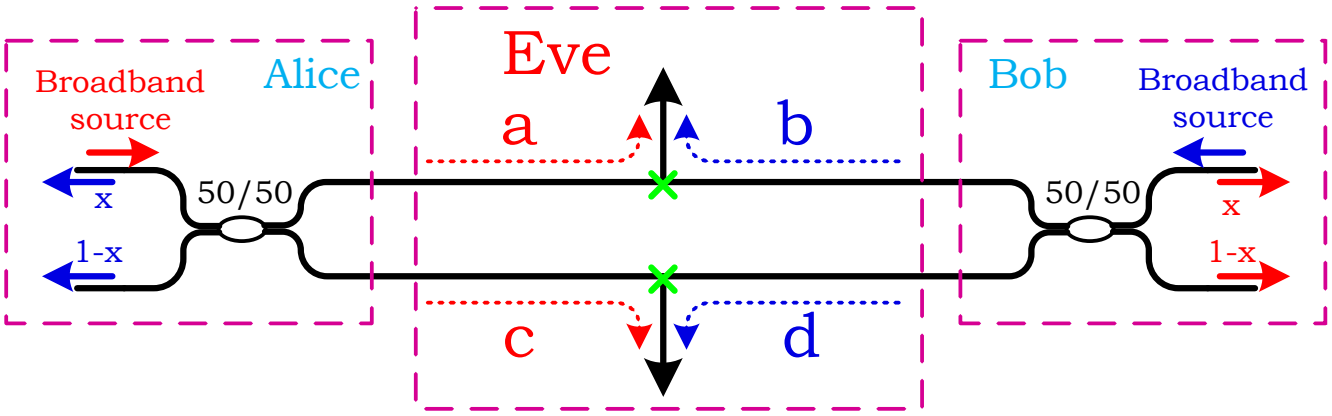

Рисунок 3.4: Система с подключенной подслушивающей аппаратурой.

ки и значительного инженерного искусства. Еве необходимо убедиться, что ее установка, включая подключение к интерферометру, элемент для выравнивания длин оптических путей и само устройство интерференции, не вносит дополнительного дрожания фазы, существенного для работы алгоритма извлечения ключа легитимными пользователями. Более того, поскольку измеряемой величиной является сила света, а не сама фаза, Еве необходимо выполнить соответствующие вычисления, чтобы выделить фазовые флуктуации в обеих частях исходного интерферометра и сложить их вместе для получения искомой разности фаз в интерферометре в целом. Даже в этом случае у нее не будет точной картины, наблюдаемой Алисой и Бобом, поскольку существует неоднозначность в выборе постоянного фазового сдвига между двумя сигналами.

Каждая операция, выполняемая Евой в реальном мире, вносит искажения и ошибки по сравнению с чистым сигналом, измеренным Алисой и Бобом. Медленный уход фазы в установке Евы также неизбежен, поэтому даже в этом случае у Евы будет дополнительная случайность, не наблюдаемая Алисой и Бобом. Как мы упоминали ранее, несмотря на то, что никаких фундаментальных ограничений, препятствующих успешному подслушиванию, не существует, всегда есть много практических и реалистичных ограничений.

Чтобы повысить защиту предлагаемой системы от такой атаки, Алиса и Боб могут создать сильную асимметрию в системе, разместив дополнительные участки волокна на контролируемой территории, как показано на Рисунке 3.5. Длина этих участков волокон должна быть достаточно большой, чтобы они создавали хаотичность фазы, сравнимую с хаотичностью, создаваемую незащищенными отрезками световодов.

В этом случае, чтобы удовлетворить условию когерентности для двух световых полей, Еве необходимо будет реализовать задержку сигнала, соответствующую длине дополнительных пролетов волокна, то есть, ей нужно будет использовать такую же волоконную линию. Волокна, используемые Евой в линии задержки, вызывают практически неизбежные случайные флуктуации фазы, которые также искажают ее измерения. Схожая модификация, улучшающая безопасность схемы, заключается в увеличении расстояния между двумя плечами интерферометра. Если эти световоды установлены на значительном расстоянии друг от друга, Еве придется обязательно покрывать это расстояние своими линиями связи, что также будет вносить дополнительные

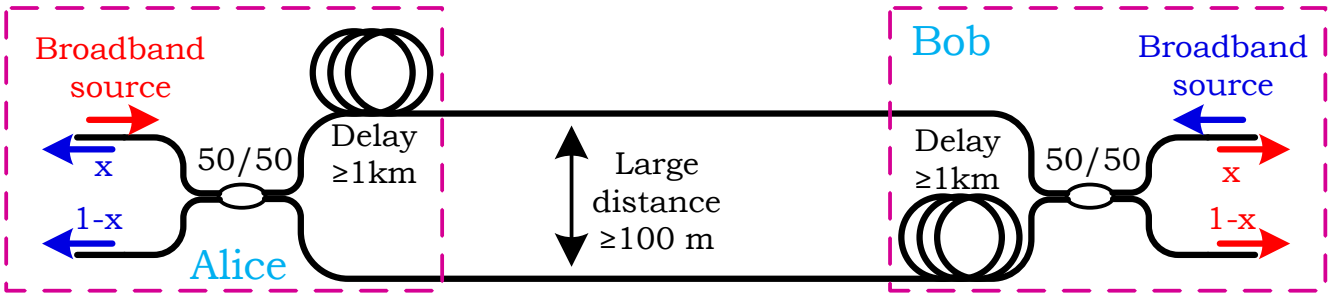

Рисунок 3.5: Система с добавленными линиями задержки, а также с физически разнесенными плечами интерферометра.

фазовые искажения.

Здесь следует упомянуть, что существуют методы стабилизации фазы в волоконно-оптических линиях связи, которые недавно были существенно усовершенствованы [87, 95, 96, 91]. Такие системы достаточно сложны и, по-видимому, в любом случае имеют небольшой остаточный фазовый джиттер. С концептуальной точки зрения неизбежные фазовые искажения, вносимые установкой Евы, приводят к плохой предсказуемости сигнала, измеренного Алисой и Бобом.

3.3.2. Атака с активным внедрением в канал

Все аппаратные реализации даже такого безупречного метода распределения ключей, как квантовая криптография, потенциально имеют ряд уязвимостей, связанных с конкретной аппаратной реализацией. Система может не отличить свой правильный режим работы от специально сконструированного активного вторжения в систему. Это подтверждается рядом успешных атак, осуществленных на коммерческих системах квантового распределения ключей [97, 98, 99, 100]. В этом смысле наша система не является исключением и требует защиты от подобных атак.

Чтобы соответствовать заявляемым техническим требованиям, система должна гарантировать, что измеренные колебания интенсивности являются результатом интерференции между двумя широкополосными оптическими сигналами. Здесь критически важно как условие широкополосности, так и условие интерференции. Например, Ева может разрезать оба волокна интерферометра и послать сигнал с модуляцией интенсивности через одно из волокон Алисе и Бобу. Алиса и Боб по-прежнему будут наблюдать колебания интенсивности, но они будут находиться под полным контролем Евы. В этом случае условие интерференции не выполняется. В качестве альтернативы Ева может использовать узкополосные спектральные фильтры, чтобы ограничить оптическую полосу пропускания сигнала, принимаемого легитимными пользователями. Это позволит измерить фазу стандартным гомодинным методом, таким образом раскрывая распределенный ключ. Это нарушает требование по широкополосности принимаемого сигнала.

Если оба условия соблюдены, система будет работать правильно. Поэтому постоянный мониторинг входящего сигнала важен для безопасности системы. Выполнение первого условия можно контролировать, отведя долю входящих сигналов перед светоделителем и контролируя их оптическую мощность. Каждое из плеч не должно иметь модуляции интенсивности, в то время как

результат их интерференции оказывается модулированным из-за наличия фазовых флуктуаций. Второе условие легко контролировать, глядя на интерференцию тех же сигналов с дополнительной задержкой в одном из плеч. Если задержка больше, чем время когерентности для широкополосного света, колебаний мощности не будет. Если вместо этого на входе окажется достаточно узкополосное излучение, его время когерентности будет существенно больше, и, в результате два пучка будут интерферировать, давая схожую картину, что и на выходе основной системы.

3.3.3. Другие соображения

Ключевым моментом модели противника, которая используется в этой работе, является неспособность Евы проводить прямые измерения оптической фазы широкополосного оптического сигнала и ее неспособность передавать (задерживать) оптические сигналы на большие расстояния без внесения дополнительных фазовых искажений. Еще раз отметим, что эти ограничения не являются фундаментальными, а скорее основаны на практической сложности реализации этих задач. Помимо двух предположений, упомянутых выше, важны еще несколько предположений.

Как и большинство других схем, включая квантовое распределение ключей, предлагаемый метод не обеспечивает аутентификации, что делает его потенциально уязвимым для атак типа «человек посередине». В нашем анализе мы предполагаем, что Алиса и Боб имеют доступ к аутентифицированному общедоступному каналу, который может прослушиваться, но не изменяться Евой. Это позволяет им обмениваться информацией для построения коррелированных битовых последовательностей из аналоговых сигналов и выполнять исправление ошибок в полученных сырых ключах. Чтобы предотвратить атаку «человек посередине», Алиса и Боб могут публично обменяться случайной выборкой из сгенерированного ключа, чтобы убедиться, что большой интерферометр связывает их непосредственно друг с другом.

Мы также предполагаем, что алгоритм формирования ключей известен Еве. Ева может подключиться к плечам интерферометра и произвести любые практически возможные измерения проходящих сигналов. Предполагается, что она знает все характеристики конкретной экспериментальной реализации, то есть любые практически измеримые величины. Чего она не может сделать, так это предсказать или косвенно измерить флуктуации фазы в волокнах на основе измерений среды, в которой размещены волокна. Даже если это потенциально приемлемо для незащищенных участков волокна, участки волокна, хранящиеся в защищенных зонах, контролируемых Алисой и Бобом, вносят дополнительную случайность, совершенно непредсказуемую Евой.

Сильным преимуществом предложенного подхода является то, что основным источником случайности, используемым для генерации ключа, является распределенная система длиной в несколько километров, а не локальный источник шума, который может контролироваться противником или быть уязвимым к воздействию на него извне. Таким образом, любые попытки локального управления системой терпят неудачу, потому что неконтролируемые части системы создают достаточно случайности. Одна потенциальная уязвимость, которую легко избежать, — это искусственное создание чрезмерного фазового шума Евой, таким образом, чтобы обеспечить

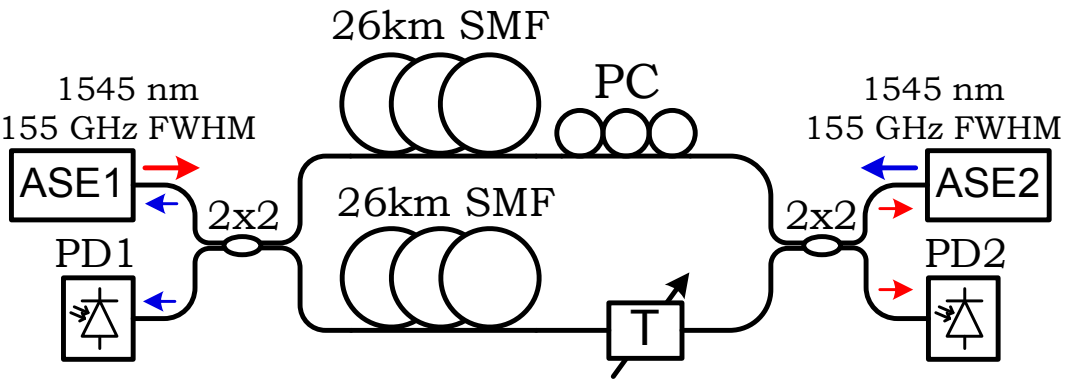

Рисунок 3.6: Схема экспериментальной установки. ASE – широкополосный источник на базе усиленного спонтанного излучения; PD – фотодиод; 2x2 – волоконный светоделитель с отношением 50/50; SMF – одномодовый световод; PC – контроллер поляризации; T – переменная линия задержки.

гораздо более сильные фазовые флуктуации, по сравнению с обычным их уровнем. В этом случае большая часть энтропии сгенерированного ключа будет напрямую связана с действиями Евы, а не распределенными фазовыми флуктуациями. Чтобы предотвратить это, разработчики системы должны оценить ожидаемую скорость генерации ключей и генерировать ошибку, если в ней наблюдаются гораздо более быстрые колебания фазы. Другими словами, скорость генерации ключей не должна превышать скорость генерации энтропии в нормальном процессе фазовых флуктуаций в плечах интерферометра, даже если *измеренные* фазовые флуктуации позволяют значительно ускорить генерацию ключей.

3.4. Экспериментальная реализация

3.4.1. Экспериментальная установка

Экспериментальная установка схематически показана на Рисунке 3.6. Она содержит два независимых широкополосных источника усиленного спонтанного излучения (ASE), ASE1 и ASE2. Каждый из них представляет собой эрбиевый волоконный усилитель (EDFA), работающий без входного сигнала и тонкопленочный полосовой фильтр, ограничивающий полосу пропускания до 155 ГГц на полувысоте. Центральные длины волн двух источников одинаковы в пределах точности стандартных тонкопленочных фильтров, использованных в установке. Далее сигнал предварительно усиливается до мощности приблизительно +6 дБм и подается на вход интерферометра. Одномодовый световод, используемый в интерферометре, — это стандартное оптоволокно типа Corning SMF-28e. Плечи интерферометра также содержат контроллер поляризации и переменную линию задержки, что позволяет регулировать относительную поляризацию и длину двух плеч. Общая длина интерферометра составляет примерно 26 030 м, что соответствует общей задержке распространения 127.5 мкс.

В работе в качестве приемников излучения использовались быстрые PIN фотодиоды на

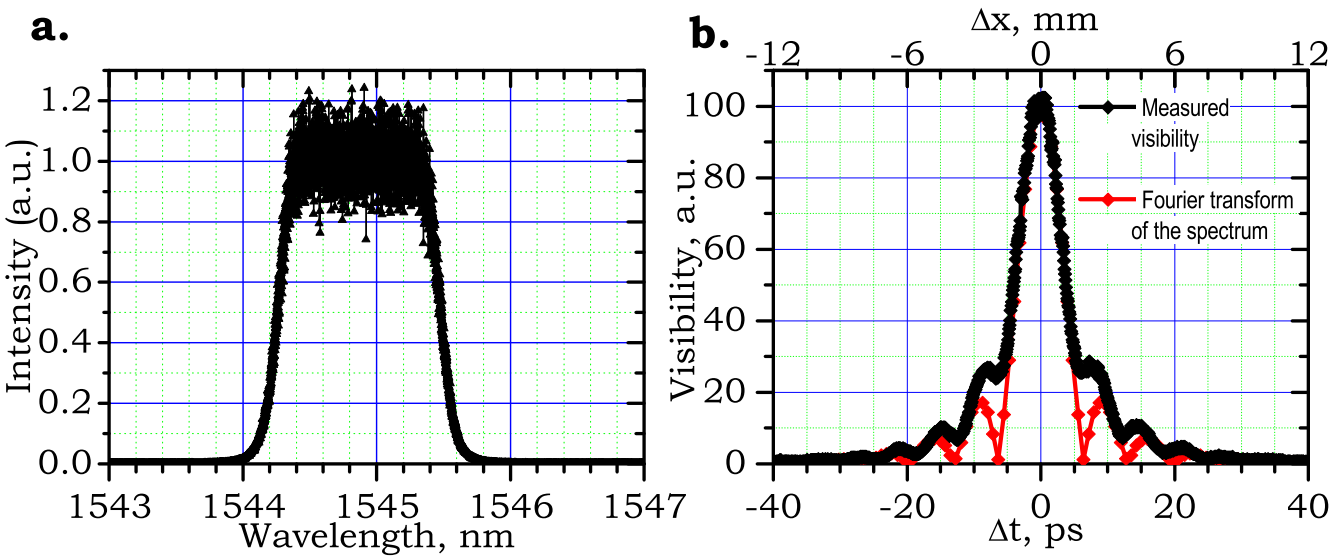

Рисунок 3.7: Характеристики широкополосного оптического сигнала, использованного в экспериментах: a. оптический спектр сигнала; b. измеренная видность интерференции в зависимости от временно́й задержки (изменения длины оптического пути), а также преобразование Фурье спектра сигнала.

базе арсенида галлия с предусилителем, обеспечивающем связь по постоянному току и полосу усиления до 10 ГГц.

Настройка интерферометра включает два этапа: выравнивание длин плеч и настройку поляризаций и оптических мощностей. Первый из них наиболее важен, потому что без выравнивания длины плеч биения между сигналами будут очень широкополосными (порядка 150 ГГц) и, следовательно, не могут быть измерены в эксперименте. Длина когерентности сигналов составляет $L_{coh} \approx c/\Delta\nu \approx 2$ мм. Измеренный спектр используемого сигнала показан на Рисунке 3.7(a). Из-за своей шумовой природы спектр такого излучения также очень зашумлен. Когда плечи интерферометра в точности равны, амплитуда регистрируемых колебаний мощности максимальна. При изменении задержки в одном из плеч амплитуда уменьшается пока колебания не перестают наблюдаться вовсе. Измеренная амплитуда колебаний в зависимости от положения линии задержки показана на Рисунке 3.7(b) черными маркерами. В идеале форма этой кривой должна соответствовать преобразованию Фурье спектра сигнала, которое показано на рисунке красной линией. Обе кривые очень похожи, однако экспериментальная кривая не спадает до нуля в своих минимумах.

Второй этап настройки системы необходим для выравнивания поляризации излучения на выходном светоделителе, а также выравнивания мощностей сигналов. Если две поляризации ортогональны друг другу, оптические поля не интерферируют, а наблюдаемая выходная мощность составит половину суммы входных мощностей, то есть будет оставаться постоянной. Если же поляризации выровнены, результат интерференции будет варьироваться от нуля (деструктивная интерференция) до суммы входных мощностей (конструктивная интерференция). Это справедливо, если два интерферирующих поля имеют одинаковую интенсивность, что всегда имеет место в этой установке. Любые отклонения от этих идеальных условий немного уменьшают глубину

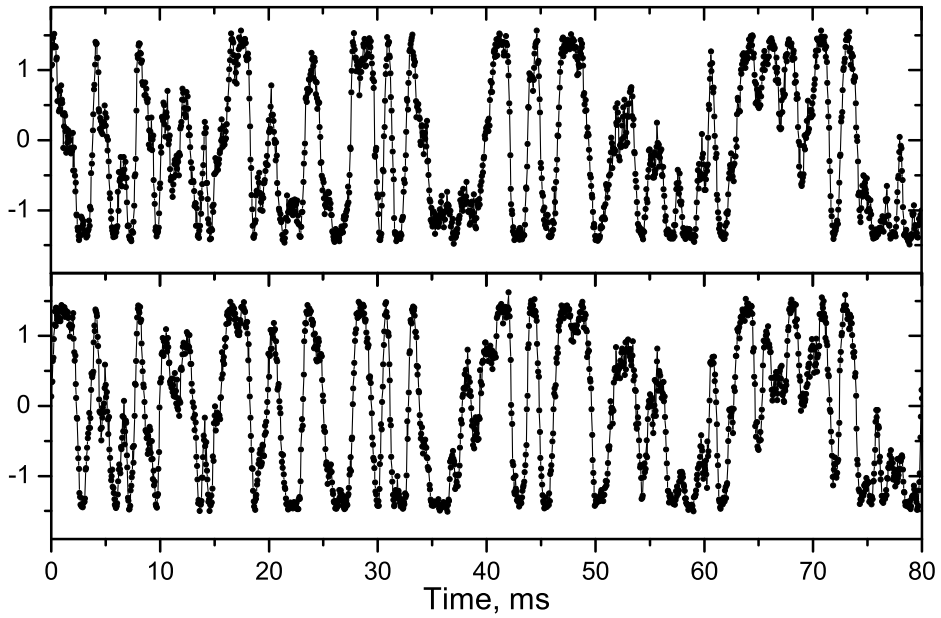

Рисунок 3.8: Пример сигналов, измеренных Алисой и Бобом на двух концах 26-километрового интерферометра Маха-Цандера. Измеренные сигналы сильно коррелированы, однако они имеют заметные различия из-за конечного времени распространение света в интерферометре.

наблюдаемых колебаний, однако, пока колебания видны, их можно использовать для генерации ключа.

3.4.2. Экстракция ключа

После того, как оборудование настроено и функционирует, Алисе и Бобу необходим протокол для извлечения бинарных ключей из полученных аналоговых сигналов, измеренных фотодетекторами. Подобные алгоритмы исследовались в серии публикаций об обеспечении безопасности беспроводной связи на физическом уровне [101, 102]. В нашей работе основной фокус нацелен на оценку достижимой скорости генерации ключей, которая является одной из ключевых рабочих характеристик для методов распределения ключей.

Реализация любой схемы извлечения ключа требует знания статистических свойств необработанных сигналов. В нашей демонстрации проводилась оцифровка полученных сигналов с помощью 16-битной платы сбора данных (National Instruments USB-6211) с частотой дискретизации 20 кГц. Пример измеренных сигналов показан на Рисунке 3.8, где два сигнала, измеренные Алисой и Бобом, показаны с одной и той же шкалой времени. Формы двух сигналов похожи, однако между ними есть заметные различия. Различия возникают в основном из-за конечного времени прохождения света через интерферометр, поэтому состояние волокна может быть слегка различным для прямой и обратной световых волн. Таким образом, условия интерференции также могут немного отличаться, что приводит к расхождению между принимаемыми сигналами.

Для наглядности были вычислены спектры мощности для одного из измеренных каналов, а также для разницы между двумя каналами. Оба спектра представлены на Рисунке 3.9. Как следует

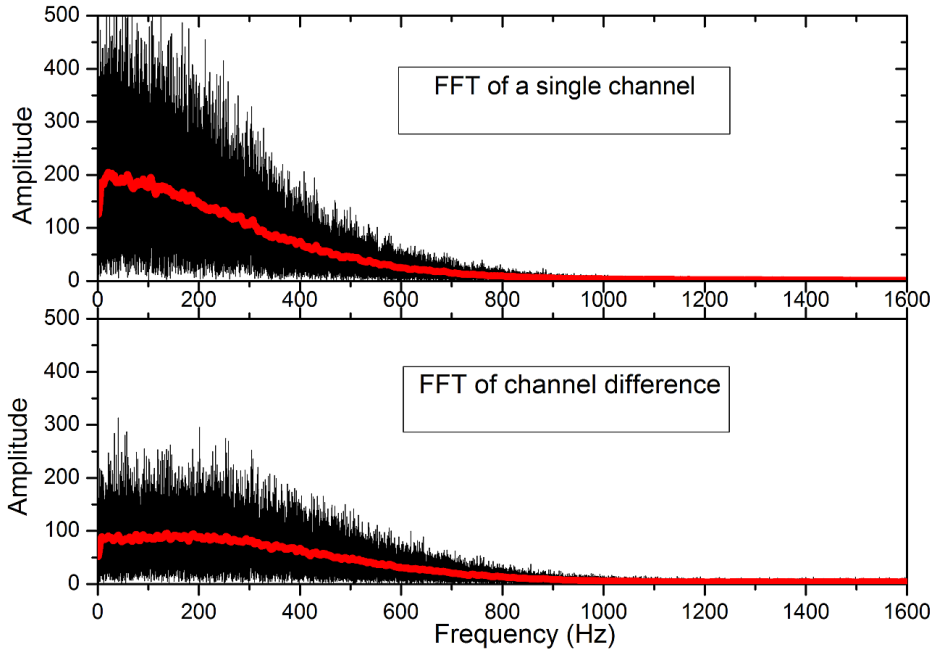

Рисунок 3.9: Вычисленный спектр мощности одного канала и разницы между двумя каналами. Сильное снижение мощности колебаний на частотах ниже 400 Гц свидетельствует о высокой корреляции низкочастотных компонентов сигналов.

из графика, спектральные составляющие выше 400 Гц почти не коррелированы, что приводит к приблизительно одинаковому спектру на обоих графиках, в то время как более низкие частоты демонстрируют значительно меньшую мощность для разницы двух сигналов, чем для одного из них. Это указывает на сильную корреляцию между каналами на частотах ниже 400 Гц.

С теоретической точки зрения, получение коррелированных сигналов требует, чтобы состояние волокна существенно не изменялось за время пролета сигнала, равное $\tau \approx 130$ мкс, что приводит к максимальной частоте коррелированных колебаний $\nu_{max} = \Delta\varphi/(2\pi\tau) = 380$ Гц, если фазовая ошибка равна $\Delta\varphi = \pi/10$. Эта простейшая модель системы, таким образом, дает результат, соответствующий непосредственным экспериментальным наблюдениям, что свидетельствует о разумности ее применения.

Еще одна интересная цифра — это коэффициент линейной корреляции и его поведение при сдвиге во времени. Поскольку корреляция между двумя сигналами является линейной, то есть формы сигналов просто повторяют друг друга, коэффициент линейной корреляции является хорошей мерой сходства форм сигналов. На Рисунке 3.10 показаны функции авто- и взаимной корреляции от временного сдвига. Взаимная корреляция при нулевом временном сдвиге, то есть максимальная взаимная корреляция, показывает, насколько похожи две формы сигнала, в то время как ширина кривых корреляции указывает на время декорреляции. Как следует из рисунка, максимальный коэффициент взаимной корреляции составляет 0.75, что свидетельствует о существенном сходстве между двумя сигналами. Полное время декорреляции для нашей реализации составляет менее 2 мс, т.е. „память“ системы соответствует времени около 2 мс. Любые два измерения, выполненные с интервалом времени более 2 мс, приводят к полностью независимым числам.

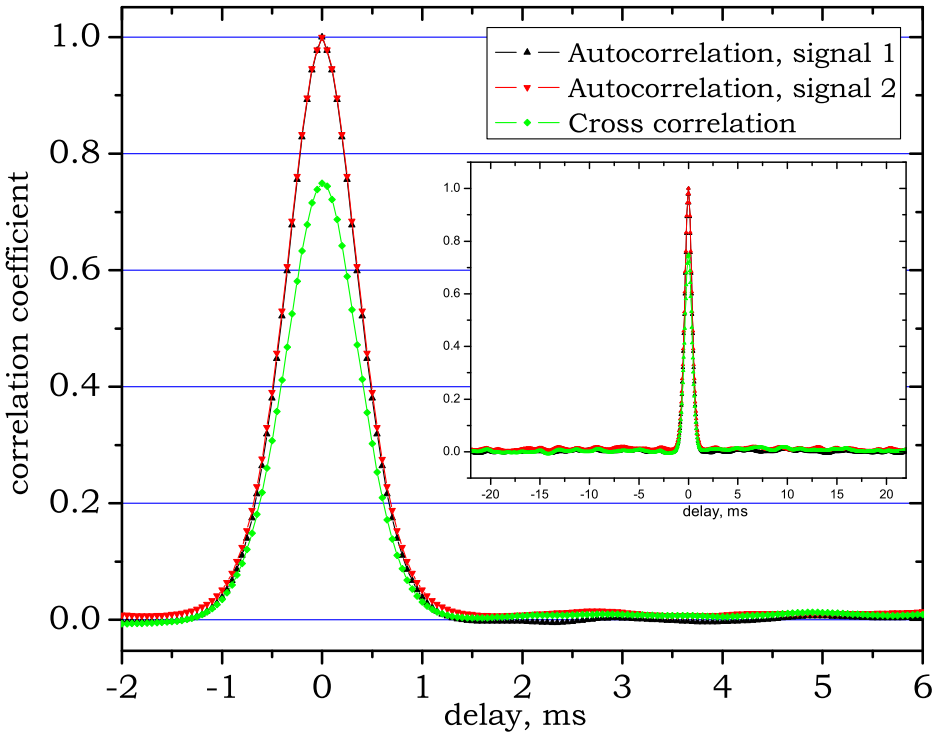

Рисунок 3.10: Автокорреляционные функции для двух сигналов, измеренных Алисой и Бобом, и взаимная корреляция между ними. На вставке показаны те же корреляционные функции для бóльшего промежутка времени, которые подтверждает полную декорреляцию сигналов для относительной задержки между ними более 2 мс.

Основываясь на представленном анализе, был реализован простой протокол экстракции ключей, который использует переходы уровня или отходы сигнала от среднего значения [102]. Сначала оцифрованные сигналы масштабируются по амплитуде для получения единичной дисперсии сигнала и сдвигаются, чтобы удалить постоянный сдвиг по времени между ними. Затем каждый из оцифрованных сигналов обрабатывается для нахождения непрерывных блоков выборок со значениями $|x_i| > 0.9$, что соответствует эмпирически выбранному порогу. Каждый такой блок представляет собой отход от среднего значения, потенциально подходящий для извлечения небольшого количества информации. Затем Алиса сообщает Бобу временные индексы начальной и конечной выборок в каждом из найденных отходов. Предполагается, что часы Алисы и Боба синхронизированы, что можно легко сделать с помощью глобальной системы позиционирования GPS/-ГЛОНАСС. Боб сравнивает найденные им отходы от среднего с найденными Алисой, и, если они перекрываются, отмечает отсчет в середине перекрывающейся области. При такой разметке Боб должен гарантировать, что временной интервал между соседними помеченными выборками больше, чем время декорреляции, чтобы избежать любых корреляций между битами в необработанном ключе. На основе помеченных отчетов он создает свой сырой ключ, в котором единице соответствуют значения выше положительного порога, а нулю — ниже отрицательного. Он также отправляет Алисе все отмеченные временны́е индексы, и она таким же образом создает свой необработанный ключ.

Для извлечения ключа мы использовали блоки данных размером 500 000 отсчетов, представляющие 25-секундные интервалы времени. Каждый блок обрабатывался независимо. Обсуждаемый простой метод извлечения ключа продемонстрировал среднюю скорость генерации необработанного ключа 160 бит/с с долей ошибок менее 4%. Эту относительно небольшую долю битовых ошибок можно легко исправить с помощью обычных алгоритмов коррекции ошибок, использующихся в квантовом распределении ключей. Например с использованием протокола *каскад* [103] или протоколов на основе кодов LDPC [104]. Полученная скорость генерации секретного ключа, очевидно, недостаточно высока для прямого шифрования данных методом одноразового блокнота, как это иногда делается в некоторых современных системах квантового распределения ключей, обеспечивающих генерацию ключа со скоростями 10 и даже 100 кбит/с [105]. Тем не менее, использование одноразового блокнота обычно и не предполагается, в частности из-за невозможности контролировать целостность данных. С другой стороны, скорость генерации ключа 160 бит/с не только более чем достаточна для своевременного обновления ключей для симметричного шифрования, такого как AES или ГОСТ Р 34.12-2018 „Кузнечик“, но также сравнима с производительностью коммерческих систем квантового распределения ключей, например ID Quantique *Cerberis*, обеспечивающий около 400 бит/с на 13 км [105]. Типичные сервисы защиты данных высокого уровня, такие как 802.1X, рекомендуют менять ключи примерно раз в час, и, таким образом, предлагаемый метод идеально подходит для снабжения их ключевым материалом, поскольку он может обновлять 256-битные ключи несколько раз в минуту.

Другой способ оценки достижимой скорости генерации ключей основан на расчетах взаимной информации между выборками, полученными Алисой и Бобом. Мы использовали два разных алгоритма для оценки взаимной информации: один основан на адаптивной группировке [106], а другой — на расстоянии до k-го ближайшего соседа [107]. Взаимная информация для одной выборки, измеренной Алисой и Бобом, была вычислена на серии из 500 000 выборок, взятых с интервалами времени 3 мс, чтобы гарантировать их независимость. Оба алгоритма показали очень похожие результаты, равные 0.51 ± 0.02 бит на измерение. Если брать независимые выборки каждые 2 мс, то скорость распределения взаимной информации превышает 250 бит/сек. Это лишь немного больше, чем было получено с помощью тривиального протокола, основанного на отклонениях сигнала. Это связано с тем, что в этой оценке мы предполагали только одну выборку за время декорреляции, в то время как учет формы сигнала внутри этого интервала приведет к гораздо большему значению взаимной информации. Таким образом, улучшение алгоритма экстракции должно легко обеспечить скорость распределения ключей до уровня не менее 250 бит секретного ключа в секунду, что является частью нашей текущей работы.

3.5. Заключение к Главе 3

Предложен и экспериментально продемонстрирован метод распределения секретных ключей, основанный на физических свойствах волоконно-оптических линий связи. 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.

Продемонстрированный метод распределения ключей использует крупномасштабный интерферометр Маха-Цандера, покрывающий все расстояние между взаимодействующими сторонами. 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 безопасного распределения ключей с помощью этого метода является наличие аутентифицированного классического канала связи между пользователями. Это позволяет избежать атаки типа «человек посередине». Представленная 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.

Глава 4

Каналы связи по открытому пространству

На этом мы заканчиваем обзор предложенных *классических* оптических решений для представления информации в виде оптических сигналов, её обработки, передачи и защиты и переходим к более наукоемкой и технически продвинутой области *квантовых* коммуникаций. Прежде чем рассмотреть непосредственно методы квантового распределения ключей, будут исследованы вопросы передачи (квантовых) оптических сигналов по открытому пространству и вопросы измерения квантовых состояний — 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: временно́го (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 этой главе предложена и экспериментально подтверждена модель каналов, предназначенных для передачи пространственных квантовых состояний света через турбулентную атмосферу, а также исследованы экспериментальные методы изучения таких каналов; следующая глава посвящена основному измерительному инструменту для пространственных квантовых состояний света — томографии пространственных квантовых состояний.

4.1. Турбулентная камера

Для начала была проведена экспериментальная работа по созданию инструментов исследования турбулентных каналов связи. При этом мы ориентировались на работы [108, 109], в которых подробно описаны генераторы турбулентности и методы измерения их параметров.

Была собрана турбулентная камера, позволяющая создавать контролируемый турбулентный

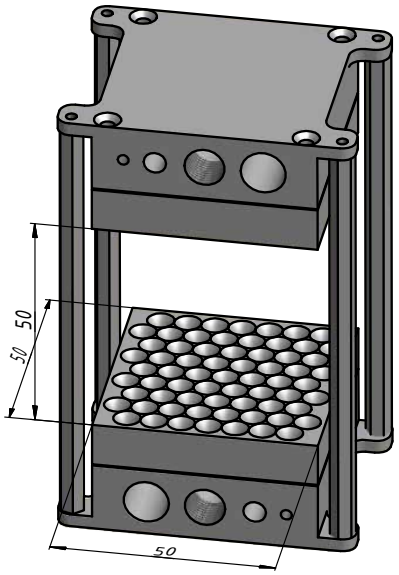

Рисунок 4.1: Чертеж устройства турбулентной камеры.

поток, через который пропускается оптический сигнал. Согласно литературным данным, данная конфигурация позволяет моделировать атмосферные оптические каналы различной длины с различными атмосферными условиями. При этом, контролируемыми параметрами, от которых зависит характер турбулентности, являются: 1) разность температур смешивающихся воздушных потоков; 2) объемный расход протекающего воздуха; 3) диаметр пучка оптического сигнала. Изменение разности температур влияет в первую очередь на амплитуду фазовых искажений оптического пучка, расход воздуха – на временны́е характеристики и размер неоднородностей, диаметр пучка подбирается с целью достижения требуемого соотношения размера неоднородности к размеру пучка.

Турбулентная камера представляет собой две многосопельные форсунки, выточенные из алюминиевого сплава, к которым по шлангам подается воздух, см. Рисунок 4.1. На Рисунке 4.2 показаны фотографии собранной камеры в рабочем состоянии.

Каждая из форсунок создает практически однородный поток по своей площади, тем самым обеспечивая образование турбулентного смешивания двух потоков, максимально однородного по объему внутреннего пространства камеры. Его размеры составляют 50x50x50 мм^3. Соотношение длины воздушных каналов внутри форсунок и их сечения таково, что можно считать температуру выходящего воздуха всегда равной температуре материала форсунок, которая измеряется встроенной термопарой. Расход воздуха задается пропусканием сжатого воздуха с контролируемым давлением через сужение-жиклер. В настоящий момент используется жиклер толщиной 3 мм с диаметром отверстия 1.6 мм. Давление перед жиклером регулируется промышленным перестраиваемым регулятором давления и контролируется с помощью манометра с диапазоном измерений 0-0.3 МПа (0-3 атм). Сопротивление остального воздушного тракта таково, что избыточное давление после жиклера составляет не более нескольких процентов от давления на входе жиклера, таким образом, входной манометр практически точно измеряет перепад давления на жиклере.

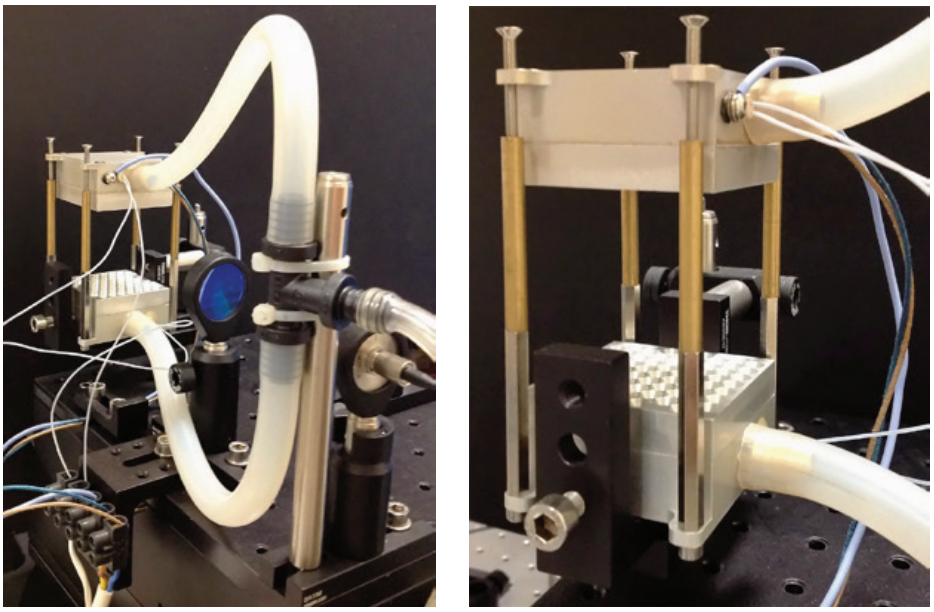

Рисунок 4.2: Внешний вид турбулентной камеры в рабочем состоянии.

Это позволяет использовать стандартные формулы для расчета потока воздуха через жиклер непосредственно по показаниям манометра. Точная калибровка была проведена с использованием промышленного измерителя потока воздуха с диапазоном измерения до 30 л/мин. К сожалению, этот диапазон не полностью покрывает возможности нашей установки, ввиду чего для бóльших потоков была проведена экстраполяция по известным формулам. Калибровочный график представлен на Рисунке 4.3. Как видно из рисунка, поток воздуха через жиклер составляет от 0 до 80 л/мин. Этот поток делится на две форсунки симметричным разветвителем, так что поток через каждую из форсунок составляет $1/2$ от указанной величины.

Для контроля разности температур используется промышленный измеритель-регулятор, работающий по пропорционально-интегрально-дифференциальному (ПИД) закону регулирования. Измерение разности температур происходит по дифференциальному напряжению двух термопар, размещенных в материале форсунок. Нагрев одной из форсунок осуществляется электрическим нагревателем, вмонтированным в нее. Нагреватель питается от сети ~220 В через твердотельное реле, управляемое измерителем-регулятором. Правильная настройка закона регулирования позволила добиться быстрого выхода на нужную разность температур практически без переколебаний. Данная камера позволяет проводить измерения при разности температур до 200 К, что более чем достаточно для моделирования даже очень сильной атмосферной турбулентности.

Расположение горячей и холодной форсунок было продиктовано особенностями движения нагретого воздуха: так как горячий воздух «всплывает» вверх из-за наличия сил гравитации, нагретая форсунка располагается над холодной и направляет свой поток воздуха вертикально вниз. В противном случае, даже без искусственного нагнетания воздуха в горячую форсунку, нагретый о тело форсунки окружающий воздух создавал бы неконтролируемый вертикальный поток вверх, который искажал бы результаты. В выбранной геометрии этого не происходит, однако для каждой разности температур существует некий порог для расхода воздуха, который

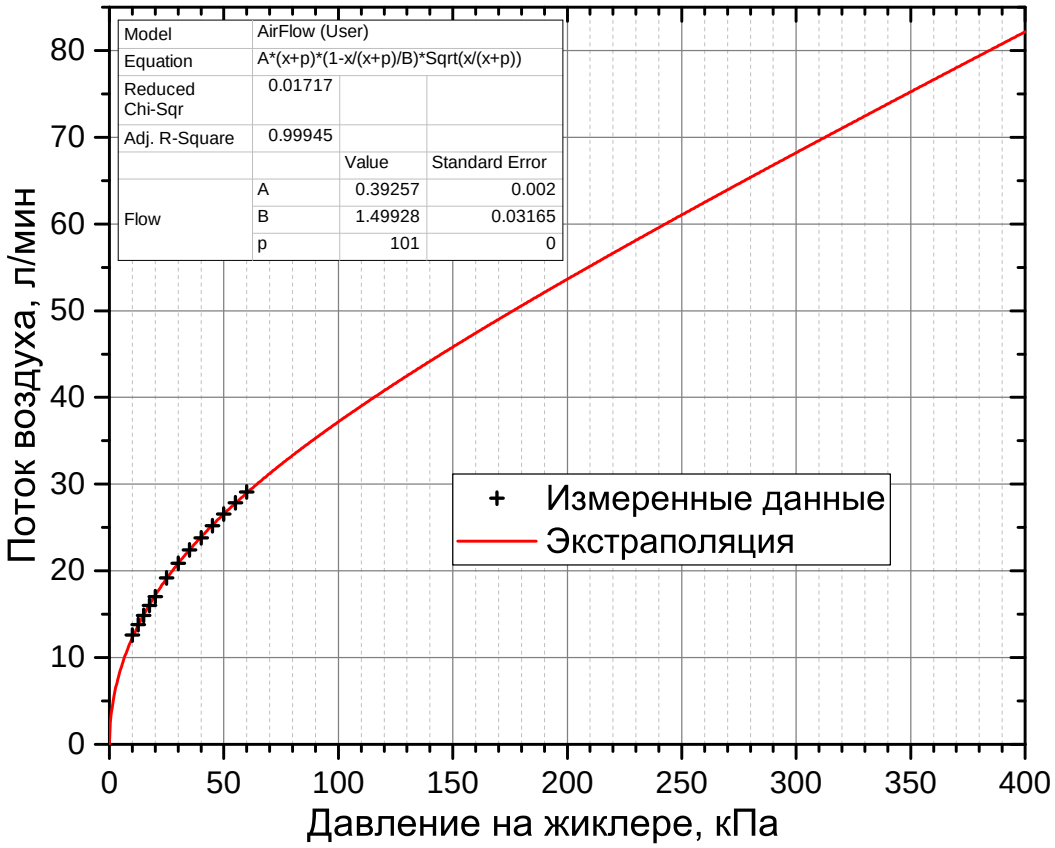

Рисунок 4.3: Калибровка потока воздуха по измеряемому давлению на жиклере.

необходимо преодолеть, для того, чтобы «продавить» горячий воздух вниз до центра камеры в противодействие архимедовой силе всплывания.

4.1.1. Измерение параметров турбулентности в камере

Влияние турбулентности на оптические сигналы описывается теорией Колмогорова с некоторыми уточнениями. Любой режим турбулентности характеризуется наличием нижней и верхней границ ее масштаба. Нижняя граница — внутренний масштаб турбулентности l_0 — характеризует минимальный размер вихря, который ограничен диссипацией энергии вследствие вязкости среды. Верхняя граница — внешний масштаб турбулентности L_0 — максимальный размер, для которого вихри еще можно считать изотропными.

Согласно теории Колмогорова спектр турбулентного возмущения описывается зависимостью

$$\frac{0.0229}{r_0^{5/3}} f^{-11/3}, \tag{4.1}$$

где f — пространственная частота, а r_0 — так называемый параметр Фрида, т.е. диаметр телескопа, который обладает такой же пространственной частотой отсечки, что и турбулентная атмосфера. По сути, r_0 — это максимальный диаметр пучка, который сохраняет когерентность при прохождении турбулентной среды. В отличие от чисто геометрических параметров l_0 и L_0 он характеризует в том числе и силу турбулентности, т.е. ее воздействие на проходящий пучок.

Однако, теория Колмогорова не описывает переход от данной спектральной зависимости, справедливой для масштабов между l_0 и L_0, к пространственным частотам, лежащим вне данных границ. Для этого мы будем использовать модель фон Кармана, в которой уточненный спектр записывается как

$$\frac{0.0229}{r_0^{5/3}}\left(f^2 + L_0^{-2}\right)^{-11/6}\exp\left(-l_0^2 f^2\right). \tag{4.2}$$

Согласно данной зависимости, частоты выше $1/l_0$ экспоненциально подавлены, а ниже $1/L_0$ — выходят на константу.

Количественное описание режима турбулентности связано с нахождениями значений данных параметров. В первую очередь, это параметр Фрида r_0, характеризующий силу турбулентности, а во вторую, геометрические параметры l_0 и L_0. Параметр Фрида является основной опорной точкой для соотношений подобия между модельной турбулентностью и турбулентностью в реальных атмосферных оптических каналах. В частности, для искусственного моделирования турбулентности наиболее важным является сохранение значения отношения диаметра пучка к данному параметру D/r_0. В реальной атмосфере при наблюдении звезд параметр r_0 составляет порядка 10-20 см на длине волны 500 нм. Таким образом, для моделирования наблюдения звезд метровым телескопом в турбулентной камере требуется обеспечить соотношение D/r_0 порядка 5-10.

Геометрические размеры играют более второстепенную роль. L_0 в первую очередь зависит от размера области с изотропной турбулентностью и вполне определяется размерами турбулентной камеры, в то время как l_0 зависит от потока энергии, которая передается от крупных вихрей к мелким и диссипирует в вихрях минимального размера.

Также определенное внимание следует уделить временны́м характеристикам турбулентного потока, а именно, частотным спектрам возмущений, измеренных определенным образом. Эта информация позволяет оценить характерные кажущиеся скорости турбулентных потоков, а также оценить частотную полосу обратной связи, необходимой для коррекции турбулентных искажений пучка.

Оценка параметра Фрида r_0

Наиболее простой и объективный способ оценки верхней границы параметра Фрида заключается в измерении усредненной по времени угловой ширины пучка и сравнение его с угловой шириной пучка при отсутствии турбулентности. Для этого формируется параллельный пучок большого диаметра, который проходит через турбулентную камеру. После этого пучок проходит через регулируемую диафрагму и фокусируется длиннофокусной линзой (F = 1000 мм) на матрицу фотокамеры. Для временно́го усреднения картинки используется длинная выдержка (T = 10 с). В эксперименте диаметр диафрагмы изменялся от 1 до 23 мм и измерялась ширина зарегистрированного пятна на полувысоте. На Рисунке 4.4 представлены измеренные зависимости для разности температур 100 К и перепаде давления на жиклере в 1, 2 и 4 атм.

Как видно из графика, при отсутствии турбулентности измеренная ширина пучка близка к дифракционному пределу для диаметров диафрагмы до 12 мм. Для бо́льших диаметров размер

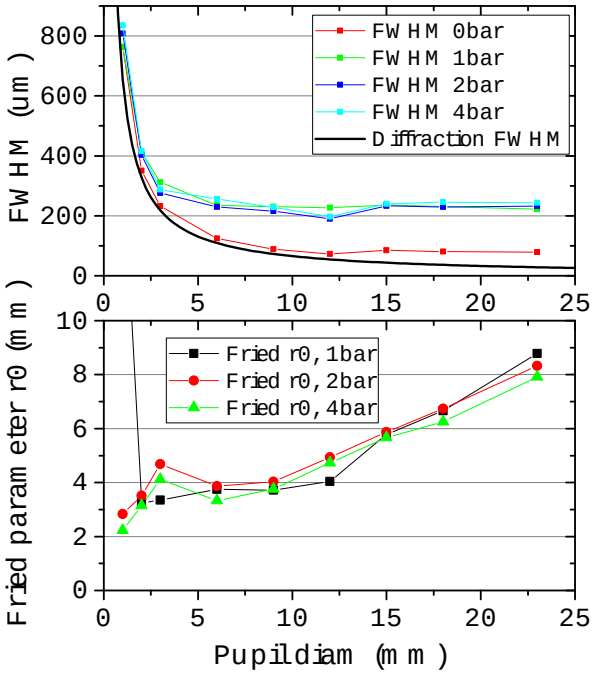

Рисунок 4.4: Зависимость ширины зарегистрированного пучка (вверху) и оценки параметра Фрида (внизу) от диаметра диафрагмы при разных давлениях на жиклере. На верхнем графике черной кривой для сравнения показан дифракционный предел — ширина пятна, получившаяся бы в идеальном эксперименте.

пучка был ограничен сферическими аберрациями используемых линз. Параметр Фрида, вернее его верхняя граница, вычисляется из отношения R диаметра пучка, уширенного турбулентностью, к диаметру без турбулентности по формуле:

$$r_0 \leq D\sqrt{\frac{1}{R^2-1}}, \tag{4.3}$$

где D — диаметр диафрагмы. Как легко видеть, наибольшая точность определения достигается в диапазоне $D = 5 - 10$ мм, так как при этом значение R уже достаточно велико, а измеренный диаметр пучка без турбулентности ограничен дифракцией, а не аберрациями оптической системы. В результате, можно утверждать, что параметр Фрида при разности температур 100 К составляет не более 3-4 мм, причем, он практически не зависит от силы потока воздуха. Такое значение является более чем достаточным для моделирования наземных атмосферных линий связи. Как уже упоминалось, в первую очередь следует добиваться сохранения соотношения D/r_0, которое в нашей установке может составлять не менее 10-12. Учитывая, что диаметр пучка в наземных линиях не превышает 1 м, а r_0 составляет порядка 10-20 см, данная камера позволяет эффективно моделировать практически любые атмосферные линии связи.

Зависимость силы и характера турбулентности от разности температур и силы потока

В экспериментах измерялись зависимости частотного спектра, глубины модуляции и визуального характера искажений от основных параметров турбулентной камеры: разности температур и

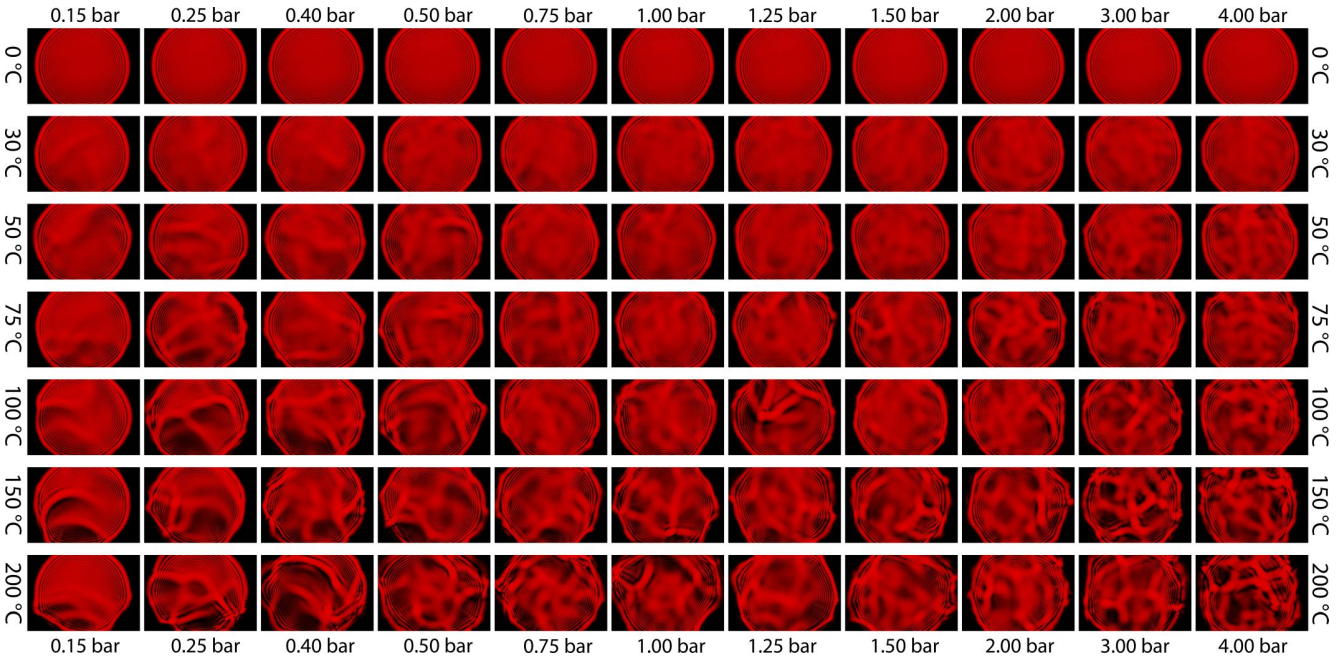

Рисунок 4.5: Измеренные примеры профилей пучков, прошедших через турбулентную камеру при различных разностях температур и давлений на жиклере.

потока воздуха. При этом использовался широкий пучок диаметром порядка 27 мм, который проходил через турбулентную камеру, распространялся в пространстве еще 450 см для дифракции на полученных фазовых неоднородностях и регистрировался камерой или фотоприемником. В первой серии экспериментов измерялся амплитудный профиль пучка при разных значениях разности температур и потока воздуха. Результаты измерений показаны на Рисунке 4.5.

Как и ожидалось, сила турбулентности возрастает с повышением температуры и силы потока воздуха из форсунок. Также можно заметить несколько особенностей данной камеры: при больших разностях температур и маленьких потоках (P = 0.15 и 0.25 бар) хорошо видна неизотропность турбулентного потока. Она связана с тем, что горячий воздух из верхней форсунки не обладает достаточной скоростью, чтобы опуститься в середину камеры и полностью смешаться с холодным. Из-за этого возникает как бы горячая «подушка» под верхней форсункой, которая приводит к характерным теням на картинках (картинки перевернуты вверх ногами, так что на них тени расположены снизу).

По данным фотографиям были вычислены коэффициенты корреляции между невозмущенной картиной и картиной с турбулентностью, результаты представлены на Рисунке 4.6.

Для количественных измерений глубины полученной амплитудной модуляции использовался фотодиод с диаметром чувствительной площадки 0.8 мм, подключенный к универсальной плате оцифровки данных NI-USB 6211. Последующий численный анализ проводился на компьютере после окончания записи данных. Вычислялась средняя глубина модуляции, как среднеквадратичное отклонение от среднего значения напряжения на фотодиоде. После этого вычислялась «видность» модуляции, как отношение глубины модуляции к среднему значению. Результаты для серий с постоянным давлением и постоянной температурой показаны на Рисунке 4.7.

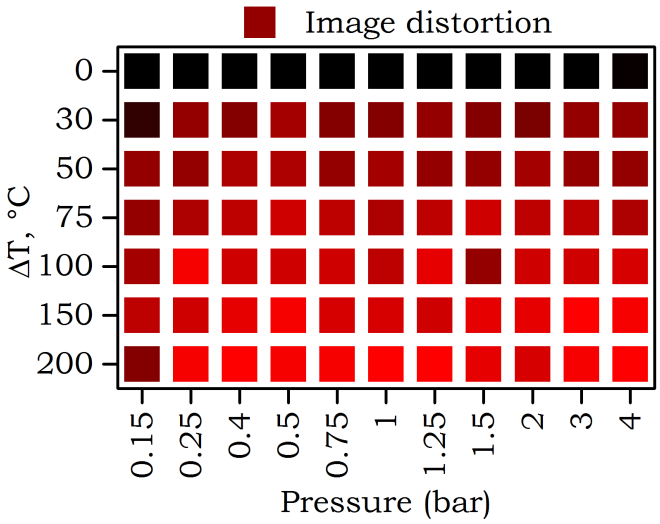

Рисунок 4.6: Степень возмущения изображений на Рисунке 4.5 относительно базового, полученного при отсутствии турбулентности.

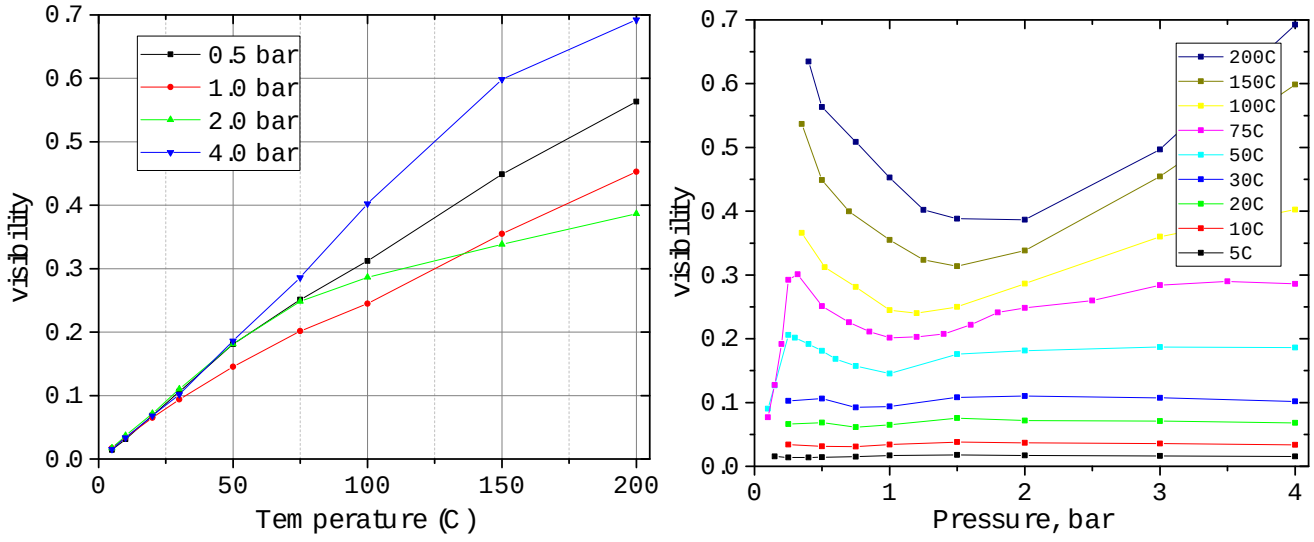

Рисунок 4.7: Зависимости видности модуляции интенсивности от разности температур и давления на жиклере.

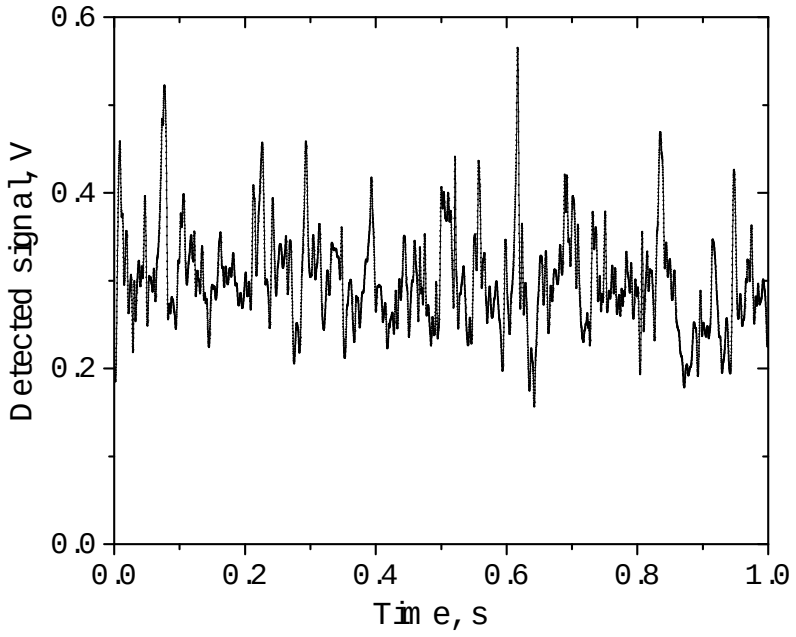

Рисунок 4.8: Временна́я зависимость регистрируемого сигнала фотодиода от времени для разности температур 50 К и давления на жиклере в 200 кПа.

Как видно из графиков, повышение температуры приводит к монотонному повышению глубины модуляции, в то время как изменение силы потока приводит к немонотонной зависимости. При определенном давлении наблюдается минимум глубины модуляции, причем положение минимума увеличивается с ростом разности температур. При самых минимальных давлениях наблюдается крутой спад глубины модуляции, связанный с уже упоминавшимся «всплыванием» горячего воздуха вверх, которое наблюдается при малых силах потока.

Частотный анализ флуктуаций интенсивности

В данной части исследований полученные ранее временные зависимости были подвергнуты спектральному анализу. На Рисунке 4.8 показана типичная зависимость сигнала от времени, соответствующая разности температур 50 К и давлению 2 бар. Как видно из рисунка характерное время изменения сигнала составляет порядка 10 мс. При оцифровке для избежания т.н. алиасинга (т.е. попадания частотных компонент выше частоты Найквиста в оцифрованный сигнал в виде искажений) использовалась заведомо более высокая частота дискретизации в 10 кГц.

Полученная временна́я зависимость (16-битная оцифровка, длина выборки $2^{21} = 2.097 \times 10^6$ точек) преобразовывалась в частотную быстрым преобразованием Фурье, вычислялись амплитуды частотных компонент, которые затем усреднялись по близким частотам. На Рисунке 4.9 показан спектр сигнала в линейном и логарифмическом масштабе для тех же параметров турбулентной камеры.

Как показывают данные измерения, основной вклад вносят частоты ниже пары сотен герц, что вполне соотносится с наблюдаемым характерным временны́м масштабом в 10 мс. Для измерения зависимости характерной частоты спектра от разности температур и давления был использован

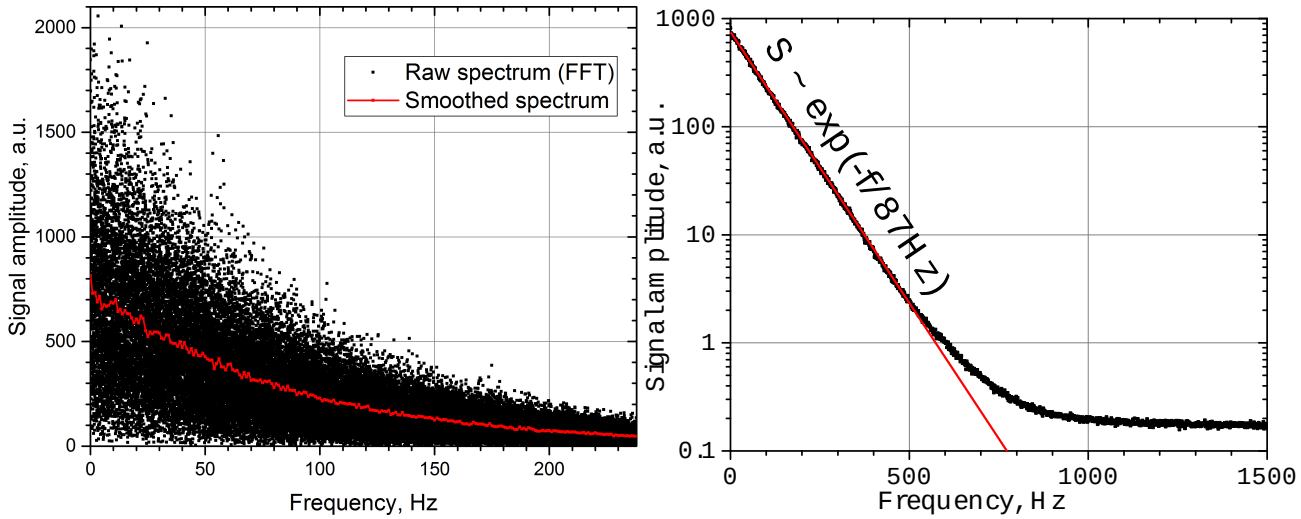

Рисунок 4.9: Частотный спектр флуктуаций интенсивности для разности температур 50 К и давления на жиклере в 200 кПа. На левом графике показан как усредненный спектр, так и неусредненный. Правый график показывает ту же усредненную зависимость в логарифмическом масштабе по амплитуде. Как видно из графика, до частоты 500 Гц спектр практически идеально описывается экспоненциальной зависимостью.

показатель так называемой частоты пересечения нуля, т.е. из зарегистрированного сигнала вычиталось его среднее значение и проводился подсчет числа пересечений нуля за время серии (210 секунд). Для подобных спектров данный показатель проявил себя лучше, чем подсчет средней частоты, которая систематически оказывалась неадекватной из-за наличия слабого широкополосного шума в сигнале. На Рисунке 4.10 показаны зависимости частоты пересечения нуля от давления и разницы температур.

Видно, что повышение давления в целом приводит к повышению характерной частоты флуктуаций сигнала, однако данная зависимость сильно неоднородна и имеет по крайней мере одну точку перелома вблизи давления 0.6 бар для разностей температур ниже 100 К. При бóльших разностях температур частота флуктуаций растет до давления 2 бар и далее практически не изменяется. В целом, график подтверждает, что повышение скорости потока монотонно влияет на характерные частоты флуктуаций сигнала, однако зависимость сильно нелинейная и это связано как с наличием нескольких независимых слоев турбулентности вдоль линии распространения сигнала, так и с наличием ненулевого внутреннего масштаба турбулентности l_0, характеризующего минимальный размер вихря в камере.

Измерение флуктуаций угла приема

Для количественных оценок параметров внутреннего и внешнего масштаба турбулентности используют так называемый метод измерения флуктуаций угла приема. Он основан на измерении флуктуаций положения центра масс пучка в фокальной плоскости фокусирующей линзы в зависимости от диаметра входной апертуры. Чем больше апертура тем больше усредняется сигнал (больше спеклов попадает в апертуру) и флуктуации уменьшаются. Напротив, уменьшение апер-

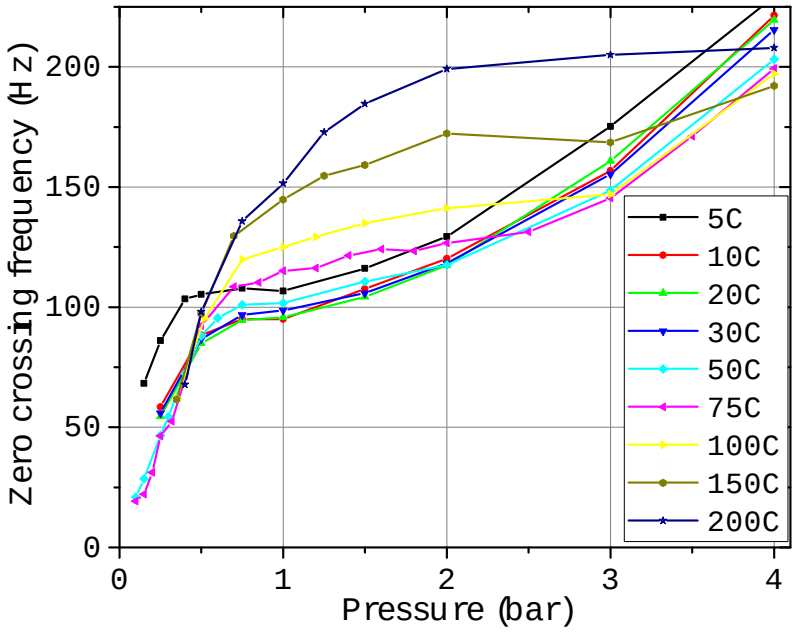

Рисунок 4.10: Зависимость характерной частоты флуктуаций интенсивности от давления и разности температур.

туры ведет к повышению таких флуктуаций. В нашем эксперименте флуктуации измерялись в фокальной плоскости собирающей линзы с фокусным расстоянием $F = 1000$ мм при варьировании диаметра апертуры от 1 до 23 мм. Измерения проводились с помощью квадрантного фотодиода, перед которым располагалось матовое стекло для усреднения картинки. Такая технология измерений угла приема хорошо зарекомендовала себя на практике при ее использовании в активной системе прицеливания для системы релятивистской квантовой криптографии (см. Главу 6).

Пример результатов наблюдений для разницы температур 100 К и давления 2 бара показан на Рисунке 4.11. Полученная зависимость хорошо согласуется с теорией, которая предсказывает степенную зависимость $D^{-1/3}$ для $l_0 = 0$ и $L_0 \to \infty$. Для конечных значений данных параметров справа и слева ожидается большее затухание, чем эта простая степенная зависимость, что и наблюдается на эксперименте. Из полученных данных с помощью численных расчетов были определены значения l_0 и L_0, которые составили $l_0 = 2.7 \pm 1$ мм, а $L_0 = 51 \pm 11$ мм.

Также в литературе определенное внимание уделяется частотным характеристикам данных флуктуаций. Нами были вычислены частотные спектры, которые для данных параметров и диаметра апертуры 6 мм показаны на Рисунке 4.12. Теория предсказывает, что на частотах выше, чем кажущаяся скорость ветра деленная на диаметр апертуры, спектр должен следовать зависимости $f^{-11/3}$, а на частотах менее данной, но выше, чем v/l_0 — зависимости $f^{-2/3}$, что и наблюдается на эксперименте. Такой медленный переход между двумя зависимостями можно объяснить наличием многих независимых слоев турбулентности вдоль линии распространения пучка, которые дополнительно усредняют сигнал и срезают подобным образом спектр.

В результате, полученные зависимости для флуктуации угла приема хорошо соотносятся с предсказаниями теории и соответственно наблюдаемым параметром естественной атмосферы, что

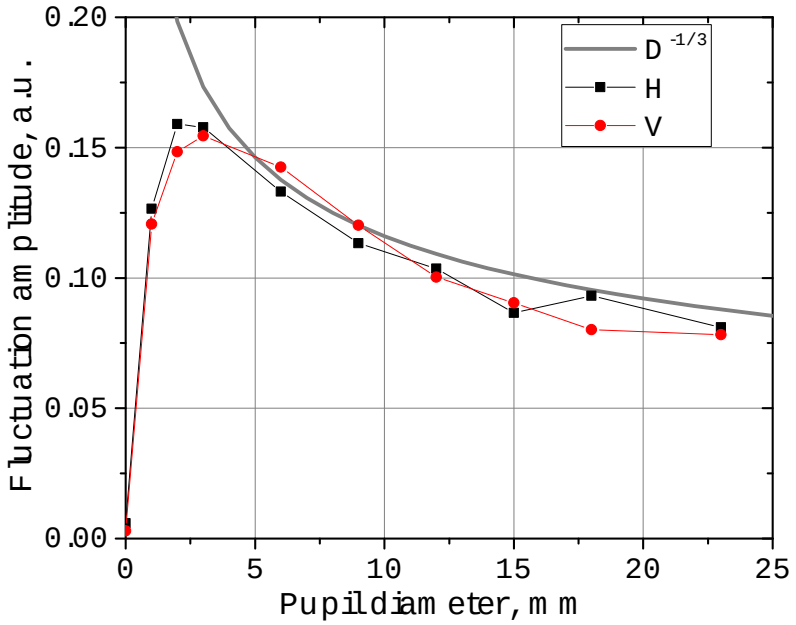

Рисунок 4.11: Зависимость амплитуды флуктуаций по двум координатам от диаметра входной диафрагмы. Сплошной линией показана теоретическая зависимость, которая наблюдалась бы при $l_0 = 0$ и бесконечно большом L_0.

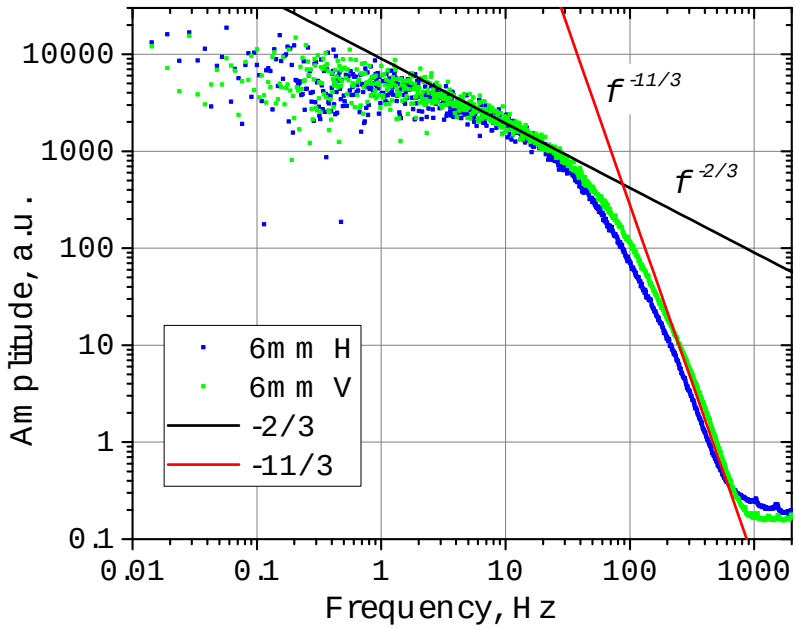

Рисунок 4.12: Частотные спектры флуктуаций угла приема. Как видно, они хорошо соответствуют двум асимптотическим степенным зависимостям, предсказываемым теорией, которые показаны на графике сплошными прямыми.

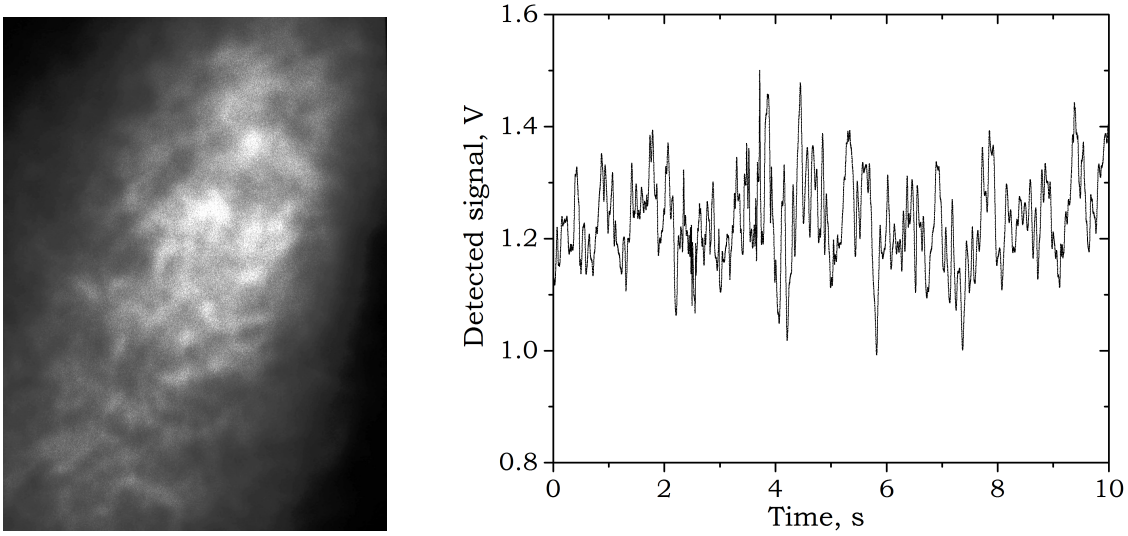

Рисунок 4.13: A. Искажения пучка после прохождения длинного атмосферного канала. B. Характерная временна́я зависимость принимаемой яркости, измеренная на площади порядка 1 мм^2 при полном размере освещенного пятна порядка 10 см.

позволяет еще раз подтвердить адекватность нашего лабораторного симулятора турбулентности.

4.1.2. Измерения реального атмосферного канала длиной 180 м

Также были проведены измерения на реальном атмосферном канале связи длиной 180 м для возможности сравнения с результатами, получаемыми в турбулентной камере. Были промерены временны́е характеристики, а также зафиксированы характерные профили распределения интенсивности. Для примера, на Рисунке 4.13A показан профиль изначально пространственно-одномодового излучения, прошедшего через атмосферный канал. На фотографии отчетливо видна пятнистая структура пучка, обусловленная турбулентными процессами в атмосфере. На Рисунке 4.13B показана зависимость сигнала в точке от времени. Как видно, большая часть флуктуаций обладает характерным периодом около 0.1 с. Более детальный частотный анализ показывает доминирование частот ниже 10 Гц, см. Рисунок 4.14.

Данные измерения проводились в подвальном помещении физического факультета МГУ, где, несмотря на закрытость помещения, сквозняки и вентиляция создавали очень существенные возмущения в канале. На Рисунке 4.15 показан данный оптический канал в процессе измерений.

4.1.3. Измерения характеристик пропускания для сравнения с теорией из следующего раздела

Экспериментальные результаты, использованные в следующей главе были получены с помощью турбулентной камеры, которая основана на двух алюминиевых соплах размером 5x5 cm^2, которые создают потоки воздуха в противоположных направлениях. Расстояние между соплами составляет 5 см, и одно из них может нагреваться для создания желаемой разницы температур. Было установлено что внутренний и внешний масштабы турбулентности примерно постоянны и не

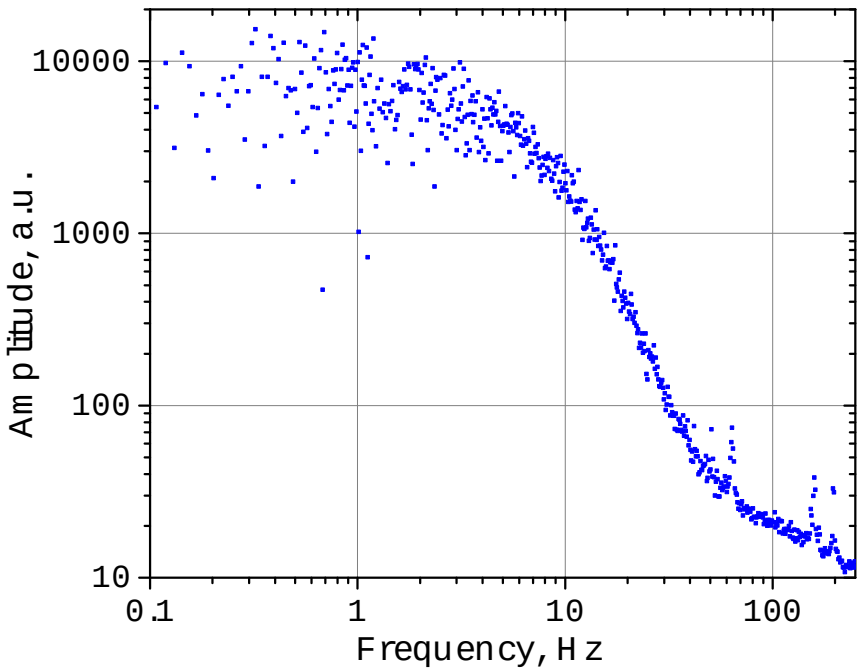

Рисунок 4.14: Измеренный спектр флуктуаций интенсивности для канала связи длиной 180 м. Для частот выше 40 Гц существенно влияние шума оцифровки (использовалась 8-битная оцифровка сигнала).

Рисунок 4.15: Проведение измерений атмосферного оптического канала связи в подвале физического факультета МГУ.

зависят от разницы температур и скорости воздушного потока. Их значения равны l_0 = 2.7 ± 1 мм и L_0 = 51 ± 11 мм соответственно. Параметр Фрида зависит почти исключительно от разницы температур, и практически неизменен при вариации скорости воздушного потока. Такое поведение является типичным для турбулентных камер [109].

В оптической части для фильтрации мод использовалось одномодовое волокно 780-HP и коллиматоры с фокусным расстоянием F = 11 мм для формирования пучка. В качестве преобразователя мод мы использовали пространственный модулятор света (SLM) на основе жидких кристаллов с пилообразными рисунками, генерируемыми компьютером [110]. Оптическая мощность, заведенная в световод, преобразовывалась в электрический сигнал с помощью фотодиода с усилителем сигнала, а затем оцифровывалась с частотой дискретизации 1000 Гц с помощью универсальной платы сбора данных.

4.2. Турбулентность и ее влияние на модовый состав излучения

Передача информации по оптическим каналам в зоне прямой видимости по открытому пространству является важным средством связи, которое человечество использовало на протяжении веков. В XX веке автоматизация первоначально ручной передачи информации и внедрение лазеров и высокоскоростной электроники привели к появлению многих важных практических применений для подобных линий связи. В то же время стали очевидны и неидеальности таких каналов, в основном связанных с атмосферной турбулентностью. Само явление атмосферной турбулентности широко изучалось в 1970-х годах. При этом использовалось предположение о большой ширине передаваемого светового пучка, который поэтому аппроксимировался плоской волной. Приемник излучения при этом воспринимался как точечный [111].

Позже потребность в *энергоэффективной* оптической связи в свободном пространстве привела к более продвинутой модели, в которой одномодовый гауссов луч от источника распространяется к приемному телескопу с большой апертурой. В этой модели турбулентные эффекты смещают и искажают гауссов пучок, в связи с чем он при распространении в пространстве частично выходит за пределы приемной апертуры, что приводит к потерям в канале. Эта модель одномодового передатчика и многомодового приемника подробно изучается в серии недавних статей [112, 113, 114, 115].

В результате дальнейшего технического прогресса, особенно связанного с прорывами в области оптических коммуникаций и квантовых технологий, назрела потребность в изучении фактических характеристик *одномодового* оптического канала связи. В этом случае приемник регистрирует только одну конкретную пространственную моду излучения, которая, как предполагается, идеально сопрягается с передаваемой модой при отсутствии турбулентности. Во-первых, такая постановка задачи важна для замены обычных одномодовых волокон атмосферными линиями связи при сохранении совместимости получаемой инфраструктуры с такими технологиями, как спектральное уплотнение [116], волоконными усилителями, методами когерентной модуляции [A16], существующими оптоволоконными системами квантового распределения ключей и

т.д. Во-вторых, приемники, чувствительные к модовому составу, позволяют реализовывать каналы с пространственной модуляцией, тем самым добиваясь повышенной эффективности за счет многомерных форматов модуляции, принципиально недоступных в волоконно-оптических аналогах [117]. В-третьих, несколько независимых потоков данных могут быть пространственно мультиплексированы в один канал по открытому пространству, что позволяет достичь беспрецедентной пропускной способности канала на одной длине волны [118]. Наконец, активно развивающиеся квантовые технологии, достигающие все более и более высокой размерности квантовых состояний, нуждаются в соответствующих квантовых каналах связи для обмена такими квантовыми состояниями [119, 120, 121]. Пространственная степень свободы может стать естественным выбором для квантовых компьютеров, взаимодействующих друг с другом с использованием многомерных пространственных квантовых состояний фотонов [122].

Сформулированная выше задача нахождения характеристик одномодового канала по открытому пространству при наличии атмосферной турбулентности, а также связанные с ней вопросы модальных перекрестных помех, вызванных турбулентностью, являются центральным вопросом данного раздела. Под одной пространственной модой мы понимаем собственное решение уравнения распространения, поэтому форма моды остается неизменной при распространении на любое расстояние. На протяжении всего текста мы предполагаем, что если бы атмосфера была идеально однородной, наша оптическая система была бы идеально съюстирована без каких-либо оптических потерь в канале или перекрестных помех между модами. Исследуемые эффекты обусловлены исключительно изменяющимися условиями рефракции в турбулентной атмосфере, которые искажают распространяющиеся моды, заставляя их значительно отклоняться от невозмущенного решения. Будет представлена структура, которая позволяет ответить практически на любой вопрос о потере мощности в конкретной моде или о связи определенной моды с другими модами, при условии, что параметры турбулентности известны. Будут выведены простые аналитические решения для решения задачи в первом приближении, а также показаны результаты численных экспериментов для более высоких порядков точности. Полученные результаты будут сравниваться с экспериментальными результатами, полученными в турбулентной камере. В частности, будет выведена очень простая связь между статистикой пропускания канала, связывающего два одномодовых световода по открытому пространству и силой турбулентности в этом канале. Эта связь может использоваться для простой оценки параметров турбулентности по измеренной статистике пропускания канала, либо для оценки статистики пропускания по известному параметру турбулентности Фрида.

4.2.1. Модель турбулентности

Турбулентные явления в атмосфере были впервые описаны Колмогоровым [123] 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 очень заинтересованы в локальных турбулентных свойствах атмосферы, будет использоваться хорошо

известный результат для протяженного атмосферного канала и модель фон Кармана, которая предсказывает следующий спектр мощности фазовых флуктуаций [124, 109]

$$W_\varphi(f) = \vartheta\, r_0^{-5/3} \left(f^2 + L_0^{-2}\right)^{-11/6} \exp(-l_0^2 f^2), \tag{4.4}$$

где

$$\vartheta = \frac{2\sqrt{2}\,\Gamma^2(11/6)}{\pi^{11/3}} \left[\frac{3}{5}\,\Gamma(6/5)\right]^{5/6} \approx 0.0229. \tag{4.5}$$

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 [109].

Одно разумное приближение, которое используется в нашем анализе, состоит в том, что прохождение излучения через турбулентный канал эквивалентно прохождению через соответствующую случайную фазовую маску, пространственный частотный спектр которой задается как (4.4). Несмотря на то, что в общем случае это неверно (луч может существенно перераспределить свой профиль мощности после дифракции на фазовых искажениях, полученных в самом начале канала), это верно для не очень сильной турбулентности, когда значительная часть мощности остается в неизменной поперечной моде. Этот режим наиболее интересен для нас, поскольку при чрезвычайно сильной турбулентности можно просто предположить, что все выходные моды будут заполнены одинаково, независимо от того, как они были возбуждены на входе, что тривиально.

Само по себе фазовое искажение является непрерывной функцией поперечных координат, поэтому мы можем использовать разложение в ряд Тейлора, чтобы корректно его представить.

$$\varphi(x, y) = \varphi_0 + ax + by + g\frac{x^2}{2} + h\frac{y^2}{2} + sxy + \ldots, \tag{4.6}$$

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

$$\begin{aligned} a &= \tfrac{\partial\varphi}{\partial x} \quad b = \tfrac{\partial\varphi}{\partial y} \\ g &= \tfrac{\partial^2\varphi}{\partial x^2}\; h = \tfrac{\partial^2\varphi}{\partial y^2}\; s = \tfrac{\partial^2\varphi}{\partial x \partial y}. \end{aligned} \tag{4.7}$$

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

Далее можно найти дисперсию параметров возмущения. Во-первых, используя (4.7), мы можем найти спектры мощности параметров возмущения:

$$\begin{aligned} W_a &= (2\pi)^2 f_x^2 W_\varphi \\ W_b &= (2\pi)^2 f_y^2 W_\varphi \\ W_g &= (2\pi)^4 f_x^4 W_\varphi \\ W_h &= (2\pi)^4 f_y^4 W_\varphi \\ W_s &= (2\pi)^4 f_x^2 f_y^2 W_\varphi. \end{aligned} \tag{4.8}$$

Где f_x и f_y — это $x-$ и $y-$ компоненты пространственной частоты f: $f_x = f\cos(\theta)$, $f_y = f\sin(\theta)$, где θ — это полярный угол.

Во-вторых, мы должны принять во внимание, что нас интересует не только точка (0,0), в которой мы берем производные (4.7), но и средние наклоны фазы по всей площади пучка. Это приводит к дополнительной функции фильтрации $|F(f)|^2$, аналогичной той, которая появляется в задаче нахождения флуктуаций угла прихода [125, 124]. В нашем случае $|F(f)|^2$ - это пространственный спектр мощности для рассматриваемой нами моды. Наконец, используя теорему Винера-Хинчина, можно найти автокорреляционную функцию коэффициентов искажения, которая является преобразованием Фурье их спектров мощности. При этом сразу можно проигнорировать ту часть автокорреляционной функции, которая зависит от x, y, и найти ее значение только для $x = y = 0$, что будет в точности соответствовать дисперсии параметров возмущения. Находя требуемое значение Фурье-образа на нулевой частоте и интегрируя по θ, получаем

$$C_a = C_b = 4\pi^3 \int_0^\infty f^3 W_\varphi(f)|F(f)|^2\, df \tag{4.9}$$

$$C_g = C_h = 12\pi^5 \int_0^\infty f^5 W_\varphi(f)|F(f)|^2\, df \tag{4.10}$$

$$C_s = 4\pi^5 \int_0^\infty f^5 W_\varphi(f)|F(f)|^2\, df, \tag{4.11}$$

где $C_\zeta(r) = \mathbb{E}[\zeta(r_0)\zeta(r_0 + r)]$ — автокорреляционная функция ζ, а $C_\zeta = C_\zeta(0)$ — наблюдаемая дисперсия ζ.

Подобно работе [112], будем предполагать, что все коэффициенты искажения являются нормально распределенными случайными величинами, поскольку они являются суммарным эффектом многих независимых возмущений на оптическом пути. Следуя той же процедуре, можно найти статистические свойства коэффициентов искажения более высокого порядка. В данной статье мы сосредоточимся только на первых двух порядках, поскольку большинство изученных эффектов могут быть достаточно точно описаны в этом приближении.

4.2.2. Приближение первого порядка — плотность вероятности для коэффициента пропускания

Вычислим плотность вероятности для коэффициента пропускания фундаментальной моды используя только приближение первого порядка. Начинаем с Гауссова пучка вида

$$E_{00} = \frac{1}{w}\sqrt{\frac{2}{\pi}} e^{-\frac{x^2+y^2}{w^2}}, \tag{4.12}$$

где w — ширина пучка. Будем использовать предположение, что длина канала не намного больше рэлеевской длины, поэтому поперечный размер пучка остается примерно одинаковым вдоль всего канала. Расчет интеграла перекрытия

$$T_{00\to 00} = \frac{\left|\int |E_{00}|^2 e^{i\varphi(x,y)}\, dx\, dy\right|^2}{\left(\int |E_{00}|^2\, dx\, dy\right)^2} \tag{4.13}$$

между исходным пучком и его искаженной по фазе копией (4.6) дает следующее выражение для коэффициента пропускания по мощности

$$T_{00\to 00} = \exp\left[-\frac{w^2}{4}\left(a^2+b^2\right)\right]. \tag{4.14}$$

Обозначим $\xi = \frac{w^2}{4}\left(a^2+b^2\right)$, т.е. безразмерный параметр возмущения. Так как a и b являются нормально распределенными случайными величинами с нулевым средним и дисперсией $C_a = C_b$, ξ обладает плотностью вероятности

$$p(\xi) = \frac{2}{w^2 C_a}\exp\left(-\frac{2\xi}{w^2 C_a}\right). \tag{4.15}$$

Для нахождения плотности вероятности для коэффициента пропускания $T = f(\xi)$ используем стандартное выражение

$$p(T) = \frac{p(\xi)}{\left|\frac{df(\xi)}{d\xi}\right|}, \text{where } \xi = f^{-1}(T). \tag{4.16}$$

Подставляя (4.14) в (4.16) получаем окончательное выражения для плотности вероятности коэффициента пропускания

$$p(T) = \frac{2}{w^2 C_a} T^{\frac{2}{w^2 C_a}-1}. \tag{4.17}$$

Видно, что в первом приближении полученная плотность вероятности является степенной функцией коэффициента пропускания T, и следовательно чем выше турбулентность, тем меньше 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 4.16. Эксперимент и теория хорошо согласуются, за исключением высоких значений коэффициента пропускания, когда приближение первого порядка не работает из-за фазовых искажений более высоких порядков.

4.2.3. Приближение первого порядка — перекрестные помехи

Следующий рассматриваемый вопрос — как мощность, потерянная из основной моды, распределяется между модами более высокого порядка. Для ответа на него, сначала нужно определить набор мод, который мы используем для расчетов. Наиболее часто используемые варианты — моды Эрмита-Гаусса и Лагерра-Гаусса. Хотя выражения для мод Эрмита-Гаусса несколько проще, хотелось бы найти более универсальное решение, что возможно путем правильной группировки мод между собой.

Существует прямое соответствие между наборами оптических мод (Эрмита- или Лагерра-Гаусса) и двумерным изотропным осциллятором [126], где N-й уровень мощности вырожден $(N+1)$ раз. С точки зрения наборов мод это означает, что можно сгруппировать все моды в соответствии с их „уровнем мощности“. Для моды Эрмита-Гаусса HG_{mn} соответствующий уровень мощности равен $N = m+n$. Для мод Лагерра-Гаусса LG_{pl} $N = 2p+|l|$. Легко показать, что N-й уровень состоит из $N+1$ различных мод.

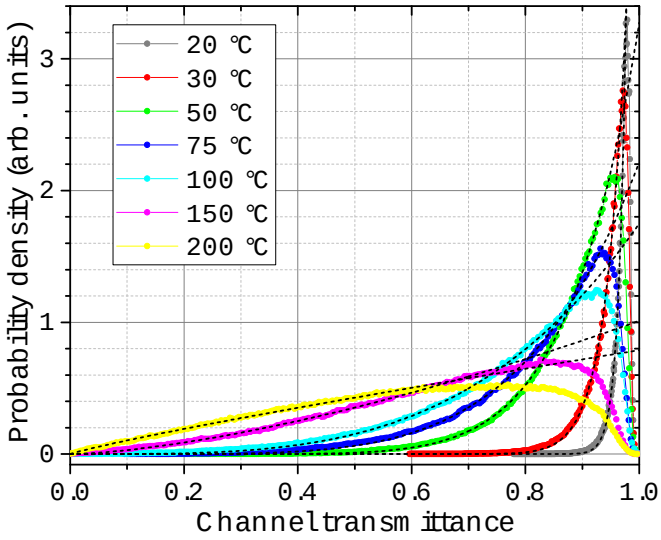

Рисунок 4.16: Распределение плотности вероятности для коэффициента пропускания канала, измеренного экспериментально, и теоретические предсказания в первом порядке теории возмущения (черные пунктирные линии). Экспериментальным параметром, определяющим силу турбулентности, является разница температур воздушных потоков, указанная в легенде. Обратите внимание, что для лучшего представления данных, распределения вероятностей не отнормированы должным образом.

Для каждой конкретной моды вычисляем интеграл перекрытия

$$T_{00\to mn} = \frac{\left|\int E^*_{mn} E_{00}\, e^{i(ax+by)}\, dx\, dy\right|^2}{\int |E_{00}|^2\, dx\, dy \int |E_{mn}|^2\, dx\, dy}. \tag{4.18}$$

После нахождения интегралов перекрытия и группировки их по „уровням мощности“ N, коэффициенты перекрестных помех могут быть записаны в терминах ξ, определенных ранее, поскольку они теряют свою индивидуальную зависимость от a и b. Здесь мы используем явную нумерацию для набора мод Эрмита-Гаусса, в то время как для набора мод Лагерра-Гаусса это будут просто другие индексы мод. Для полноты картины мы также добавили полученный ранее результат для коэффициента пропускания основной моды.

$$\begin{aligned} T_0 &= T_{00\to 00} = e^{-\xi} \\ T_1 &= T_{00\to 10,01} = \xi e^{-\xi} \\ T_2 &= T_{00\to 20,11,02} = \tfrac{\xi^2}{2} e^{-\xi} \\ T_3 &= T_{00\to 30,21,12,03} = \tfrac{\xi^3}{6} e^{-\xi} \\ T_N &= T_{00\to mn:m+n=N} = \tfrac{\xi^N}{N!} e^{-\xi}. \end{aligned} \tag{4.19}$$

Легко можно видеть, что полная мощность сохраняется, так как полученный ряд суммируется в единицу.

Используя (4.15) и (4.16) находим соответствующие плотности вероятности. Производная

$$\frac{df}{d\xi} = \left(1 - \frac{\xi}{N}\right) \frac{\xi^{N-1}}{(N-1)!} e^{-\xi} \tag{4.20}$$

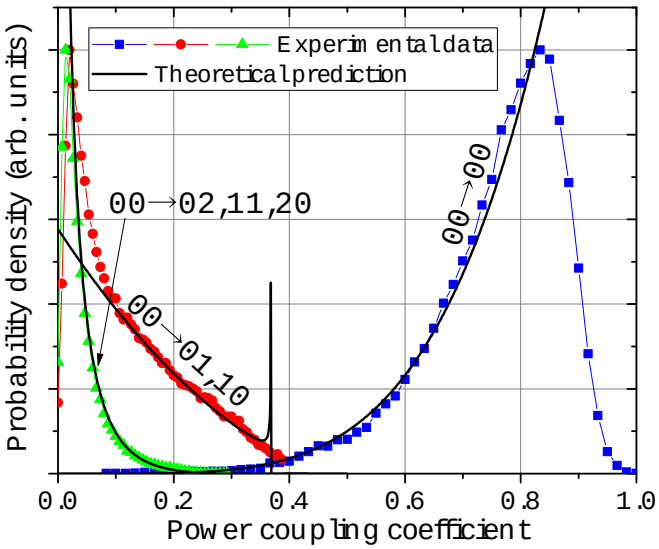

Рисунок 4.17: Экспериментальные результаты и теоретические предсказания коэффициента заведения мощности из основной моды в моды более высокого порядка.

Решение уравнения $x^N e^{-x}/N! = a$ — это $x = -N\,W\left(-\frac{(aN!)^{1/N}}{N}\right)$, где $W(a)$ W-функция Ламберта, т.е. решение уравнения $xe^x = a$.

Окончательное выражение для плотности вероятности коэффициента заведенной мощности для $N \geq 1$

$$p(T_N) = \frac{2}{w^2 C_a T}\left(\frac{\xi_1}{|N-\xi_1|}e^{-\frac{2\xi_1}{w^2 C_a}} + \frac{\xi_2}{|N-\xi_2|}e^{-\frac{2\xi_2}{w^2 C_a}}\right), \tag{4.21}$$

где

$$\xi_{1,2} = -N\,W\left(-\frac{(TN!)^{1/N}}{N}\right). \tag{4.22}$$

Максимальная заведенная мощность для определенной группы мод $T_{N\max} = \frac{N^N}{N!}e^{-N}$.

Были проведены экспериментальные измерения в турбулентной камере с перепадом температур 100 °C для N от 0 до 2. Полученные результаты представлены на Рисунке 4.17. Значение C_a было получено путем аппроксимации кривой $00 \to 00$ степенным законом (4.17), а две другие кривые были рассчитаны на основе этого значения. Как и в предыдущем случае, наибольшее расхождение между теорией и экспериментом возникает при малых значениях возмущения ξ, поскольку это приближение не учитывает фазовые возмущения более высоких порядков.

4.2.4. Приближение второго и более высоких порядков

Линейные фазовые искажения, изученные ранее, дают первый не обращающийся в ноль член в выражении для коэффициента пропускания канала. Однако сам по себе этот эффект плохо описывает прогнозируемую плотность вероятности при малых возмущениях ξ, поскольку в этом случае начинают преобладать члены более высокого порядка. В этом разделе в функцию фазовых искажений добавляются квадратичные члены и вычисляется улучшенное предсказание для плотности вероятности пропускания основной моды.

С учетом квадратичных членов, интеграл перекрытия (4.13) дает

$$T = \left(1 + \frac{w^4}{16}\left(g^2 + h^2 + 2s^2\right) + \frac{w^8}{256}\left(s^2 - gh\right)^2\right)^{-1/2} \times \exp\left[-\frac{w^2}{16}\frac{4(a^2+b^2)+\frac{w^4}{4}(s^2a^2+s^2b^2+a^2h^2+b^2g^2-2absg-2absh)}{1+\frac{w^4}{16}(g^2+h^2+2s^2)+\frac{w^8}{256}(s^2-gh)^2}\right]. \quad (4.23)$$

К сожалению, в этом случае едва ли могут быть найдены аналитические выражения для плотности вероятности коэффициента пропускания. Поэтому для нахождения желаемого распределения нами использовалось численное моделирование. Также было выполнено сравнение экспериментальных данных с результатами моделирования. В отличие от предыдущих разделов, где был только один параметр турбулентности C_a, здесь необходимо вычислить C_g и C_s. Для этого использовались независимо измеренные внутренние и внешние масштабы турбулентности l_0 и L_0 и был немного скорректирован известный параметр Фрида r_0, чтобы он соответствовал мощности (4.17). Это было необходимо, потому что точность независимо измеренных r_0 около 10% была недостаточна для того, чтобы распределение точно соответствовало ожидаемому степенному закону. На основе найденных параметров турбулентности были рассчитаны C_g и C_s и проведено численное моделирование. Результаты сравнения показаны на Рисунке 4.18. Теория достаточно хорошо соответствует эксперименту, что свидетельствует о том, что представленная теоретическая модель может использоваться для оценки различных зависимых свойств одномодового канала.

До сих пор мы исследовали только пропускание канала по открытому пространству, основанного на фундаментальной поперечной моде в первом и втором приближении, а также перекрестные помехи между модами основного и высшего порядков в первом приближении. Это вызывало наибольший интерес из-за полученных аналитических выражений, которые можно использовать для грубой оценки параметров. Однако представленная теоретическая структура турбулентности позволяет получить результаты для любых мод и точностей приближения фазовых искажений.

Для конкретного порядка приближения фазовых искажений необходимо найти соответствующие дисперсии, как показано в (4.8 – 4.11). Далее можно построить статистически правильные функции для фазового искажения (4.6) и вычислить интеграл перекрытия (4.18) для рассматриваемых мод. Повторяя это много раз, можно получить желаемое распределение вероятностей. Основываясь на наших измерениях в турбулентной камере, представленная теория дает разумные результаты, хорошо согласующиеся с экспериментально измеренными значениями.

4.2.5. Обсуждение результатов

Представленная вычислительная конструкция основана исключительно на модели турбулентности фон Кармана, которая, в свою очередь, хорошо зарекомендовала себя как в экспериментах по передаче информации по открытому пространству, так и во многих астрономических исследованиях [127]. Таким образом, независимо от конкретной экспериментальной реализации, полученные результаты являются еще одним шагом к пониманию турбулентных эффектов в одномодовых оптических каналах и системах с мультиплексированием мод.

Одним из важных практических примеров является реализация активной системы трекинга

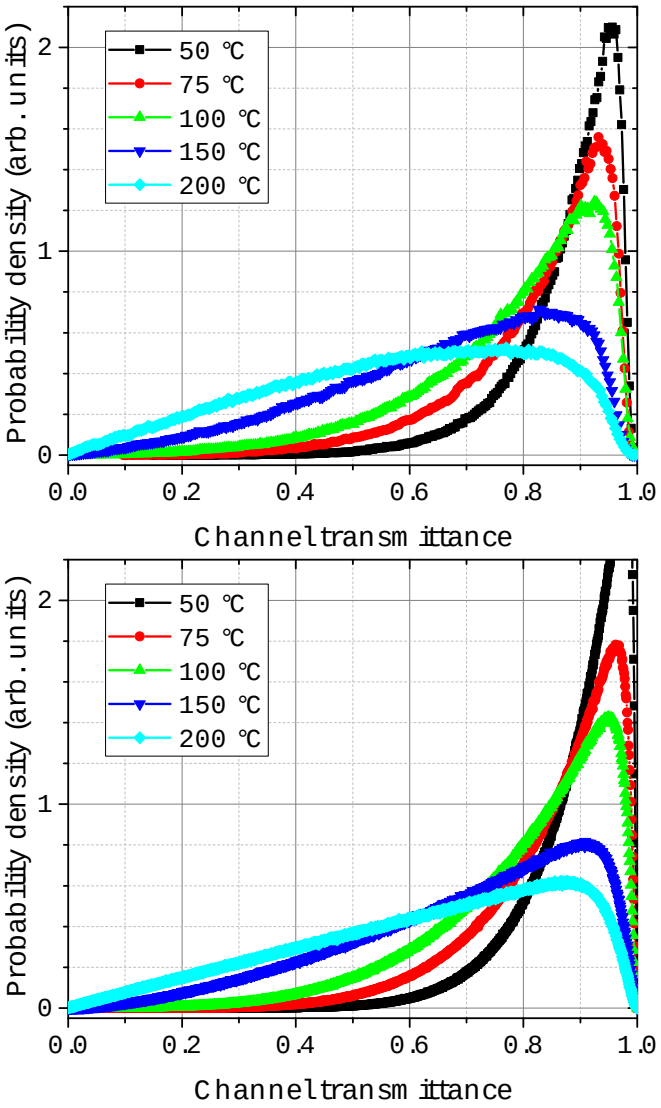

Рисунок 4.18: Плотность вероятности для коэффициента пропускания основной моды: сравнение экспериментально измеренных данных (вверху) и предсказаний теории второго порядка (внизу).

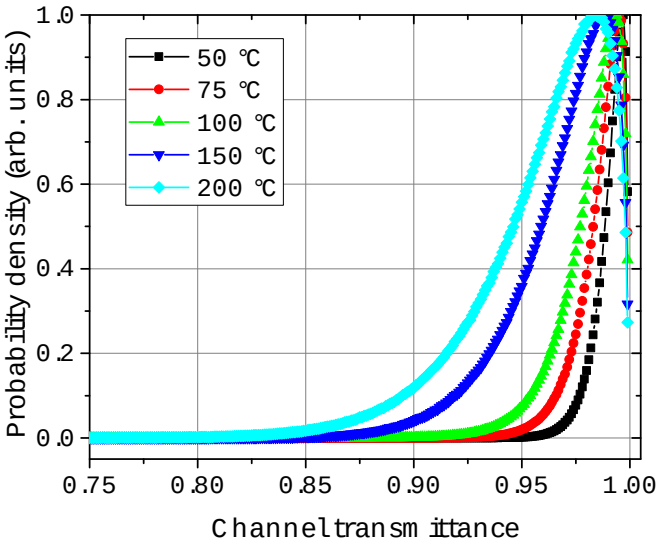

Рисунок 4.19: Вычисленная плотность вероятности пропускания для канала по открытому пространству из Рисунка 4.18 при наличии идеальной системы активного трекинга. Средний коэффициент пропускания становится лучше 95%, что намного выше, чем без такой системы.

в одномодовом оптическом канале по открытому пространству. Хорошо известно, что наиболее сильным турбулентным эффектом является блуждание луча как целого [112], то есть фазовое искажение первого порядка. Эффекты более высокого порядка, которые изменяют профиль луча, могут быть намного слабее. В то же время простой контур обратной связи с быстрым качающимся зеркалом, которое управляет направлением луча, решает проблему ошибки наведения при условии, что время прохождения сигнала туда и обратно намного короче, чем характерный временной масштаб турбулентного процесса. Поскольку это почти всегда так, активные системы слежения существенно улучшают качество оптических каналов по открытому пространству, особенно тех, которые доставляют излучение в одномодовое волокно [128, 129].

Используя разработанную схему расчета, можно легко оценить коэффициент пропускания канала при условии, что реализована идеальная система слежения. Для этого численное моделирование из предыдущего раздела модифицируется так, что ошибки первого порядка a и b всегда равны нулю. Результаты такого моделирования показаны на Рисунке 4.19, где наблюдается существенное улучшение характеристик канала.

Другой пример — оценка параметра Фрида на основе статистики пропускания для простого одномодового канала. Статистические данные по измеренному коэффициенту пропускания приближаются степенной функцией, и находится параметр C_a. Для оценки параметра Фрида используется (4.9) и априорные знания о внутреннем и внешнем масштабах турбулентности. В реальной атмосфере значения l_0 и L_0 более-менее известны [109], в то время как для турбулентных камер L_0 часто совпадает с размером камеры, а l_0 равно 2–6 мм [108]. В любом случае C_a слабо зависит от l_0 и L_0, и основной вклад вносит именно параметр Фрида r_0. Полученное значение параметра Фрида в наших экспериментах всегда было в пределах 10% от независимо измеренного, поэтому можно считать, что описанный метод дает надежные результаты.

Таким образом, была представлена схема расчета, которая позволяет ответить на большинство вопросов, касающихся характеристик одномодовых каналов или каналов с модовым мультиплексированием по открытому пространству в турбулентной атмосфере. Приближения первого порядка дают простые аналитические результаты, которые удобно использовать для быстрой оценки параметров системы. Основные результаты данного исследования опубликованы в [A17]. Также были получены аналитические выражения для потерь мощности основной моды и перекрестных потерь между основной модой и модами более высокого порядка. Для более точного моделирования каналов, учитывающих фазовые искажения второго и более высокого порядка, требуются численные расчеты. Многие полученные теоретические результаты подтверждаются экспериментальными измерениями в турбулентной камере. В целом, есть хорошее соответствие между экспериментом и расчетами, что и ожидалось. Необходимое условие такого соответствия — чтобы модель турбулентности фон Кармана соответствовала реальной среде, по которой проходит оптический канал связи.

4.3. Заключение к Главе 4

В этой 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. Была разработана и реализована турбулентная камера с контролируемыми параметрами турбулентности, были проведены экспериментальные измерения ее основных параметров. Также было разработано необходимое теоретическое описание каналов связи для передачи пространственных квантовых состояний, которое показало хорошее качественное сходство с результатами прямых измерений.

Ключевым результатом данного исследования является простое аналитическое выражение для плотности вероятности коэффициента пропускания одномодового атмосферного канала связи в линейном приближении:

$$p(T) = \frac{2}{w^2 C_a} T^{\frac{2}{w^2 C_a}-1}, \tag{4.24}$$

где w – ширина Гауссова пучка, а C_a – параметр, зависящий от силы турбулентности в канале. Продемонстрированное согласие теории и эксперимента свидетельствует о корректности выбранной модели и позволяет предсказывать характеристики каналов для квантовой коммуникации с использованием пространственных квантовых состояний при различной степени турбулентности среды.

Глава 5

Томография пространственных квантовых состояний с помощью деформируемого зеркала

Представление квантовой информации в виде оптических сигналов и её передача требует наличия соотвествующих 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 настоящей главе предлагается и экспериментально демонстрируется метод томографии пространственных квантовых состояний света с помощью деформируемого зеркала. Его использование позволяет значительно превзойти традиционный метод с использованием пространственного фазового модулятора (ПФМ, spatial light modulator) с точки зрения скорости и эффективности, а кроме того, позволяет достичь полную нечувствительность к поляризации. Результаты, приведенные в настоящей главе, опубликованы в работе [A19].

Томография квантовых состояния — это стандартная процедура определения неизвестного квантового состояния путем выполнения серии измерений на большом количестве его копий [130, 131, 132]. Эта процедура активно исследуется как теоретически, так и экспериментально [A8, A9]. В нашем исследовании интерес сосредоточен на томографии поперечных пространственных квантовых состояний света, которые часто используются в качестве модельной системы кудитов [133, 134, 135].

В отличие от двумерного случая, где легко доступны эффективные экспериментальные инструменты для квантовых измерений, реализация общих измерений в более высокоразмерных системах обычно является гораздо более сложной задачей. В некоторых случаях, например, для составной системы кубитов, по-прежнему легко выполнить *факторизованное* измерение [136], эффективно сводя общую задачу к измерениям одного кубита. Напротив, более высокоразмерные *пространственные* квантовые состояния света используют степени свободы одной и той же частицы, поэтому не существует универсального и эффективного решения для их измерения.

Много усилий было направлено на разработку так называемых сортировщиков пространственных мод [137, 138, 139, 140]. Их можно использовать для разделения различных пространственных мод, которые представляют собой естественный (*вычислительный*) базис для рассматриваемой квантовой системы. Однако, сортировщики мод формально допускают только один тип измерения, а именно измерения в вычислительном базисе, что явно недостаточно для полной томографии состояния. Типичным решением для проекционного измерения общего вида является использование ПФМ на основе жидких кристаллов для преобразования мод, за которым следует одномодовый волоконный фильтр, который выполняет проекцию результирующего поля на нулевую поперечную моду — фундаментальную моду световода [141, 142]. Несмотря на то, что этот метод по сути является стандартным подходом к проекционным измерениям в пространстве поперечных мод, метод измерения на основе ПФМ имеет ряд существенных недостатков, в первую очередь, связанных с относительно низкой скоростью переключения ПФМ, невысокой эффективностью и поляризационной чувствительностью.

Цель этой главы — показать возможность замены измерительного ПФМ на деформируемое микроэлектромеханическое зеркало, которое можно переключать с гораздо большей скоростью и в то же время обеспечивать преобразование мод практически без потерь и зависимости от поляризации. В результате, квантовая томография достаточно ярких источников потенциально может быть выполнена за миллисекундные временные интервалы и даже быстрее, что далеко от возможного с помощью обычных ПФМ. Предлагаемое решение может найти применение для томографии турбулентных оптических атмосферных каналов в реальном времени, а также в других нестационарных экспериментальных условиях.

Мы экспериментально демонстрируем томографию квантовых состояний света с адекватной точностью в 4х-мерном гильбертовом пространстве с помощью деформируемого зеркала.

5.1. Квантовая томография

Целью квантовой томографии является восстановление неизвестной матрицы плотности ρ с помощью серии измерений, выполненных на копиях рассматриваемого квантового состояния. Согласно правилу Борна, вероятность наблюдения результата γ для POVM измерения M с элементами $\{M_\gamma\}$ равна $P(\gamma\,|\rho) = \mathrm{Tr}(M_\gamma \rho)$. Экспериментально полученные вероятности для достаточного количества различных POVM элементов позволяют вычислить искомую матрицу плотности ρ. Как упоминалось ранее, реалистичный метод измерения ограничен только проекционными измерени-

ями, поэтому общий POVM формализм может быть сведен к следующей форме M_γ: $M_\gamma = |P_\gamma\rangle\langle P_\gamma|$.

В последнее время был достигнут значительный прогресс в методах реконструкции квантовых состояний, включая создание адаптивного [143], самонаводящегося [144], усовершенствованного нейронной сетью [145, 146] и многих других алгоритмов томографии, включая так называемую теневую томографию [147]. Однако, в настоящей работе акцент делается в первую очередь не на самом протоколе томографии, а на экспериментальном инструменте, который используется для реализации протокола. Для демонстрации представленной концепции томографии используется наиболее простой протокол, основанный на оценке максимального правдоподобия. В нашем понимании, предлагаемый экспериментальный инструмент эффективно может использоваться с протоколами томографии, основанным на фиксированном количестве измерений. Это, по-видимому, исключает все по-настоящему адаптивные протоколы, в которых подразумевается непрерывный смещение проекционных измерений. Однако некоторые стратегии, такие как исправление ошибок приготовления состояний и ошибок измерения нейросетью [146], определенно могут улучшить получаемые результаты. Для краткости в дальнейшем тексте мы не делаем никаких дополнительных предположений об используемом протоколе и показываем пример реализации всей схемы с самым базовым протоколом томографии, подробно описанном ниже. Более продвинутые версии томографии квантовых состояний могут быть построены на основе представленной демонстрации.

Минимальное количество проекторов, необходимое для полной томографии в d-мерном гильбертовом пространстве, составляет d^2. Набор таких проекторов можно выбрать как набор симметричных, информационно полных (symmetric informationally complete, SIC) POVM элементов. Это дало бы наиболее равномерное распределение ожидаемой точности реконструкции среди всех возможных квантовых состояний. В этой работе используется избыточный набор из $d\,(d+1)$ проекторов на элементы взаимно несмещенных базисов (ВНБ), который сохраняет ту же равномерность покрытия, что и SIC-POVM измерения, но приводит к гораздо более симметричному и простому в реализации массиву состояний деформируемого зеркала.

Когда дело доходит до экспериментальной реализации проекционных измерений, особенно с помощью сплошного деформируемого зеркала, реальные проекторы могут существенно отличаться от планируемых как по эффективности, так и по точности. Фактически, проекции без потерь на элементы ВНБ невозможно реализовать даже с помощью идеальной фазовой маски. Таким образом, перед проведением томографии самих квантовых состояний необходимо выполнить так называемую *томографию детектора*, чтобы найти реальные проекторы, которые реализуются в эксперименте [148, 149].

5.2. Экспериментальная реализация

В нашей демонстрации мы работаем со следующим набором пространственных мод Эрмита-Гаусса, составляющих вычислительный базис: HG_{00}, HG_{01}, HG_{10}, и HG_{11}, поэтому размерность соответствующего гильбертова пространства равна $d = 4$. Такой выбор сделан из-за прямоуголь-

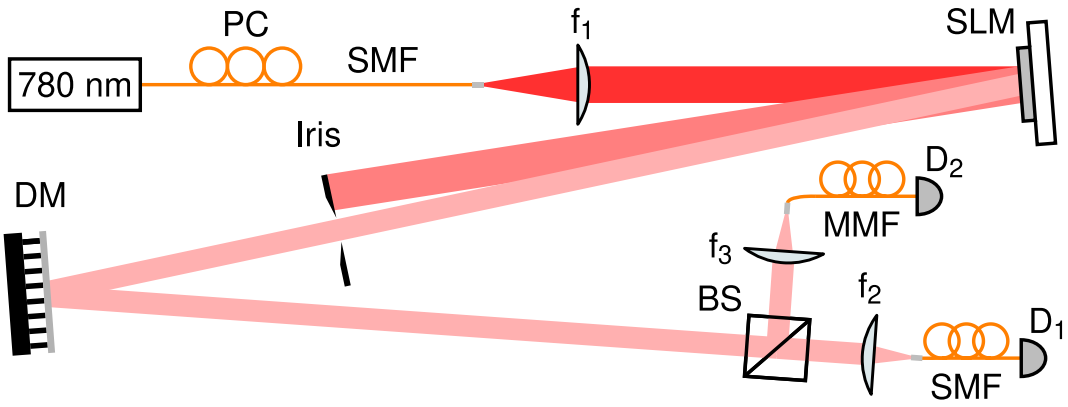

Рисунок 5.1: Экспериментальная установка. PC — контроллер поляризации, SMF — одномодовый световод, DM — деформируемое зеркало, BS — симметричный светоделитель, MMF — многомодовый световод; $D_{1,2}$ — однофотонные лавинные фотодетекторы.

ной геометрии массива актюаторов зеркал MEMS, которая хорошо соответствует модам Эрмита-Гаусса. Вычислительные базисы с другими типами симметрии, например осевой симметрией для мод Лагерра-Гаусса или мод с орбитальным угловым моментом, менее удобны для нашего подхода, так как для них требуется больше независимых пикселей для аппроксимации соответствующих элементов ВНБ прямоугольной сеткой актюаторов зеркала. Полученные результаты томографии можно легко преобразовать в любое другое базисное представление, так как они полностью эквивалентны [126]. В качестве показателя качества реконструкции квантового состояния мы используем *меру соответствия* (англ. fidelity), определяемую как

$$F = \left[\mathrm{Tr}\left(\sqrt{\sqrt{\rho}\rho'\sqrt{\rho}}\right)\right]^2. \tag{5.1}$$

Экспериментальная установка, собранная для демонстрации метода, показана на Рисунке 5.1. Приготовление состояния выполняется с помощью ПФМ с использованием стандартной методики синтеза поперечных мод, предложенной в [110]. Дифракция нулевого порядка блокируется диафрагмой, расположенной на расстоянии около 1 метра от ПФМ. Томография состояний реализована на деформируемом зеркале Boston Micromachines Mini-3.5, состоящем из 32 активных элементов, расположенных в виде матрицы 6x6 с отсутствующими углами. Выходное излучение фокусируется в одномодовое оптоволокно (SMF), по которому оно попадает в однофотонный детектор (ОФД). Поскольку количество фотонов в синтезированных модах меняется в зависимости от моды, в установку добавлен опорный канал с многомодовым волокном, в который излучение попадает после отражения от симметричного светоделителя, установленного на оптическом пути.

Рабочая длина волны составляет 780 нм, а параметр перетяжки пучков Эрмита-Гаусса составляет $w_0 = 0.9$ мм. Поскольку расстояние между ПФМ и деформируемым зеркалом, равное 1.92 м, сравнимо с длиной Рэлея $z_\mathrm{R} = 3.26$ м, голограмма для ПФМ была скорректирована таким образом, чтобы перетяжка луча находилась прямо в плоскости деформируемого зеркала. Помимо очевидных изменений кривизны фронта и размера голограммы, это также потребовало корректного учета фазы Гуи для того, чтобы получить правильные относительные фазы для суперпозиций мод. Этим

способом с помощью ПФМ можно синтезировать произвольное пространственное квантовое состояние в плоскости деформируемого зеркала. Сформированный таким образом сигнал попадает на вход на следующей части установки, где реализована *томография* этого состояния. Методика синтеза мод может считаться идеальной, так как она демонстрирует меру соответствия не менее 0.99.

Модель томографии, которую мы используем, требует измерения проекций входящих состояний на 20 элементов ВНБ, показанных на Рисунке 5.2. В явном виде эти элементы ВНБ записываются в виде 5 базисов по 4 элемента в каждом:

$$
\begin{aligned}
&\{\Phi_1,\Phi_2,\Phi_3,\Phi_4\} = \{(1,0,0,0),(0,1,0,0),(0,0,1,0),(0,0,0,1)\},\\
&\{\Phi_5,\Phi_6,\Phi_7,\Phi_8\} = \left\{\tfrac{1}{2}(1,1,1,1),\tfrac{1}{2}(1,1,-1,-1),\tfrac{1}{2}(1,-1,-1,1),\tfrac{1}{2}(1,-1,1,-1)\right\},\\
&\{\Phi_9,\Phi_{10},\Phi_{11},\Phi_{12}\} = \left\{\tfrac{1}{2}(1,-1,-i,-i),\tfrac{1}{2}(1,-1,i,i),\tfrac{1}{2}(1,1,i,-i),\tfrac{1}{2}(1,1,-i,i)\right\},\\
&\{\Phi_{13},\Phi_{14},\Phi_{15},\Phi_{16}\} = \left\{\tfrac{1}{2}(1,-i,-i,-1),\tfrac{1}{2}(1,-i,i,1),\tfrac{1}{2}(1,i,i,-1),\tfrac{1}{2}(1,i,-i,1)\right\},\\
&\{\Phi_{17},\Phi_{18},\Phi_{19},\Phi_{20}\} = \left\{\tfrac{1}{2}(1,-i,-1,-i),\tfrac{1}{2}(1,-i,1,i),\tfrac{1}{2}(1,i,-1,i),\tfrac{1}{2}(1,i,1,-i)\right\}.
\end{aligned}
\tag{5.2}
$$

Идеальное томографическое устройство без потерь преобразовало бы любой из элементов ВНБ в основную моду, идеально соответствующую моде одномодового световода. Другими словами, если запустить сигнал в обратном направлении, требуется, чтобы томографическое устройство было способно преобразовать выходной сигнал одномодового световода (Гауссов пучок) в любой из элементов ВНБ. Это может быть легко выполнено с помощью ПФМ, как это обычно делается во многих экспериментах. Однако у него есть уже упомянутые недостатки: значительная потеря сигнала, весьма ограниченная скорость переключения и сильная поляризационная чувствительность.

Чтобы преодолеть эти ограничения, вместо ПФМ используется деформируемое зеркало. У него есть свои недостатки, и наиболее очевидным из них является плохое пространственное разрешение. Действительно, с помощью деформируемого зеркала невозможно синтезировать произвольное пространственное состояние из Гауссова пучка. Однако хорошая новость заключается в том, что для выполнения томографии нам не нужно проецировать именно на элементы ВНБ. Если знать какие в точности проекторы реализуются в эксперименте, можно реконструировать состояния с высокой точностью, даже если проекторы достаточно далеки от желаемых элементов ВНБ. Чтобы измерить получаемые проекторы, выполняется томография детектора. Эта процедура полностью эквивалентна томографии всех квантовых состояний, которые получились бы после деформируемого зеркала, если бы свет подавался в обратном направлении, то есть от одномодового световода к деформируемому зеркалу.

В эксперименте с помощью ПФМ один за другим синтезируются все 20 элементов ВНБ и проводится оптимизация формы деформируемого зеркала для того, чтобы добиться наилучшего заведения этих 20 элементов ВНБ в одномодовый световод. Основная идея заключается в том, чтобы выпрямить фазу, и таким образом достигнуть наилучшего перекрытия результирующего поля с Гауссовой модой. В результате, находится требуемая геометрия состояний деформируемого зеркала, наиболее близких к проекторам на элементы ВНБ. Вся проделанная оптимизация заключалась

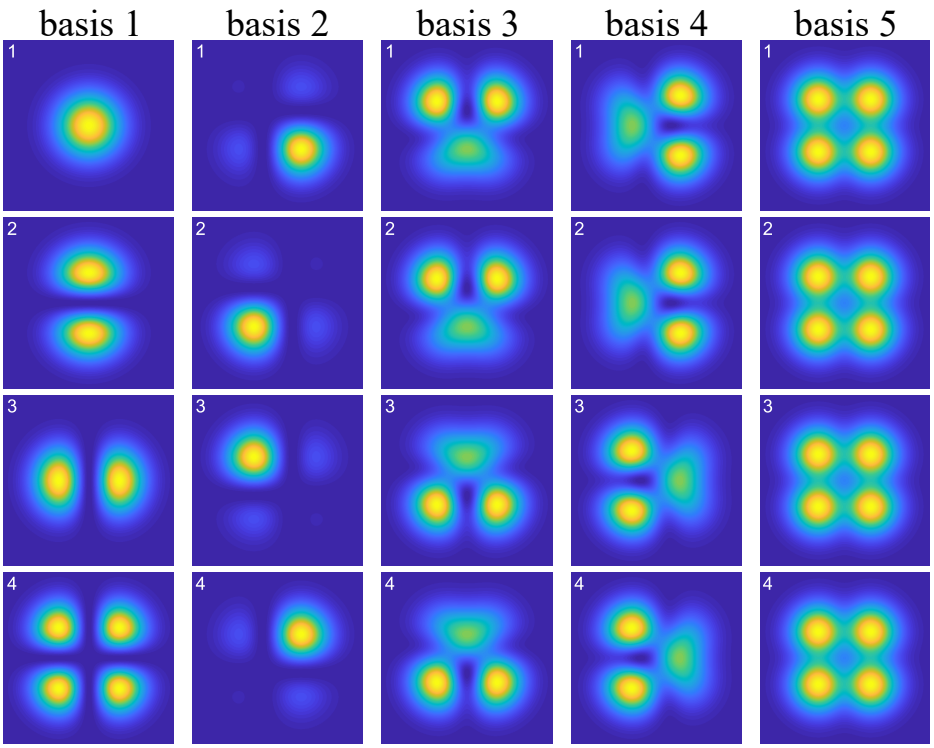

Рисунок 5.2: Пространственное распределение амплитуд для всех 20 элементов ВНБ, используемых для томографии: 5 ВНБ по 4 элемента в каждом. Одинаково выглядящие моды различаются фазовым распределением, которое здесь не показано.

в корректировке амплитуд сдвигов деформируемого зеркала. В итоге были получены проекции на что-то, приблизительно напоминающее требуемые элементы ВНБ. Чтобы использовать их в качестве томографических измерений, нам необходимо точно знать, что они из себя представляют, т.е. выполняется томография детектора.

В общем случае, преобразование мод в деформируемом зеркале может быть описано унитарной матрицей M' в гильбертовом пространстве большей размерности, которое включает высшие пространственные моды:

$$\begin{bmatrix} a_1 \\ a_2 \\ a_3 \\ a_4 \\ a_5 \\ \vdots \\ a_n \end{bmatrix} = M' \begin{bmatrix} b_1 \\ b_2 \\ b_3 \\ b_4 \\ b_5 = 0 \\ \vdots \\ b_n = 0 \end{bmatrix}, \tag{5.3}$$

где мы подразумеваем, что входное состояние ограничено размерностью $d = 4$.

Таким образом, томография состояний деформируемого зеркала позволяет найти левый

верхний угол матрицы M':

$$M' = \begin{bmatrix} m_{11}\, m_{12}\, m_{13}\, m_{14} \cdots \\ m_{21}\, m_{22}\, m_{23}\, m_{24}\ . . \\ m_{31}\, m_{32}\, m_{33}\, m_{34}\ . . \\ m_{41}\, m_{42}\, m_{43}\, m_{44}\ . . \\ \ldots\ldots\ldots\ldots\ldots\ldots \\ \ldots\ldots\ldots\ldots\ldots\ldots \end{bmatrix}. \tag{5.4}$$

Будем называть его M. Это матрица с собственными числами $|\lambda_k| \leq 1$, так как в общем случае мощность уходит в том числе в моды высшего порядка.

В эксперименте мы непосредственно (с точностью до постоянного коэффициента деления и эффективности детекторов) измеряем вероятности P_{ij} заведения фотона в одномодовый световод, где i - номер входного состояния $|\Phi_i\rangle$, а j — номер состояния деформируемого зеркала; $i, j \in \{1, 2 \ldots 20\}$. Он равен

$$P_{ij} = \left|\langle \Psi_{00}|M_j|\Phi_i\rangle\right|^2, \tag{5.5}$$

где $|\Psi_{00}\rangle$ — фундаментальная мода световода (Гауссово распределение), а $|\Phi_i\rangle$ — соответствующий элемент ВНБ.

Если бы деформируемое зеркало было идеальным устройством для томографии, оно работало бы так, что $M_j^\dagger |\Psi_{00}\rangle = |\Phi_j\rangle$, то есть j-й проектор был бы просто проектором на $|\Phi_j\rangle$. В результате получилась бы матрица значений P_{ij}, показанная на Рисунке 5.3a. На самом деле зеркало даже с бесконечным размером и пространственным разрешением не способно реализовать такие преобразование. Даже при идеальном выпрямлении фазы профили амплитуды мод остаются разными, что приводит к значительным отклонениям наблюдаемых вероятностей. Эта ситуация с идеальным зеркалом смоделирована на Рисунке 5.3b. Как можно видеть, некоторые элементы ВНБ, особенно 4 и 5-8 (см. Рисунок 5.2), имеют плохое перекрытие профилей интенсивности с основной модой и, следовательно, меньшую вероятность прохождения.

Фактические результаты томографии детектора, т.е. экспериментально измеренная матрица P_{ij}, показаны на Рисунке 5.3c. Несмотря на значительное отклонение от идеального деформируемого зеркала, что не удивительно, поскольку мы используем зеркало с очень малым числом актюаторов и непрерывной отражающей мембраной, общая картина сохраняется неизменной. Предполагается, что даже такие искаженные проекторы сохраняют достаточно высокий порядок симметрии для эффективного выполнения томографии произвольного квантового состояния. Отсутствие высокого пространственного разрешения вместе с небольшими ошибками совмещения приводит к заметным отклонениям от Рисунка 5.3b. Например, некоторые недиагональные элементы на графике больше диагональных. Преимущество продемонстрированного подхода состоит в том, что это нарушение не может существенно повлиять на результаты томографии, поскольку мы измеряем проекторы на этапе томографии детектора, а затем используем эти знания для восстановления неизвестных состояний.

Чтобы решить переопределенную систему уравнений (5.5) для нахождения M_j, проще использовать более общий формализм. Пусть входное состояние описывается матрицей плотности

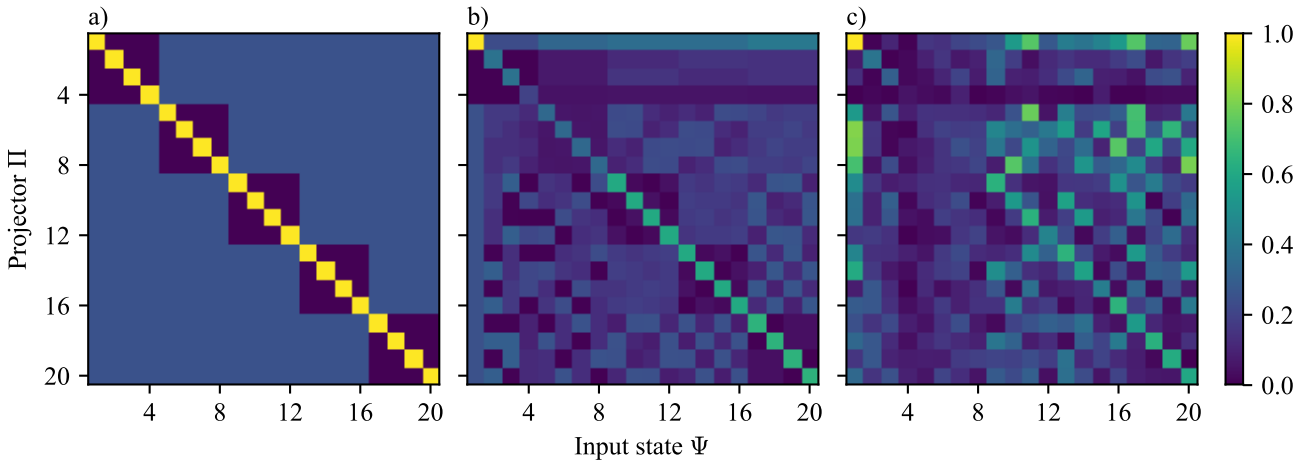

Рисунок 5.3: Матрица результатов измерения для протокола на ВНБ в гильбертовом пространстве размерности 4: вероятностью прохождения состояния Φ_i через проектор Π_j a) идеальные проекторы на элементы ВНБ Φ_j; b) идеальное деформируемое зеркало с бесконечным размером и пространственным разрешением; c) экспериментально измеренные результаты.

ρ, которая измеряется конкретным зеркалом. установка j. Тогда измеренная вероятность равна

$$P_j = \mathrm{Tr}\left(\rho \cdot M_j^\dagger \left|\Psi_{00}\right\rangle \left\langle\Psi_{00}\right| M_j\right). \tag{5.6}$$

Это уравнение, которое по сути является скалярным произведением Гильберта-Шмидта для двух матриц, может быть переписано с использованием векторизованной нотации [150, 151]

$$P_j = \left\langle\!\left\langle \rho \left| M_j^\dagger \left|\Psi_{00}\right\rangle \left\langle\Psi_{00}\right| M_j \right\rangle\!\right\rangle. \tag{5.7}$$

На этапе томографии детектора входные состояния известны и описываются как $\rho_i = \left|\Phi_i\right\rangle \left\langle\Phi_i\right|$, а матрицу измерений $\Pi_j = M_j^\dagger \left|\Psi_{00}\right\rangle \left\langle\Psi_{00}\right| M_j$ необходимо определить. По построению эта матрица Π_j является неправильно нормированным проектором, т.е. имеет только одно ненулевое собственное значение, соответствующее собственному вектору $\left|P_j\right\rangle = M_j^\dagger \left|\Psi_{00}\right\rangle$. Само собственное значение показывает эффективность проекции. Для каждого j нужно решить переопределенную систему линейных уравнений для изменяющегося i:

$$P_{ij} = \left\langle\!\left\langle \rho_i \left| M_j^\dagger \left|\Psi_{00}\right\rangle \left\langle\Psi_{00}\right| M_j \right\rangle\!\right\rangle. \tag{5.8}$$

Система решается в смысле метода наименьших квадратов. Из-за наличия экспериментальных ошибок, особенно в случае переопределенной системы, результирующая матрица Π_j содержит более одного ненулевого собственного значения. На этапе томографии детектора все второстепенные собственные значения отбрасываются, чтобы явно сохранить форму этого оператора как $\Pi_j = \left|P_j\right\rangle \left\langle P_j\right|$.

Томография неизвестных квантовых состояний — это обратная задача по отношению к детекторной томографии: зная Π_j и P_j для всех j, нужно решить систему (5.7) для нахождения неизвестного ρ.

Достаточно ясно, что для томографии кудита достаточно почти любых $d^2 = 16$ различных состояний деформируемого зеркала. Однако, очевидно, что одни наборы более оптимальны, чем другие. Количественной мерой может быть отношение между наибольшим и наименьшим сингулярными значениями матрицы, образованной набором векторизованных матриц измерений $\left|\Pi_j\right\rangle\!\rangle$: $\eta = \max\lambda_k / \min\lambda_k$. Действительно, если η близко к 1, инвертирование системы (5.7) дает наименьшую неопределенность из-за экспериментального шума. Напротив, очень большие значения η приводят к сильному проникновению даже небольшого экспериментального шума в решение.

Идеальный случай $\Pi_j = |\Phi_j\rangle\langle\Phi_j|$ соответствует $\eta = \sqrt{5} \approx 2.2$. Зеркало с бесконечным разрешением дает $\eta \approx 5.0$; идеальное зеркало 6x6 с независимыми пикселями и тем же размером пикселя, что и в эксперименте, соответствует $\eta \approx 10.5$. Найденное значение для измеренной матрицы составляет $\eta \approx 33$, что не так уж далеко от идеализированного случая. Основное различие между двумя последними значениями связано с большим межпиксельным перекрестным взаимодействием нашего деформируемого зеркала. Это неизбежный недостаток зеркал с непрерывной отражающей мембраной, где соседние пиксели в значительной степени связаны ей между собой. Соответствующая η потенциально может быть вычислена путем тщательного моделирования зеркала, однако это не слишком реально, поскольку далеко не все известно о его внутренней структуре. Мы можем только сделать вывод, что совокупный эффект этого перекрестного взаимодействия и всех других экспериментальных неидеальностей, включая постоянно присутствующие незначительные ошибки юстировки, приводит к трехкратному увеличению η, что выглядит довольно правдоподобно. Наконец, как упоминалось ранее, значение η не имеет прямого влияния на получаемую точность. Бесшумный и идеально повторяемый эксперимент в любом случае всегда дает идеально точные результаты. Большая η означает лишь более сильное влияние шума на результаты томографии.

После того, как калибровочная матрица для деформируемого зеркала (Рисунок 5.3c) была экспериментально измерена, были вычислены все 20 измерительных матриц Π_j, т.е. был получен результат томографии детектора. Затем эти данные были использованы для томографии квантовых состояний: для восстановления предположительно неизвестных входных состояний ρ после их измерения всеми 20 проекторами Π_j каждый. Однако в нашем эксперименте все входные состояния заранее известны, потому что они синтезируются с помощью ПФМ. Следовательно, мы всегда можем вычислить меру соответствия между восстановленным и фактическим состояниями.

Прежде всего, мы выполнили томографию 20 состояний $|\Phi_i\rangle$, которая показала среднюю меру соответствия восстановления 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 5.4 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 размерности 4. Хорошо известен экспериментальный факт, что чем больше размерность реконструируемого состояния, тем меньше типичная точность восстановления [142]. В основном это связано с экспериментальными ошибками, ко-

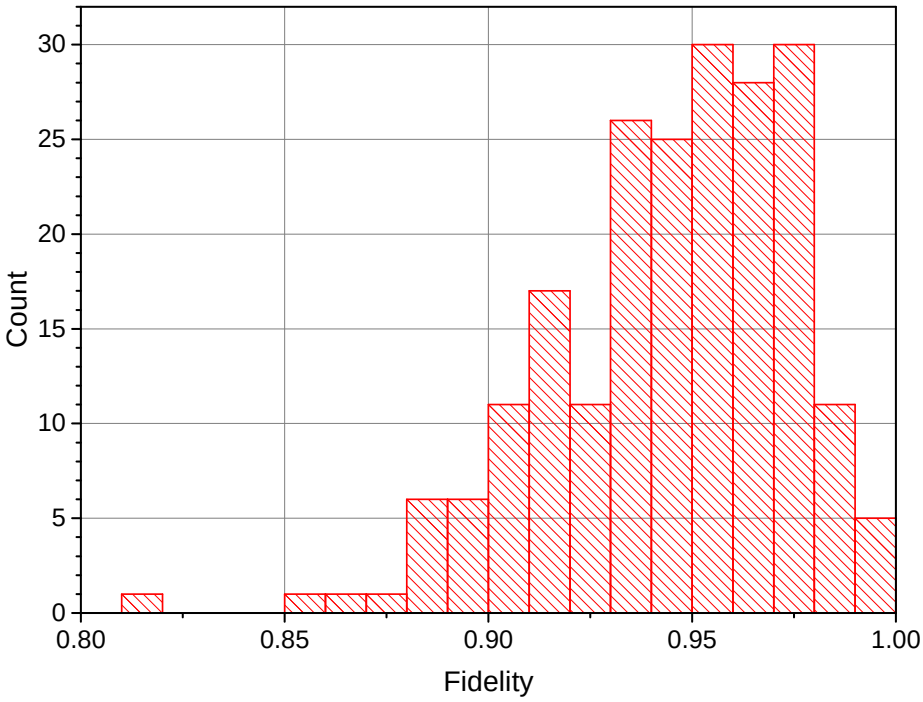

Рисунок 5.4: Гистограмма распределения значений меры соответствия для 210 случайных чистых квантовых состояний.

торые затем переходят на полученные результаты восстановления. В этом смысле пространственные квантовые состояния очень чувствительны к внешним воздействиям и ошибкам юстировки. В то же время, снижение точности восстановления несколько компенсируется тем фактом, что математическое ожидание для значения меры соответствия между двумя случайными чистыми состояниями равна $\langle F_{\text{rnd}} \rangle = 1/d$ с точным распределением вероятностей $P(F) = (d-1)(1-F)^{d-2}$ [152], поэтому, например, доля состояний, имеющих значение меры соответствия по отношению к заданному $F > 0.9$ в 4-х размерном пространстве составляет всего 10^{-3}.

5.3. Обсуждение результатов

Выполненная экспериментальная демонстрация показывает состоятельность метода томографии пространственных кудитов с помощью деформируемого зеркала. Полученная экспериментально точность реконструкции очень похожа на другие томографические эксперименты с пространственными квантовыми состояниями [142, 146].

Использование деформируемого зеркала вместо ПФМ дает три основных преимущества: 1. эффективность преобразования мод; 2. поляризационная нечувствительность; 3. скорость работы. Повышение эффективности связано с принципом работы жидкокристаллического ПФМ. Его использование в качестве фазового экрана обычно выполняется в первом порядке дифракции, в то время как все остальные порядки, включая 0-й, приводят к потере сигнала. Фазовые сдвиги сильно зависят от поляризации, ограничивая возможности томографии на ПФМ только поляризованными сигналами. Деформируемое зеркало, напротив, отражает почти 100% падающего на

него излучения, практически не создавая потерь.

Скорость работы ПФМ на базе жидких кристаллов ограничена несколькими сотнями герц, поскольку такие большие молекулы недостаточно подвижны, чтобы двигаться быстрее под действием приложенного электрического поля. Устройства на основе микроэлектромеханики легко показывают частоту переключения в килогерцы и сильно больше [153, 154], поэтому управляемое деформируемое зеркало может переключать состояния на порядки быстрее, чем обычные ПФМ. Еще одна веская причина для использования деформируемых зеркал — гораздо более приемлемый объем данных и, соответственно, вычислений, необходимых для записи нового состояния. В нашей установке достаточно всего 32 байтов данных, чтобы полностью определить положения всех 32 доступных актюаторов. Более современные деформируемые зеркала обычно имеют не менее 100 и до нескольких тысяч актюаторов, что достаточно для выполнения томографии в гораздо большем гильбертовом пространстве, чем в представленной демонстрации. С другой стороны, типичный ПФМ — это устройство размера порядка мегапикселя, которому требуется не менее 1 МБ данных для определения его состояния. Эти значения должны быть сначала вычислены и затем переданы на устройство. Только это, само по себе, занимает как минимум на 3 порядка больше времени, чем передача долей килобайта для деформируемого зеркала. Интерфейс к ПФМ также обычно ограничен поддерживаемой частотой кадров HDMI/DVI контроллера в несколько сотен Гц.

В результате, томография на основе деформируемого зеркала может сыграть ключевую роль в томографии нестационарных состояний, где важна высокая скорость измерений. Например, его можно использовать в каналах связи по открытому пространству для измерения возмущения передаваемых пространственных квантовых состояний, а также в других динамических экспериментах, где квантовые состояния меняются во времени. Также его можно использовать для измерения модового состава классических ярких пучков света, как, например, в классической связи по открытому пространству.

Хотя преимущество в эффективности не так уж очевидно, деформируемые зеркала также могут заменить ПФМ для повышения общей эффективности детектирования, что имеет решающее значение во многих применениях квантовых технологий. Особенно это может касаться томографии неполяризованных источников.

5.4. Заключение к Главе 5

В этой главе продемонстрировано использование деформируемого зеркала для томографии пространственных квантовых состояний света. Квантовая томография является важнейшим экспериментальным инструментом в области квантовой информации. В проведенных экспериментах продемонстрирована квантовая томография в четырехмерном гильбертовом пространстве путем проведения измерений во взаимно несмещенных базисах. Достигнуто среднее значение меры соответствия (fidelity), равное 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.

Глава 6

Квантовая криптография

Эта, заключительная глава диссертации посвящена разработке методов защиты информации от несанкционированного доступа путем применения квантовой криптографии. Квантовая криптография существует на стыке оптических коммуникаций и квантовой оптики и стала очень активно развиваться в последние два десятилетия. Квантовая криптография позволяет организовать обмен секретными ключами с доказуемой секретностью. История такого подхода началась в 1984 году с публикации первого протокола [155], позже названного BB84. Несмотря на состоятельность этого, самого первого протокола квантовой криптографии, четкие доказательства его секретности появились сильно позже [156]. 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 обладают совершенно другими физическими свойствами.

В этой главе рассмотрен так называемый релятивистский протокол квантовой криптографии, позволяющий качественно решить проблему замены однофотонных состояний когерентными. Кроме того, предложена конструкция протокола на геометрически-однородных состояниях, обладающая рядом преимуществ по сравнению со стандартной реализацией квантового распределения ключей на базе протокола BB84. Также, в квантовой криптографии важнейшую роль играет генерация случайных чисел — одна из основ обеспечения защищенности протокола. По понятным причинам в квантовой криптографии нельзя использовать псевдослучайные генераторы, поэтому единственный выход из данной ситуации — пользоваться физическими генераторами случайности. В разделе ниже приводятся результаты исследования по созданию такого генератора, основанного на исключительно квантовом эффекте — однофотонном детектировании многомодового оптического излучения.

Немаловажная причина, по которой квантовая криптография демонстрирует колоссальный прогресс в последнее время, это активное развитие другой квантовой технологии — квантовых вычислений. Как было показано Петером Шором, квантовый компьютер позволяет за полиномиальное время раскладывать числа на множители. Это ставит под угрозу всю используемую в настоящий момент криптографию с открытым ключом. Таким образом, задача распределения сек-

ретных ключей становится еще более актуальной. Параллельно идет активное исследование так называемой пост-квантовой криптографии, т.е. криптографии с открытым ключом, потенциально устойчивой к квантовым алгоритмам взлома.

6.1. Генерация случайных чисел для задач квантовой криптографии

В этом разделе представлена простая и надежная конструкция квантового генератора случайных чисел (КГСЧ), работающая в реальном времени [A15], [P5]. Выбранный минималистический подход гарантирует стабильную работу устройства, а также его простую и понятную аппаратную реализацию в виде автономного модуля. В качестве источника случайности в приборе использовано измерение временны́х интервалов между щелчками однофотонного детектора. Полученная необработанная последовательность длительностей интервалов затем фильтруется и обрабатывается детерминированным экстрактором случайности, который реализован в виде фиксированной таблицы преобразований. Это обеспечивает высокую скорость обработки „на лету“ без необходимости проведения сложных вычислений. Общая производительность устройства составляет около 1 случайного бита на каждое срабатывание детектора, что в нашей реализации обеспечивает скорость генерации около 1.2 Мбит/с.

Генерация случайных чисел с помощью квантовых процессов стала привлекать большое внимание, с развитием остальных квантовых технологий. Квантовая генерация случайных чисел открывает доступ к универсальной случайности квантовой механики. При этом в рамках в классической физики, случайности как таковой нет в принципе — есть лишь неточно известные начальные условия. За последние 20 лет появилось много различных подходов к генерации случайных чисел, а также предложений по её практической реализации. В данной работе была задача создать предельно простой и практичный в реализации КГСЧ, который будет обеспечивать стабильную работу благодаря своей простоте. Для этого намеренно рассматривались только конструкции с одним однофотонным детектором. Наряду с физической частью КГСЧ не менее важным является выбор алгоритма экстракции случайности, который сам по себе должен гарантировать генерацию независимых и несмещенных битов на выходе при любых условиях.

В литературе описано множество различных подходов к генерации квантовой случайности [157, 158, 159, 160, 161, 162, 163, 164, 165, 166, 167]. Тем не менее, достаточно трудно провести четкое различие между подходами, которые можно назвать „квантовыми“, и теми, которые в некотором смысле относятся к статистической физике. Мы связываем понятие „квантовый“ с использованием простых квантовых измерений и наличием однофотонных детекторов (ОФД) или детекторов других частиц. Мы также полагаем, что большинство других методов относятся к случаю классической физики: в этом случае сложнее объяснить, что делает источник случайности действительно непредсказуемым и, следовательно, ответить на вопрос, может ли он в принципе генерировать истинную случайность. Среди источников на основе однофотонных детекторов

достаточно выгодно использовать один такой прибор во всей установке. Помимо очевидного преимущества по надежности всего устройства, это также исключает необходимость какой-либо аппаратной калибровки, поскольку ОФД обычно имеют большой разброс рабочих параметров даже среди идентичных устройств. Использование более одного ОФД также не дает преимущества в скорости генерации: обычно результат такой же, как и для соответствующих нескольких отдельных устройств на одном ОФД.

Выходной сигнал ОФД содержит только информацию о времени срабатывания (это также может быть и число фотонов, но обычные ОФД его не разрешают), то есть о моментах, когда конкретный фотон вызвал лавинный отклик в детекторе. Это единственный источник информации, доступный для извлечения случайных чисел. Для реализации квантового измерения могут потребоваться специальные оптические импульсы, например, в эксперименте „какой путь“ [159] или в эксперименте „множественный выбор“ [168], но с точки зрения производительности эти конфигурации неоптимальны: вместо того, чтобы использовать произвольные моменты времени, отсчитываемые тактовыми сигналами, импульсы намеренно ограничивают доступный диапазон моментов срабатывания лишь строго избранными. Таким образом, оптимальная в этом смысле конструкция должна использовать постоянно работающий источник излучения.

Простейшим вариантом реализации такого метода является измерение моментов прихода фотонов от непрерывного когерентного источника [157, 161, 162, 165, 167]. Такое измерение дает чистую пуассоновскую статистику, с которой просто работать. Также возможна модификация с модифицированным по времени источником непрерывного сигнала [169], который дает несколько лучшую производительность, но за счет увеличения сложности системы и снижения её надежности, что не очень соответствует выбранной концепции КГСЧ.

Сбор информации о моментах срабатывания детектора обычно осуществляется в двух разных формах: с помощью отметки времени приходящих фотонов по значению автономно работающего тактового счетчика, как в [157, 161, 170, 167], или путем подсчета количества тактов между соседними событиями детектирования [162, 165]. Эти два варианта полностью идентичны по объему получаемой информации: каждый формат данных может быть легко преобразован в другой. Однако, во втором варианте получаемый поток данных состоит из независимых целых значений, а в первом неизбежно содержится внутренняя корреляция между значениями. Она возникает из-за медленно изменяющихся старших битов счетчика времени. Прямой расчет [157] показывает, что для того, чтобы корреляцией можно было пренебречь, нужно потребовать, чтобы значения битов изменялись примерно в 15 раз быстрее, чем средняя скорость счета. Это накладывает существенные ограничения на количество получаемой случайной информации. Таким образом, замер именно временны́х интервалов между щелчками детектора обладает явным преимуществом, поскольку, по определению процесса Пуассона, все такие значения абсолютно независимы. Они распределены по экспоненциальному закону, т.е. малые значения наиболее вероятны, а дальнейшее распределение экспоненциально затухает в сторону больших значений.

Другим, не менее важным аспектом такого подхода к генерации случайных чисел является генерация детектируемого излучения. С теоретической точки зрения, было бы идеально использо-

вать одномодовый (в поперечном, временно́м и поляризационном смысле) когерентный источник оптического излучения непрерывного действия. Однако на практике такое нереализуемо. Вместо этого мы используем альтернативный подход, основанный на усреднении мод. Даже если статистика одной моды не обязательно является пуассоновской, чем больше мод мы обнаруживаем, тем ближе выходной сигнал будет напоминать пуассоновский процесс вследствие теоремы Пальма–Хинчина [171]. Таким образом, существенно многомодовое детектирование позволяет достичь пуассоновской статистики вне зависимости от статистики фотонов в каждой из мод.

После получения сырого потока случайных данных, их необходимо обработать, чтобы получить случайные и независимые биты информации. Эта обработка, или экстракция, может выполняться разными способами, соответствующими двум глобальным подходам: с использованием детерминированных алгоритмов и с помощью случайных экстракторов. Второй подход гораздо более универсальный, поскольку он способен извлекать случайность из любого типа частично случайной последовательности, однако в этой работе мы придерживаемся первого подхода. Для работы случайных экстракторов требуются случайные конфигурационные значения (затравка, seed). До недавнего времени такие алгоритмы требовали больше случайной информации в качестве затравки, чем они производили из сырых входных данных, например такая ситуация возникает при использовании матриц Тёплица [167]. Позже было найдено новое семейство экстракторов Тревисана [172], которое позволяет генерировать больше случайности, чем было использовано в качестве затравки. Эти экстракторы также позволяют повторно использовать их внутреннюю конфигурацию для будущих преобразований [173].

Основная сложность использования случайных экстракторов с затравкой заключается в том, что они сконструированы для определенной скорости генерации мин-энтропии, обеспечиваемой источником сырых данных. После того, как она была определена, экстрактор конфигурируется для обеспечения соответствующей степень сжатия исходной последовательности, которая уже ни от чего не зависит, включая фактическое качество необработанной последовательности. Это порождает огромный недостаток в системе: если по какой-либо причине сырая последовательность ухудшается, выход случайного экстрактора перестанет быть действительно случайным. Такие алгоритмы по своей сути лишены какой-либо адаптивности и могут легко выдавать коррелированные последовательности, например, из-за временно́го дрейфа экспериментальных параметров, влияющих на количество генерируемой энтропии.

Вторая проблема связана с корректной оценкой мин-энтропии источника и реализацией такого экстрактора, особенно из семейства Тревисана, в режиме реального времени. Строго говоря, невозможно измерить мин-энтропию любого заданного источника за конечное время. Знание внутренней структуры источника помогает, но не делает проблему тривиальной. В то же время, скорость генерации энтропии остается единственным параметром, который определяет, является ли вывод КГСЧ случайным или нет. Это может стать еще более критичной проблемой при использовании выхода экстрактора в качестве затравки для дальнейших преобразований. Обработка данных в реальном времени — это скорее технический, но, тем не менее, немаловажный вопрос. Недавние результаты показывают, что реализация алгоритма Тревисана на современных компью-

терах дает выходную скорость данных около 17 кбит/с [174]. Это на порядки меньше скорости генерации энтропии типичным ОФД. Такой ресурсоемкий алгоритм экстракции трудно применять, если стоит вопрос о повышении скорости генерации случайной битовой последовательности.

Основываясь на приведенной информации, было решено, что детерминированные алгоритмы экстракции, если они применимы, лучше подходят для наших целей. Здесь мы должны заметить, что популярный подход [165] использования стандартных хэш-функций, таких как SHA-256, строго говоря, некорректен [165], поскольку он не извлекает случайность, а только сжимает необработанные данные каким-то своеобразным образом. Он не гарантирует независимости выходных битов и обладает теми же недостатками, что и случайные экстракторы с затравкой.

Говоря о детерминированных экстракторах, нужно хорошо понимать свойства входных данных. Как было показано ранее, мы рассматриваем поток положительных и независимых целых чисел с экспоненциальным распределением вероятностей. Цель экстрактора - преобразовать этот поток в несмещенные и независимые биты.

Самый простой, но неэффективный метод — преобразовать поток в независимые, но смещенные биты, взяв целые числа по модулю 2, а затем устранить смещение с помощью алгоритма фон Неймана [175]. Мы используем обобщение этого метода на конечный алфавит из $M > 2$ букв — расширенный алгоритм Элиаса [176], который является асимптотически эффективным, сходящимся к энтропии источника (см. также [177]). Важно отметить, что здесь можно использовать любое детерминированное преобразование полученных натуральных чисел в конечный алфавит, так как это не влияет на качество вывода экстрактора. Однако, желательно приблизиться к равномерному распределению вероятностей в алфавите, чтобы уменьшить потери энтропии при экстракции.

Реализация алгоритма экстракции Элиаса явно приведена в [178]. Вкратце, входная последовательность разбивается на слова по N букв каждое. Вероятность получить конкретное слово точно такая же, как и для всех слов, которые представляют собой перестановки букв исходного. Общее количество таких перестановок дает количество равновероятных состояний, одно из которых реализовалось как исходное слово. Все такие состояния можно пронумеровать, а номер полученного состояния можно преобразовать в случайные биты, используя его двоичное представление.

Пример извлечения для $M = N = 4$ показан на Рисунке 6.1. Строки AAAA, …, DDDD отображаются в пустое множество, потому что все они имеют разные вероятности появления, если только вероятность появления отдельных букв A, B, C и D в точности не равна. Шаблоны ABBB, BABB, BBAB и BBBA и т.п. генерируют два выходных бита: если появление букв является независимым друг от друга, каждая комбинация букв имеет 4 равновероятных перестановки, независимо от вероятности появления отдельных букв A, …, D. Наибольшее количество перестановок наблюдается для слова ABCD, дающее 24 варианта; каждый из них дает 3 или 4 выходных бита.

Следуя выбранному минималистическому подходу, целью было максимально упростить требуемую обработку сигналов. Учитывая, что ожидаемая пропускная способность экстрактора должна быть в диапазоне Мбит/с, мы слегка пожертвовали эффективностью экстракции, но сде-

(4,0,0,0)	(3,1,0,0)	(2,2,0,0)	(2,1,1,0)	(1,1,1,1)
AAAA→ ∅	BBBC→ 00	AACC→ 00	ABBD→ 000 } 8	ABCD→ 0000 } 16
	BBCB→ 01	ACAC→ 01	ABDB→ 001	ABDC→ 0001
	BCBB→ 10	ACCA→ 10	... ...	... ...
	CBBB→ 11	CAAC→ 11	BDAB→ 111	CBDA→ 1111
		CACA→ 0	BDBA→ 00	CDAB→ 000 } 8
		CCAA→ 1	DABB→ 01	CDBA→ 001
			DBAB→ 10	... ...
			DBBA→ 11	DCBA→ 111
$f = 4/256$	$f = 48/256$	$f = 36/256$	$f = 144/256$	$f = 24/256$

Рисунок 6.1: Извлечение случайных битов для $M = N = 4$. Первая строка показывает образец слова, то есть отсортированный список повторений каждой буквы. Соответствующий процесс извлечения приведен ниже на примере одного семейства перестановок. Значение f показывает долю определенного шаблона во всех $M^N = 256$ возможных входных словах; оно совпадает с реальной частотой появления, если все буквы равновероятны.

лали его пригодным для реализации в виде фиксированной таблицы преобразований, зашитой в стандартный чип памяти. В нашей реализации используется алфавит из $M = 4$ букв, а преобразования выполняются, с использованием блоков из $N = 10$ таких значений. Это соответствует 20-битному адресному пространству используемой микросхемы флэш-памяти 2 МБ. Другим ограничением, которое также дает преимущество меньшему размеру алфавита и более коротким блокам обработки, является требование стационарности процесса: если параметры процесса изменяются во времени, выходная последовательность может перестать быть случайной и несмещенной. Процесс должен быть стационарным в течение времени, необходимого для прохождения всех возможных комбинаций в блоке обработки, что по порядку величины соответствует обработке M^N блоков. Таким образом, для существенного увеличения размера алфавита и длины блока также потребуется гарантировать стабильность не в течение секунд, а в течения часов и даже дней, что практически невозможно гарантировать на практике: любой контур обратной связи в системе, например для поддержания постоянной уровня отсчетов в секунду, должен быть существенно медленнее этого времени, что делает систему чрезвычайно непрактичной.

На Рисунке 6.2 показана смоделированная эффективность алгоритма извлечения для изменяющегося размера двоичного буфера $b = N\lceil \log M \rceil$, необходимого для хранения всего блока обработки. Эффективность была вычислена для равновероятного распределения входных символов. На графике показаны линии для разных размеров алфавита M, которые удобно выбирать в качестве степеней двойки. Видно, что для выбранной пары $M = 4$ и $N = 10$ алгоритм генерирует 1.2 бит на входной символ. Легко заметить, что масштабирование с размером памяти довольно слабое: даже для 40-битного адресного пространства, что на практике нереально и неизбежно вызовет проблемы с временно́й стабильностью, эффективность экстракции приближается только к значению 1.8 бит на символ. Таким образом, даже с учетом того, что мы пожертвовали скоростью генерации ради простоты системы и более высокого качества генерируемой последовательности, мы все еще не слишком далеки от возможного потенциала такой схемы.

Обсуждаемые принципы и идеи были реализованы в нашей экспериментальной реализации,

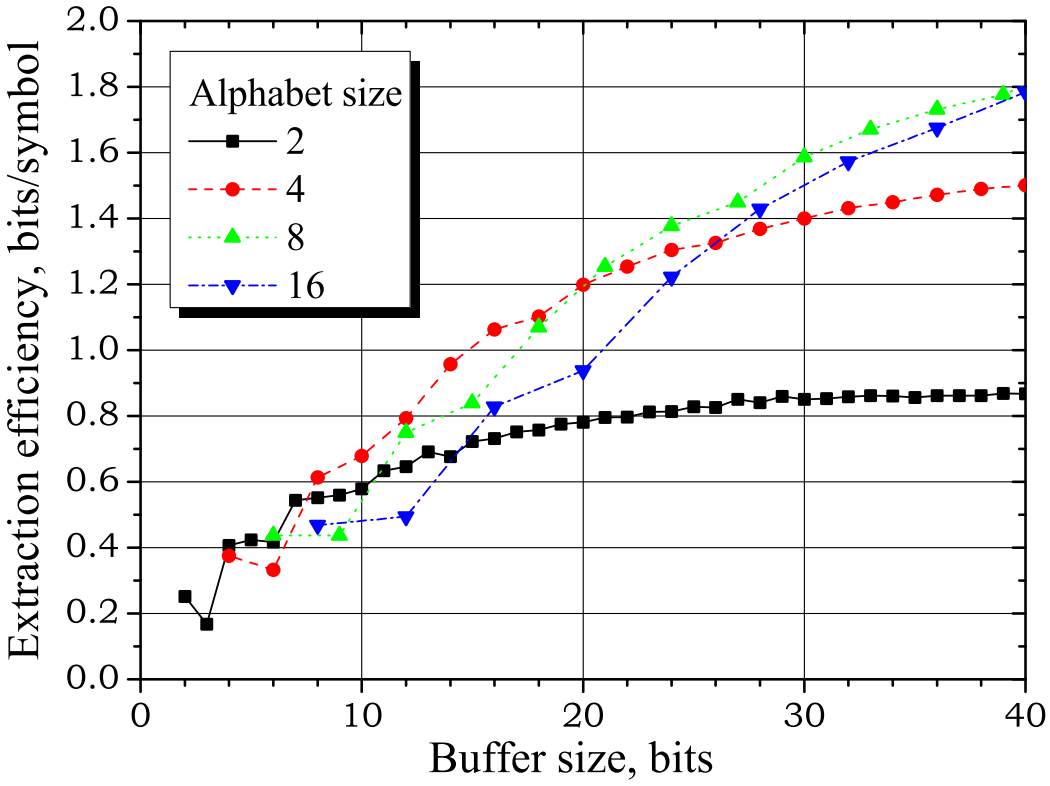

Рисунок 6.2: Эффективность экстракции реализованного алгоритма в зависимости от размера буфера для разных размеров алфавита. Реально созданный генератор использует 20-битный буфер и 4-х символьный алфавит, что соответствует скорости генерации 1.2 бит на сырой символ.

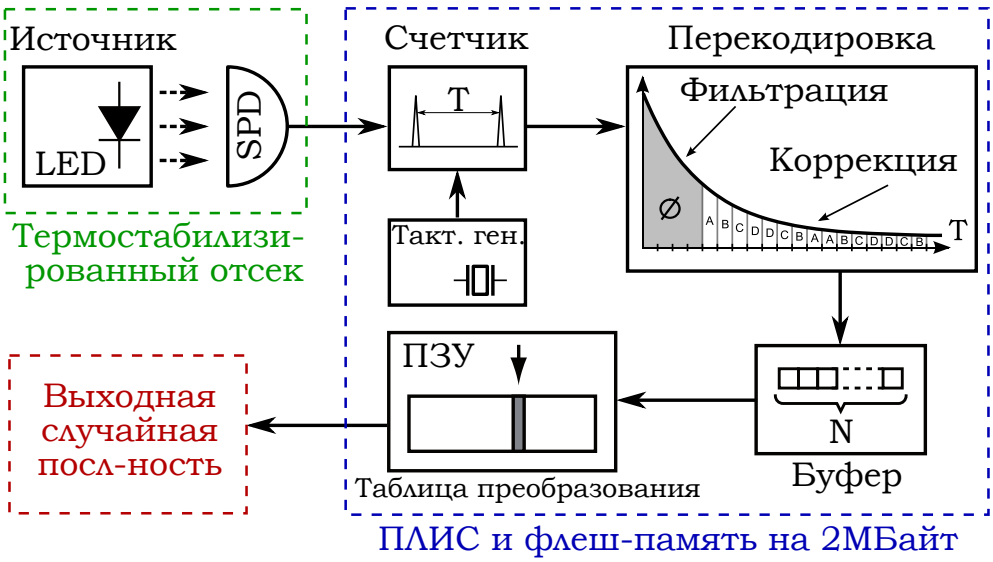

Рисунок 6.3: Блок-схема экспериментальной установки.

показанной на Рисунке 6.3. Установка основана на кремниевом ОФД с тонким обедняющим 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. Вся сборка, включающая светодиод и ОФД, стабилизирована по температуре с уставкой +25° C. Для стабилизации средней частоты срабатывания ОФД путем регулировки тока светодиода используется контур обратной связи с постоянной времени 16 с. Такая медленная обратная связь требуется для того, чтобы гарантировать стационарность процесса на временной шкале порядка M^N отсчетов.

Главный недостаток экспериментальной системы с точки зрения теории — неидеальные характеристики ОФД. Для представленной структуры КГСЧ это, прежде всего, временны́е параметры ОФД. В то время как процесс прихода фотонов является пуассоновским, процесс генерации щелчков детектора — нет. Он имеет очень низкую вероятность детектирования сразу после предыдущего щелчка — эффект, известный как мертвое время детектора. ОФД также может иметь противоположный по смыслу эффект уже с другим временным распределением, называемый послеимпульсами, то есть самопроизвольное срабатывание детектора, вызванное предыдущими отсчетами.

Наше исследование реального процесса детектирования постоянного оптического сигнала было выполнено при той же средней скорости отсчетов, что и в конечном устройстве, а именно 1.2 МГц. На Рисунке 6.4 показана гистограмма частоты отсчетов как функция задержки между последовательными срабатываниями. Она идеально соответствует ожидаемому экспоненциальному распределению, за исключением интервалов короче 150 нс. Отклонение от ожидаемого распределения хорошо описывается экспоненциальной функцией затухания с постоянной времени 40 нс.

Какова бы ни была природа этих неидеальностей, если можно измерить максимальную задержку, на которой они еще влияют на распределение, мы можем легко отфильтровать такие

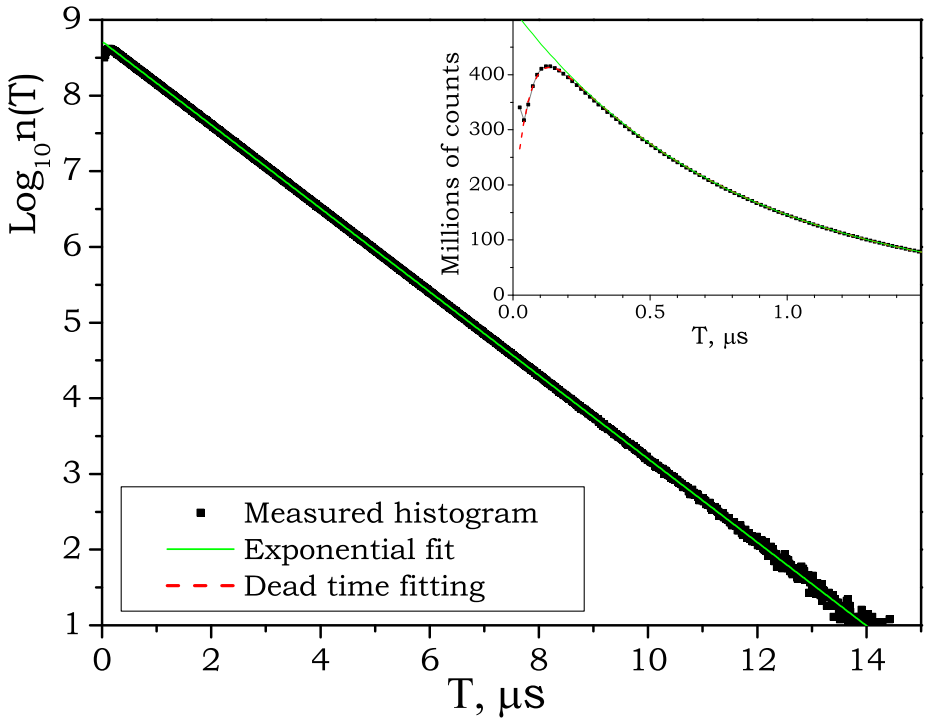

Рисунок 6.4: Измеренная гистограмма для времени ожидания между срабатываниями ОФД при средней частоте отсчетов 1.2 МГц. Сильное отклонение от ожидаемого экспоненциального поведения наблюдается при $T \lesssim 150$ нс.

зависимые события, убедившись, что ни один временной интервал короче указанного времени не используется для генерации случайных чисел на выходе. Другими словами, реальный ОФД моделируется как идеальный детектор, дающий пуассоновскую статистику, с неким возмущением, имеющим память длительностью не более τ. Чтобы избавиться от зависимых событий, мы используем простой цифровой фильтр, который отбрасывает все временные интервалы короче τ = 160 нс, снижая частоту генерации событий с 1.2 до 1.0 МГц.

Еще один существенный недостаток самой системы — наличие темновых отсчетов. Частота темновых отсчетов используемого детектора составляет около 200 Гц, что почти на 4 порядка меньше штатной скорости счета. Хотя природа темновых отсчетов намного сложнее и не столь явно „квантовая“, как события фотодетектирования, они, тем не менее, также обладают почти пуассоновской статистикой и не влияют на какие-либо полученные результаты. Можно лишь констатировать, что 0.01% генерируемой энтропии может быть недостаточно „квантовым“.

Срабатываниям детектора присваиваются временны́е метки с разрешением 16 нс, и вычисляются длительности соответствующих временны́х интервалов. Все интервалы короче 160 нс отбрасываются, а оставшиеся преобразуются в 4-хсимвольный алфавит, как показано на Рисунке 6.5. Выбранная схема преобразования дает более равномерное распределение, чем тривиальное взятие остатка по модулю 4. Блоки из 10 последовательных символов, представленные в виде десяти 2-хбитных строк, образуют 20-битный адрес для микросхемы памяти, указывающий на 2-хбайтовое предварительно вычисленное значение. Количество выходных бит на каждый символ варьирует-

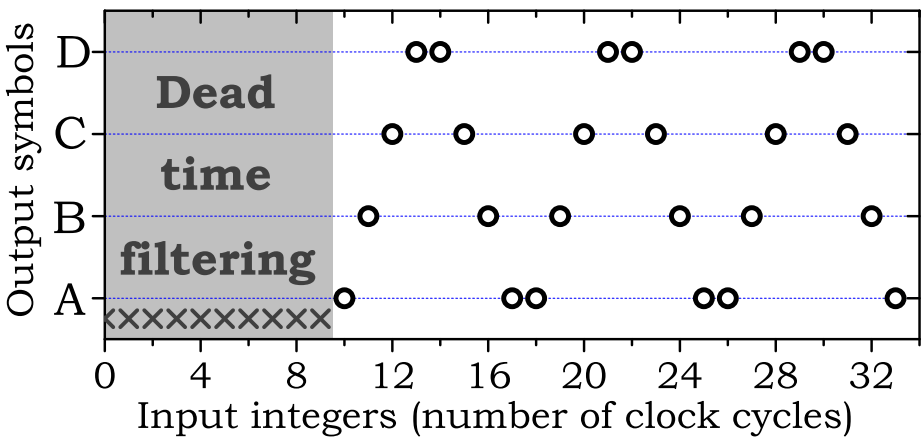

Рисунок 6.5: Преобразование оцифрованных временных интервалов в 4-хбуквенный алфавит с уменьшением смещения за счет двунаправленного кодирования и фильтра временно́й отсечки на 10 тактов.

ся от нуля (когда все 10 символов одинаковы) до 14 бит (максимальное количество перестановок составляет $10!/(3!3!2!2!) = 25200$). Чтобы реализовать этот вывод с переменным размером, используется простое двоичное кодирование, когда фактические выходные данные дополняются слева единицей и нулями, чтобы сформировать 16-битную строку $\underbrace{0\ldots0}_{15-k}\,1\,\underbrace{ab\ldots yz}_{k}$, где k - размер выходной строки, а $ab\ldots yz$ — сама строка.

Сгенерированные случайные битовые последовательности были изучены с использованием набора статистических тестов NIST [179] на случайность. Тестирование последовательных блоков данных размером 1 Гбит с параметром $\alpha = 0.01$ и использованием 1000 битовых потоков по 10^6 бит показало, что коэффициент прохождения значительно превышает 0.98 для всех тестов. P-value$_T$ для χ^2-теста однородности полученных P-values для каждого потока, составляет 0.68, что выше уровня достоверности 0.0001. Все полученные результаты свидетельствуют о том, что сгенерированные последовательности неотличимы от истинно случайных по конкретным тестам NIST. Широкий спектр тестов в этом наборе, а также понятные принципы работы продемонстрированного КГСЧ подтверждают, что сгенерированные случайные последовательности имеют высокое качество и могут использоваться в критически важных приложениях.

В заключение, мы экспериментально продемонстрировали квантовый генератор случайных чисел, основанный на измерении периодов между срабатываниями ОФД. Основная концепция продемонстрированного устройства — простота, надежность и возможность работы в режиме реального времени. Используемый детерминированный экстрактор случайности вместе с простой обработкой сырых данных обеспечивает адаптивное извлечение случайных битов, что гарантирует качество вывода независимо от фактической энтропии источника.

6.2. Релятивистский протокол квантового распределения ключей

Практические системы квантовой криптографии сильно отличаются от модельных экспериментов, предлагаемых теоретиками. В результате, ряд атак, включая атаку путём измерений с определенным исходом, потенциально может угрожать безопасности таких систем, особенно при высоком уровне потерь сигнала в канале связи. Чтобы качественно решить проблему, не прибегая к „заплаткам“ типа использования протоколов с состояниями-ловушками, предлагается принципиально-новый подход, основанный на принципе релятивистской причинности [A14, A16]. Реализованная система использует канал связи по открытому пространству и обладает простым и понятным доказательством секретности, основанным на базовых информационно-теоретических принципах квантовой механики.

6.2.1. Мотивация и начальные соображения

Базовым протоколом для практической реализации квантовой криптографии по сути всегда был протокол BB84 [155], чья красота и совершенство непосредственно связано с использованием для передачи информации идеальных одиночных фотонов. Такие носители информации также позволяют осуществить законченное доказательство секретности [180, 156, 181] этого протокола без дополнительных предположений о возможностях злоумышленника и сценариях атак. В то же время, в практических реализациях квантовой криптографии использование идеальных одиночных фотонов едва ли осуществимо в настоящее время: на практике, все перспективные протоколы используют ослабленные классические импульсы — слабые когерентные состояния (weak coherent pulses). Поскольку такие состояния формально являются бесконечномерными квантовыми системами, всегда существует ненулевая вероятность успеха при реализации злоумышленником измерения с определенным исходом в квантовом канале [182, 183, 184]. Следовательно, начиная с определенного уровня потерь, все традиционные протоколы на слабых когерентных состояниях неизбежно утрачивают безусловную секретность. Соответствующие границы хорошо известны для простых протоколов, таких как B92 [185] и BB84 на когерентных состояниях [184], но, насколько нам известно, еще не были найдены для таких популярных протоколов, как COW [186] и DPS [187], а, следовательно, их доказательства секретности, возможно еще недостаточно полны. Мы считаем, что для защиты от подобных „дыр“ в традиционных протоколах при больших уровнях потерь в канале связи, было бы уместно применять дополнительные меры защиты на уровне дизайна протокола, чтобы запретить злоумышленниками „прятать“ неудачные попытки измерений с определенным исходом в потерях канала связи.

Значительные усилия были ранее направлены на разработку защиты против намного более специфического типа атаки, а именно, атаки с разделением по числу фотонов (photon number splitting, PNS). В результате, были разработаны различные схемы с состояниями-ловушками (decoy states) [188, 189], которые, по-видимому, обеспечивают необходимую защиту с помощью

отслеживания дополнительных характеристик канала связи помимо простого наблюдения за уровнем потерь. Это реализуется путем использования различных амплитуд слабых когерентных импульсов, посылаемых в канал связи. Пример использования протокола с состояниями-ловушками подробно разобран в разделе 6.3 настоящей диссертации. В общем и целом, подход с состояниями-ловушками — это признание несостоятельности использования слабых когерентных состояний в протоколах типа BB84 и попытка заделать соответствующую брешь в протоколе набором дополнительных проверок. Более конструктивным решением проблемы может оказаться поиск новых протоколов, непосредственно сконструированных для работы со слабыми когерентными состояниями.

Известный, хотя и безосновательно дискредитированный в настоящее время, подобный протокол — это протокол B92 с яркими опорными импульсами. В этом протоколе наличие классического опорного импульса делает невозможным для Евы отправку вакуумного состояния если измерение с определенным исходом не дало состоятельного результата. Другая альтернатива, изначально предложенная в работе [190] для одиночных фотонов, а затем приведенная к практически-реализуемой форме в работе [A14], — это использование релятивистских ограничений в квантовой криптографии. Они позволяют заставить Еву принимать решения о ее дальнейших действиях *перед тем*, как она сможет получить результат измерения состояния в канале связи. Следовательно, между результатами измерения и её действиями не может существовать причинно-следственной связи, что, как можно показать, приводит к невозможности реализации успешных атак на протокол, несмотря на использования слабых когерентных состояний.

6.2.2. Релятивистский протокол квантовой криптографии

Протокол релятивистской квантовой криптографии схематично показан на Рисунке 6.6 в виде пространственно-временной диаграммы. Его ключевой элемент - это передача квантовых состояний со скоростью света в двух временны́х окнах, разделенным измеримым временны́м интервалом ΔT. При этом, сама механика генерации ключей практически идентична протоколу B92 [191]. 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 временно́м окне и сигнальное состояние $|e^{ib_A\varphi}\alpha\rangle$ во втором. 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.

В традиционном протоколе B92 стратегия подслушивания достаточно проста: существует определенная ненулевая вероятность успешного измерения с определенным исходом по различению состояний $|\alpha\rangle$ и $|e^{i\varphi}\alpha\rangle$. В случае успеха Ева перепосылает корректно определенное состояние.

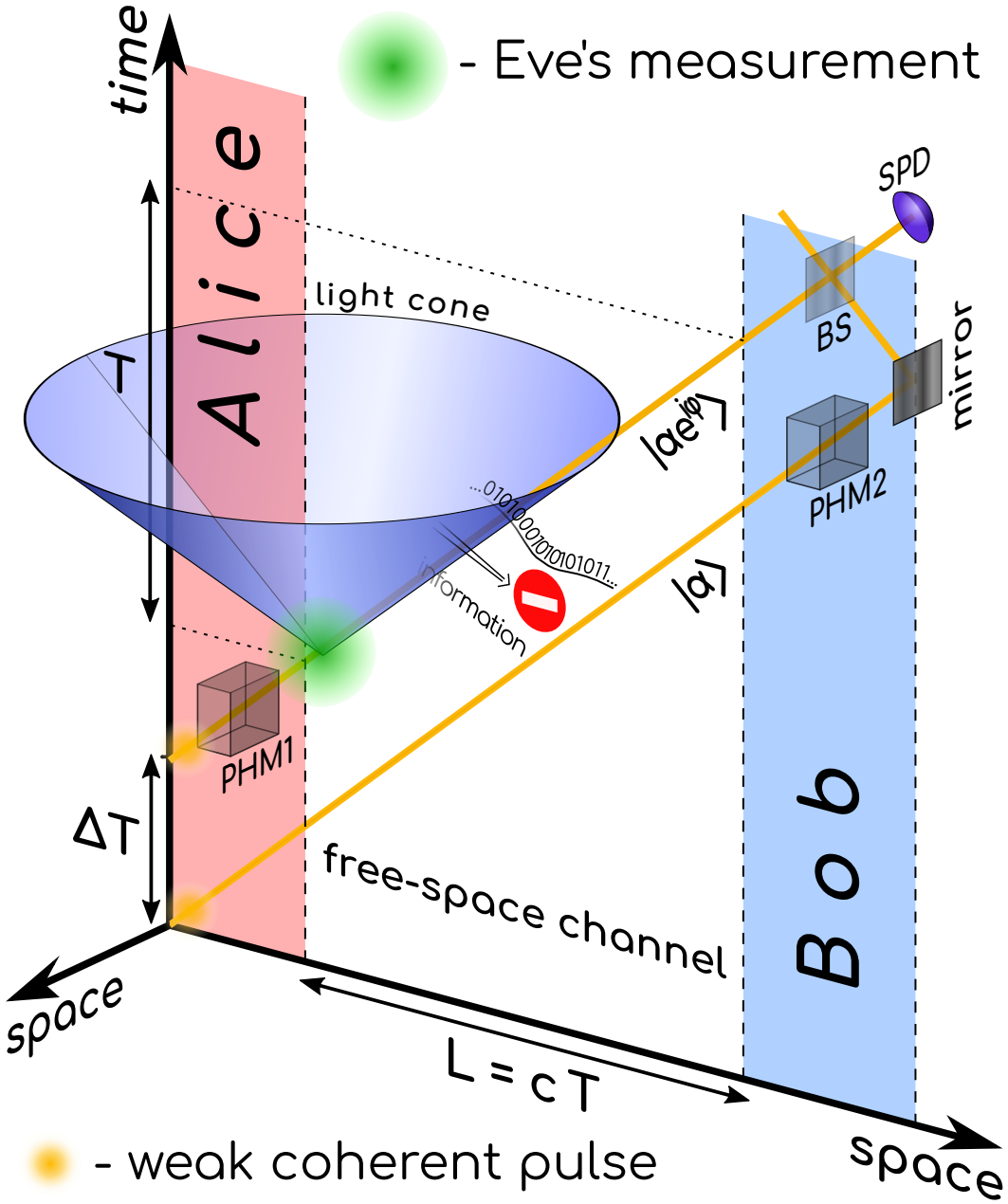

Рисунок 6.6: Пространственно-временная диаграмма релятивистского протокола квантового распределения ключей. Два импульса распространяются со скоростью света, тем самым исключая возможность злоумышленника воздействовать на первый импульс в зависимости от результата измерения второго, модулированного импульса. PHM – фазовый модулятор, BS – симметричный светоделитель, SPD – однофотонный детектор.

Если же измерение не завершилось успехом, Ева может блокировать оба импульса, что никак не будет отличаться для Алисы и Боба от обычных потерь в квантовом канале.

Напротив, в *релятивистском* протоколе первый импульс всегда находится снаружи светового конуса по отношению к расположению второго. Это исключает возможность причинно-следственной связи между вторым и первым импульсами. Другими словами, результат измерения информационного импульса никак не может повлиять на действия Евы по отношению к опорному импульсу.

Для обеспечения корректного пространственно-временного расположения импульсов, расстояние L между Алисой и Бобом должно быть известно априори, так как оно является важнейшим параметром для обеспечения безопасности протокола. Все сигналы, которые задерживаются в канале на время, большее чем L/c, где c – скорость света, должны быть проигнорированы. В таком модифицированном протоколе у Евы нет возможности заблокировать опорный сигнал в зависимости от результата измерения информационного. В противном случае, это нарушало бы принцип релятивистской причинности. В то же время, если один из двух импульсов в канале будет отсутствовать, результаты измерения Боба уже не будут коррелировать с состояниями, отправленными Алисой, что приведет к появлению ошибок в сыром ключе, т.е. будет непосредственно наблюдаемым. Действительно, если Ева пропускает опорный сигнал к Бобу, но *позднее* не может успешно измерить фазу информационного сигнала, она неизбежно вызывает ошибки в сыром ключе. И наоборот, если она блокирует опорный импульс, но перепосылает даже правильно измеренное информационное состояние, это точно так же вызывает ошибки в сыром ключе.

Полученная картина во многом схожа с версией протокола B92 с ярким опорным импульсом. В этом случае классический опорный импульс не может быть удален из канала, так как его пропажа непосредственно наблюдаема. Если же он присутствует, но не дополнен корректным квантовым информационным состоянием, он неминуемо вызывает ошибки на приемной стороне. Оба рассмотренных подхода обеспечивают реальную защиту против атак путем измерений с определенным исходом. Однако, мы считаем, что предлагаемый релятивистский протокол более прост в реализации и поэтому может быть более перспективным, чем оригинальная версия протокола B92.

Каждое срабатывание детектора дает Бобу один бит информации, так как он, фактически, реализует пост-селекцию, т.е. выбирает только те события, для которых его измерение успешно. Действия же Евы, напротив, не могут зависеть от результата измерения. В случае если это не так, Боб будет наблюдать некоррелированные с битами Алисы результаты измерения. В тот момент когда Ева получает результат измерения, т.е. не ранее, чем второе временное окно, уже слишком поздно для воздействия на содержимое первого временного окна, лежащее за световым конусом [192]. Таким образом, информация Евы для каждой посылки фундаментально ограничена классической „пропускной способностью“ такого бинарного квантового канала, задаваемую границей Холево [193, 194]. Разница между информацией Боба и фундаментально ограниченной информацией Евы дает возможность для распределения секретных ключей. В результате, получается, что передача квантовых состояний со скоростью света по прямому каналу известной дли-

ны совместно с точной синхронизацией станций и отслеживанием задержек дает принципиально новый компонент обеспечения секретности в квантовом распределении ключей, который обеспечивает защиту против измерений с определенным исходом, а также любых других атак типа прием-перепосыл.

Прежде чем мы перейдем к рассмотрению практических реализаций данного протокола, хочется привести ссылки на исследования, посвященные первому условно релятивистскому протоколу [190], т.е. тому, в котором в явном виде используется пространственно-временная картина всей коммуникации. В дискуссии [195, 196] обсуждалось название оригинальной статьи, в котором его авторы используют выражение протокол на „ортогональных состояниях“. В целом это не совсем соответствует действительности, что и подчеркивается в комментарии. Следующие работы развивают идеи подобного протокола и предлагают соответствующие экспериментальные реализации [197, 198, 199].

Другой, независимой ветвью [200, 201, 202, 203] проходили теоретические исследования практически-значимого релятивистского протокола, который экспериментально продемонстрирован в настоящей диссертации.

6.2.3. Двухпроходная реализация

Рассмотрим для начала более простой в реализации двухпроходный протокол релятивистской квантовой криптографии. Как подчеркивалось ранее, релятивистский подход требует точного учета моментов времени, в которые станции испускают и регистрируют квантовые состояния. Двухпроходный вариант предполагает, что оптические импульсы генерируются Бобом, отправляются к станции Алисы в виде классических импульсов, а после того, как Алиса их регистрирует, ослабляются в ее станции до однофотонного уровня, модулируются и отправляются обратно к Бобу. Следовательно, большое внимание должно быть уделено вопросу синхронизации станций, так как если Ева сможет ее нарушить, система перестанет обеспечивать защищенность генерируемых ключей.

Синхронизация реализована следующим образом. Боб испускает исходные импульсы апериодически: в каждом тактовом цикле он случайным образом выбирает одно из двух временны́х окон для отправки исходного импульса, как показано на Рисунке 6.7. Этот дополнительный бит информации не может достичь Алисы ранее, чем это происходит при обычной работе системы, так как импульсы распространяются от Боба к Алисе по прямой со скоростью света. Любые попытки Евы заранее отправить Алисе свои фейковые импульсы неминуемо приведут к отличающейся временно́й последовательности, в противном случае это означало бы передачу этой последовательности со сверхсветовой скоростью. В соответствии с протоколом, после каждой серии посылок Алиса и Боб сверяют свои полученные временны́е последовательности, измеренные несинхронизированными, но точными в относительных измерениях часами. Если они обнаруживают несоответствия этих двух последовательностей, вся серия отбрасывается.

Реализованная экспериментальная установка показана на Рисунке 6.8. Это оптоволоконная

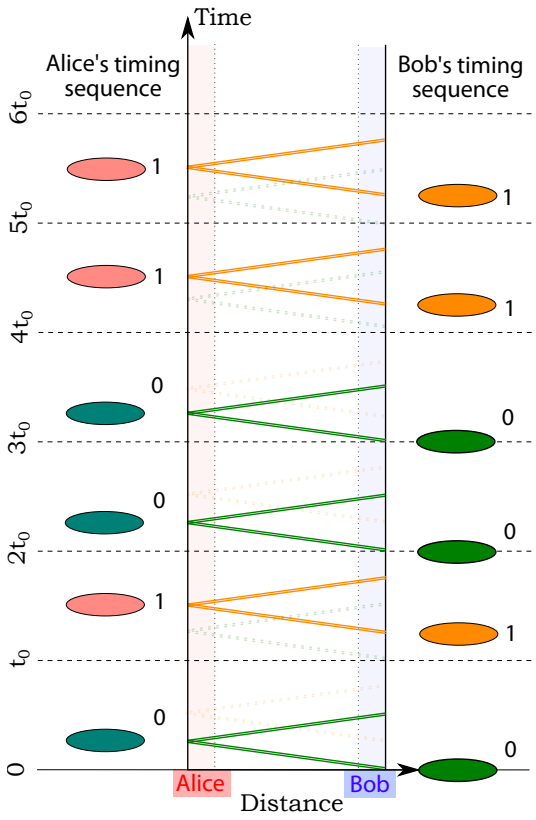

Рисунок 6.7: Пространственно-временная диаграмма серии посылок, реализующая синхронизацию часов между Алисой и Бобом. Инициируя каждую посылку, Боб случайным образом выбирает, отправлять ли импульс в начале такта длительностью t_0 или передавать его с дополнительной задержкой. Это создает уникальную временну́ю последовательность, формируемую Бобом. Алиса сравнивает измеренную ей временную последовательность с последовательностью Боба и если они отличаются, Алиса и Боб исключают из рассмотрения всю серию посылок. Фактически, если временна́я последовательность Боба достигает Алисы с максимально возможной скоростью — скорость света, — попытки Евы заранее спровоцировать Алису на отправку квантовой посылки неизбежно терпят поражение, так как для сохранения временно́й последовательности ей требуется передача этой информации быстрее скорости света.

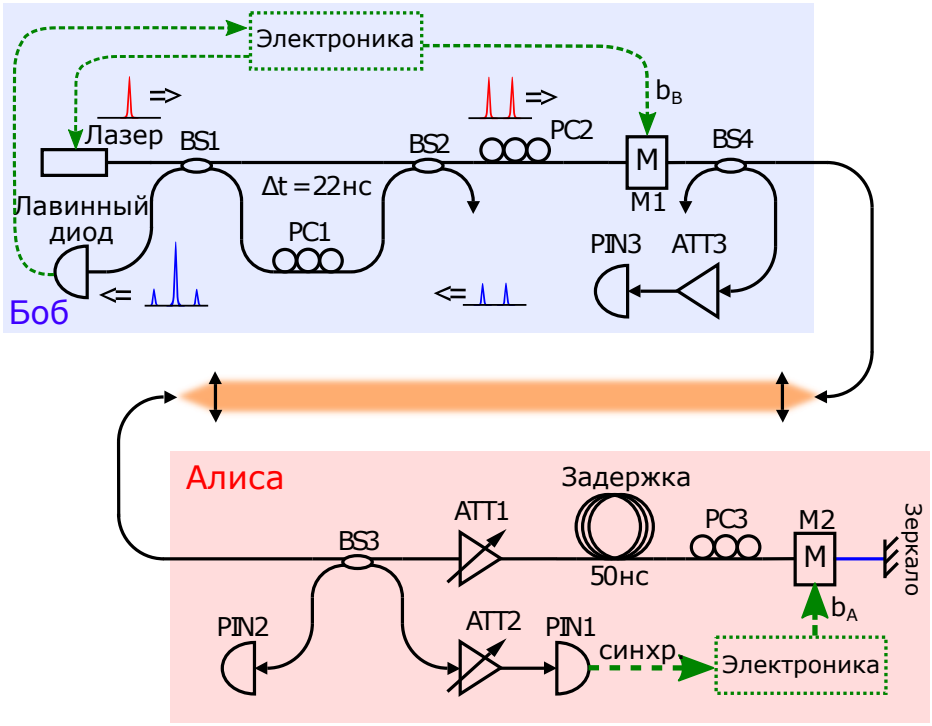

Рисунок 6.8: Экспериментальная установка для двухпроходного протокола релятивистской квантовой криптографии. BS – светоделитель, PC – контроллер поляризации, M – фазовый модулятор, PIN – PIN фотодиод, ATT - аттенюатор. Установка состоит из двух волоконно-оптических модулей, Алисы и Боба, и канала связи по открытому пространству между ними. Фазово-временное кодирование и декодирование осуществляется в одном и том же волоконном интерферометре задержки, расположенном на стороне Боба. Регистрация фотонов однофотонным детектором происходит в центральном временно́м окне, соответствующем интерференции между двумя половинами переданного импульса.

система, работающая на длине волны 850 нм. Для генерации оптических импульсов используется лазерный диод типа Фабри-Перо с прямой токовой модуляцией (QPhotonics QFLD-850-75S), который излучает импульсы длительностью 4 нс. Интерферометр задержки изготовлен из одномодового волоконного световода типа HP780 и содержит контроллер поляризации (General Photonics PCD-M02-4X-NC-4) в одном из плечей. Для дальнейшей обработки сигнала используется электрооптический фазовый модулятор на базе ниобата лития (Photline NIR-MPX800-LN-05) и механически перестраиваемый аттенюатор (OZ Optics FORF-11P-850-5 / 125-P). Канал связи по открытому пространству состоит из пары коллиматоров Micro Laser Systems, Inc. FC20-NIR-T 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 (OZ Optics FORF-11P-850-5 / 125-P).

Все генераторы случайных чисел в системе (два случайных бита используются для управления фазовыми модуляторами, а третий необходим для формирования временно́й последовательности синхронизации) эмулируются парой псевдослучайных генераторов на базе регистра сдвига с линейной обратной связью и длиной последовательности $2^{20} - 1$, работающих синхронно с обеих сторон канала. В результате, в этой конкретной схеме не требуется классический канал связи, так как каждая из станций знает значения „случайных“ битов, используемых другой станцией. Регистрация одиночных фотонов осуществляется с помощью термоэлектрически охлаждаемого лавинного фотодиода (Excelitas C30902SH) со схемой активного гашения лавины. Его квантовая эффективность составляет 30%.

В целом, вся система состоит из двух модулей — модуля Алисы и модуля Боба — и пары штативов с установленными на них коллиматорами, см. Рисунок 6.9b,c. Вся оптическая схема внутри модулей реализована в виде набора оптоволоконных компонентов и не содержит традиционной оптики. Каждый модуль подключается к коллиматору одномодовым световодом, а также может подключаться к компьютеру через интерфейс USB.

Вся электроника, управляющая генерацией, обработкой и регистрацией оптических сигналов, упакована в те же блоки вместе с оптическими компонентами, как показано на Рисунке 6.10. Скоростные электронные алгоритмы выполняются в ПЛИС, которая является ядром каждого из блоков. Вспомогательные функции, такие как подключение к компьютеру, управление дисплеем, и т.д. выполняются микроконтроллером.

Остановимся отдельно на конфигурации одномодового канала связи по открытому пространству. В отличие от одной из предыдущих глав мы не учитываем турбулентные явления атмосферы, а лишь рассматриваем геометрию такого канала. Идеальный одномодовый канал по открытому пространству описывается параксиальным волновым уравнением с решением в виде гауссова пучка. Дифракция луча ограничивает максимальную длину линии, которая зависит от диаметра

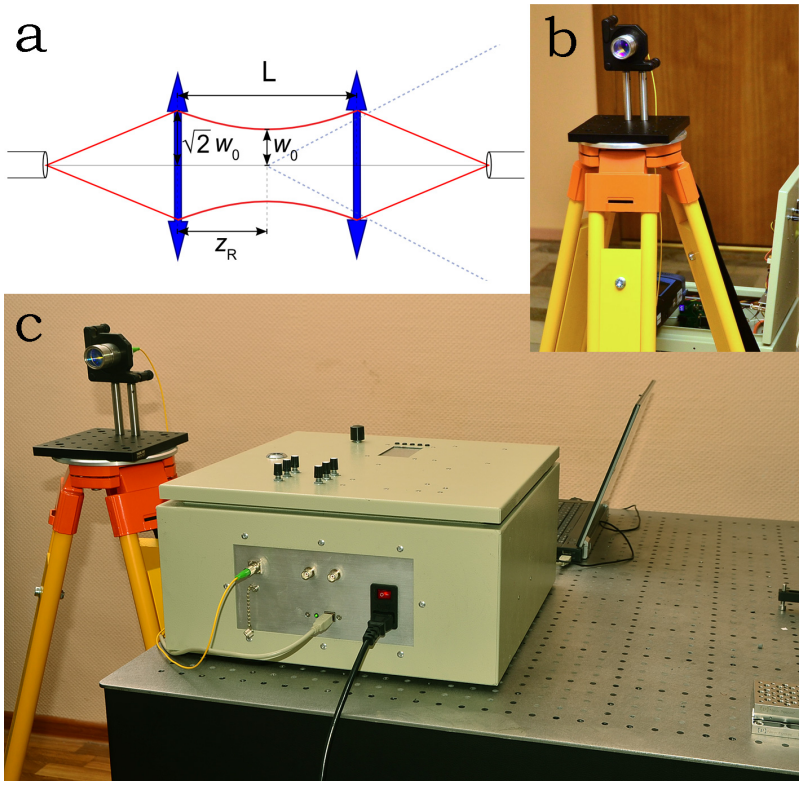

Рисунок 6.9: Экспериментальная реализация двухпроходной схемы релятивистской квантовой криптографии. **a,** Оптимальная конфигурация канала по открытому пространству, в которой достигается максимальная дальность L; w_0 – перетяжка пучка, z_R – релеевская длина. На рисунке показаны два конца одномодовых световодов и две линзы, формирующие гауссов пучок. Горизонтальный масштаб для наглядности искажен. **b,** Станция 'Алиса' с коллиматором на треноге. **c,** Станция 'Боб', состоящая из коллиматора, модуля самой станции и ноутбука, необходимого для сбора и обработки данных.

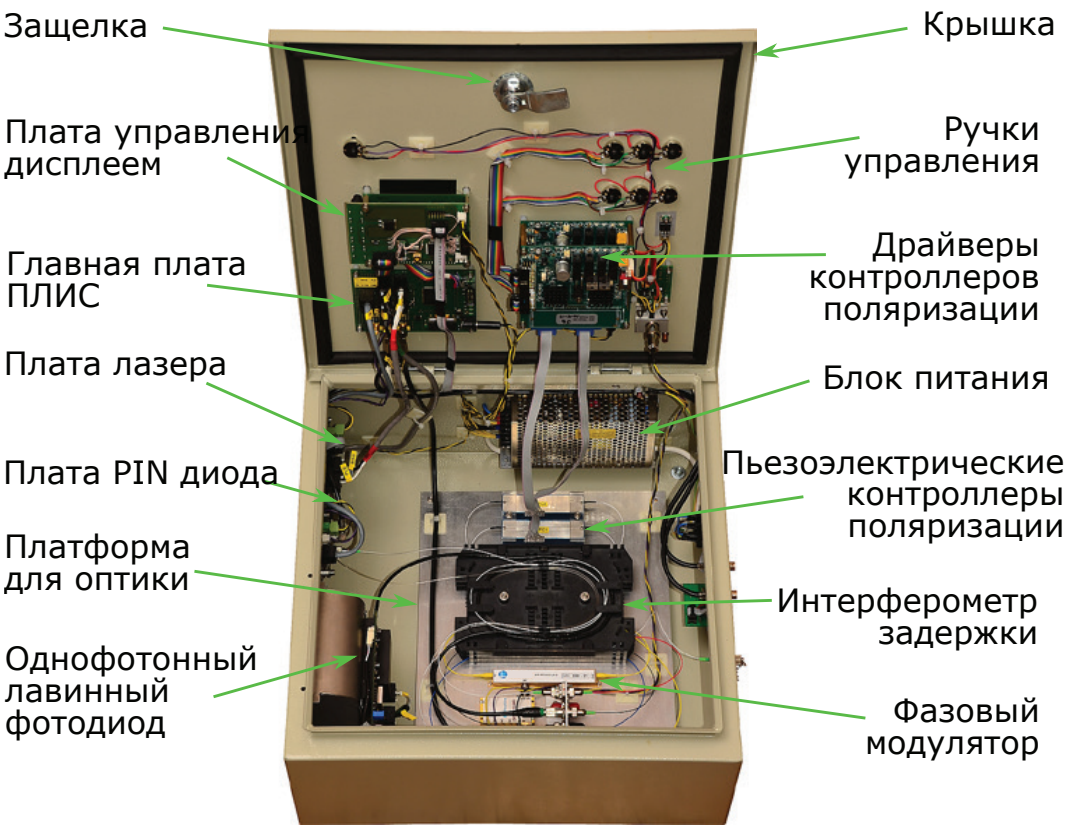

Рисунок 6.10: Аппаратная реализация станции Боба. Станция упакована в металлический ящик с крышкой, на которой расположены ручки управления, кнопки и небольшой ЖК-дисплей для визуализации основных параметров работы. Ящик подключается к компьютеру через USB-интерфейс для передачи полученных сырых ключей, а также для обмена управляющей информацией.

используемой оптики. В общем случае при симметричной конфигурации длина канала составляет

$$L = \frac{2\pi w^2}{\lambda}\frac{w_0}{w}\sqrt{1-\left(\frac{w_0}{w}\right)^2},$$

где w_0 — радиус перетяжки пучка, а w – радиус пучка на коллиматорах. Длина канала максимизируется при $w_0/w = 1/\sqrt{2}$, как показано на Рисунке 6.9а. В этой конфигурации

$$L = \frac{\pi w^2}{\lambda} = 2\frac{\pi w_0^2}{\lambda} = 2z_R,$$

где z_R — релеевская длина.

В эксперименте использованы коллиматоры с диаметром апертуры 23 мм, радиус w для них составляет 5.8 мм, что позволяет осуществлять передачу на расстояние до $L \approx 125$ м. Реальная длина канала в экспериментах составляла 55 м и ограничивалась длиной коридора, а не какими-то свойствами оптического тракта. Бóльшая дальность передачи может быть достигнута путем использования оптики с большими апертурами. Так как потери в длинных каналах связи по открытому пространству сильно изменяются во времени, скорость генерации ключей с такими каналами также может сильно изменяться. Однако, благодаря отсутствию связи между потерями в линии и защищенностью системы от взлома, работа *релятивистского* протокола в этих условиях также более чем возможна.

Рассмотрим теперь вопрос о скорости генерации секретного ключа. Приведем краткий асимптотический анализ производительности протокола. Более совершенный анализ с конечными последовательностями представлен в работе [192]. Скорость генерации секретного ключа ограничена выражением

$$R = \lim_{n\to\infty}\frac{l_{secr}}{n} \le (1-\eta)(1-C(\varphi)) - \eta - h(p_e),$$

где η — доля ошибок в принимаемой временно́й последовательности синхронизации (во всех предыдущих рассуждениях предполагалась равной нулю), $h(x)$ — бинарная энтропийная функция, p_e — вероятность битовых ошибок, а $C(\varphi)$ — граница Холево [194] для классической пропускной способности бинарного квантового канала с состояниями $|\alpha\rangle$ и $|e^{i\varphi}\alpha\rangle$; $C(\varphi) = h\left(\frac{1-\varepsilon}{2}\right)$, где $\varepsilon = |\langle\alpha|e^{i\varphi}\alpha\rangle| = \exp\left(-2\mu\sin^2(\varphi/2)\right)$.

Обычно в эксперименте (когда нет активного подслушивания) ошибок в полученных временны́х последовательностях нет, поэтому мы выбрали простую стратегию отбрасывания всех пакетов с ошибками синхронизации. В этом случае $\eta = 0$, и приведенное выше выражение упрощается до $R \le 1 - C(\varphi) - h(p_e)$, которое имеет простую интуитивную интерпретацию: если мы предположим, что вся классическая информация, которая может быть получена из квантового канала известна Еве, из каждого сырого бита ключа мы должны вычесть информацию Евы $C(\varphi)$ и энтропию, связанную с необходимостью исправлять битовые ошибки в сырой последовательности $h(p_e)$.

Также можно видеть некоторую неоднозначность в выборе μ и φ для достижения конкретного значения $C(\varphi)$. С практической точки зрения удобно выбирать значение φ близкое к π для минимизации эффекта от экспериментальных ошибок. В представленной реализации $C(\varphi) =$

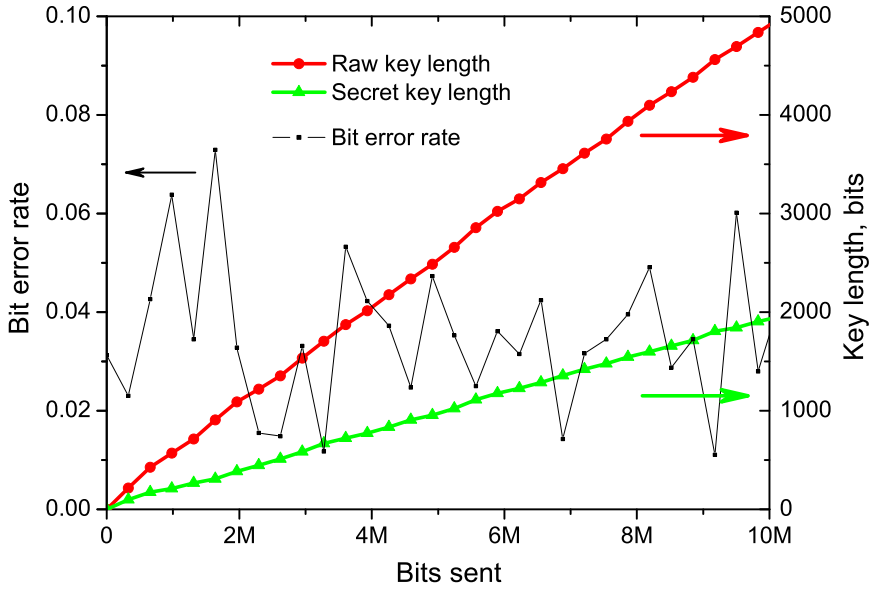

Рисунок 6.11: Экспериментально измеренная доля битовых ошибок и полученные размеры ключей. Во время измерений на 55-метровом канале связи Алиса регистрировала наблюдаемую временную последовательность и сравнивала ее с той, которая использовалась Бобом. Ошибок в синхронизирующей последовательности обнаружено не было. Среднее число фотонов в модулированном импульсе поддерживалось на уровне $\mu = 0.1$, а глубина фазовой модуляции составляла $130°$. Регистрация приходящих фотонов выполнялась Бобом во временном окне размером 4 нс, что в 5.5 раза меньше, чем расстояние между импульсами $\Delta t = 22$ нс. Это удовлетворяет требованиям релятивистского протокола.

0.387 бит, а скорость генерации ключей зависит от наблюдаемой доли ошибок p_e. Важно отметить, что если скорость генерации R становится нулевой или даже отрицательной, как в случае большого μ и ненулевого значения p_e, секретная информация между Алисой и Бобом не может возникнуть, то есть весь полученный сырой ключ должен быть отброшен.

В результате экспериментов была продемонстрирована работа системы через канал связи по открытому пространству длиной 55 метров. При этом использовалась тактовая частота посылок 250 кГц и среднее число фотонов в импульсе $\mu = 0.1$. В серии из 32768 посылок в среднем получалось 16.1 бит сырого ключа с долей ошибок 3.5%, как показано на Рисунке 6.11. Это соответствует средней скорости генерации сырого ключа в 123 бит/с, и асимптотической скорости генерации секретного ключа 47 бит/с.

6.2.4. Однопроходная реализация

Более эффективная экспериментальная реализация может быть выполнена на базе однопроходной схемы. 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 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 квантовые 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 является 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 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 стабильный на протяжении нескольких часов работы. Стабильность канала на бóльших промежутках времени не проверялась. Более подробная информация об одномодовом квантовом канале связи и системе слежения представлена в конце настоящего раздела. Там также обсуждается разница между групповой скоростью оптических импульсов в воздухе и скоростью света, которая оказывается несущественной для реализованных параметров протокола.

Другой экспериментальной задачей, решенной в однопроходной схеме, является правильная подстройка интерферометра задержки на приемной стороне. Чтобы упростить установку, мы полностью отказались от интерферометра задержки на передающей стороне и использовали вместо него непрерывный лазер. Таким образом, сторона Алисы содержит только узкополосный непрерывный лазер (диодный лазер с внешним резонатором), фазовый модулятор и аттенюатор, как показано на Рисунке 6.12. На приемной стороне расположен интерферометр задержки на базе световода, сохраняющего поляризацию. Фазовый модулятор, расположенный в одном из его плеч, одновременно служит как для подстройки интерферометра (квазипостоянное смещение) так и для модуляции квантовых состояний при квантовом распределении ключей (импульсная модуляция). Напряжение смещения постоянно корректируется по количеству одиночных отсчетов детектора фотонов при смещении относительной фазы в интерферометре на $\pi/2$ ниже и выше нормального уровня, соответствующего полностью деструктивной интерференции. Полный цикл работы модулятора показан на Рисунке 6.13. Подробнее об юстировке интерферометра сказано в конце настоящего раздела.

Основные параметры работы установки следующие. Каждый переданный квантовый символ представляет собой отрезок непрерывного лазерного излучения длиной 10 нс на длине волны λ = 780 нм с выходной интенсивностью -92.9 …-78.9 дБм, что соответствует 0.02 …0.5 фотонов на импульс. Задержка ΔT в приемном интерферометре составляет 20 нс, поэтому каждый переданный символ интерферирует в нем с соответствующим фрагментом излучения, идущего впереди на ΔT (окно опорной фазы). Глубина фазовой модуляции составляет 0.8π. Символы с фазовой модуляцией идут в пакетах по 65536 бит в каждом со средней скоростью 25 МГц. Пакет может быть отправлен в любом цикле фазового модулятора, который длится 16 мс (см. Рисунок 6.13). Однако фактическая скорость передачи пакетов была ограничена временем, необходимым для обмена буферами случайных данных и результатами измерений с компьютером через интерфейс USB, поэтому фактическая скорость была около 2 пакетов/сек.

Вся система состоит из двух одинаковых станций, каждая из которых содержит блок с электроникой и оптоволоконные элементы, а также систему активного трекинга для канала связи по открытому пространству, размещенную на штативе, как показано на Рисунке 6.14. В одномодовом квантовом канале по открытому пространству используются дифракционно-ограниченные асферические линзы диаметром 1 дюйм для коллимации излучения в и из одномодовых волокон, сохраняющих поляризацию. Квантовые сигналы смешиваются с излучением маяка с длиной волны 850 нм, который используется системой трекинга. Излучение маяка регистрируется квадрантным фотодиодом, который является датчиком угловой ошибки в системе обратной связи. Управляющим элементом в ней является пьезоуправляемое качающееся зеркало. Квадрантный фотодиод

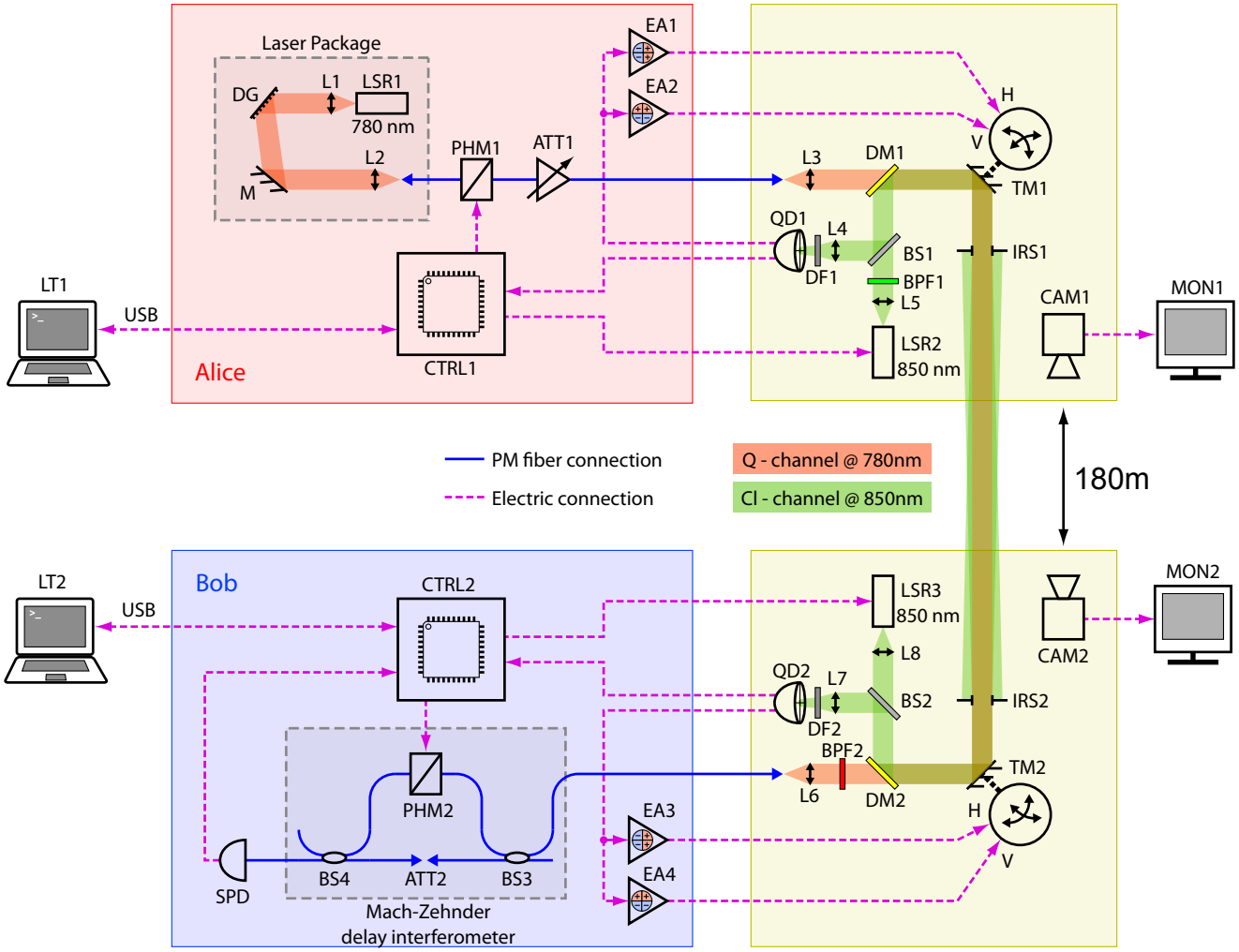

Рисунок 6.12: Схема экспериментальной установки. LT – абонентский терминал на базе ноутбука; DG – дифракционная решетка в схеме Литтроу; L – линза; M – зеркало; PHM – электрооптический фазовый модулятор с оптоволоконными выходами с частотной полосой 150 МГц; ATT – переменный оптический аттенюатор; CTRL – 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.

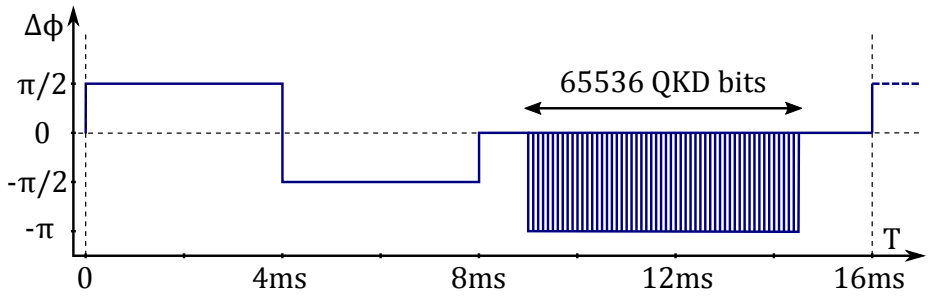

Рисунок 6.13: Работа фазового модулятора в приемном интерферометре задержки. В каждом цикле из 16 мс, он сначала измеряет частоту отсчетов в двух квадратурных точках для подстройки смещения, а затем отрабатывает последовательность для квантового распределения ключей.

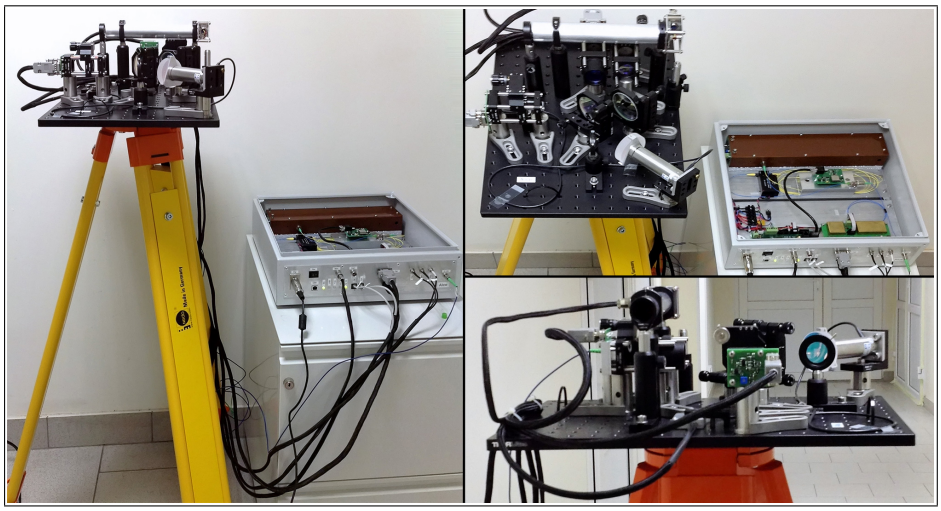

Рисунок 6.14: Станция Алисы: тренога с системой активного трекинга и блок с электроникой и волоконно-оптическими компонентами.

также является приемником классического канала связи 25 Мбит/с, в котором используется манчестерская кодировка. Этот канал используется для безопасной синхронизации станций, а также для передачи вспомогательной информации между ними. Была продемонстрирована работа системы при длине канала 180 м, который был фактически ограничен длиной здания. Сама система была спроектирована для работы на расстояниях до 400 м.

Система работает в двух режимах: с псевдослучайными битовыми последовательностями (ПСП) и с реальными случайными битами. Первый используется для тестирования, поскольку он обеспечивает простой способ вычисления доли квантовых битовых ошибок (QBER) без использования классического канала (станциям известны псевдослучайные последовательности, используемые на другом конце линии). Второй режим работает с реальными случайными битами из квантового генератора случайных чисел (КГСЧ), см. раздел 6.1, хранящимися на ноутбуках. На рисунке 6.15 показана скорость генерации ключа и QBER для режима работы с ПСП для разных средних чисел фотонов в импульсе.

Для оценки асимптотической скорости генерации секретного ключа мы используем подход, основанный на взаимной информации. Сырой ключ, полученный Бобом, должен быть сокращен,

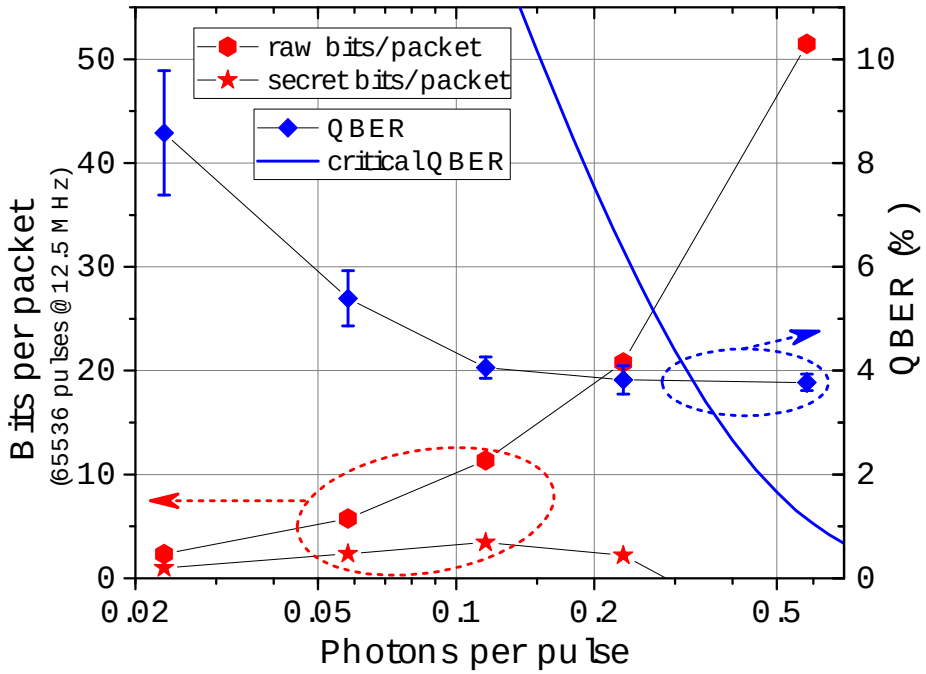

Рисунок 6.15: Скорость генерации сырого ключа и QBER, измеренные в режиме работы с ПСП, в зависимости от среднего числа фотонов в импульсе. На рисунке также показано рассчитанное количество секретных битов в асимптотическом пределе на один переданный пакет данных, а также критический QBER, выше которого секретные биты не могут быть извлечены. Ошибки на графике QBER являются чисто статистическими неопределенностями, соответствующими оценкам QBER на конечном числе полученных битов. Более точно, они отображают 95%-ный доверительный интервал для всех битов сырого ключа, накопленных в конкретной конфигурации системы.

чтобы исключить информацию Евы, или, точнее, информацию, которая потенциально могла стать доступной Еве. Поскольку сырой ключ всегда содержит битовые ошибки, часть необработанного ключа также должна быть использована для исправления ошибок. Как обсуждалось ранее, реализованная релятивистская схема запрещает Еве воздействовать на принимаемые квантовые состояния таким образом, что ее действия зависят от результатов ее измерений. Без этой возможности пост-селекции Ева не может решать, какие импульсы пройдут к Бобу и произведут отсчеты детектора, а какие она заблокирует, фактически увеличив тем самым потери в канале. В лучшем случае она может получить среднюю доступную информацию за импульс. Фактически, информация Евы ограничена величиной Холево [193, 194]:

$$\chi(\mu,\varphi) = h\left(\frac{1-\exp(-2\mu\sin^2(\varphi/2)}{2}\right), \tag{6.1}$$

где $h(p) = -p\log(p) - (1-p)\log(1-p)$; $\varphi = 0.8\pi$ – глубина модуляции, а μ - среднее количество фотонов в импульсе. Идеальная асимптотическая коррекция ошибок требует $h(\mathrm{QBER})$ бит, поэтому общая асимптотическая скорость генерации секретного ключа равна $\mathbf{R} = 1 - \chi(\mu,\varphi) - h(\mathrm{QBER})$. Следует отметить, что здесь мы не принимаем во внимание какие-либо эффекты конечного размера последовательностей, поскольку они качественно не меняют результаты. Некоторые разработки для последовательностей конечного размера опубликованы в работе [202].

При малых μ информация Евы незначительна, но реальная длина секретного ключа сильно ограничена высоким значением QBER. При больших μ QBER уменьшается, однако в этом случае ограничивающим фактором становится информация Евы. Максимальная эффективность наблюдается при $\mu = 0.1$, как следует из Рисунка 6.15.

Для демонстрации реального распределения сырых ключей использовались предварительно сохраненные данные из КГСЧ. 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 6.16 показаны экспериментально измеренные данные — длина сырого ключа и QBER, — 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 $\mu = 0.116$, где скорость генерации сырого ключа (внутри пакета) равна 2170 бит/сек, а асимптотическая скорость секретного ключа оценивается как 660 бит/сек. Как упоминалось ранее, средние скорости существенно ниже из-за медленного обмена данными с ноутбуками: 20 и 6,2 бит/с соответственно.

Еще один момент, о котором следует упомянуть, — это функционирование самого одномодового канала связи в открытом пространстве. Хотя эксперимент проводился внутри здания, наличие воздушных потоков от систем отопления и вентиляции приводили к значительным искажениям оптического пучка. Типичная частота блуждания пучка была не выше 10 Гц, поэтому система активного трекинга с полосой пропускания в 10 Гц существенно помогла снизить потери. Тем не

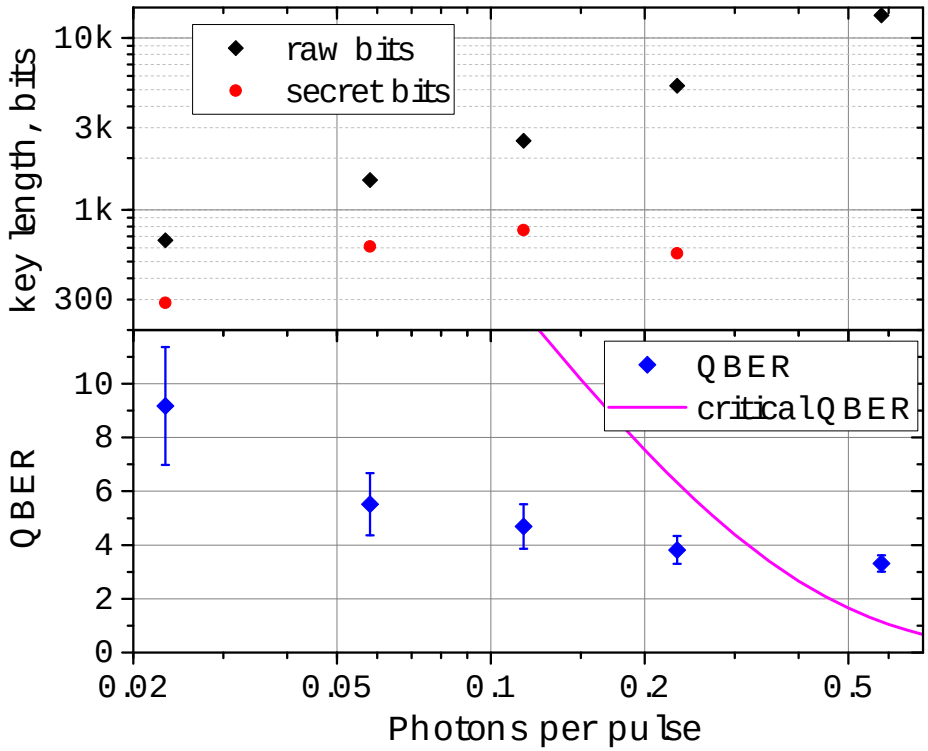

Рисунок 6.16: Длины полученных ключей и QBER в зависимости от среднего числа фотонов для квантового распределения ключей со случайными данными из КГСЧ. Каждая точка является результатом распределения ключей с входным буфером размером 16 Мбит, т.е. для 256 переданных пакетов. Величина ошибок на графике QBER показывает 95%-ный доверительный интервал биномиальной пропорции для конкретного сырого ключа, полученного в соответствующей точке.

менее, реализованная система активного трекинга может компенсировать только сдвиг луча как целого, но не искажение профиля моды. Измеренные потери в квантовом канале по открытому пространству (отношение между передаваемой мощностью и мощностью, заведенной в приемный волоконный световод) составляют около 13 дБ. При этом общая эффективность системы, то есть отношение числа зарегистрированных фотонов к числу отправленных, составляла 1.5×10^{-3}.

6.2.5. Обсуждение результатов

Представленная концепция *релятивистской* квантовой криптографии или квантового распределения ключей, основанного на принципах релятивистской причинности, открывает новые возможности для традиционной квантовой криптографии. Его главное преимущество - полная независимость между потерями в квантовом канале связи и уровнем безопасности получаемых ключей. Для гарантии теоретико-информационной безопасности не требуется никаких дополнительных проверок (по крайней мере, теоретически), кроме стандартного усиления секретности и коррекции ошибок в сырых ключах. В этом смысле предложенный протокол имеет много общего с оригинальным протоколом B92, в котором используются яркие опорные импульсы. В то же время, релятивистский протокол оказывается менее требовательным в технической реализации, поскольку оригинальный B92 требует чрезвычайно высокого коэффициента контрастности между сигналом и опорным импульсом. Краткая оценка показывает, что при типичной эффективности системы 10^{-3} и среднем количестве фотонов в сигнале $0,1$ опорные импульсы должны содержать по крайней мере 10^4 фотонов за импульс, чтобы их мог надежно детектировать приемник. Таким образом, они должны быть в 10^5 раз более яркими, чем сигнальные импульсы. С экспериментальной точки зрения поддерживать стабильную интерференцию между ними очень сложно, поскольку большинство оптических элементов, таких как светоделители, имеют типичный контраст не более 10^3 из-за паразитных отражений и рассеяния. Вероятно, это основная причина, по которой, насколько нам известно, экспериментальной демонстрации оригинального протокола B92 пока нет. Относительная простота представленного протокола, однако, дается в обмен на дополнительные требования к каналу, а именно, требуется априорное знание длины квантового канала связи.

Длина канала или, точнее, *расстояние* между Алисой и Бобом играет важную роль в гарантии защищенности релятивистского протокола. Это важный параметр безопасности, который должен быть известен заранее, чтобы гарантировать безопасность протокола. Формально, нельзя доверять безопасности сгенерированных ключей на более высоком уровне доверия, чем уверенность в фактическом расстоянии между абонентами. Однако, это требование можно облегчить, установив жесткое ограничение только на нижнюю границу длины канала.

Фактически, увеличивая задержку ΔT между двумя импульсами, можно разрешить большее расхождение между фактическим временем пролета и L/c. Более подробно этот предмет обсуждается в конце раздела, но вкратце для обеспечения безопасности необходимо лишь убедиться, что второй импульс не может догнать первый, даже если второй проходит по прямой линии между Алисой и Бобом со скоростью света. Таким образом, минимальная требуемая задержка между

импульсами равна $\Delta T_{\min} = 2(T_o - L_{\min}/c)$,, где T_o — *наблюдаемое* время пролета, $L_{\min}$ — нижняя граница достоверности для значения L, и коэффициент 2 включен, потому что в этой конкретной реализации процесс синхронизации полагается на тот же канал, что и для квантовых сигналов и, следовательно, может быть скомпенсирован на ту же самую величину. В принципе, это значение можно сократить вдвое, если использовать какую-либо внешнюю схему доверенной синхронизации.

Поскольку L всегда положительно, выбор $\Delta T > 2T_o$ в любом случае гарантирует безопасность, однако может оказаться очень непрактичным для экспериментальной реализации. Чтобы обеспечить приемлемую на эксперименте конфигурацию, лучше требовать $\Delta T \ll T_o$. Это возможно, например, для распределения ключей на большое расстояние по открытому пространству на движущийся объект, локализованный в ограниченной по размеру и относительно небольшой области, например, внутри города. Другой потенциально возможной стратегией является использование фотонно-кристаллических световодов с полой сердцевиной, где эффективный показатель преломления составляет всего 1,003, а оптические потери, как ожидается, будут ниже, чем у обычных телекоммуникационных световодов [204]. Будущая инфраструктура с использованием таких полых световодов может стать естественной основой для реализации релятивистской сети квантового распределения ключей, поскольку разница между скоростью распространения импульсов в таких волокнах и скоростью света минимальна.

Еще одна практическая возможность — использовать одно и то же оборудование для фазового кодирования либо в обычном (когда нет достоверной информации о расстоянии между абонентами), либо в релятивистском режиме. Это может быть хорошим компромиссом для достижения наилучшего сценария безопасности в зависимости от конкретных обстоятельств.

В заключение, была продемонстрирована система *релятивистской* квантовой криптографии, которая, в отличие от традиционных протоколов, обеспечивает внутреннюю устойчивость к атакам, основанным на измерениях с определенным исходом, при произвольно больших потерях в канале и при использовании слабых когерентных состояний в качестве носителей информации. Представленная экспериментальная установка работает через однонаправленный одномодовый квантовый канал связи с активной системой слежения длиной 180 м по открытому пространству. Благодаря своей простой структуре и понятным основам безопасности, этот протокол может стать первым практически-значимым протоколом квантового распределения ключей с простым и таким же общим доказательством секретности, как и оригинальный протокол BB84. Преимущества предложенного протокола наилучшим образом могут проявиться в городских атмосферных каналах связи в зоне прямой видимости с протяженностью до нескольких километров или в будущих сетях на основе световодов с полой сердцевиной. В таких каналах связи высокие требования к обеспечиваемой безопасности сочетаются с простотой экспериментальной реализации представленного протокола квантового распределения ключей.

6.2.6. Подробности экспериментальной реализации

В качестве источника сигнала для квантового канала используется пространственно-одномодовый лазерный диод мощностью 90 мВт с длиной волны 780 нм, работающий в непрерывном режиме. Для стабилизации его длины волны используется внешний резонатор на основе дифракционной решетки 1800 штрихов на мм в конфигурации Литтроу. Модуляция сигнала производится электрооптическим фазовым модулятором на основе ниобата лития в оптоволоконном исполнении с поляризационно-сохраняющими световодами на входе и выходе. Используется низкочастотная версия модулятора (до 100 МГц), которая отличается от высокочастотных модуляторов бегущей волны отсутствием электрического волновода и согласующего сопротивления 50 Ом. Такой тип модулятора выбран из-за того, что он может одновременно использоваться как для подстройки интерферометра так и для фазовой модуляции квантового канала благодаря устойчивости к большим напряжениям смещения. Используемый детектор одиночных фотонов основан на кремниевом лавинном фотодиоде, работающем в режиме счета фотонов. Используется готовая сборка с внутренним термоэлектрическим охладителем. Квантовая эффективность детектора на рабочей длине волны составляет 35%, а частота темновых отсчетов составляет около 700 Гц. В системе слежения используются пьезоэлектрические наклоняемые платформы PI S-330.80L с зеркалами диаметром 50.8 мм. Основная резонансная частота для этой конфигурации зеркала прицеливания составляет около 920 Гц. В качестве источника излучения маяков системы трекинга использован лазерный диод с длиной волны 850 нм мощностью 10 мВт. Для передачи информации осуществляется его прямая токовая модуляция. Излучение лазера коллимируется с помощью асферической линзы 0.5NA $F = 8$ мм. В датчике угла прихода лучей использованы квадрантные фотодиоды с активной площадью 3×3 мм^2, которые расположены в фокальной плоскости фокусирующей линзы $F = 80$ мм. Для сглаживания отклика системы обратной связи перед квадрантным диодом расположен диффузор из матового стекла с зернистостью 1500 grit. Переменная составляющая зарегистрированного сигнала суммируется по всем четырем квадрантам, корректируется по частоте, усиливается и преобразуется в поток двоичных данных - так реализуется классический канал связи. Квазипостоянная составляющая сигнала усиливается отдельно для всех квадрантов, а затем путем попарного вычитания соответствующих сигналов формируются вертикальный и горизонтальный каналы ошибок. Сигналы ошибки масштабируются относительно общей принятой мощности и вводятся в два контура ПИД-регулирования. Точная синхронизация между станциями выполняется системой ФАПЧ, которая синхронизируется с принятым цифровым сигналом классического канала. В канале данных используется манчестерское кодирование, которое обеспечивает необходимое для работы ФАПЧ количество переходов через ноль независимо от передаваемых данных.

6.3. Протокол на геометрически однородных квантовых состояниях

Очевидно, что релятивистский протокол квантовой криптографии может использоваться далеко не везде, например, с ним возникают большие трудности при передаче на движущиеся объекты, а также просто при передаче на большие расстояния, так как, по-видимому, его удобная реализация совместима только с пространственно-одномодовым приемом.

В связи с этим, хотелось бы разработать и традиционный вариант протокола квантового распределения ключей, который был бы более совершенным с точки зрения защищенности ключей, чем BB84 с состояниями-ловушками. Такой протокол предложен в этом разделе [A18, A20]. Несмотря на то, что все выкладки относятся к его реализации с фазовым кодированием, их практически без изменений можно переложить на поляризационную кодирование. Такой поляризационный вариант наиболее удобен в использовании с каналами связи по открытому пространству.

Поскольку анализ секретности этого протокола базируется на понятии оптимальной унитарной атаки, рассмотрим сначала ее более подробно, а потом обратимся к конструированию самого протокола и доказательству его секретности.

6.3.1. Унитарная атака на примере протокола BB84

Рассмотрим применение унитарной атаки для достижения точной границы скорости генерации секретного ключа. Впервые ее достижение было показано в [205] и позднее в [206].

Рассмотрим систему квантовой криптографии на базе однофотонного протокола BB84 [155]. Обозначим состояния, используемые в протоколе как $|0\rangle$, $|1\rangle$, $|+\rangle$, $|-\rangle$. При этом,

$$|\pm\rangle = \frac{|0\rangle \pm |1\rangle}{\sqrt{2}}. \tag{6.2}$$

Для реализации атаки Ева использует дополнительное квантовое состояние $|E\rangle$ произвольной размерности и использует запутывающий унитарный оператор U, приводящий систему в состояние $U(|a\rangle \otimes |E\rangle)$, где $|a\rangle$ — квантовое состояние, отправленное Алисой.

Как показано в [207], оптимальным видом такого оператора является

$$\begin{aligned} U(|0\rangle \otimes |E\rangle) &= \sqrt{1-Q}\,|0\rangle \otimes |\psi_0\rangle + \sqrt{Q}\,|1\rangle \otimes |\theta_0\rangle \\ U(|1\rangle \otimes |E\rangle) &= \sqrt{1-Q}\,|1\rangle \otimes |\psi_1\rangle + \sqrt{Q}\,|0\rangle \otimes |\theta_1\rangle\,, \end{aligned} \tag{6.3}$$

где Q - параметр, определяющий силу искажения исходных квантовых состояний. В силу желаемой симметрии этой атаки, рассмотренной в [207], данный параметр является общим для всех вариантов преобразования. Аналогично, для линейных комбинаций этих квантовых состояний имеем

$$\begin{aligned} U(|+\rangle \otimes |E\rangle) &= \sqrt{1-Q}\,|+\rangle \otimes |\psi_+\rangle + \sqrt{Q}\,|-\rangle \otimes |\theta_+\rangle \\ U(|-\rangle \otimes |E\rangle) &= \sqrt{1-Q}\,|-\rangle \otimes |\psi_-\rangle + \sqrt{Q}\,|+\rangle \otimes |\theta_-\rangle\,. \end{aligned} \tag{6.4}$$

Разумный выбор данного запутывающего оператора, состоит в ортогональности соответствующих выходных состояний, т.е.

$$\langle\psi_i|\theta_i\rangle = 0, \qquad i \in \{|0\rangle, |1\rangle, |+\rangle, |-\rangle\}. \tag{6.5}$$

Умножая (6.4) слева на $\langle+|$ и пользуясь разложением (6.2), а также (6.3), получаем следующие соотношения для квантовых состояний Евы

$$\begin{aligned} 2\sqrt{1-Q}\,|\psi_+\rangle &= \sqrt{1-Q}(|\psi_0\rangle + |\psi_1\rangle) + \sqrt{Q}(|\theta_0\rangle + |\theta_1\rangle) \\ 2\sqrt{Q}\,|\theta_+\rangle &= \sqrt{1-Q}(|\psi_0\rangle - |\psi_1\rangle) + \sqrt{Q}(|\theta_1\rangle - |\theta_0\rangle). \end{aligned} \tag{6.6}$$

Возводя любое из уравнений (6.6) скалярно в квадрат получаем следующую связь между скалярными произведениями состояний Евы и параметром Q

$$1 - Q = \frac{1 + \langle\theta_0|\theta_1\rangle}{2 + \langle\theta_0|\theta_1\rangle - \langle\psi_0|\psi_1\rangle}. \tag{6.7}$$

Как подробно обсуждается в [207], наиболее оптимальной является симметричная атака, в которой можно считать оба скалярных произведения равными между собой и являющимися действительными числами. Пусть тогда

$$c^{\mathrm{E}} = \langle\theta_0|\theta_1\rangle = \langle\psi_0|\psi_1\rangle, \tag{6.8}$$

что в результате дает простое соотношение между данной величиной и параметром Q

$$c^{\mathrm{E}}(Q) = 1 - 2Q. \tag{6.9}$$

Из (6.3) и (6.4) легко видеть, что параметр Q в то же время является вероятностью ошибки при измерении передаваемых битов на стороне Боба. Таким образом, соотношение (6.9) является связью между ошибками, индуцированными атакой, и эффективностью атаки. Чем меньше c^{E} тем более различимы соответствующие состояния Евы, т.е. она больше информации получает о ключе. С другой стороны, это неизбежно сопровождается большей долей ошибок, наблюдаемых легитимными пользователями.

Основная суть квантовой криптографии заключается в наличии этой связи: невозможно получить информацию о ключах не внося ошибок в канал легитимных пользователей. В данном случае, эта связь позволяет найти точную границу для скорости генерации секретного ключа при определенном наблюдаемом уровне ошибок.

Для нахождения предельной скорости генерации ключа требуется найти величину Холево [193, 194] $\chi(Q)$, которая ограничивает условную энтропию для информации Алисы при данной информации Евы

$$H(X|E) \geq 1 - \chi(Q). \tag{6.10}$$

По определению, величина Холево равняется

$$\chi(Q) = H\left(\frac{1}{4}\sum_x \rho_x^{\mathrm{E}}\right) - \frac{1}{4}\sum_x H\left(\rho_x^{\mathrm{E}}\right), \tag{6.11}$$

где $H(\rho) = -\mathrm{tr}(\rho \log \rho)$ — энтропия фон Неймана, а $x \in \{0, 1, +, -\}$. Соответствующие матрицы плотности Евы находятся из состояний (6.3) и (6.4) с последующим взятием частичного следа по подсистеме Алисы.

Общая матрица плотности в выражении (6.11) равняется

$$\frac{1}{4}\sum_x \rho_x^{\mathrm{E}} = \frac{1}{2}\begin{bmatrix} 1-Q & (1-Q)c^{\mathrm{E}}(Q) & 0 & 0 \\ (1-Q)c^{\mathrm{E}}(Q) & 1-Q & 0 & 0 \\ 0 & 0 & Q & Qc^{\mathrm{E}}(Q) \\ 0 & 0 & Qc^{\mathrm{E}}(Q) & Q \end{bmatrix}. \tag{6.12}$$

Ее собственные значения равны

$$\begin{aligned} \lambda_{1,2} &= (1-Q)\left(\frac{1 \pm c^{\mathrm{E}}(Q)}{2}\right) \\ \lambda_{3,4} &= Q\left(\frac{1 \pm c^{\mathrm{E}}(Q)}{2}\right). \end{aligned} \tag{6.13}$$

Частичные матрицы плотности в качестве собственных значений имеют величины Q и $1-Q$.

Используя найденные собственные значения, получаем

$$\chi(Q) = h\left(\frac{1-c^{\mathrm{E}}}{2}\right), \tag{6.14}$$

где $h(t) = -t\log(t) - (1-t)\log(1-t)$ — бинарная энтропийная функция.

Для нахождения предельной скорости генерации ключа также учтем, что эффективно между Алисой и Бобом реализуется бинарный симметричный канал с вероятностью ошибки Q. Следовательно, при использовании идеального алгоритма коррекции ошибок в асимптотическом пределе получаем $1 - h(Q)$ бит информации на каждый бит просеянного ключа. Т.е. величину по крайней мере $h(Q)$ необходимо потратить на коррекцию ошибок. В реальной ситуации, доступная условная энтропия $H(X|E)$ является изначально тем ресурсом, из которого необходимо сформировать секретные ключи (остальная информация становится доступной Еве). В результате, получаем окончательную величину асимптотической скорости генерации секретного ключа в пересчете на биты просеянного ключа

$$R = 1 - 2h(Q). \tag{6.15}$$

Полученное выражение является хорошо известной величиной [180, 156, 181]. Критическая доля ошибок, при которой скорость генерации ключа обращается в ноль равна $Q_c \approx 11\%$. Изначально она была найдена без привязки к конкретному методу атаки, с использованием энтропийных соотношений неопределенности для состояний BB84. Как видно из нашего примера, прямое построение унитарной атаки общего вида позволяет конструктивно дойти до фундаментальной границы, найденной независимо. Это еще раз независимо подтверждает плотность данной границы.

Скажем несколько слов о том, как была построена настоящая атака, чтобы понять не ограничиваем ли мы общность рассуждений при ее конструировании.

- Унитарность атаки не ограничивает ее общность, так как известно, что любые физически реализуемые неунитарные преобразования могут рассматриваться как унитарные для системы большей размерности [207].

- Данная атака является коллективной, т.е. каждое из квантовых состояний независимо взаимодействует с соответствующей дополнительной квантовой системой Евы. В дальнейшем, получив все состояния, запутанные с системой Алиса-Боб, Ева реализует их коллективное измерение, подразумеваемое для возможности достижения границы Холево. Очевидно, используя индивидуальные измерения, достижение этой границы Евой невозможно. Важный результат заключается в том, что наиболее общая когерентная атака, в которой предполагается доступ ко всем квантовым состояниям в канале одновременно, не имеет никаких преимуществ перед предлагаемой коллективной атакой [208]. В результате, такая конструкция атаки не ограничивает ее эффективность.

- Построенная атака является симметричной, т.е. она вносит одинаковые возмущения во все четыре квантовых состояния, использующиеся легитимными пользователями. Логично, что такая атака является более эффективной, чем любые „смещенные“ атаки. Данный вопрос подробно изучен в [207], где показано, что такая симметричная конструкция никак не ограничивает эффективность ее применения, а наоборот является наиболее сильной конструкцией для атаки на квантовый канал.

В результате, мы получили мощный инструмент для анализа секретности различных протоколов квантовой криптографии. Все приведенные рассуждения справедливы для однофотонных протоколов квантовой криптографии, где не существует других более эффективных вариантов атаки, таких как, например, разделения по числу фотонов, измерений с определенным исходом, вероятностное усиление различимости состояний с блокировкой неудачных посылок и т.п. Как будет показано в следующем разделе, реалистичные протоколы квантовой криптографии могут быть сведены к однофотонным с помощью протокола с состояниями-ловушками (decoy state).

6.3.2. Основные соображения для конструирования протокола на геометрически-однородных квантовых состояниях

Нашей основной задачей является построение протокола квантовой криптографии, пригодного для практического применения. Несмотря на достаточно хорошую изученность ряда протоколов, дальнейшее их усовершенствование целесообразно с точки зрения дальнейшего переосмысления основ обеспечения защищенности, а также различных атак на системы квантовой криптографии.

В то время, как базовые протоколы квантовой криптографии подразумевают использование одиночных фотонов, все практические системы основаны на ослабленных классических импульсах — слабых когерентных состояниях (weak coherent pulses). Эта замена приводит к целому множеству трудностей с обеспечением защищенности распределяемых ключей, по сравнению с их

теоретической версией. Например, безусловно секретный протокол [155], на практике становится уязвим для атак с разделением по числу фотонов [209] и путем измерений с определенным исходом [210].

В настоящее время не существует единого универсального решения проблемы безопасности протоколов на когерентных состояниях. По-видимому, наиболее приемлемым считается использование так называемых состояний-ловушек (decoy state), которые позволяют проанализировать долю истинно однофотонных состояний, отправленных Алисой, которые достигли Боба и были зарегистрированы.

Хорошо известно, что реализация оригинального протокола BB84 на когерентных состояниях перестает обеспечивать секретность ключей начиная с достаточно небольшого уровня потерь в канале [210], в то время, как некоторые более перспективные альтернативы были предложены еще в 2004 году [211]. В данном разделе мы сконструируем протокол квантовой криптографии, основанный на давно известных решениях, повышающих защищенность системы, и объединим его с методом на состояниях-ловушках. В результате, полученный протокол будет защищенным не только за счет использования состояний-ловушек, но и за счет его более совершенной внутренней структуры.

В дальнейших рассуждениях мы будем предполагать фазовую модуляцию, которая более подходит для оптоволоконной реализации. В этой схеме каждый лазерный импульс расщепляется на две одинаковые половины в двух временных окнах, а информация кодируется в относительной оптической фазе между ними. Мы также будем предполагать, что источник когерентных состояний генерирует каждый импульс со случайной фазой. Сначала мы определим протокол на геометрически-однородных квантовых состояниях (ГОКС), далее мы рассмотрим поведение протокола при оптимальной унитарной атаке, аналогичной ранее рассмотренной атаке на протокол BB84. В заключение, мы добавим к протоколу состояния-ловушки и проанализируем секретность получившегося протокола.

6.3.3. Протокол квантового распределения ключей на ГОКС

Протокол на ГОКС использует N различных геометрически-однородных квантовых состояний, определяемых унитарным преобразованием U, таким, что $U^N = I$. В результате, $|\psi_j\rangle = U^j |\psi_0\rangle$. В случае фазового кодирования $|\psi_j\rangle = |\alpha\rangle_1 \otimes |e^{i\frac{2\pi}{N}j}\alpha\rangle_2$, где индексы 1 и 2 относятся к двум временным окнам, в которых расположены когерентные состояния $|\alpha\rangle$. Понятно, что это определение достаточно общее и включает такие протоколы как B92 [191] в котором $N = 2$, BB84 [155] и SARG04 [211] где $N = 4$. Как и в случае протокола BB84, состояния группируются попарно в $N/2$ логических базисов: каждый базис содержит два состояния с определенным углом между ними, которые соответствуют логическим нулю и единице. Общее количество состояний N принимается за четное число. Примеры протоколов на ГОКС с различным выбором логических базисов показаны на Рисунке 6.17.

Протокол выглядит следующим образом:

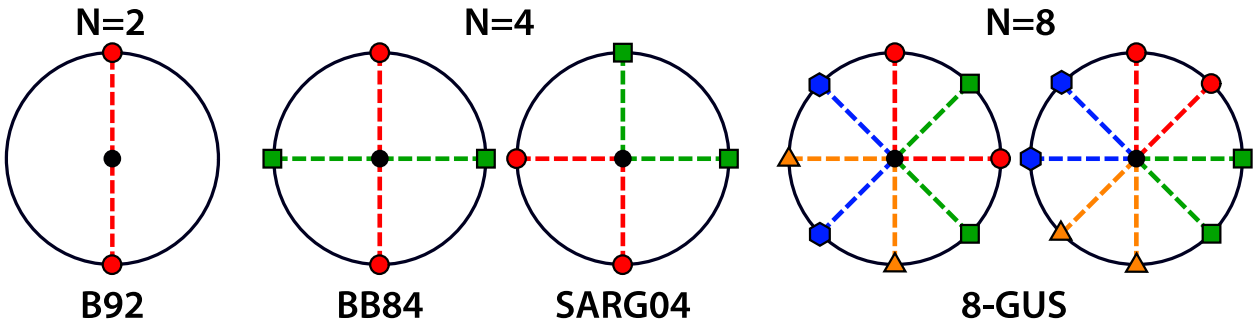

Рисунок 6.17: Информационные состояния и логические базисы в различных ГОКС протоколах, показанные на фазовой плоскости. Логические базисы показаны различными цветами и формой отметок. Для протоколов 8-ГОКС существует два удобных выбора базисов: с углом между состояниями $\Delta\varphi = \pi/2$ и $\Delta\varphi = \pi/4$, как показано на последних двух диаграммах.

1. *Генерация состояний и их передача.* Алиса случайным образом генерирует значение бита, 0 или 1. Она также случайно выбирает один из $N/2$ логических базисов. Затем соответствующее квантовое состояние формируется и отправляется в канал связи. Все квантовые состояния отличаются друг от друга относительной фазой между двумя когерентными состояниями. Эта фаза принимает одно из N различных значений и полностью определено значением бита и выбором базиса. Несмотря на то, что это может быть произвольным отображением N элементов в N, мы ограничимся изучением случая, когда внутри одного базиса угол между нулем и единицей фиксирован и равен $\Delta\varphi$ как было показано на Рисунке 6.17.

2. *Измерение состояний.* Боб случайно выбирает один из $N/2$ базисов и одно из двух вариантов измерения по типу протокола B92 в выбранном базисе. Более подробно про конструкцию таких измерений будет рассказано далее в тексте. Затем, Боб выполняет соответствующее измерение.

Шаги 1 и 2 повторяются множество раз. Очевидно, если Алиса и Боб выбрали один и тот же базис, детектор Боба сработает только если его измерение соответствует значению бита, отправленному Алисой. Если же базисы отличаются, для простоты анализа будем считать, что такие события отбрасываются, даже несмотря на то, что может существовать некоторая корреляция между отправленным и принятым значением бита.

3. *Просеивание ключа.* Боб сообщает Алисе в каких импульсах его детектор сработал и какой базис был использован для измерения. Алиса в ответ сообщает Бобу для каких из этих импульсов её базис совпал с тем, который использовал Боб. Значения битов, ассоциированных с этими импульсами, таким образом, образуют *сырой ключ*. Вся остальная информация отбрасывается.

После всей процедуры Алиса и Боб получают сильно коррелированные сырые ключи, для которых выполняется стандартная классическая процедура исправления ошибок и усиления сек-

ретности. Далее мы будем анализировать долю доступной секретной информации, содержащейся в этих коррелированных битовых последовательностях.

Поскольку фаза θ исходного когерентного состояния $|\alpha\rangle = |e^{i\theta}|\alpha|\rangle$ совершенно случайна, информационные состояния в канале являются смешанными состояниями с рандомизированными фазами, описываемыми матрицей плотности

$$\rho = \int_0^{2\pi} \frac{d\theta}{2\pi} |\psi\rangle \langle\psi| . \tag{6.16}$$

Этой же матрицей плотности обладает некогерентная смесь Фоковских состояний с Пуассоновским распределением вероятностей [212]:

$$\rho(\varphi) = \sum_{k=0}^{\infty} P_k(\mu) |\psi_k(\varphi)\rangle\langle\psi_k(\varphi)|, \quad P_k(\mu) = e^{-2\mu} \frac{(2\mu)^k}{k!}, \tag{6.17}$$

$$|\psi_k(\varphi)\rangle = \sqrt{\frac{k!}{2^k}} \sum_{m=0}^{k} \frac{e^{im\varphi} |m\rangle_1 \otimes |k-m\rangle_2}{\sqrt{m!(k-m)!}}, \tag{6.18}$$

где $\mu = |\alpha|^2$ является средним числом фотонов в каждом из двух когерентных состояний. Из-за физической неразличимости разных интерпретаций одной и той же матрицы плотности, мы вправе пользоваться второй интерпретацией для дальнейшего анализа, не ограничивая при этом общность рассуждений.

Подходящий выбор размера используемого алфавита N тесно связан с защитой системы от атаки путем измерений с определенным исходом. В общем случае безошибочное различение N квантовых состояний возможно, когда эти состояния являются линейно независимыми [213]. Если мы рассмотрим различные Фоковские компоненты смеси (6.17), измерения с определенным исходом для различения N состояний возможно только для $k \geq N - 1$ [214]. В результате, вероятность успеха P_D для безошибочного различения состояний не превышает долю соответствующих состояний в смеси, т.е.

$$P_D < \sum_{k=N-1}^{\infty} P_k(\mu). \tag{6.19}$$

Более точные значения для P_D могут быть найдены с использованием теории для ГОКС [213, 182]. Соответствующие вероятности, вычисленные для релевантных значений N как функции среднего числа фотонов в импульсе μ, построены на Рисунке 6.18.

Если P_D превышает вероятность регистрации состояния Бобом, Ева в принципе может полностью получить всю информацию, распределенную между Алисой и Бобом, путем измерений с определенным исходом с последующей перепосылкой успешно измеренных состояний. Для практически реализуемых систем, полная эффективность которых составляет по крайней мере $10^{-6} \ldots 10^{-5}$ можно безопасно использовать значение $N = 8$. В то же время, выбор $N = 4$, как в большинстве обычно реализуемых протоколов, не может обеспечить защищенности ключей. Конечно, атака путем измерений с определенным исходом должна детектироваться с помощью состояний-ловушек. Однако, к настоящему времени, соответствующие границы для подобных атак в протоколах с состояниями-ловушками неизвестны. Также следует отметить, что реализация измерений с определенным исходом не требует ни неразрушающих измерений ни квантовой

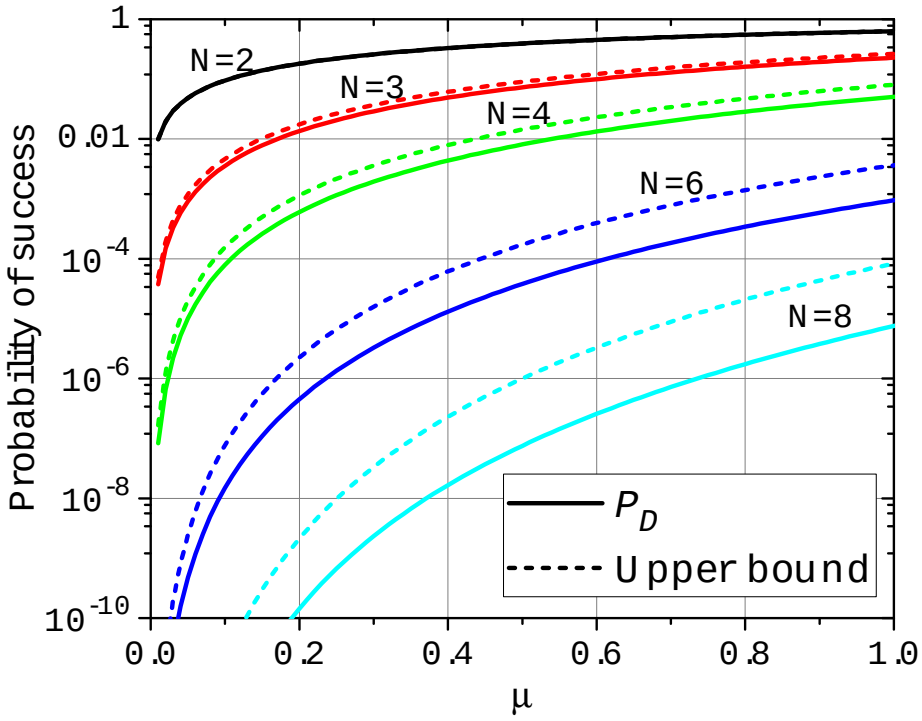

Рисунок 6.18: Вероятность успешного безошибочного различения N ГОКС как функция среднего числа фотонов в импульсе μ. Сплошными линиями показан точный результат, а пунктирными — простейшая верхняя граница (6.19).

памяти. Поэтому она может быть более простой в практической реализации, чем, например, атака с разделением по числу фотонов, про которую речь пойдет позже. Следуя представленной логике, мы считаем случай с $N = 8$ наиболее практически значимым на настоящий день. Будущие реализации, которые могут работать при более низкой эффективности всей системы, могут использовать протоколы с $N = 16$, которые обеспечивают защиту при эффективности канала порядка 10^{-12}.

Выбор угла между состояниями в логическом базисе также напрямую связан с защищенностью системы от взлома. Как показано в [211], использование неортогональных состояний внутри базиса делает протокол более защищенным, по сравнению со случаем ортогональных состояний, как, например в BB84. Разница становится очевидной, если мы рассмотрим злоумышленника, реализующего атаку с разделением по числу фотонов. Такая атака предполагает, что при ее реализации Ева обладает точными копиями всех состояний, зарегистрированных Бобом. Данные копии хранятся в квантовой памяти Евы до раскрытия базисов Алисой и Бобом. В случае, если состояния внутри базиса ортогональны, становится возможным их детерминистическое различение, что приводит к моментальному взлому всей системы. Если же, напротив, состояния внутри каждого базиса не являются ортогональными, Ева сможет извлечь из измерений лишь частичную информацию о распределенном ключе. Вероятность успешного безошибочного различения между

состояниями внутри логического базиса ограничена величиной

$$p_k^{\mathrm{USD}} = 1 - |\langle\psi_k(\varphi_0)|\psi_k(\varphi_1)\rangle| = 1 - \left[\cos\left(\frac{\Delta\varphi}{2}\right)\right]^k, \tag{6.20}$$

где $\Delta\varphi = \varphi_1 - \varphi_0$ — угол между логическим нулем и единицей, а k — число имеющихся фотонов. Для случая протоколов 8-ГОКС удобным выбором угла $\Delta\varphi$ является $\pi/2$ или $\pi/4$. Первый дает более высокую скорость генерации ключа, в то время как второй может работать при более высоких уровнях ошибок в сыром ключе.

6.3.4. Оптимальная атака на однофотонную компоненту

До сих пор мы рассматривали поведение протокола при атаках с нулевым уровнем индуцированных ошибок, т.е. тех, в которых Ева получала информацию о ключах не внося ошибки в сырые ключи легитимных пользователей. Это, однако, недостаточно для полного анализа секретности данного протокола. В этом разделе мы исследуем взаимосвязь между информацией, полученной Евой и количеством индуцированных ошибок с помощью оптимальной унитарной атаки, как это было сделано в разделе 6.3.1.

Унитарная атака — это оптимально сконструированный унитарный оператор, который порождает квантовую запутанность между информационными состояниями в канале и дополнительным квантовым состоянием (анцилла) Евы. Модифицированные информационные состояния распространяются по линии связи к Бобу, в то время как анциллы сохраняются в квантовой памяти Евы до раскрытия базисов Алисой и Бобом. После этого Ева может реализовать коллективное квантовое измерение над всем содержимым квантовой памяти, для получения максимального количества информации о ключах. Оптимальная стратегия для Евы заключается в максимизации этой информации для конкретного наблюдаемого уровня ошибок в сырых ключах Q. Следует отметить, что *унитарность* атаки в данном случае не ограничивает общность рассмотрения, как это показано в разделе 6.3.1 и в работе [207].

Конструирование оптимального оператора для подслушивания — достаточно трудная задача. Вместо этого, мы вычислим консервативную оценку сверху, что гораздо проще. Для цели этих вычислений мы предположим, что в момент измерения Ева знает логический базис, в котором закодирована конкретная посылка. Таким образом, задача Евы существенно упрощается: ей требуется оптимальным образом различить два неортогональных состояния внутри базиса. Как показано в [207, 205, 206] оптимальная стратегия Евы может быть реализована с помощью симметричного унитарного оператора, в котором роли логической единицы и нуля, по сути, одинаковы. Это также означает, что наблюдаемые Бобом битовые ошибки будут подчиняться статистике для *бинарного симметричного канала*. В рамках сформулированных предположений, мы можем записать соответствующий квантовый оператор в явном виде.

Обозначим $|\Psi_k(0)\rangle = |\psi_k(\varphi_0)\rangle$, $|\Psi_k(1)\rangle = |\psi_k(\varphi_1)\rangle$, и $c_k = \left|\langle\Psi_k(0)|\Psi_k(1)\rangle\right|$ в известном логическом базисе. После применения запутывающего оператора общее квантовое состояние

записывается как

$$\begin{aligned}
|\Phi_k(0)\rangle_{BE} &= U_{BE}(|\Psi_k(0)\rangle_B \otimes |E\rangle_E) \\
&= A_k|\Psi_k(0)\rangle_B \otimes |E_k(0)\rangle_E \\
&\quad + B_k|\Psi_k(1)\rangle_B \otimes |E_k(1)\rangle_E, \\
|\Phi_k(1)\rangle_{BE} &= U_{BE}(|\Psi_k(1)\rangle_B \otimes |E\rangle_E) \\
&= A_k|\Psi_k(1)\rangle_B \otimes |E_k(1)\rangle_E \\
&\quad + B_k|\Psi_k(0)\rangle_B \otimes |E_k(0)\rangle_E,
\end{aligned} \tag{6.21}$$

где U_{BE} — унитарное преобразование, реализуемое Евой, $|E\rangle_E$ — анцилла, а $|\Phi_k(0,1)\rangle_{BE}$ — результирующее запутанное состояние между Алисой и Бобом; $|E_k(0,1)\rangle_E$ является измененной анциллой, а параметры A_k и B_k зависят от выбора такого унитарного оператора. Задачей Евы является добиться максимального разделения между $|E_k(0)\rangle$ и $|E_k(1)\rangle$, которое определяется через из скалярное произведение $c_k^{\mathrm{E}} = \left|{}_E\langle E_k(0)|E_k(1)\rangle_E\right|$. Когда измененные состояния достигают Боба, мы можем их рассматривать как смешанные состояния после взятия частичного следа по подсистеме Евы:

$$\rho_k(0,1) = \mathrm{Tr}_E\Big[|\Phi_k(0,1)\rangle_{BEBE}\langle|\Phi_k(0,1)|\Big]. \tag{6.22}$$

Для нахождения взаимосвязи между c_k^{E} и наблюдаемым уровнем битовых ошибок, мы определим процедуру измерения Бобом входящих состояний. Несмотря на то, что невозмущенные состояния наиболее эффективно можно различать специальным обобщенным измерением (POVM) с вероятностью (6.20), на практике пользуются субоптимальной процедурой, основанной на проекционных измерениях. Фаза приемного интерферометра задержки выставляется таким образом, чтобы регистрировать или логический ноль или логическую единицу. Таким образом, реализуемое проекционное измерение определяется следующим разложением единицы

$$I_k = |\Psi_k(j)\rangle_{BB}\langle\Psi_k(j)| + |\Psi_k^{\perp}(j)\rangle_{BB}\langle\Psi_k^{\perp}(j)|, \tag{6.23}$$

где $j = 0, 1$ — выбранное измерение. Первое слагаемое соответствует неопределённому результату, а второе — успешному определению состояния $|\Psi_k(1-j)\rangle$. Вероятность успешного различения, при условии, что измерение правильно выбрано, составляет

$$\begin{aligned}
P_k(0|0) = P_k(1|1) = \mathrm{Tr}_B\Big[&|\Psi_k(j)\rangle_{BB}\langle\Psi_k(j)| \\
&\big(I_k - |\Psi_k(1-j)\rangle_{BB}\langle\Psi_k(1-j)|\big)\Big] = 1 - c_k^2
\end{aligned} \tag{6.24}$$

Если состояния изменены из-за действий Евы, Боб видит правильные значения битов с вероятностью

$$\begin{aligned}
\mathrm{P}_k(j|j) = \mathrm{Tr}_B\Big[\rho_k(j)\big(I_k - |\Psi_k(1-j)\rangle_{BB}\langle\Psi_k(1-j)|\big)\Big] \\
= |A_k|^2\big(1 - c_k^2\big),
\end{aligned} \tag{6.25}$$

а ошибочные биты с вероятностью

$$\begin{aligned} \mathrm{P}_k(1-j|j) = \mathrm{Tr}_B\Big[\rho_k(j)\big(I_k - |\Psi_k(j)\rangle_{BB}\langle\Psi_k(j)|\big)\Big] \\ = |B_k|^2\big(1-c_k^2\big). \end{aligned} \tag{6.26}$$

Наблюдаемый уровень ошибок, таким образом, равен

$$Q_k = \frac{|B_k|^2}{|A_k|^2 + |B_k|^2}. \tag{6.27}$$

Без потери общности, мы можем также предположить, что A_k и $\langle\Psi_k(0)|\Psi_k(1)\rangle$ являются действительными числами. В таком случае из условий нормировки $|\Phi_k(j)\rangle$ легко следует, что B_k и $\langle E_k(0)|E_k(1)\rangle$ также являются действительными. Как следует из условия унитарности U_{BE},

$$c_k \langle\Phi_k(0)|\Phi_k(0)\rangle = \langle\Phi_k(0)|\Phi_k(1)\rangle . \tag{6.28}$$

Подставляя (6.21) в (6.28), получаем

$$c_k\big(1-c_k^{\mathrm{E}}\big)\big(A^2+B^2\big) = 2\big(1-c_k^2c_k^{\mathrm{E}}\big)AB, \tag{6.29}$$

что в свою очередь непосредственно связано с индуцированным уровнем битовых ошибок соотношением

$$\frac{2AB}{A^2+B^2} = \sqrt{1-(1-2Q_k)^2}. \tag{6.30}$$

Искомая граница на различимость состояний Евы для определенного наблюдаемого уровня ошибок описывается в результате соотношением

$$c_k^{\mathrm{E}}(Q_k) = \frac{c_k - \sqrt{1-(1-2Q_k)^2}}{c_k\left[1 - c_k\sqrt{1-(1-2Q_k)^2}\right]}. \tag{6.31}$$

После нахождения максимального разделения состояний для конкретного уровня ошибок, мы можем вычислить соответствующую долю доступной секретной информации. После успешных измерений Боба, Ева обладает следующими редуцированными матрицами плотности:

$$\begin{aligned} \rho_k^{\mathrm{E}}(0) &= \frac{A^2\,|E_k(0)\rangle\langle E_k(0)| + B^2\,|E_k(1)\rangle\langle E_k(1)|}{A^2+B^2} \\ \rho_k^{\mathrm{E}}(1) &= \frac{A^2\,|E_k(1)\rangle\langle E_k(1)| + B^2\,|E_k(0)\rangle\langle E_k(0)|}{A^2+B^2} \end{aligned} \tag{6.32}$$

Условная энтропия между Алисой и Евой ограничена границей Холево $\chi_k(Q_k)$ [193, 194]:

$$H_k(X|E) \geq 1 - \chi_k(Q_k), \tag{6.33}$$

где

$$\chi_k(Q_k) = H\left(\frac{\rho_k^{\mathrm{E}}(0)+\rho_k^{\mathrm{E}}(1)}{2}\right) - \frac{H\big(\rho_k^{\mathrm{E}}(0)\big)+H\big(\rho_k^{\mathrm{E}}(1)\big)}{2}, \tag{6.34}$$

Она может быть найдена с использованием следующих уравнений:

$$H\left(\frac{\rho_k^{\mathrm{E}}(0)+\rho_k^{\mathrm{E}}(1)}{2}\right) = h\big(\Lambda_k(Q_k)\big), \tag{6.35}$$

где собственные значения $\Lambda_k^{\pm}(Q_k) = \left(1 \pm c_k^{\mathrm{E}}(Q_k)\right)/2$ и $h(x) = -x\log(x) - (1-x)\log(1-x)$.

Аналогично,

$$H\left(\rho_k^{\mathrm{E}}(0)\right) = H\left(\rho_k^{\mathrm{E}}(1)\right) = h(\lambda_k) \tag{6.36}$$

с собственными значениями

$$\lambda_k^{\pm}(Q_k) = \frac{1}{2}\left(1 \pm \sqrt{1 - 4Q_k\left(1 - c_k^{\mathrm{E}}(Q_k)^2\right)(1-Q_k)}\right). \tag{6.37}$$

В результате, мы нашли выражение, описывающее нижнюю границу условной энтропии $H_k(X|E)$ для определенного уровня индуцированных ошибок. Тут следует обратить внимание, что, несмотря на то, что унитарная атака Евы была проанализирована для произвольного числа фотонов k, она является оптимальной стратегией Евы лишь для однофотонной компоненты $k = 1$. Для числа фотонов больше единицы, Ева может выбрать другие варианты атаки, которые могут привести к подслушиванию большего количества информации. Таким образом, в дальнейшем положительный вклад в секретный ключ будет рассматриваться лишь для однофотонной компоненты. Вопрос может ли быть положительным вклад от компонент с $k > 1$ является открытым, и консервативная оценка, очевидно, не должна такой вклад учитывать.

Чтобы вычислить долю секретной информации в реалистичных условиях, мы должны учесть, что наблюдаемый уровень ошибок в общем случае выше, чем его теоретическая граница, в то время как вероятности регистрации наоборот ниже. Обозначим соответствующие наблюдаемые величины буквами с верхними черточками

Полная вероятность регистрации k-фотонной компоненты

$$\overline{P}_k = \frac{1}{2}\left(\overline{P}_k(0|0) + \overline{P}_k(1|0) + \overline{P}_k(1|1) + \overline{P}_k(0|1)\right), \tag{6.38}$$

а соответствующий уровень ошибок

$$\overline{Q}_k = \frac{\overline{P}_k(1|0) + \overline{P}_k(0|1)}{2\overline{P}_k}. \tag{6.39}$$

Полная вероятность регистрации равна, таким образом

$$\overline{P} = \sum_{k=0}^{\infty} e^{-2\mu}\frac{(2\mu)^k}{k!}\overline{P}_k, \tag{6.40}$$

а асимптотическая доля секретной информации составляет по крайней мере

$$R(\mu) = 2\mu e^{-2\mu}\overline{P}_1\left[1 - \chi_1(\overline{Q}_1)\right] - \overline{P}\,h(\overline{Q}), \tag{6.41}$$

где $\overline{Q}$ — общий наблюдаемый уровень ошибок. Доля информации $\overline{P}\,h(\overline{Q})$ — минимальное значение утечки информации для реализации классического алгоритма коррекции ошибок в Шенноновском пределе.

6.3.5. Протокол с состояниями ловушками для практической реализации квантового распределения ключей

Поскольку Алиса и Боб в общем случае не знают значений $\overline{P}_k$ и $\overline{Q}_k$ для каждого из k-фотонных компонентов, практические системы должны опираться на более консервативный подход, в котором фигурируют лишь непосредственно наблюдаемые параметры. Подход с состояниями-ловушками [215] позволяет найти соответствующие границы для однофотонной компоненты, которая, как уже упоминалось, является ключевой для распределения секретной информации.

В соответствии со стратегией использования состояний-ловушек, кроме стандартных информационных импульсов со средним числом фотонов μ, Алиса также случайным образом отправляет более слабые «состояния-ловушки» с соответствующими средними числами фотонов ν_1 и ν_2 ($0 \approx \nu_2 < \nu_1 < \mu$). Поскольку Ева в общем случае не может с уверенностью определить принадлежность конкретного импульса к информационному или ловушке, классическая атака с разделением по числу фотонов приведёт к измеримому отличию статистики импульсов на приеме. Если мы резонно предположим, что поведение k-фотонной компоненты не зависит от амплитуды исходного когерентного состояния, мы можем найти непосредственную связь между параметрами её регистрации и наблюдаемыми величинами. В частности, показывается [215], что минимальная вероятность детектирования однофотонной компоненты составляет

$$\overline{P}_1 \geq \frac{1/2}{\nu_1 - \nu_2 - \frac{\nu_1^2 - \nu_2^2}{\mu}} \left[\overline{P}(\nu_1) e^{2\nu_1} - \overline{P}(\nu_2) e^{2\nu_2} - \frac{\nu_1^2 - \nu_2^2}{\mu^2} \left(\overline{P}(\mu) e^{2\mu} - P_0 \right) \right], \tag{6.42}$$

где

$$\overline{P}_0 \geq \max \left\{ \frac{\nu_1 e^{2\nu_2} \overline{P}(\nu_2) - \nu_2 e^{2\nu_1} \overline{P}(\nu_1)}{\nu_1 - \nu_2}, 0 \right\}. \tag{6.43}$$

Аналогично, верхняя граница на долю ошибок в однофотонной компоненте равна

$$\overline{Q}_1 \leq \frac{e^{2\nu_1} \overline{P}(\nu_1) \overline{Q}(\nu_1) - e^{2\nu_2} \overline{P}(\nu_2) \overline{Q}(\nu_2)}{2(\nu_1 - \nu_2) \overline{P}_1}. \tag{6.44}$$

В принципе, аналогичным образом можно найти и подобные границы для $k \geq 2$, но это потребует более чем три различных амплитуды исходных когерентных состояний [216]. Это не только сделает всю систему менее практичной, но и не принесет ощутимой пользы, так как вклад многофотонных компонентов в секретную информацию неочевиден. Поэтому, большинство практических систем полагаются исключительно на однофотонную компоненту.

В результате, получаем следующее выражение для доли секретной информации в распределенных ключах:

$$R'(\mu) = 2\mu e^{-2\mu} \overline{P}_1 \left[1 - \chi_1(\overline{Q}_1) \right] - \overline{P}(\mu)\, h\left(\overline{Q}(\mu) \right). \tag{6.45}$$

Легко видеть, что это выражение зависит лишь от измеряемых параметров и, таким образом, может быть использовано в реальных системах для оценки доли секретной информации.

6.3.6. Оценка доли секретной информации для реалистичных систем

Легко видеть, что без влияния со стороны Евы, работа системы определяется уровнем оптических потерь в линии, а также эффективностью детектирования η. Если базисы Алисы и Боба совпали, вероятность детектирования однофотонной компоненты составляет $\overline{P}_1 = p_d + \eta(1 - c_1^2)T(L)/2 = p_d + \eta \sin^2(\Delta\varphi/2)T(L)/2$, где p_d — вероятность темнового отсчета детектора за одно временно́е окно регистрации, $T(L)$ — общий коэффициент пропускания оптической системы, а множитель $1/2$ связан с вероятностью реализации правильного варианта измерения. Аналогично,

$$\overline{P}_k = p_d + \frac{1}{2}\left(1 - \left[1 - \eta \sin^2\left(\Delta\varphi/2\right) T(L)\right]^k\right). \tag{6.46}$$

Из приведенных результатов легко показать, что общая вероятность регистрации сигнальных импульсов равна

$$\overline{P}(\mu) = p_d + \frac{1}{2}\Big(1 - \exp\big[-2\mu\eta \sin^2(\Delta\varphi/2)T(L)\big]\Big), \tag{6.47}$$

в то время как соответствующая доля ошибок составляет

$$\overline{Q}(\mu) = \frac{p_d}{2\overline{P}(\mu)} \tag{6.48}$$

Такие же выражения могут быть записаны для состояний-ловушек путем замены μ на ν_1 и ν_2.

Теперь этого достаточно, чтобы оценить эффективность работы реальной системы. Используя найденные выражения для $\overline{P}(x)$ и $\overline{Q}(x)$ ($x = \mu, \nu_1, \nu_2$), мы вычисляем „наблюдаемые“ границы для $\overline{P}_1$ и $\overline{Q}_1$, и подставляем их в (6.45) для того, чтобы найти асимптотическую долю секретной информации. Для примера, мы будем использовать следующие типичные значения параметров установки: $\eta = 0.1$, $T(L) = 10^{-aL/10}$, где $a = 0.2$ dB/km, $p_d = 10^{-6}$. Для максимизации эффективности оценки параметров однофотонной компоненты, мы используем следующие средние числа фотонов: $2\nu_1 = 0.05$ и $2\nu_2 = 10^{-3}$. Для сигнальных состояний в качестве среднего числа фотонов будем использовать значения из набора $2\mu = \{0.1; 0.25; 0.5; 0.9\}$.

Для лучшей визуализации результатов будем использовать следующие два показателя работы системы: во-первых, число секретных бит, на каждый бит просеянного ключа, определяемое как $R'(\mu)/\overline{P}(\mu)$. Эта величина обладает большой практической значимостью, так как определяет минимальное необходимое сжатие ключевого материала, необходимое для достижения конечной цели распределения ключей. Второй показатель — это нормированная доля секретной информации $R'(\mu)/[\eta T(L)]$, которая показывает какое количество секретных бит мы получаем по сравнением с количеством актов регистрации импульсов в аналогичной линии связи с идеальным однофотонным детектором. Этот показатель позволяет сравнивать относительную скорость генерации секретного ключа в разных конфигурациях.

Результаты вычисления показаны на Рисунке 6.19. Как следует из полученных графиков, чем меньше μ тем больше доля секретной информации в просеянном ключе. При $\mu = 0.1$ практически вся полученная информация в просеянном ключе является секретной. Это следствие того факта, что при таких μ практически все зарегистрированные состояния были испущены всего с одним

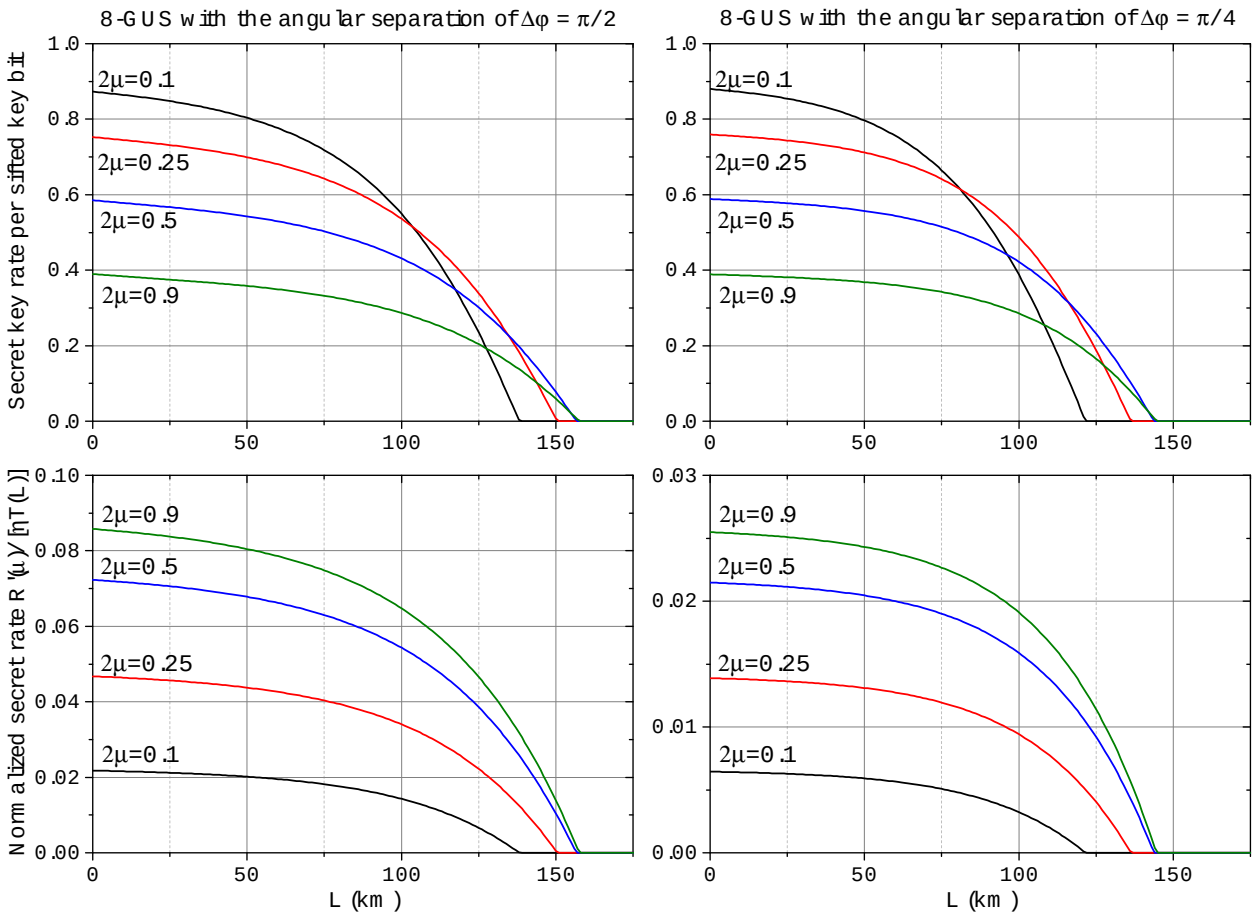

Рисунок 6.19: Вычисленная доля секретной информации на бит просеянного ключа (сверху) и нормированная скорость генерации секретного ключа (снизу) для протокола 8-ГОКС как функция длины канала L. Две колонки соответствуют различным значениям $\Delta\varphi$, а разные кривые на каждом из графиков — различным значениям среднего числа фотонов в информационных импульсах μ.

фотоном. И наоборот, большие значения μ приводят к снижению доли однофотонной компоненты. Общая скорость генерации секретного ключа, нормированная на эффективность системы $\eta T(L)$ растет с увеличением μ так ка больше фотонов достигают детектора. Фактически, значение $2\mu = 0.9$ является близким к оптимальному для длины канала 100 км в смысле скорости генерации секретной информации.

6.3.7. Обсуждение результатов

Построение безопасного и в то же время практически реализуемого протокола очень непростая задача. В настоящее время наиболее широкоиспользующимся протоколом является BB84 с состояниями-ловушками. Его конструкция непосредственно сфокусирована на защите от атаки с разделением по числу фотонов, которая также подразумевается при доказательстве секретности. Однако, практическая реализация такой атаки при сегодняшнем уровне технологии едва ли возможна: атака требует, во-первых, неразрушающего измерения числа частиц, а во-вторых, квантовую па-

мять. С другой стороны, существует атака на базе измерений с определенным исходом, которая может быть экспериментально реализована с помощью имеющихся технологий. Она не требует ни наличия оптических каналов связи без потерь ни квантовой памяти. Измеренные состояния могут быть перепосланы с достаточной энергией, чтобы компенсировать потери между Евой и приемником Боба. Таким образом, с точки зрения безопасности ключей, разумно рассматривать такую атаку, как более реалистичную угрозу для практических систем.

Как известно, атака на базе измерений с определенным исходом, может быть легко использована для взлома обычного протокола BB84 на когерентных состояниях. Состояния-ловушки, предположительно, должны защищать и от этой атаки в частности, однако, насколько нам известно, конкретные границы безопасности для этой атаки и ее комбинаций с другими типами атак, до сих пор неизвестны. Более того, никакая экспериментальная реализация не является идеальной и любая компрометация устройств, отвечающих за генерацию состояний-ловушек, мгновенно приводит к полной потере секретности всей схемы распределения ключей, даже если Ева ограничена сегодняшним уровнем технологии, т.е., например, не может выполнять разделение по числу фотонов.

В настоящем разделе мы продемонстрировали простое решение проблемы, которое делается на уровне протокола квантового распределения ключей, и полностью совместимо с технологией использования состояний-ловушек. Предлагаемый протокол не только устойчив в смысле крайне низкой вероятности измерений с определенным исходом, но и развивает идеи, представленные в [211], что позволяет кардинально ограничить доступную Еве информацию о ключах даже при использовании разделения по числу фотонов: логическая организация квантовых состояний в неортогональные пары состояний запрещает их детерминистическое различение.

Следует заметить, что повышение числа логических базисов неизбежно приводит к бóльшим потерям информации на фазе просеивания ключа. Также как и скорость генерации ключа в протоколе SARG04 меньше, чем в протоколе BB84, предложенный протокол в два раза менее эффективен чем SARG04 если $\Delta\varphi = \pi/2$ и еще хуже с точки зрения скорости если $\Delta\varphi = \pi/4$. Однако, как хорошо известно, квантовое распределение ключей призвано не повысить скорость распределения ключей, а обеспечить их фундаментальную безопасность. Современные симметричные системы шифрования обладают беспрецедентным уровнем защиты данных, которые, по-видимому, не теряют своей состоятельности даже при наличии у злоумышленников квантового компьютера [217, 218]. Таким образом, нет особой потребности в генерации гигабайтов ключей для реализации шифрования типа «одноразовый блокнот»: достаточно пользоваться симметричным шифрованием и регулярно заменять ключи. Таким образом, этот несущественный недостаток, связанный с более низкой скоростью генерации ключей, не играет особой роли для практических применений. Все остальные параметры предложенного протокола, такие как максимальная дальность передачи, обладают типичными значениями для традиционных протоколов.

6.4. Заключение к Главе 6

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

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. Созданная экспериментальная установка продемонстрировала асимптотическую скорость генерации секретных ключей в сотни бит в секунду при дальности канала по открытому пространству 180 м.

Наконец, был разработан протокол квантовой криптографии на геометрически-однородных квантовых состояниях 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.

В целом, данное направление, как теоретическое, так и экспериментальное, 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 экспериментально 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 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 использованных сокращений

AES	Advanced Encryption Standard — стандарт симметричного шифрования в США
ASE	Amplified Spontaneous Emission — усиленное спонтанное излучение
AWG	Arrayed Waveguide Ggrating — планарная волноводная решетка
B92	протокол квантовой криптографии, предложенный в [191]
BB84	протокол квантовой криптографии, предложенный в [155]
CDMA	Code Division Multiple Access — множественный доступ с кодовым разделением
CDR	Clock and Data Recovery — восстановление тактовой частоты и данных
COW	Coherent One-Way — протокол квантовой криптографии, предложенный в [186]
DPS	Differential Phase Shift — протокол квантовой криптографии, предложенный в [187]
DVI	Digital Visual Interface — цифровой видеоинтерфейс
EDFA	Erbium Doped Fiber Amplifier — эрбиевый волоконный усилитель
GPS	Global Positioning System — система глобального позиционирования
HD	Heavily-Doped — оптоволокно, сильно допированное GeO_2
HDMI	High Definition Multimedia Interface — мультимедийный интерфейс
ITU	International Telecommunication Union — международный союз электросвязи
LDPC	Low-Density Parity-Check — тип кода, исправляющего ошибки
MEMS	Microelectromechanical Systems — микроэлектромеханические системы
NA	Numerical aperture — числовая апертура
NIST	The National Institute of Standards and Technology — национальный институт стандартов и технологий США
OFDM	Orthogonal Frequency Division Multiplexing — мультиплексирование на ортогональных подчастотах
PNS	Photon Number Splitting — атака с разделением по числу фотонов
PON	Passive Optical Network — пассивная оптическая сеть
POVM	Positive Operator-Valued Measure — квантовое измерение общего вида
QAM	Quadrature Amplitude Modulation — квадратурная модуляция
QBER	Quantum Bit Error Ratio — доля ошибок в квантовом канале
QPSK	Quadrature Phase-Shift Keying — квадратурная фазовая модуляция
RIE	Reactive-Ion Etching — реактивное ионное травление

RSA	Rivest, Shamir и Adleman — алгоритм криптографии с открытым ключом
SARG04	протокол квантовой криптографии, предложенный в [211]
SMF	Single-Mode Fiber — одномодовый световод
SOA	Semiconductor Optical Amplifier — полупроводниковый оптический усилитель
SOI	Silicon On Insulator — структура кремний на изоляторе
STDP	Spike Time Dependent Plasticity — процесс настройки биологической нейронной сети
TOAD	Terahertz Optical Asymmetric Demultiplexer — оптический вентиль из работы [54]
USB	Universal Serial Bus — стандатный компьютерный интерфейс для периферийных устройств
WDM	Wavelength Division Multiplexing — мультиплексирование с разделением по длине волны
XOR	eXclusive OR — логическая операция исключающее или
АЦП	Аналогово-Цифровой Преобразователь
БПФ	Быстрое Преобразование Фурье
ВНБ	Взаимно Несмещенный Базис
ГОКС	Геометрически-Однородные Квантовые Состояния
ДПФ	Дискретное Преобразование Фурье
КГСЧ	Квантовый Генератор Случайных Чисел
ОДПФ	Обратное Дискретное Преобразование Фурье
ОФД	ОдноФотонный Детектор
ПЗС	Прибор с Зарядовой Связью
ПИД	Пропорционально-Интегрально-Дифференцирующий — тип обратной связи
ПЛИС	Программируемая Логическая Интегральная Схема
ПСП	ПсевдоСлучайная Последовательность
ПФМ	Пространственный Фазовый Модулятор
СБИС	СверхБольшая Интегральная Схема
СЭМ	Сканирующий Электронный Микроскоп
ФАПЧ	Фазовая АвтоПодстройка Частоты
ЦАП	Цифро-Аналоговый Преобразователь

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 Flled: 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 C1 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] Benlachtar Yannis, Watts Philip M., Bouziane Rachid et al. Generation of optical OFDM signals using 21.4 GS/s real time digital signal processing // Opt. Express. — 2009. — Sep. — Vol. 17, no. 20. — P. 17658–17668.

[5] Yang Qi, Chen Simin, Ma Yiran, Shieh William. Real-time reception of multi-gigabit coherent optical OFDM signals // Opt. Express. — 2009. — May. — Vol. 17, no. 10. — P. 7985–7992.

[6] Buchali F., Dischler R., Klekamp A. et al. Statistical Transmission Experiments Using a Real-Time 12.1 Gb/s OFDM Transmitter // Conference on Optical Fiber Communication, OFC. — paper OMS3. — San Diego, CA, 2010.

[7] Chen S., Ma Y., Shieh W. 110-Gb/s Multi-Band Real-Time Coherent Optical OFDM Reception after 600-km Transmission over SSMF Fiber // Conference on Optical Fiber Communication, OFC. — paper OMS2. — San Diego, CA, 2010.

[8] Hillerkuss D., Schellinger T., Schmogrow R. et al. Single source optical OFDM transmitter and optical FFT receiver demonstrated at line rates of 5.4 and 10.8Tb/s // Conference on Optical Fiber Communication, OFC. — paper PDPC1. — San Diego, CA, 2010.

[9] Chen Hongwei, Chen Minghua, Xie Shizhong. All-Optical Sampling Orthogonal Frequency-Division Multiplexing Scheme for High-Speed Transmission System // J. Lightwav. Technol. — 2009. — Nov. — Vol. 27, no. 21. — P. 4848–4854.

[10] Gunning F. C. Garcia, Ibrahim S. K., Frascella P. et al. High symbol rate OFDM transmission technologies // Conference on Optical Fiber Communication, OFC. — paper OThD1. — San Diego, CA, 2010.

[11] Lee Kyusang, Thai Chan T.D., Rhee June-Koo Kevin. All optical discrete Fourier transform processor for 100 Gbps OFDM transmission // Opt. Express. — 2008. — Mar. — Vol. 16, no. 6. — P. 4023–4028.

[12] Takiguchi K., Oguma M., Takahashi H., Mori A. PLC-based eight-channel OFDM demultiplexer and its demonstration with 160 Gbit/s signal reception // Conference on Optical Fiber Communication, OFC. — paper OThB4. — San Diego, CA, 2010.

[13] Huang Y., Qian D., Saperstein R. E. et al. Dual-polarization 2x2 IFFT/FFT optical signal processing for 100-Gb/s QPSK-PDM all-optical OFDM // Conference on Optical Fiber Communication, OFC. — paper OTuM4. — San Diego, CA, 2009.

[14] Hillerkuss D., Winter M., Teschke M. et al. Simple all-optical FFT scheme enabling Tbit/s real-time signal processing // Opt. Express. — 2010. — Apr. — Vol. 18, no. 9. — P. 9324–9340.

[15] Lowery Arthur James. Design of arrayed-waveguide grating routers for use as optical OFDM demultiplexers // Opt. Express. — 2010. — Jun. — Vol. 18, no. 13. — P. 14129–14143.

[16] Doerr Christopher Richard, Okamoto Katsunari. Advances in Silica Planar Lightwave Circuits // J. Lightwav. Technol. — 2006. — Dec. — Vol. 24, no. 12. — P. 4763–4789.

[17] Smit M.K., Van Dam C. PHASAR-based WDM-devices: Principles, design and applications // IEEE J. Sel. Top. Quantum Electron. — 1996. — Vol. 2, no. 2. — P. 236–250.

[18] Cincotti Gabriella, Wada Naoya, Kitayama Ken-ichi. Characterization of a Full Encoder/Decoder in the AWG Configuration for Code-Based Photonic Routers - Part I: Modelling and Design // J. Lightwav. Technol. — 2006. — Vol. 24, no. 1. — P. 103–112.

[19] Takada K., Abe M., Shibata M. et al. Low-crosstalk 10-GHz-spaced 512-channel arrayed-waveguide grating multi/demultiplexer fabricated on a 4-in wafer // IEEE Photon. Technol. Lett. — 2001. — Vol. 13, no. 11. — P. 1182–1184.

[20] Takada K., Abe M., Okamoto K. Low-cross-talk polarization-insensitive 10-GHz-spaced 128-channel arrayed-waveguide grating multiplexer–demultiplexer achieved with photosensitive phase adjustment // Opt. Lett. — 2001. — Jan. — Vol. 26, no. 2. — P. 64–65.

[21] Ellis A.D., Gunning F.C.G. Spectral density enhancement using coherent WDM // IEEE Photonics Technology Letters. — 2005. — Vol. 17, no. 2. — P. 504–506.

[22] Chandrasekhar S., Liu X., Zhu B., Peckham D. W. Transmission of a 1.2 Tb/s 24-carrier no-guad-interval coherent OFDM superchannel over 7200-km of Ultra-Large-Area Fiber // ECOC. — paper PD2.6. — Vienna, Austria, 2009.

[23] Wang X., Wada N., Miyazaki T. et al. Field Trial of 3-WDM x 10-OCDMA x 10.71-Gb/s Asynchronous WDM/DPSK-OCDMA Using Hybrid E/D Without FEC and Optical Thresholding // J. Lightwav. Technol. — 2007. — Vol. 25, no. 1. — P. 207–215.

[24] Babin S., Bugrov A., Cabrini S. et al. Digital optical spectrometer-on-chip // Appl. Phys. Lett. — 2009. — Vol. 95, no. 4. — P. 041105.

[25] Etemad Shahab, Agarwal Anjali, Banwell Thomas et al. An Overlay Photonic Layer Security Approach Scalable to 100 Gb/s // IEEE Commun. Mag. — 2008. — Vol. 46, no. 8. — P. 32–39.

[26] Babin S., Peroz C., Bugrov A. et al. Fabrication of novel digital optical spectrometer on chip // J. Vacuum Science & Technol. B. — 2009. — Vol. 27, no. 6. — P. 3187–3191.

[27] Peroz C., Dhuey S., Goltsov A. et al. Digital spectrometer-on-chip fabricated by step and repeat nanoimprint lithography on pre-spin coated films // Microel. Eng. — 2011. — Vol. 88, no. 8. — P. 2092–2095.

[28] Optical Code Division Multiple Access: Fundamentals and Applications / Ed. by Paul R. Prucnal. — Taylor & Francis Ltd., 2006.

[29] Agarwal A., Toliver P., Menendez R. et al. Fully programmable ring-resonator-based integrated photonic circuit for phase coherent applications // J. Lightwav. Technol. — 2006. — Vol. 24, no. 1. — P. 77–87.

[30] Yan Meng, Yao Minyu, Zhang Hongming et al. En/Decoder for Spectral Phase-Coded OCDMA System Based on Amplitude Sampled FBG // IEEE Photon. Technol. Lett. — 2008. — Vol. 20, no. 10. — P. 788–790.

[31] Xu Qianfan, Soref Richard. Reconfigurable optical directed-logic circuits using microresonator-based optical switches // Opt. Express. — 2011. — Mar. — Vol. 19, no. 6. — P. 5244–5259.

[32] Reed G. T., Mashanovich G., Gardes F. Y., Thomson D. J. Silicon optical modulators // Nature Photon. — 2010. — Vol. 4, no. 8. — P. 518–526.

[33] Vlasov Yurii, Green William M. J., Xia Fengnian. High-throughput silicon nanophotonic wavelength-insensitive switch for on-chip optical networks // Nature Photon. — 2008. — Vol. 2, no. 4. — P. 242–246.

[34] Dong Po, Shafiiha Roshanak, Liao Shirong et al. Wavelength-tunable silicon microring modulator // Opt. Express. — 2010. — May. — Vol. 18, no. 11. — P. 10941–10946.

[35] Asquini Rita, Gilardi Giovanni, d'Alessandro Antonio, Assanto Gaetano. Integrated Bragg reflectors in low-index media: enabling strategies for wavelength tunability in electro-optic liquid crystals // Opt. Engineering. — 2011. — Vol. 50, no. 7. — P. 1–10.

[36] Tang Pingsheng, Towner D. J., Hamano T. et al. Electrooptic modulation up to 40 GHz in a barium titanate thin film waveguide modulator // Opt. Express. — 2004. — Nov. — Vol. 12, no. 24. — P. 5962–5967.

[37] Wang Chein-Hsun, Jenkins B. Keith. Subtracting incoherent optical neuron model: analysis, experiment, and applications // Applied Optics. — 1990. — Vol. 29, no. 14. — P. 2171–2186.

[38] Grigor'yants A. V., Dyuzhikov I. N. Formation of a neuron-like pulsed response in a semiconductor resonator cavity with competing optical nonlinearities // Kvant. Elektron. — 1994. — Vol. 21, no. 6. — P. 511–512. — [Sov. J. Quantum Electron. **24**, 469–470 (1994)].

[39] Tariq Salim, Habib Mahmoud K., Helmy Hanan A. Opto-Electronic Neuron-Type Operation via Stimulated Raman Scattering in Optical Fiber // J. Lightwav. Technol. — 1997. — Vol. 15, no. 6. — P. 938–947.

[40] Mos E. C., Hoppenbrouwers J. J. L., Hill M. T. et al. Optical Neuron by Use of a Laser Diode with Injection Seeding and External Optical Feedback // IEEE Trans. Neural Netw. — 2000. — Vol. 11, no. 4. — P. 988–996.

[41] Moagar-Poladian Gabriel. Reconfigurable optical neuron based on photoelectret materials // Applied Optics. — 2000. — Vol. 39, no. 5. — P. 782–787.

[42] Hill Martin T., Frietman Edward E. E., de Waardt Huig et al. All Fiber-Optic Neural Network Using Coupled SOA Based Ring Lasers // IEEE Trans. Neural Netw. — 2002. — Vol. 13, no. 6. — P. 1504–1513.

[43] Moagar-Poladian G., Bulinski M. Optical reconfigurable neuron by using the transverse Pockels effect // J. Optoel. Adv. Mat. — 2002. — Vol. 4, no. 4. — P. 929–936.

[44] Vogelstein R. Jacob, Mallik Udayan, Vogelstein Joshua T., Cauwenberghs Gert. Dynamically reconfigurable silicon array of spiking neurons with conductance-based synapses // IEEE Trans. Neural Netw. — 2007. — Vol. 18, no. 1. — P. 253–265.

[45] Indiveri G., Chicca E., Douglas R. A VLSI array of low-power spiking neurons and bistable synapses with spike-timing dependent plasticity // IEEE Trans. Neural Netw. — 2006. — Vol. 17, no. 1. — P. 211–221.

[46] Pashaie Rarnin, Farhat Nabil H. Optical realization of bioinspired spiking neurons in the electron trapping material thin film // Applied Optics. — 2007. — Vol. 46, no. 35. — P. 8411–8418.

[47] Romariz Alexandre R. S., Wagner Kelvin H. Tunable vertical-cavity surface-emitting laser with feedback to implement a pulsed neural model. 1. Principles and experimental demonstration // Applied Optics. — 2007. — Vol. 46, no. 21. — P. 4736–4745.

[48] Romariz Alexandre R. S., Wagner Kelvin H. Tunable vertical-cavity surface-emitting laser with feedback to implement a pulsed neural model. 2. High-frequency effects and optical coupling // Applied Optics. — 2007. — Vol. 46, no. 21. — P. 4746–4753.

[49] Beri Stefano, Mashall Lilia, Gelens Lendert et al. Excitability in optical systems close to Z_2-symmetry // Phys. Lett. A. — 2010. — Vol. 374, no. 5. — P. 739–743.

[50] Koch Christof. Biophysics of Computation. — Oxford University Press, 1999.

[51] Pulsed Neural Networks / Ed. by Wolfgang Maass, Christopher M. Bishop. — The MIT Press, 1999.

[52] Sarpeshkar Rahul. Analog Versus Digital: Extrapolating from Electronics to Neurobiology // Neural Computation. — 1998. — Vol. 10. — P. 1601–1638.

[53] 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.

[54] Sokoloff J. P., Prucnal P. R., Glesk I., Kane M. A terahertz optical asymmetric demultiplexer (TOAD) // IEEE Photon. Technol. Lett. — 1993. — Vol. 5, no. 7. — P. 787–790.

[55] Dianov Evgeny M., Mashinsky Valery M. Germania-Based Core Optical Fibers // J. Lightwav. Technol. — 2005. — Vol. 23, no. 11. — P. 3500–3508.

[56] Aida T., Davis P. Storage of optical pulse data sequences in loop memory using multistable oscillations // Electron. Lett. — 1991. — Vol. 27, no. 17. — P. 1544–1546.

[57] Nakazawa M., Suzuki K., Yamada E. et al. Experimental demonstration of soliton data transmission over unlimited distances with soliton control in time and frequency domains // Electron. Lett. — 1993. — Vol. 29, no. 9. — P. 729–730.

[58] Doerr C. R., Wong W. S., Haus H. A., Ippen E. P. Additive-pulse mode-locking/limiting storage ring // Opt. Lett. — 1994. — Vol. 19, no. 21. — P. 1747–1749.

[59] Moores J. D., Hall K. L., LePage S. M. et al. 20-GHz optical storage loop/laser using amplitude modulation, filtering, and artificial fast saturable absorption // IEEE Photon. Technol. Lett. — 1995. — Vol. 7, no. 9. — P. 1096–1098.

[60] Arute Frank, Arya Kunal, Babbush Ryan et al. Quantum supremacy using a programmable superconducting processor // Nature. — 2019. — Vol. 574, no. 7779. — P. 505–510.

[61] Wang Hui, Qin Jian, Ding Xing et al. Boson Sampling with 20 Input Photons and a 60-Mode Interferometer in a 10^{14}-Dimensional Hilbert Space // Phys. Rev. Lett. — 2019. — Dec. — Vol. 123. — P. 250503.

[62] Zhong Han-Sen, Wang Hui, Deng Yu-Hao et al. Quantum computational advantage using photons // Science. — 2020. — Vol. 370, no. 6523. — P. 1460–1463.

[63] Mathur S., Miller R., Varshavsky A. et al. ProxiMate: proximity-based secure pairing using ambient wireless signals // MobiSys '11 Proceedings of the 9th international conference on Mobile systems, applications, and services. — 2011. — P. 211–224.

[64] Ren Kui, Su Hai, Wang Qian. Secret key generation exploiting channel characteristics in wireless communications // IEEE Wireless Communications. — 2011. — Vol. 18, no. 4. — P. 6–12.

[65] Wells Willard, Stone Russell, Miles Edward. Secure Communications by Optical Homodyne // IEEE J. Sel. Areas Commun. — 1993. — Vol. 11, no. 5. — P. 770–777.

[66] Menders J., Diamond Cornelius, Miles Edward. Interferometric Generation of Random Binary Keys for Secure Optical Communication // Proc. SPIE. — 2001. — Vol. 4471. — P. 208–213.

[67] Wells Willard, Menders Jim, Miles Ed et al. Another Alternative to Quantum Cryptography // Quant. Inform. Processing. — 2002. — Vol. 1, no. 1. — P. 91–106.

[68] Hodara Henri, Miles Edward, Menders James, Wells Willard. Secure Fiberoptic Communications // Fiber and Integrated Optics. — 2003. — Vol. 22, no. 1. — P. 47–61.

[69] Fok Mable P., Wang Zhexing, Deng Yanhua, Prucnal Paul R. Optical Layer Security in Fiber-Optic Networks // IEEE Trans. Inf. Forensics Security. — 2011. — Vol. 6, no. 3. — P. 725–736.

[70] Wu Bernard B., Narimanov Evgenii E. A method for secure communications over a public fiber-optical network // Opt. Express. — 2006. — Vol. 14, no. 9. — P. 3738–3751.

[71] Kravtsov K., Wu B., Glesk I. et al. Stealth Transmission over a WDM Network with Detection Based on an All-Optical Thresholder // Proc. of LEOS 2007. — Lake Buena Vista, FL USA, 2007. — Oct..

[72] Goldberg S., Menendez R.C., Prucnal P.R. Towards a Cryptanalysis of Spectral-Phase Encoded Optical CDMA with Phase-Scrambling // Proc. of OFC/NFOEC 2007 OThJ7. — Anaheim, CA USA, 2007. — Mar.. — P. 1–3.

[73] Hirota Osamu, Katob Kentaro, Shomac Masaki, Usuda Tsuyoshi Sasaki. Quantum key distribution with unconditional security for all optical fiber network // Proc. SPIE. — 2004. — Vol. 5161. — P. 320–331.

[74] Corndorf Eric, Liang Chuang, Kanter Gregory S. et al. Quantum-noise randomized data encryption for wavelength-division-multiplexed fiber-optic networks // Phys. Rev. A. — 2005. — Vol. 71, no. 6. — P. 062326.

[75] Glesk Ivan, Huang Yue-Kai, Brès Camille S., Prucnal Paul R. Design and demonstration of a novel optical CDMA platform for use in avionics applications // Opt. Commun. — 2007. — Vol. 271, no. 1. — P. 65–70.

[76] Kitayama Ken-Ichi, Sasaki Masahide, Araki Soichiro et al. Security in Photonic Networks: Threats and Security Enhancement // J. Lightwav. Technol. — 2011. — Vol. 29, no. 21. — P. 3210–3222.

[77] Liu P.-L. A Key Agreement Protocol Using Band-Limited Random Signals and Feedback // J. Lightwav. Technol. — 2009. — Vol. 27, no. 23. — P. 5230–5234.

[78] Liu P.-L. Key Exchange Using Random Signals and Feedback-Statistical Analysis // J. Lightwav. Technol. — 2010. — Vol. 28, no. 1. — P. 65–70.

[79] Kish L. L., Zhang B., Kish L. B. CRACKING THE LIU KEY EXCHANGE PROTOCOL IN ITS MOST SECURE STATE WITH LORENTZIAN SPECTRA // Fluct. and noise lett. — 2010. — Vol. 9, no. 1. — P. 37–45.

[80] Scheuer Jacob, Yariv Amnon. Giant Fiber Lasers: A New Paradigm for Secure Key Distribution // Phys. Rev. Lett. — 2006. — Vol. 97, no. 14. — P. 140502.

[81] Zadok Avi, Scheuer Jacob, Sendowski Jacob, Yariv Amnon. Secure key generation using an ultra-long fiber laser: transient analysis and experiment // Opt. Express. — 2008. — Vol. 16, no. 21. — P. 16680–16690.

[82] Bar-Lev Doron, Scheuer Jacob. Enhanced key-establishing rates and efficiencies in fiber laser key distribution systems // Phys. Lett. A. — 2009. — Vol. 373. — P. 4287–4296.

[83] LeCong Phung. Secure communication system // U.S. Patent. — Mar. 2, 1993. — no. 5,191,614.

[84] Udd Eric. Secure fiber optic communication system based on the Sagnac interferometer // Proc. SPIE. — 1996. — Vol. 2837. — P. 172–176.

[85] Grosche G., Terra O., Predehl K. et al. Optical frequency transfer via 146 km fiber link with 10^{-19} relative accuracy // Opt. Lett. — 2009. — Vol. 34, no. 15. — P. 2270–2272.

[86] Amemiya Masaki, Imae Michito, Fujii Yasuhisa et al. Precise Frequency Comparison System Using Bidirectional Optical Amplifiers // IEEE Trans. Instr. Meas. — 2010. — Vol. 59, no. 3. — P. 631–640.

[87] Ma Long-Sheng, Jungner P., Ye J., Hall John L. Delivering the same optical frequency at two places: accurate cancellation of phase noise introduced by an optical fiber or other time-varying path // Opt. Lett. — 1994. — Vol. 19, no. 21. — P. 1777–1779.

[88] Foreman Seth M., Ludlow Andrew D., de Miranda Marcio H. G. et al. Coherent Optical Phase Transfer over a 32-km Fiber with 1 s Instability at 10^{-17} // Phys. Rev. Lett. — 2007. — Vol. 99. — P. 153601.

[89] Williams P. A., Swann W. C., Newbury N. R. High-stability transfer of an optical frequency over long fiber-optic links // J. Opt. Soc. Am. B. — 2008. — Vol. 25, no. 8. — P. 1284–1293.

[90] Cho Seok-Beom, Noh Tae-Gon. Stabilization of a long-armed fiber-optic single-photon interferometer // Opt. Express. — 2009. — Vol. 17, no. 21. — P. 19027–19032.

[91] Xavier G. B., von der Weid J. P. Stable single-photon interference in a 1 km fiber-optic Mach-Zehnder interferometer with continuous phase adjustment // Opt. Lett. — 2011. — Vol. 36, no. 10. — P. 1764–1766.

[92] Xavier G.B., da Silva T.R., Tempora G.P., von der Weid J.P. Polarisation drift compensation in 8 km-long Mach-Zehnder fibre-optical interferometer for quantum communication // Electron. Lett. — 2011. — Vol. 47, no. 10. — P. 608–609.

[93] Minář J., de Riedmatten H., Simon C. et al. Phase-noise measurements in long-fiber interferometers for quantum-repeater applications // Phys. Rev. A. — 2008. — Vol. 77, no. 5. — P. 052325.

[94] Babak Azimi-Sadjadi, Aggelos Kiayias, Alejandra Mercado, Bulent Yener. Robust key generation from signal envelopes in wireless networks // CCS '07 Proceedings of the 14th ACM conference on Computer and communications security. — 2007. — P. 401–410.

[95] Coddington I., Swann W. C., Lorini L. et al. Coherent optical link over hundreds of metres and hundreds of terahertz with subfemtosecond timing jitter // Nature Photon. — 2007. — Vol. 1. — P. 283 – 287.

[96] Foreman Seth M., Holman Kevin W., Hudson Darren D. et al. Remote transfer of ultrastable frequency references via fiber networks // Rev. Sci. Instrum. — 2007. — Vol. 78. — P. 021101.

[97] Fung C.-H. F., Qi B., Tamaki K., Lo H.-K. Phase-remapping attack in practical quantum-key-distribution systems // Phys. Rev. A. — 2007. — Vol. 75, no. 3. — P. 032314.

[98] Zhao Y., Fung C.-H. F., Qi B. et al. Quantum hacking: Experimental demonstration of time-shift attack against practical quantum-key-distribution systems // Phys. Rev. A. — 2008. — Vol. 78, no. 4. — P. 042333.

[99] Xu F., Qi B., Lo H.-K. Experimental demonstration of phase-remapping attack in a practical quantum key distribution system // New J. Phys. — 2010. — Vol. 12, no. 11. — P. 113026.

[100] Lydersen Lars, Wiechers Carlos, Wittmann Christoffer et al. Hacking commercial quantum cryptography systems by tailored bright illumination // Nature Photon. — 2010. — Vol. 4, no. 10. — P. 686–689.

[101] Patwari Neal, Croft Jessica, Jana Suman, Kasera Sneha Kumar. High-Rate Uncorrelated Bit Extraction for Shared Secret Key Generation from Channel Measurements // IEEE Trans. Mobile Computing. — 2010. — Vol. 9, no. 1. — P. 17–30.

[102] Ye C., Mathur S., Reznik A. et al. Information-Theoretically Secret Key Generation for Fading Wireless Channels // IEEE Trans. Inf. Forensics Security. — 2010. — Vol. 5, no. 2. — P. 240–254.

[103] Brassard Gilles, Salvail Louis. Secret-key reconciliation by public discussion // EUROCRYPT '93: Workshop on the theory and application of cryptographic techniques on Advances in cryptology. — Secaucus, NJ, USA, 1994. — P. 410–423.

[104] Gallager R. Low-density parity-check codes // IRE Transactions on Information Theory. — 1962. — Vol. 8, no. 1. — P. 21–28.

[105] Sasaki M., Fujiwara M., Ishizuka H. et al. Field test of quantum key distribution in the Tokyo QKD Network // Opt. Express. — 2011. — May. — Vol. 19, no. 11. — P. 10387–10409.

[106] Fraser A. M., Swinney H. L. Independent coordinates or strange attractors from mutual information // Phys. Rev. A. — 1986. — Vol. 33, no. 2. — P. 1134–1140.

[107] Kraskov A., Stögbauer H., Grassberger P. Estimating mutual information // Phys. Rev. E. — 2004. — Vol. 69. — P. 066138.

[108] Keskin Onur, Jolissaint Laurent, Bradley Colin. Hot-air optical turbulence generator for the testing of adaptive optics systems: principles and characterization // Applied Optics. — 2006. — Vol. 45, no. 20. — P. 4888–4897.

[109] 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.

[110] Bolduc Eliot, Bent Nicolas, Santamato Enrico et al. Exact solution to simultaneous intensity and phase encryption with a single phase-only hologram // Opt. Lett. — 2013. — Vol. 38, no. 18. — P. 3546–3549.

[111] Strohbehn J. W. Laser Beam Propagation in the Atmosphere. — Berlin; Heidelberg; New York : Springer-Verlag, 1978.

[112] Vasylyev D. Yu., Semenov A. A., Vogel W. Toward Global Quantum Communication: Beam Wandering Preserves Nonclassicality // Phys. Rev. Lett. — 2012. — Vol. 108. — P. 220501.

[113] Vasylyev D., Semenov A. A., Vogel W. Atmospheric Quantum Channels with Weak and Strong Turbulence // Phys. Rev. Lett. — 2016. — Vol. 117. — P. 090501.

[114] Vasylyev D., Semenov A. A., Vogel W. et al. Free-space quantum links under diverse weather conditions // Phys. Rev. A. — 2017. — Vol. 96. — P. 043856.

[115] Vasylyev D., Vogel W., Semenov A. A. Theory of atmospheric quantum channels based on the law of total probability // Phys. Rev. A. — 2018. — Vol. 97. — P. 063852.

[116] Young David W., Sluz Joseph E., Juarez Juan C. et al. Demonstration of High Data Rate Wavelength Division Multiplexed Transmission over a 150 km Free Space Optical Link // Military Communications Conference, (MILCOM 2007). — Orlando, FL, USA, 2007. — Oct..

[117] Krenn Mario, Handsteiner Johannes, Fink Matthias et al. Twisted light transmission over 143 km // PNAS. — 2016. — Vol. 113, no. 48. — P. 13648–13653.

[118] Wang Jian, Yang Jeng-Yuan, Fazal Irfan M. et al. Terabit free-space data transmission employing orbital angular momentum multiplexing // Nature Photon. — 2012. — Vol. 6, no. 7. — P. 488–496.

[119] Nicolas A., Veissier L., Giner L. et al. A quantum memory for orbital angular momentum photonic qubits // Nature Photon. — 2014. — Vol. 8, no. 3. — P. 234–238.

[120] Mirhosseini Mohammad, Magana-Loaiza Omar S, O'Sullivan Malcolm N et al. High-dimensional quantum cryptography with twisted light // New J. Phys. — 2015. — Vol. 17. — P. 033033.

[121] Sit Alicia, Bouchard Frederic, Fickler Robert et al. High-dimensional intracity quantum cryptography with structured photons // Optica. — 2017. — Vol. 4, no. 9. — P. 1006–1010.

[122] Krenn Mario, Handsteiner Johannes, Fink Matthias et al. Twisted photon entanglement through turbulent air across Vienna // PNAS. — 2015. — Vol. 112, no. 46. — P. 14197–14201.

[123] Колмогоров А. Н. Рассеяние энергии при локально изотропной турбулентности // Докл. АН СССР. — 1941. — Vol. 32. — P. 19–21.

[124] 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.

[125] Borgnino Julien, Martin Francois, Ziad Aziz. Effect of a finite spatial-coherence outer scale on the covariances of angle-of-arrival fluctuations // Opt. Commun. — 1992. — Vol. 91, no. 3-4. — P. 267–279.

[126] Danakas Sotiris, Aravind P. K. Analogies between 2 optical-systems (photon-beam splitters and laser-beams) and 2 quantum-systems (the 2-dimensional oscillator and the 2-dimensional hydrogen-atom) // Phys. Rev. A. — 1992. — Vol. 45, no. 3. — P. 1973–1977.

[127] Irbah A., Borgnino J., Djafer D. et al. Solar seeing monitor MISOLFA: A new method for estimating atmospheric turbulence parameters // Astronomy & Astrophysics. — 2016. — Vol. 591. — P. A150.

[128] Arimoto Y. Multi-Gigabit Free-Space Laser Communications Using Compact Optical Terminal with Bidirectional Beacon Tracking // IEEE International Conference on Communications, (ICC 2007). — Kyoto, Japan, 2007. — Jun..

[129] Arimoto Yoshinori. Operational condition for direct single-mode-fiber coupled free-space optical terminal under strong atmospheric turbulence // Opt. Engineering. — 2012. — Vol. 51, no. 3. — P. 031203.

[130] Wootters William K., Fields Brian D. Optimal state-determination by mutually unbiased measurements // Annals of Physics. — 1989. — May. — Vol. 191, no. 2. — P. 363–381.

[131] James Daniel F. V., Kwiat Paul G., Munro William J., White Andrew G. Measurement of qubits // Phys. Rev. A. — 2001. — Oct. — Vol. 64. — P. 052312.

[132] Řeháček Jaroslav, Englert Berthold-Georg, Kaszlikowski Dagomir. Minimal qubit tomography // Phys. Rev. A. — 2004. — Nov. — Vol. 70. — P. 052321.

[133] Mair Alois, Vaziri Alipasha, Weihs Gregor, Zeilinger Anton. Entanglement of the orbital angular momentum states of photons // Nature. — 2001. — Jul.. — Vol. 412, no. 6844. — P. 313–316.

[134] Leach Jonathan, Padgett Miles J., Barnett Stephen M. et al. Measuring the Orbital Angular Momentum of a Single Photon // Phys. Rev. Lett. — 2002. — Jun. — Vol. 88. — P. 257901.

[135] Molina-Terriza Gabriel, Torres Juan P., Torner Lluis. Twisted photons // Nature Physics. — 2007. — May. — Vol. 3, no. 5. — P. 305–310.

[136] Struchalin G. I., Kovlakov E. V., Straupe S. S., Kulik S. P. Adaptive quantum tomography of high-dimensional bipartite systems // Phys. Rev. A. — 2018. — Sep. — Vol. 98. — P. 032330.

[137] Berkhout Gregorius C. G., Lavery Martin P. J., Courtial Johannes et al. Efficient Sorting of Orbital Angular Momentum States of Light // Phys. Rev. Lett. — 2010. — Oct. — Vol. 105. — P. 153601.

[138] Huang Hao, Milione Giovanni, Lavery Martin P. J. et al. Mode division multiplexing using an orbital angular momentum mode sorter and MIMO-DSP over a graded-index few-mode optical fibre // Scientific Reports. — 2015. — Oct.. — Vol. 5, no. 1. — P. 14931.

[139] Ruffato Gianluca, Girardi Marcello, Massari Michele et al. A compact diffractive sorter for high-resolution demultiplexing of orbital angular momentum beams // Scientific Reports. — 2018. — Jul.. — Vol. 8, no. 1. — P. 10248.

[140] Fontaine Nicolas K., Ryf Roland, Chen Haoshuo et al. Laguerre-Gaussian mode sorter // Nature Commun. — 2019. — Vol. 10, no. 1. — P. 1865.

[141] Molina-Terriza G., Vaziri A., Řeháček J. et al. Triggered Qutrits for Quantum Communication Protocols // Phys. Rev. Lett. — 2004. — Apr. — Vol. 92. — P. 167903.

[142] Bent N., Qassim H., Tahir A. A. et al. Experimental Realization of Quantum Tomography of Photonic Qudits via Symmetric Informationally Complete Positive Operator-Valued Measures // Phys. Rev. X. — 2015. — Oct. — Vol. 5. — P. 041006.

[143] Straupe Stanislav S. Adaptive quantum tomography // JETP Lett. — 2016. — Vol. 104, no. 7. — P. 510–522.

[144] Ferrie Christopher. Self-Guided Quantum Tomography // Phys. Rev. Lett. — 2014. — Nov. — Vol. 113. — P. 190404.

[145] Ahn D., Teo Y. S., Jeong H. et al. Adaptive Compressive Tomography with No a priori Information // Phys. Rev. Lett. — 2019. — Mar. — Vol. 122. — P. 100404.

[146] Palmieri Adriano Macarone, Kovlakov Egor, Bianchi Federico et al. Experimental neural network enhanced quantum tomography // npj Quantum Information. — 2020. — feb. — Vol. 6, no. 1. — P. 20.

[147] Huang Hsin-Yuan, Kueng Richard, Preskill John. Predicting many properties of a quantum system from very few measurements // Nature Physics. — 2020. — jun.

[148] Lundeen J. S., Feito A., Coldenstrodt-Ronge H. et al. Tomography of quantum detectors // Nature Physics. — 2008. — Nov.. — Vol. 5, no. 1. — P. 27–30.

[149] Bobrov I. B., Kovlakov E. V., Markov A. A. et al. Tomography of spatial mode detectors // Opt. Express. — 2015. — Jan. — Vol. 23, no. 2. — P. 649–654.

[150] Gilchrist Alexei, Terno Daniel R., Wood Christopher J. Vectorization of quantum operations and its use. — 2009. — arXiv:0911.2539 [quant-ph].

[151] Wood Christopher James. Initialization and Characterization of Open Quantum Systems : Ph. D. thesis / Christopher James Wood ; University of Waterloo. — Waterloo, Ontario, Canada, 2015.

[152] Życzkowski Karol, Sommers Hans-Jürgen. Average fidelity between random quantum states // Phys. Rev. A. — 2005. — Mar. — Vol. 71. — P. 032313.

[153] Andersen Geoff, Gelsinger-Austin Paul, Gaddipati Ravi et al. Fast, compact, autonomous holographic adaptive optics // Opt. Express. — 2014. — Apr. — Vol. 22, no. 8. — P. 9432–9441.

[154] Zhang Christian C., Foster Warren B., Downey Ryan D. et al. Dynamic performance of MEMS deformable mirrors for use in an active/adaptive two-photon microscope // Adaptive Optics and Wavefront Control for Biological Systems II / Ed. by Thomas G. Bifano, Joel Kubby, Sylvain Gigan. — SPIE, 2016. — Mar..

[155] 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.

[156] Christandl Matthias, Renner Renato, Ekert Artur. A Generic Security Proof for Quantum Key Distribution // arXiv. — 2004. — arXiv:quant-ph/0402131.

[157] Vincent C. H. The generation of truly random binary numbers // J. Phys. E: Sci. Instr. — 1970. — Vol. 3. — P. 594–598.

[158] Jennewein Thomas, Achleitner Ulrich, Weihs Gregor et al. A fast and compact quantum random number generator // Rev. Sci. Instrum. — 2000. — Vol. 71, no. 4. — P. 1675–1680.

[159] Stefanov Andre, Gisin Nicolas, Guinnard Olivier et al. Optical quantum random number generator // J. Mod. Opt. — 2000. — Vol. 47, no. 4. — P. 595–598.

[160] Fiorentino M., Santori C., Spillane S. M. et al. Secure self-calibrating quantum random-bit generator // Phys. Rev. A. — 2007. — Vol. 75. — P. 032334.

[161] Dynes J. F., Yuan Z. L., Sharpe A. W., Shields A. J. A high speed, postprocessing free, quantum random number generator // Appl. Phys. Lett. — 2008. — Vol. 93. — P. 031109.

[162] Wayne Michael A., Jeffrey Evan R., Akselrod Gleb M., Kwiat Paul G. Photon arrival time quantum random number generation // J. Mod. Opt. — 2009. — Vol. 56, no. 4. — P. 516–522.

[163] Kanter Ido, Aviad Yaara, Reidler Igor et al. An optical ultrafast random bit generator // Nature Photon. — 2010. — Vol. 4. — P. 58–61.

[164] Gabriel Christian, Wittmann Christoffer, Sych Denis et al. A generator for unique quantum random numbers based on vacuum states // Nature Photon. — 2010. — Vol. 4. — P. 711–715.

[165] Wahl Michael, Leifgen Matthias, Berlin Michael et al. An ultrafast quantum random number generator with provably bounded output bias based on photon arrival time measurements // Appl. Phys. Lett. — 2011. — Vol. 98. — P. 171105.

[166] Sanguinetti Bruno, Martin Anthony, Zbinden Hugo, Gisin Nicolas. Quantum random number generation on a mobile phone // Phys. Rev. X. — 2014. — Vol. 4. — P. 031056.

[167] Nie You-Qi, Zhang Hong-Fei, Zhang Zhen et al. Practical and fast quantum random number generation based on photon arrival time relative to external reference // Appl. Phys. Lett. — 2014. — Vol. 104. — P. 051110.

[168] Lutkenhaus Norbert, Cohen Jayson L., Lo Hoi-Kwong. Efficient use of detectors for random number generation // U.S. Patent No. 7,197,523. — Mar. 27, 2007. — no. 7,197,523.

[169] Wayne Michael A., Kwiat Paul G. Low-bias high-speed quantum random number generator via shaped optical pulses // Opt. Express. — 2010. — Vol. 18, no. 9. — P. 9351–9357.

[170] Fürst Martin, Weier Henning, Nauerth Sebastian et al. High speed optical quantum random number generation // Opt. Express. — 2010. — Vol. 18, no. 12. — P. 13029–13037.

[171] Heyman Daniel P., Sobel Matthew J. Stochastic Models in Operations Research: Stochastic Processes and Operating Characteristics. — Mineola, NY, USA : Dover Publications, 2004. — P. 158.

[172] Trevisan Luca. Extractors and pseudorandom generators // Journal of the ACM. — 2001. — Vol. 48, no. 4. — P. 860–879.

[173] Ma Xiongfeng, Xu Feihu, Xu He et al. Postprocessing for quantum random-number generators: Entropy evaluation and randomness extraction // Phys. Rev. A. — 2013. — Vol. 87. — P. 062327.

[174] Mauerer Wolfgang, Portmann Christopher, Scholz Volkher B. A modular framework for randomness extraction based on Trevisan's construction. — 2012. — arXiv:1212.0520 [cs.IT].

[175] von Neumann J. Various techniques used in connection with random digits. Monte Carlo Method. // Applied Mathematics Series, U.S. National Bureau of Standards, No. 12. — 1951. — no. 12. — P. 36–38.

[176] Elias Peter. The Efficient Construction of an Unbiased Random Sequence // Ann. Math. Statist. — 1972. — Vol. 43, no. 3. — P. 865–870.

[177] Peres Yuval. Iterating von Neumann's procedure for extracting random bits // Ann. Statistics. — 1992. — Vol. 20, no. 1. — P. 590–597.

[178] Juels Ari, Jakobsson Markus, Shriver Elizabeth, Hillyer Bruce K. How to Turn Loaded Dice into Fair Coins // IEEE Trans. Inform. Theory. — 2000. — Vol. 46, no. 3. — P. 911–921.

[179] NIST Statistical Test Suite. — https://csrc.nist.gov/projects/random-bit-generation/documentation-and-software. — 2010. — Accessed: 2022-02-20.

[180] Shor Peter W., Preskill John. Simple Proof of Security of the BB84 Quantum Key Distribution Protocol // Phys. Rev. Lett. — 2000. — Vol. 85, no. 2. — P. 441–444.

[181] Tomamichel Marco, Lim Charles Ci Wen, Gisin Nicolas, Renner Renato. Tight finite-key analysis for quantum cryptography // Nature Commun. — 2012. — Vol. 3. — P. 634.

[182] Chefles A., Barnett S. M. Optimum unambiguous discrimination between linearly independent symmetric states // Phys. Lett. A. — 1998. — Vol. 250. — P. 223–229.

[183] Chefles Anthony. Quantum state discrimination // Contemporary Physics. — 2000. — Vol. 41, no. 6. — P. 401–424.

[184] Dusek Miloslav, Jahma Mika, Lutkenhaus Norbert. Unambiguous state discrimination in quantum cryptography with weak coherent states // Phys. Rev. A. — 2000. — Vol. 62. — P. 022306.

[185] Peres Asher. How to differentiate between non-orthogonal states // Phys. Lett. A. — 1988. — Vol. 128. — P. 19.

[186] Stucki Damien, Brunner Nicolas, Gisin Nicolas et al. Fast and simple one-way quantum key distribution // Appl. Phys. Lett. — 2005. — Vol. 87. — P. 194108.

[187] Inoue K., Waks E., Yamamoto Y. Differential-phase-shift quantum key distribution using coherent light // Phys. Rev. A. — 2003. — Vol. 68, no. 2. — P. 022317.

[188] Hwang W. Y. Quantum Key Distribution with High Loss: Toward Global Secure Communication // Phys. Rev. Lett. — 2003. — Vol. 91, no. 5. — P. 057901.

[189] Wang X. B. Beating the Photon-Number-Splitting Attack in Practical Quantum Cryptography // Phys. Rev. Lett. — 2005. — Vol. 94, no. 23. — P. 230503.

[190] Goldenberg L., Vaidman L. Quantum Cryptography Based on Orthogonal States // Phys. Rev. Lett. — 1995. — Vol. 75, no. 7. — P. 1239–1243.

[191] Bennett C. H. Quantum cryptography using any two nonorthogonal states // Phys. Rev. Lett. — 1992. — Vol. 68, no. 21. — P. 3121–3124.

[192] Molotkov S. N. On the resistance of relativistic quantum cryptography in open space at finite resources // JETP Lett. — 2012. — Vol. 96, no. 5. — P. 342–348.

[193] Холево А. С. Некоторые оценки для количества информации, передаваемого квантовым каналом связи // Пробл. передачи информ. — 1973. — Vol. 9, no. 3. — P. 3–11.

[194] Холево А. С. Квантовые теоремы кодирования // УМН. — 1998. — Vol. 53, no. 6. — P. 193–230.

[195] Peres A. Quantum Cryptography with Orthogonal States? // Phys. Rev. Lett. — 1996. — Vol. 77, no. 15. — P. 3264.

[196] Goldenberg L., Vaidman L. Goldenberg and Vaidman Reply // Phys. Rev. Lett. — 1996. — Vol. 77, no. 15. — P. 3265.

[197] Koashi Masato, Imoto Nobuyuki. Quantum Cryptography Based on Split Transmission of One-Bit Information in Two Steps // Phys. Rev. Lett. — 1997. — Vol. 79, no. 12. — P. 2383–2386.

[198] Avella Alessio, Brida Giorgio, Degiovanni Ivo Pietro et al. Experimental quantum cryptography scheme based on orthogonal states // Phys. Rev. A. — 2010. — Vol. 82. — P. 062309.

[199] Xavier G. B., Temporao G. P., von der Weid J. P. Employing long fibre-optical Mach-Zehnder interferometers for quantum cryptography with orthogonal states // Electron. Lett. — 2012. — Vol. 48, no. 13. — P. 775–777.

[200] Молотков С. Н. Релятивистская квантовая криптография // ЖЭТФ. — 2011. — Vol. 139, no. 3. — P. 429–439.

[201] Молотков С. Н. Релятивисткая квантовая криптография для открытого пространства без синхронизации часов на приемной и передающей стороне // Письма в ЖЭТФ. — 2011. — Vol. 94, no. 6. — P. 504–512.

[202] Молотков С. Н. О стойкости релятивистской квантовой криптографии в открытом пространстве при конечных ресурсах // Письма в ЖЭТФ. — 2012. — Vol. 96, no. 5. — P. 374–380.

[203] Кравцов К.С., Радченко И.В., Корольков А.В. et al. О двухпроходной схеме без фарадеевского зеркала для релятивистской квантовой криптографии в открытом пространстве // ЖЭТФ. — 2013. — Vol. 143, no. 5. — P. 820–830.

[204] Poletti F., Wheeler N. V., Petrovich M. N. et al. Towards high-capacity fibre-optic communications at the speed of light in vacuum // Nature Photon. — 2013. — Vol. 7. — P. 279.

[205] Молотков С. Н., Тимофеев А. В. Явная атака на ключ в квантовой криптографии (протокол BB84), достигающая теоретического предела ошибки Qc = 11% // Письма в ЖЭТФ. — 2007. — May. — Vol. 85, no. 10. — P. 632–637.

[206] Pirandola Stefano. Symmetric collective attacks for the eavesdropping of symmetric quantum key distribution // Int. J. Quant. Inf. — 2008. — Vol. 6, no. supp01. — P. 765–771.

[207] Fuchs Christopher A., Gisin Nicolas, Griffiths Robert B. et al. Optimal eavesdropping in quantum cryptography. I. Information bound and optimal strategy // Phys. Rev. A. — 1997. — Aug. — Vol. 56. — P. 1163–1172.

[208] Renner Renato. Security of Quantum Key Distribution : Ph. D. thesis / Renato Renner ; Swiss federal institute of technology, Zurich. — 2005. — 9.

[209] Huttner B., Imoto N., Gisin N., Mor T. Quantum cryptography with coherent states // Phys. Rev. A. — 1995. — mar. — Vol. 51, no. 3. — P. 1863–1869.

[210] Brassard Gilles, Lutkenhaus Norbert, Mor Tal, Sanders Barry C. Limitations on Practical Quantum Cryptography // Phys. Rev. Lett. — 2000. — aug. — Vol. 85, no. 6. — P. 1330–1333.

[211] 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.

[212] Acín Antonio, Gisin Nicolas, Scarani Valerio. Coherent-pulse implementations of quantum cryptography protocols resistant to photon-number-splitting attacks // Phys. Rev. A. — 2004. — Jan. — Vol. 69. — P. 012309.

[213] Chefles Anthony. Unambiguous discrimination between linearly independent quantum states // Phys. Lett. A. — 1998. — mar. — Vol. 239, no. 6. — P. 339–347.

[214] Chefles Anthony. Unambiguous discrimination between linearly dependent states with multiple copies // Phys. Rev. A. — 2001. — Nov. — Vol. 64. — P. 062305.

[215] Ma Xiongfeng, Qi Bing, Zhao Yi, Lo Hoi-Kwong. Practical decoy state for quantum key distribution // Phys. Rev. A. — 2005. — Jul. — Vol. 72. — P. 012326.

[216] Lo Hoi-Kwong, Ma Xiongfeng, Chen Kai. Decoy State Quantum Key Distribution // Phys. Rev. Lett. — 2005. — Vol. 94, no. 23. — P. 230504.

[217] Chen L., Jordan S., Liu Y.-K. et al. Report on Post-Quantum Cryptography // NIST Tech. Rep. — 2016. — Apr. — Vol. 8105.

[218] Mavroeidis Vasileios, Vishi Kamer, Zych Mateusz D., Jøsang Audun. The Impact of Quantum Computing on Present Cryptography // International Journal of Advanced Computer Science and Applications. — 2018. — Vol. 9, no. 3. — P. 405–414.