Фадеев Максим Алексеевич
Fadeev Maxim Alekseevich

Гетеродинный прием сигналов в системе квантового распределения ключей на боковых частотах с применением оптической инжекции

Heterodyne detection of signals in a subcarrier-wave quantum key distribution system using optical injection

Оглавление

Реферат

Общая характеристика диссертации

Актуальность темы

Квантовое распределения ключа (КРК) - актуальная технология, развившаяся из теории квантовой информатики, позволяющая распределить симметричную битовую последовательность с помощью квантовых методов у двух и более пользователей для использования этой последовательности в качестве ключа для симметричного шифрования данных и одновременным обнаружением несанкционированного доступа со стороны нелегитимных пользователей. Использование квантовых состояний света при распределении ключа позволяет достичь уровня секретности, недоступного для классических протоколов шифрования. Такие квантовые состояния могут быть представлены в виде одиночных фотонов. Их квантовые свойства не позволяют злоумышленнику скопировать их состояния или считать их без изменения и без внесения ошибок. Такие квантовые состояния возможно передавать как по волоконно-оптическим линиям связи (ВОЛС), как по атмосферным каналам, так и в космическом пространстве с помощью спутников. Принцип работы данных систем следующий. На стороне передатчика (Алиса) формируются квантовые состояния. Для этого используется когерентное лазерное излучение, ослабленное до одиночных фотонов с помощью аттенюатора. В подготовленные кванты света вносится изменение в поляризацию или фазовый свдиг фотона. Подготовленное таким образом состояние передается по каналу связи к приемнику (Боб). На приемной стороне происходит независимое от Алисы повторное измерение состояния фотона. В случае корреляции у Боба принятый одиночный фотон регистрируется детектором одиночных фотонов. Благодаря свойствам одиночного фотона в виде невозможности клонирования, невозможности из-

мерения без разрушения и его неделимости возможно отследить воздействие злоумышленника, так как его действия будут приводить к появлению ошибок в полученной битовой последовательности. Так обеспечивается контроль несанкционированного допуска.

Отдельным классом выделяются системы квантового распределения ключа на непрерывных переменных (КРКНП). В таких системах квантовое состояние, подготовленное и переданное Алисой, на приемной стороне взаимодействует с сильным лазерным излучением. И результат этого взаимодействия регистрируется балансным детектором. Основными отличиями данного детектора от детектора одиночных фотонов является использование двух классических фотоприемников, подключенных таким образом, что их фототоки взаимно вычитаются, что позволяет уменьшить шум системы, и отстуствие охлаждения до температур порядка -40 ° градусов Цельсия. Все это позволяет упростить конечную систему. К преимуществам КРКНП можно отнести большую скорость выработки секретного ключа по сравнению с системами КРК на дискретных переменных, в которых применяются детекторы одиночных фотонов.

Среди сложностей систем КРКНП выделяется способ передачи сильного лазерного излучения или локального осциллятора (ЛО) на приемную сторону и его разделения с квантовым сигналом. В первых системах КРКНП с Гауссовой модуляцией Локальный осциллятор и квантовые состояния генерировались у передатчика, объединялись и передавались совместно в квантовый канал. На приемной стороне локальный осциллятор и квантовый сигнал разделяются, ЛО задерживается специальной линией задержки и снова соединяются на светоделителе для взаимодействия. Результатом этого взаимодействия является интерфереционная картина, распределение интенсивности которой зависит от закодированного Алисой состояния. Полученное поле регистрируется балансным детектором, на выходе такого формируется уровень напряжения, который в дальнейшем подвергается пост-обработке. Передача локального осциллятора через канал ограничивает дальность работы системы такого типа и ограничивает скорость выработки ключа, так как для лучшей работы системы необходим ЛО как можно большей мощности. Второй проблемой является возможности

злоумышленника манипулировать локальным осциллятором для создания каналов утечки информации. В качестве альтернативы предлагается использовать локальный осциллятор, сгенерированный на приемной стороне. Такое решение позволит увеличить дальность передачи ключа, скорость его выработки и закрыть уявзимость к атаке на ЛО.

Одним из перспективных подходов к реализации систем квантовой коммуникации на непрерывных переменных является система квантовой коммуникации на боковых частотах модулированного излучения. В основе данного метода лежит вынесение квантового канала на боковые частоты, которые появляются в результате модуляции оптического излучения переменным электрическим полем. Благодаря этому повышается устойчивость передаваемого сигнала ко внешним воздействиями и обеспечивается высокая спектральная эффективность, а также обеспечивается показатели по отношению скорости выработки ключа к дальности между блоками приемника и передатчика, сравнимые с другими системами квантовой коммуникации. Данный метод подходит и для реализации протоколов на непрерывных переменных с когерентными методами детектирования. В частности, в данной работе рассматривается гетеродинный метод, при котором квантовые состояния, подготовленные Алисой, передаются по волоконной линии связи к приемнику, в нем попадают на светоделитель с формулой 2x2 и коэффициентом деления 50:50 и смешиваются на нем с мощным локальным осциллятором, который отстроен по частоте от передающего лазера на величину, которая превышает частоту смены состояний. Результат интерференции регистрируется балансным детектором. На выходе балансного детектора формируется сигнал на промежуточной частоте от всего спектра сигнала, переданного Алисой. Для извлечения инфорамции требуется провести фильтрацию с помощью фильтра низких частот и демодуляцию полученного сигнала для генерации сырого ключа.

Одной из проблем при реализации гетеродинного метода детектирования для распределения ключа является необходимость компенсации фазовых шумов. Для этого применяют различные методы. Первым из таких методов является передача "пилотного"импульса, при детектировании которого измеряется

фазовый шум, внесенный каналом. После этого измеренное значение учитывается в постобработке состояний. Второе - это реализация обратной связи в различных формах. В рамках данной работы предлагается использовать метод оптической обратной связи для системы квантового распределения ключа на боковых частотах на непрерывных переменных. Суть данного метода заключается в инжекции лазерного излучения от ведущего лазера, который является лазером передатчика, в лазер ведомый, который используется в качестве локального осциллятора в приемнике. Данный метод позволяет стабилизировать длину волны ЛО и уменьшить фазовые шумы из-за того, что оба источника являются генераторами когеретного излучения со случайной фазой.

Метод оптической инжекции требует дополнительного канала для передачи создания обратной связи. Такой канал усложняет систему и повышает требования к волоконно-оптической линии связи (ВОЛС), что особенно критично в городских линиях связи, где выделение дополнительного волокна или канала в сетях с мультиплексированием затруднительно. Решением данной проблемы может являтся система квантового распределения ключа на непрерывных переменных с применением гетеродинного детектирования с независимым ЛО. Суть данной системы заключается в том, что на приемнике и передатичке установленны лазеры со стабилизацией длины волны и со шириной спектральной линии менее 10 кГц. Такой подход позволяет не прибегать к постоянной подстройке длин волн лазеров и уменьшить фазовый шум, связанный с независимостью источников излучения. Однако, фазовый шум при этом не исчезает, поэтому его все еще необходимо компенсировать. В случае реализации такого метода детектирования сигналов для протокола квантового распределения ключа на боковых частотах для этого можно использовать несущую частоту, измеряя ее фазу и внося корректировки в постобработке.

Отличия реальных систем КРК от моделей, используемых для теориетических доказательств, могут быть использованы злоумышленником для проведения различных типов атак на оборудование, входящее в состав системы. В работах ранее было показано, что источники лазерного излучения на основе полупроводниковых кристаллов могут быть уязвимы к "засеву"внешним

излучением злоумышленника на длине волны близкой к той, что использует передатчик. В результате этой атаки изменяется форма излучаемого импульса и увеличивается выходная мощность, в отдельных случаях можно наблюдать и изменение длины волны. Эти эффекты приводят к увеличению среднего числа фотонов, излучаемых передатчиком, что открывает возможность для злоумышленника атаки с расщеплением числа фотонов.

Однако в литературе не рассматривались атака "засевом"лазерным излучением на других длинах волн. Атака такого типа опаснее тем, что для защиты от нее используются пассивные волоконно-оптические элементы, вносящие дополнительное затухание, например изоляторы или DWDM фильтры. Но существуют работы, которые демонстрируют, что величина затухания в таких элементах может уменьшаться при существенном изменении падающей длины волны излучения. Например, изолятор с рабочей длиной волны 1550 нм вносит 50 дБ потерь при обратном прохождении, когда при облучении излучением на длине волны 1310 нм эта величина составляет 20 дБ. А в случае с DWDM фильтром, он практически не вносит затухание на длине волны 1310 нм. Таким образом, злоумышленнику гораздо проще осуществить атаку "засевом"лазерным излучением, так как на данной длине волны вносимое затухание меньше.

Такой тип атаки носит название "атака оптической накачкой". Ее суть заключается в том, что злоумышленник зондирует лазер длиной волны, отличной от рабочей. При этом это излучение поглащается активной средной лазера передатчика так, что поглощенное излучение выступает в роли оптической накачки, которая работает как дополнение к электрической накачки полупроводникового лазера. В этом случае изменяется Ватт-Амперная характеристика лазера и его квантовая эффективность. Это приводит к тому, что изменяется энергия излученных импульсов увеличивается при неизменной величине тока накачки. В рамках данной работы впервые обозначен данный тип атаки, определена нижняя граница необходимой мощности излучения на длние волны 1310 нм для изменения характеристик изучаемого лазера и измерено влияние оптической накачки на характеристики лазера.

В системах квантового распределения применяются источники лазерного излучения на основе оптической инжекции. Такие источники построены следующим образом: применяются два лазера - ведущий и ведомый, соединенных циркулятором. Излучение ведомого лазера позволяет снизить дрожание излучаемых импульсов, стабилизировать мощность выходного излучения и сузить спектральную линию. Однако такие источники не исследовались на устойчивость ко внешнему излучению. Ранее показанные работы по лазерному "засеву"были проведены только для одиночных источников излучения. Источник, построенный на основе оптической инжекции, имеет несколько преимуещств относительного одиночного: наличие изоляции от квантового канала за счет оптического циркулятора и наличие внешнего излучения ведущего лазера. В рамках данной работы изучается влияние мощного лазерного излучения на длительность, дрожание и амплитуду излучаемых импульсов , продемонстрирована нижняя граница мощности излучения необходимого для внесения изменений в работу данной системы.

Цель

(научная концепция; новая научная идея, обогащающая научную концепцию, новая экспериментальная методика, позволившая выявить качественно новые закономерности исследуемого явления, повысить точность измерений с расширением границ применимости полученных результатов и т.п.)

Задачи

Задача 1 анализ обзор (сравнение авторских данных и данных, полученных ранее по рассматриваемой тематике)

Задача 2 по построению классификации методов исследования, методики проведения эксперимента, .

(комплекс существующих базовых методов исследования, в т.ч. численных методов, экспериментальных методик и т.п.)

Задача 3 по дизайну эксперимента

(современные методики сбора и обработки исходной информации, представительные выборочные совокупности с обоснованием подбора объектов (единиц) наблюдения и измерения и т.п.)

Задача 4 - разработка экспериментальной установки, стенда, программы и т.п.

(результаты получены на сертифицированном оборудовании, обоснованы калибровки, показана воспроизводимость результатов исследования в различных условиях и т.п.)

Задача 5 по обработке результатов эксперимента

(сравнение авторских данных и данных, полученных ранее по рассматриваемой тематике)

Задача 6 по разработке рекомендаций

(модель эффективного применения знаний, система практических рекомендаций и т.п.)

Методы исследования

(на анализе практики, обобщении передового опыта и т.п.)

Основные положения, выносимые на защиту

(положения, идеи, аргументы, доказательства, элементы теории, аксиомы, гипотезы, факты, этапы, тенденции, стадии, факторы, условия и т.п.)

Научная новизна

Научная новизна 1 - основной результат позволяющий достичь заявленную цель
(теоремы, леммы, положения, методики, вносящие вклад в расширение представлений об изучаемом явлении, расширяющие границы применимости полученных результатов, и т.п.)

Научная новизна 2 (существенные проявления теории: противоречия, несоответствия; выявление новых проблем и т.п.)

Научная новизна 3 (связи данного явления с другими, генезис процесса, внутренние и внешние противоречия, факторы, причинно-следственные связи и т.п.)

Научно-техническая задача

Объект исследования

Предмет исследования

(существующих математических моделей, алгоритмов и/или численных методов, обеспечивающих получение новых результатов по теме диссертации, и т.п.)

Теоретическая значимость

(перспективность использования новых идей в науке, в практике, наличие закономерностей, неизвестных связей, зависимостей и т.п.)

Практическая значимость

(пределы и перспективы практического использования теории на практике и т.п.)

(модель эффективного применения знаний, система практических рекомендаций и т.п.)

Определение новых терминов и понятий

(новые понятия, измененные трактовки старых понятий, новые термины и т.п.)

Достоверность

(построена на известных, проверяемых данных, фактах, в т.ч. для предельных случаев, согласуется с опубликованными экспериментальными данными по теме диссертации или по смежным отраслям и т.п.)

Внедрение результатов работы

(указать степень внедрения) (технологии, новые универсальные методики измерений, образовательные технологии, и т.п.)

Апробация результатов работы

Личный вклад автора

(включенное участие соискателя на всех этапах процесса, непосредственное участие соискателя в получении исходных данных и научных экспериментах, личное участие соискателя в апробации результатов исследования, разработка экспериментальных стендов и установок (ключевых элементов эксперимен-

тальных установок), выполненных лично автором или при участии автора, обработка и интерпретация экспериментальных данных, выполненных лично автором или при участии автора, подготовка основных публикаций по выполненной работе и т.п.)

Структура и объем диссертации

Публикации

Основные результаты по теме диссертации изложены в 9 публикациях. Из них 4 изданы в журналах, рекомендованных ВАК, 1 опубликована в изданиях, индексируемых в базе цитирования Scopus. Также имеется 1 свидетельство о государственной регистрации программ для ЭВМ.

В международных изданиях, индексируемых в базе данных Scopus:

1.
2.
3.

В изданиях из перечня ВАК РФ:

1.
2.
3.

В иных изданиях:

1.
2.
3.

Основное содержание работы

Во введении обосновывается актуальность исследований, проводимых в рамках диссертационной работы, определяется цель исследования, ставятся задачи работы, обозначается научная новизна работы, ее теоретическая и практическая значимость, а так же возможность внедрения ее результатов.
В первой главе приводится обзор состояния науки и техники по тематике квантового распределения ключа. Рассматриваются протоколы квантовой коммуникаций с использованием как дискретных, так и непрерывных переменных. Проводится описание и анализ особенностей методов когерентного детектирования, используемых в системах квантового распределения ключа. Освещается вопрос наличия фазовых шумов в стисемах квантового распределения ключа. Демонстрируются примеры методов компенсации фазовых шумов, таких как применение пилотных импульсов и создание обратной связи. Показаны известные атаки злоумышелнника на оборудование в составе систем КРК. Описывается атака "засевом"лазерным излучением на лазер передатчика, ее влияние и возможные методы защиты. Другим рассматриваемым аспектом явлестя атака на мощность локального осциллятора, передаваемого в канале, для систем квантового распределения ключа на непрерывных переменных, принцип ее реализации, результат атаки и методы противодействия ей. Во второй главе исследуется метод оптической инжекции для реализации обратной связи в системе квантового распределения ключа на боковых частотах. Метод оптической инжекции заключается в том, что существует пара лазеров: ведущий и ведомый. Излучение ведущего лазера вводится в резонатор ведомого. Такой подход позволяет улучшить характеристики излучения ведомого лазера в частности:

- сужение спектральной линии выходного излучения
- уменьшение нелинейностей и подавление релаксационных колебаний
- уменьшение чирпа выходных импульсов и увеличение стабильности их амплитуды

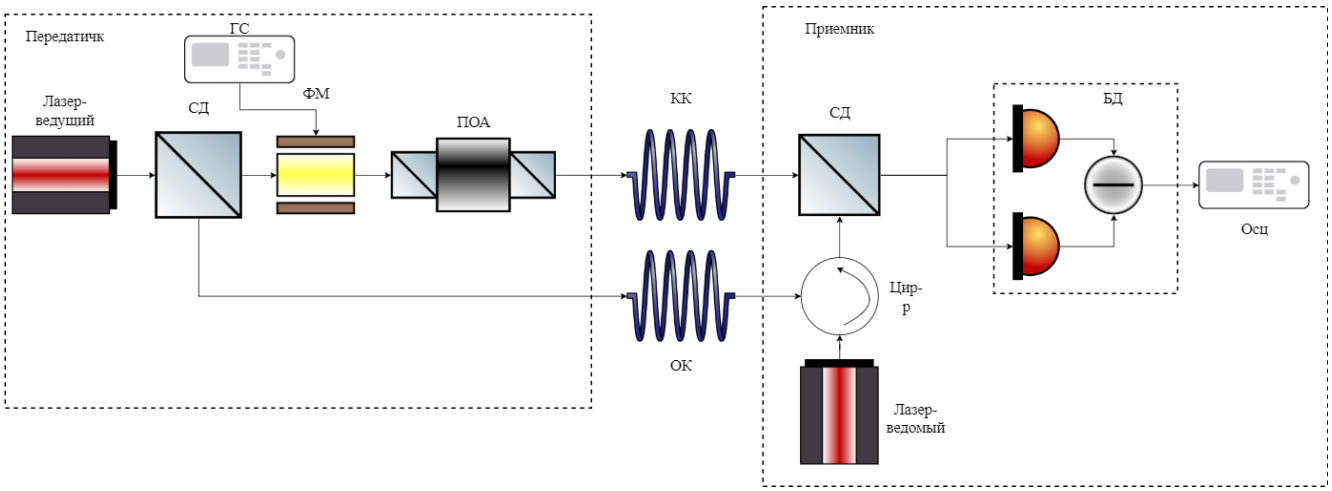

Рисунок 0.1 — Схема эксперимента системы КРК с применением оптической инжекции. СД - светоделитель, ФМ - фазовый модулятор, ГС - генератор сигналов, ПОА - перестраиваемый оптический аттенюатор, КК - квантовый канал, ОК - открытый канал, Цир-р - циркулятор, БД - балансный детектор, Осц - осциллограф.

Данный подход позволяет синхронизировать частоты ведущего и ведомого лазера, и как следствие, уменьшить их относительные фазовые шумы, достигнув фазового синхронизма. Именно этот эффект позволяет использовать оптическую инжекцию в качестве реализации обратной связи для локального осциллятора в системе КРК на боковых частотах с применением непрерывных переменных. Результатом применения обратной связии будет стабилизация промежуточной частоты и уменьшение фазовых шумов. Для реализаци данного метода используется отдельный канал и циркулятор для разделение излучения ведущего и ведомого лазера. Этот метод может быть применен для системы квантового распределения ключа на боковых частотах. Данная система, оптическая схема которой изображена на рисунке 0.1, работает следующим образом. На стороне передатчика излучение, сгенерированное лазером, разделяется на две части. Первая часть излучения попадает на фазовый модулятор Алисы, где происходит фазовая модуляция переменным электрическим сигналом, в который вносятся фазовые сдвиги для кодирования информации.В качестве кодирования может использоваться квадратурно-фазовая манипуляция или Quadrature Phase Shift Keying (QPSK) модуляция. Данный цифровой способ модуляции вносит фазовые сдвиги, соответствующие значениям 45°, 135°, 225°и 315°. Этим значениям фазовых сдвигов присваивается значение бит 00, 01, 10,

11. В результате этого в спектре появляются три гармоники сигнала: ω - центральная частота лазера, ω - Ω - нижняя боковая частота и $\omega + \Omega$ - верхняя боковая частота, где Ω - частота модуляции. Излучение после модуляции описывается уравнением:

$$F_s(t) = A_0 * \sin(\omega_0 t + \varphi_0) + \frac{A_0 * m}{2} * (\sin((\omega_0 + \Omega)t + (\varphi_0 + \varphi(t))) - \\ - \frac{A_0 * m}{2} * (\sin((\omega_0 - \Omega)t + (\varphi_0 - \varphi(t))), \quad (1)$$

где A_0 - амплитуда исходного излучения, ω - центральная частота лазера, ω - Ω - нижняя боковая частота и $\omega + \Omega$ - верхняя боковая частота, Ω - частота модуляции, φ_0 - фаза исходного излучения, $\varphi(t)$ - фаза модулирующего излучения, t - время, m - индекс модуляции. Индекс модуляции - величина отношения мощности на боковых частотах к мощности во всем спектре. Индекс модуляции пропорционален амплитуде модулирующего электрического сигнала. Полученный спектр попадает на переменный оптический аттенюатор, затухание которого выстраивается таким образом, чтобы на боковых частотах была мощность соответствующая заданному среднему числу фотонов, когда несущая может оставаться классической. Подготовленные квантовые состояния передаются в квантовый канал. Вторая же часть излучения проходит по отдельному волоконно-оптическому каналу на сторону приемника, где попадает в волоконно-оптический циркулятор так, что излучение заходит в резонатор ведомого лазера. Пришедшее излучение из квантового канала попадает на первый вход волоконного светоделителя с двумя входами и двумя выходами и коэффициентом деления 50:50. На второй же вход светоделителя попадает локальный осциллятор, представляющий собой излучение, сгенерированное отдельным лазером на приемной стороне. Благодаря наличию обратной связи в виде оптической инжекции, длина волны лазера на приемной стороне синхронизирована с длиной волны лазера Алисы. В результате ЛО и квантовые состояния интерферируют на светоделителе. В результате этой интерференции на выходе светоделителя появляются дополнительные гармоники на промежуточной частоте. Эти гармоники - ω - f - центральная частота лазера Алисы минус частота ЛО, (ω - Ω) - f - нижняя боковая частота минус частота ЛО

и (ω + Ω) - f - верхняя боковая частота минус частота ЛО, где Ω - частота модуляции, ω - частота лазера Алисы, f - частота ЛО.

Результат этой интерференции регистрируется балансным детектором. Это устройство представляет собой два классических фотодиода, подключенных так, чтобы их токи вычитались. Такое подключение позволяет уменьшить собственные шумы детектора. После этого полученный ток попадает на фильтр низких частот для фильтрации постоянной составляющей. Полученный сигнал усиливается каскадом усилителей и передается на АЦП. В результате на выходе балансного детектора формируется только один сигнал на частоте, совпадающей с частотой модуляции на стороне передатичка. Происходит это по той причине, что длина волны ЛО и лазера передатчика совпадают благодаря обратной связи в виде оптической инжекции. Таким образом на выходе детектора остается только составляющая (ω + Ω) - f, а остальные преобразуются в постоянную составляющую, которые фильтруются. Полученное колебание на выходе балансного детектора несет в себе информацию о фазе, закодированную Алисой. Данный сигнал обрабатывается цифровыми методами обработки сигналов для извлечения значения фаз сигнала.

Полученная последовательность бит является сырым ключом. Полученный ключ просеивается. В полученном просеянном ключе оценивается квантовый коэффициент ошибок по битам или QBER, предварительно открыв часть ключа. И последним этапом происходит усиление секретности с помощью HASH-функций.

К плюсам данного метода реализации КРК можно отнести простоту системы, благодаря тому, что отстуствует активный выбор базиса в виде модулятора любого типа. Наличие обратной связи в виде оптической инжекции позволяет решить несколько проблем: стабилизация длины волны ЛО, что так же упрощает конечную систему, и уменьшает фазовые шумы, связанные со случайностью фазы лазерного излучения, сгенерированного разными источниками. Применение же гетеродинного метода приема позволяет использовать любой тип модуляции, что позволяет гибко настраивать протокол под различные задачи и оставляет задел на будущее для увеличения скорости выработки ключей.

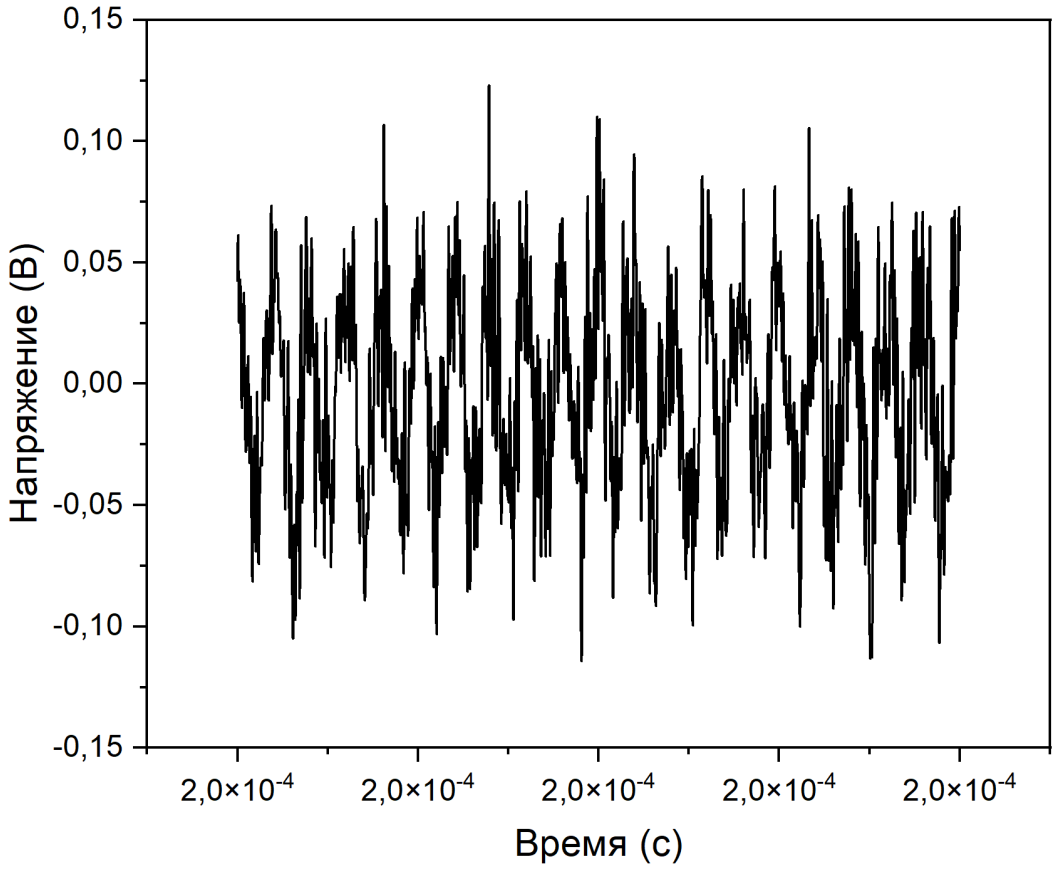

Рисунок 0.2 — Зашумленный сигнал на выходе балансного детектора

К недостаткам данной системы можно отнести необходимость дополнительного волоконно-оптического канала связи для организации обратной связи, что частично нивелируется тем, что реальные системы КРК встраиваются в уже существующие системы передачи данных, которые работают с технологией мультплексирования и сигнал оптической инжекции можно встроить в уже применяемые каналы, так как у него нет требований к уровню сторонних шумов. Второй же недостаток - это уязвимость к атаке засева лазера, который требует дополнительного изучения и контрмер.

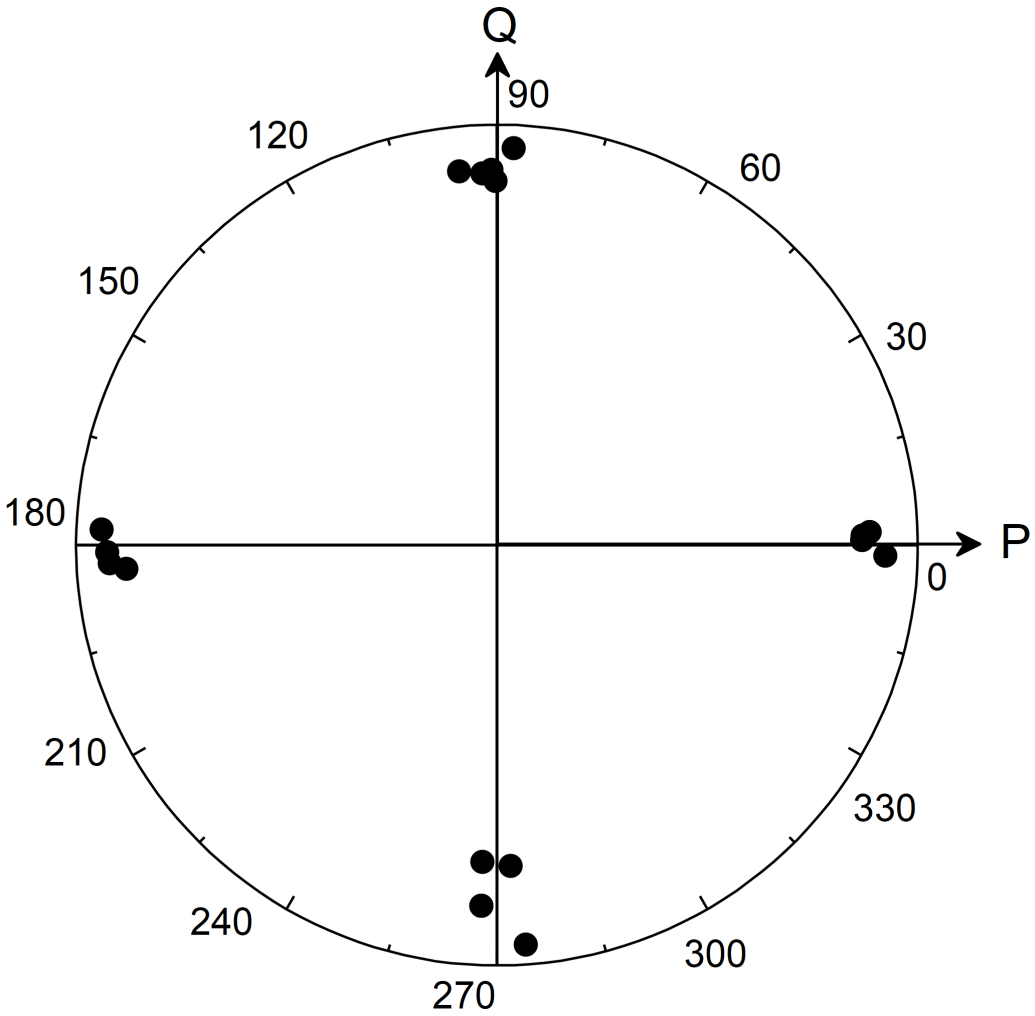

Рисунок 0.3 — Полученные значения фазы после цифровой обработки

В третьей главе рассматривается схема применения гетеродинного метода детектирования сигналов с двумя независимыми источниками сигналов для протокола квантовой коммуникации на боковых частотах. Особенностью данной системы является перенос квантовых состояний света на боковые частоты, которые появляются в спектре излучения. Основная реализация данного протокола предполагает использование дискретных переменных и детекторов одиночных фотонов на основе лавинных фотодиодов для регистрации сигналов. Однако этот протокол возможно адаптировать и для использования когерентных методов детектирования.

В данной работе предлагается использование гетеродинного метода детектирования сигналов для системы квантовой коммуникации на боковых частотах. Данная система работает следующим образом. Лазер на передающей стороне форимрует когерентное излучение. Это излучение, пройдя необходимые пассив-

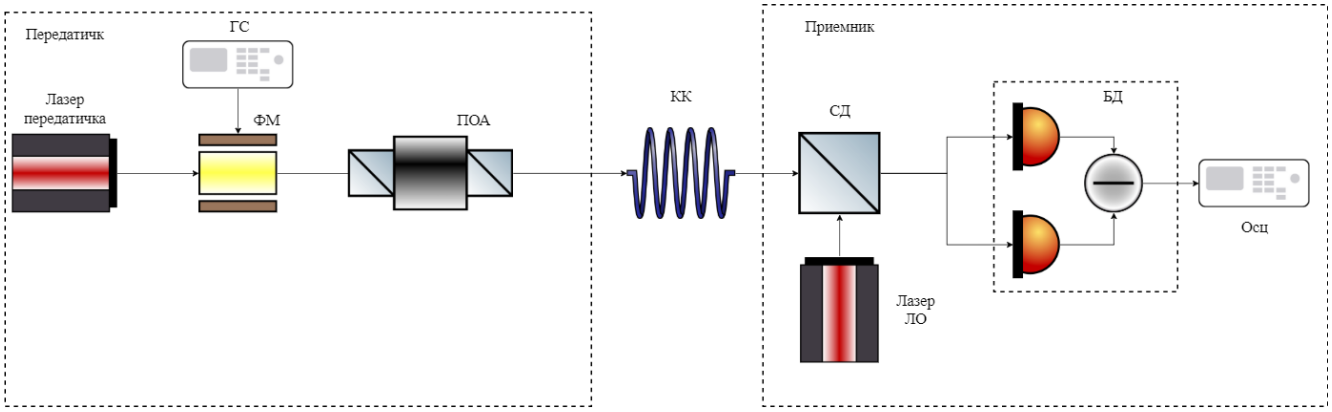

Рисунок 0.4 — Схема системы квантового распределения ключа на боковых частотах с независимым локальным осциллятором. СД - светоделитель, ФМ - фазовый модулятор, ГС - генератор сигналов, ПОА - перестраиваемый оптический аттенюатор, КК - квантовый канал, БД - балансный детектор, Осц - осциллограф.

ные элементы в виде оптических изоляторов, попадает на кристалл фазового модулятора. На электрический же вход фазового модулятора передается переменное напряжение на частоте модуляции. В это напряжение вносится фазовый свдиг, который соответсвует битам информации. Для примера в данной работе используется квадраратурно-фазовая манипуляция или quadrature phase-shift keying (QPSK). Значения фазовых сдвигов в таком случае это 45°, 135°, 225°и 315° и этим фазовым сдвигам соответствуют следующие биты информации 00, 01, 10, 11. В результате такой модуляции в спектре излучения после фазового модулятора появляются три гармоники, в двух из которых закодирована информация от передатичка. Подготовленное излучение ослабляется переменным аттенюатором для достижения уровня мощности на боковых частотах меньше 1 фотона в среднем. Полученные таким образом квантовые состояния передаются по волоконно-оптической линии связи на приемную сторону.

Переданный сигнал от Алисы после прохождения ВОЛС попадает на контроллер поляризации для компенсации искажений, внесенных прохождением через волокно. После этого установленный поляризационный светоделитель выделяет лишь нужную поляризацию и пропускает излучение с нужной поляризацией дальше. После этого квантовые состояния смешиваются с ЛО, сгенерированным отдельным лазером, на светоделителе с двумя входами и двумя выходами и коэффициентом деления 50:50. Эти сигналы интерферируют и в результате

этой интерференции спектр излучения обогощается дополнительными гармониками. Эти гармоники появляются из-за того, что частоты ЛО и лазера Алисы не совпадают. Появившиеся гармоники находятся на различных частотах - суммарная, разностная и комбинационные. Но с учетом ограниченности полосы пропускания балансного детектора, мы можем наблюдать на его выходе только гармоники на разностных частотах, которые в нее попадают. Суммарные и другие комбинационные частоты не попадают в полосу пропускания БД и регистрируются как постоянная составляющая, которая теряет всю информацию, закодированную в их фазы. Когда как гармонические колебания на разностной промежуточной частоте проходят усилительный каскад без изменений и сохраняют информацию, закодированную в фазу излучения Алисой. Таким образом происходит перенос спектра из оптической области в радиочастотную, где упрощается усиление и обработка сигналов.

Балансный детектор - это устройство, которое представляет собой два фотоприемных диода, подключенных так, чтобы их фототоки взаимно вычитались. После этого полученный сигнал подвергается фильтрации, чтобы исключить влияние постоянной составляющей фототока. После этого полученный сигнал попадает на каскад усилителей для увеличение его амплитуды. Наличие каскада усилителей ограничивает полосу пропускания всего устройства. Типичная ширина полосы пропускания может варьироваться от 100 МГц до 1.2 ГГц. Это ограничивает диапазон принимаемых частот и скорость выработки сырого ключа.

Полученный сигнал после усиления необходимо перевести в цифровую форму с помощью АЦП для его дальнейшей обработки. В качестве обработки могут применятся различные методы цифровой обработки сигналов, такие как Быстрое Преобразование Фурье или Преобразование Гильберта. В результате этой обработки из гармонического сигнала, полученного после АЦП, генерируются фазовые значения, которым соответствуют заданные значения бит, из которых формируется битовая последовательность, называемая сырым ключом. Однако использование ЛО на стороне приемника требует подстройки поляризации его и поляризации квантовых состояний для эффективной интерференции на

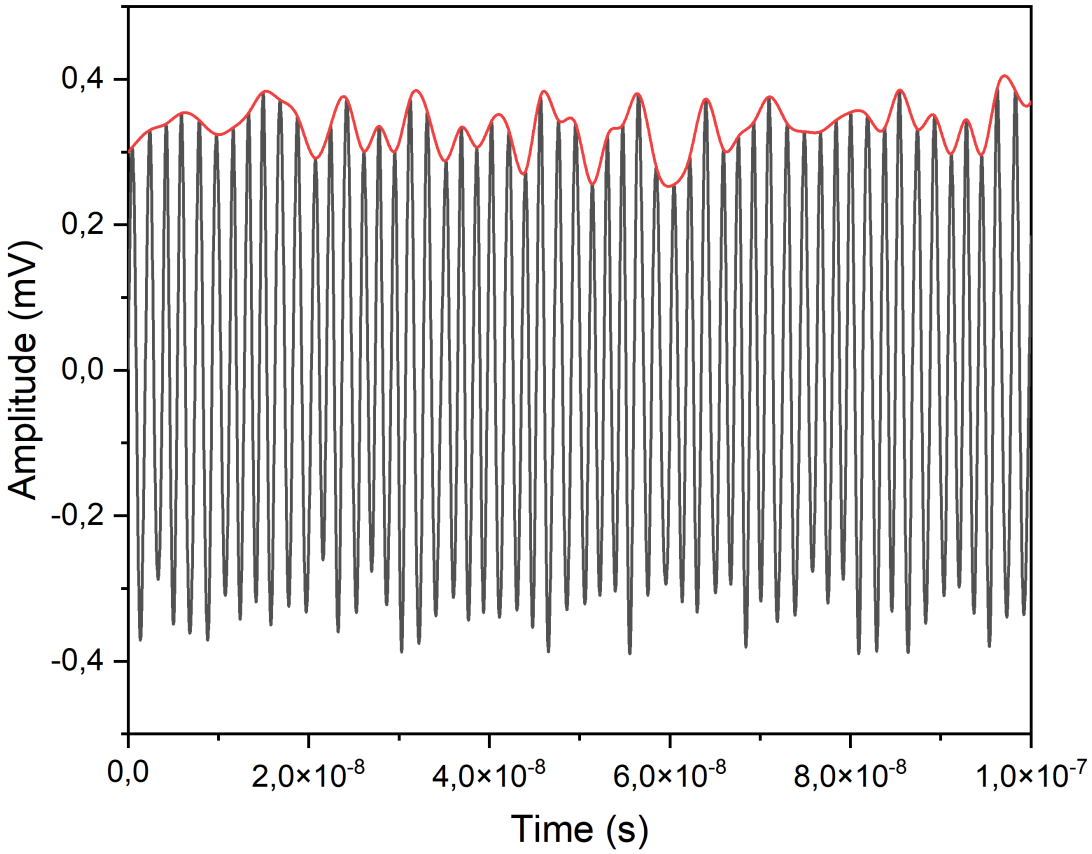

Рисунок 0.5 — Сигнал на выходе балансного детектора после гетеродинного приема.

приемнике. В рамках данной работы предлагается алгоритм контроля поляризации на основе Быстрого Преобразования Фурье. Суть данного алгоритма заключается в том, что при использовании поляризационного светоделителя частота модуляции, которая несет в себе информацию от передатчика, удваивается. Это появление удвоенной частоты возможно отследить в частотной области. Для этого применяется следующий алгоритм

1. Применение БПФ к принятому сигналу
2. Анализ спектрального состава сигнала
3. Поворот поляризации сигнала до уничтожения гармоники на удвоенной частоте модуляции
4. Дальнейший поворот поляризации сигнала до максимума гармоники на частоте модуляции

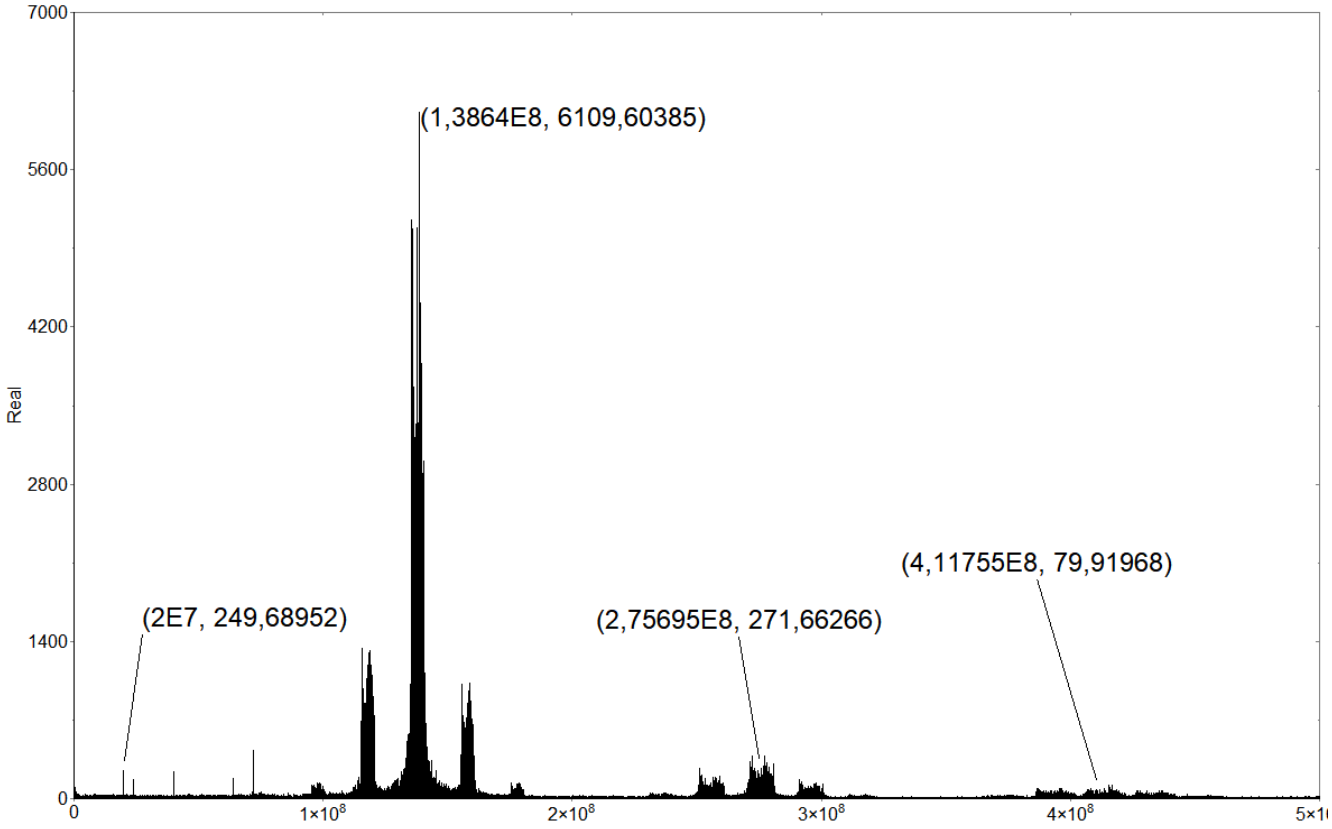

Рисунок 0.6 — Спектр сигнала с искаженной поляризацией

В результате его работы возможна как подстройка поляризации за счет применения активного контроля поляризации, который будет использовать результат БПФ как обратную связь, так и для ее постоянной подстройки. На рисунке 0.6 изображен спектр информационного сигнала с искаженной поляризацией. Информация о наличии удвоенной частоте модуляции подается на контроллер поляризации и он начинает свою работу до того момента, пока истинная частота модуляции не будет максимальной, а удвоенная частота модуляции - пропадет. Результат работы алгоритма изображен на рисунке 0.7. На спектре сигнала при нормальной поляризации не содержит гармоники на удвоенной частоте и при этом гармоника на частоте модуляции максимальна.

К достоинствам данного метода можно отнести гибкость выбора протокола, так как перенос информации на промежуточную частоту позволяет анализировать практически любую модуляцию без необходимости внесения дополнительных элементов, например, фазового модулятора для выбора базиса. Использование двух независимых источников когерентного излучения позволяет не использовать системы обратной связи, которые требуют дополнительного оптического

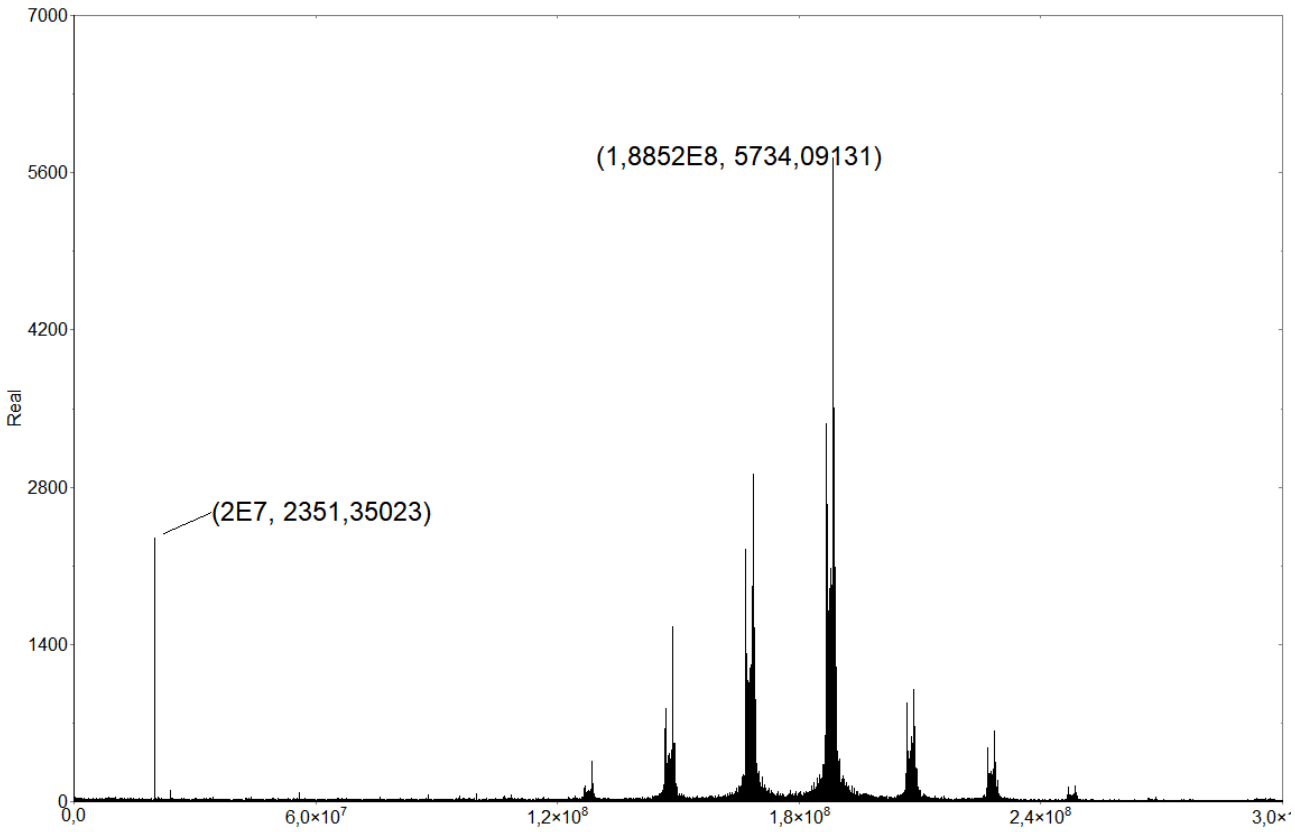

Рисунок 0.7 — Спектр сигнала с искаженной поляризацией

канала и открывают дополнительные возможности для злоумышленника. Генерация локального осциллятора на стороне приемника позвволяет увеличить его мощность, по сравнению с протоколами, в которых ЛО передается по квантовому каналу, что позволяет уменьшить шумы, связанные с рассеянием в ВОЛС и увеличить соотношение сигнал/шум, что положительно влияет на скорость выработки бит.

Из недостатков же можно выделить необходимость подстройки частоты, так как два независимых генератора нуждаются в периодической подстройке частоты. Эта проблема решается особенностью протокола квантовой коммуникации на боковых частотах за счет того, что в спектре присутствует мощная несущая, которая так же сбивается с локальным осциллятором и переносится на промежуточную частоту. Анализируя эту частоту после обработки БПФ, можно подстраивать частоту ЛО для того, чтобы все сигналы попадали в полосу пропускания балансного детектора. Другим же недостатком является случайный фазовый шум из-за случайности процесса генерации лазерного излучения в двух независимых источниках. Данная проблема решается анализом фазы про-

межуточной частоты между локальным осциллятором и оптической несущей, полученной после фазовой модуляции Алисы. Этот сигнал будет содержать фазовый шум и ЛО, и лазера передатчика, который можно учесть в постобработке, сделав предварительную обработку цифровыми методами.

Четвертая глава посвещена изучению влияния излучения злоумышленника на длине волны 1310 нм на источник когерентного излучения на основе полупроводникового лазерного диода с распределенной обратной связью. Данная уязвимость в технической реализации получила название атака оптической накачкой. Данный тип атаки схож с атакой оптическим "засевом"(Laser Seeding) тем, что Ева инжектирует свое излучение в резонатор лазера на передатичке для изменений его характеристик. Однако есть существенное различие. В случае атаки "засевом"злоумышленник использует ту же или близкую длину волны к рабочей длине волны атакуемого лазера. В то время как в случае атаки оптической накачкой Ева использует длину волны лазера, отличающуюся на 50 и более нанометров от рабочей длины волны лазера Алисы. Эта особенность позволяет эффективнее обходить контрмеры с применением пассивных волоконно-оптических элементов в виде изоляторов. Их коэффициент изоляции имеет спектральную зависимость, что приводит к тому, что вносимая изоляция на длине волны 1310 нм существенно меньше, чем на длине волны 1550 нм. В результате злоумышленнику требуются меньшая зондирующая мощность, чтобы достичь необходимого эффекта.

Данная атака строится следующим образом. Злоумышленник устанавливает в разрыв волоконно-оптической линии связи волоконный циркулятор с тремя портами. В первый порт подлючается зондирующий лазер Евы. Второй порт подключается в волоконно-оптическую линию связи в сторону отправителя, а третий порт - в сторону приемника. Таким образом излучение злоумышленника будет заходить в оптическую схему передатчика, а излучение Алисы будет проходить по волокну в сторону приемника без проблем. Излучение злоумышленника, проходя оптическую схему передатичка, претерпевает затухание, поэтому необходимо иметь достаточную мощность зондирующего излучения для внесения изменений в характеристики лазера. Прошедшее излучение попадает в кристалл лазера и поглощается в нем. Это приводит к тому, что создается дополнительная инверсия населенности, приводящая к смещению Ватт-Амперной характеристики лазера при неизменном токе накачки. В результате этого калиброванный источник излучения на стороне передатичка начинает излучать

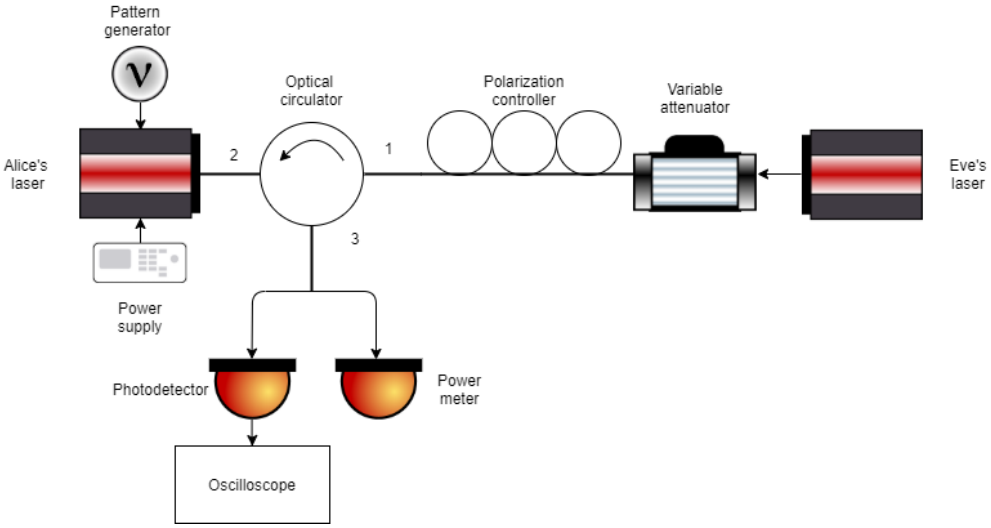

Рисунок 0.8 — Схема эксперимента по засеиванию лазера. Alice's Laser - Лазер Алисы, Pattern generator - генератор последовательности импульсов, Power Supply - лабораторный блок питания, optical circulator - оптический циркулятор, polarization controller - контроллер поляризации, varriable attenuator - перестраиваемый аттенюатор, Eve's laser - лазер злоумышленника, Photodetector - фотоприемник, power meter - измеритель мощности, Oscilloscope - осциллограф.

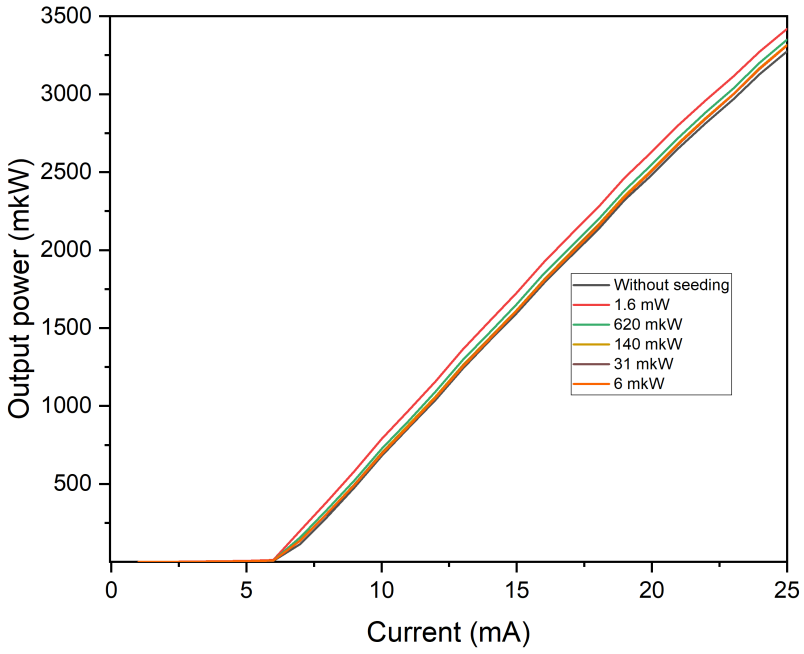

Рисунок 0.9 — Изменение Ватт-Амперных характеристик под различными мощностями накачки на длине волны 1310 нм. Output power - выходная мощность в микроваттах, current - ток в миллиамперах

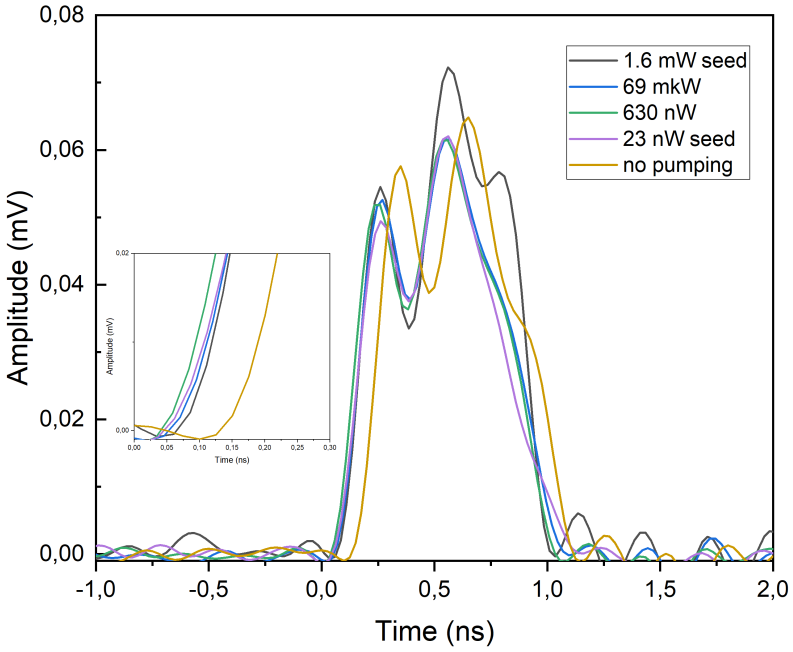

Рисунок 0.10 — Измнение формы импульса под действием внешней оптической накачки на разных мощностях на длине волны 1310 нм. Amplitude - амплитуда в милливольтах, Time - время в наносекундах, seed - засеивание, pumping - накачка.

большую мощность, чем предполагалось изначально. В итоге это приводит к тому, что выходное среднее число фотонов увеличивается, генерируется большее количество многофотонных состояний, что открывает возможности по реализации атаки с ращиплением числа фотонов. Этот же эффект проявляется в изменении формы импульса. Оптическая накачка увеличивает площадь импульса и, соответсвенно, его энергию. Отдельно стоит отметить, что в случае оптической накачки, генерация импульса начинается раньше, чем при обычном режиме работы лазера передатичка, что злоумышленник так же может использовать для различения состояний ловушек и квантовых состояний в протоколах с использованием состояний ловушек.

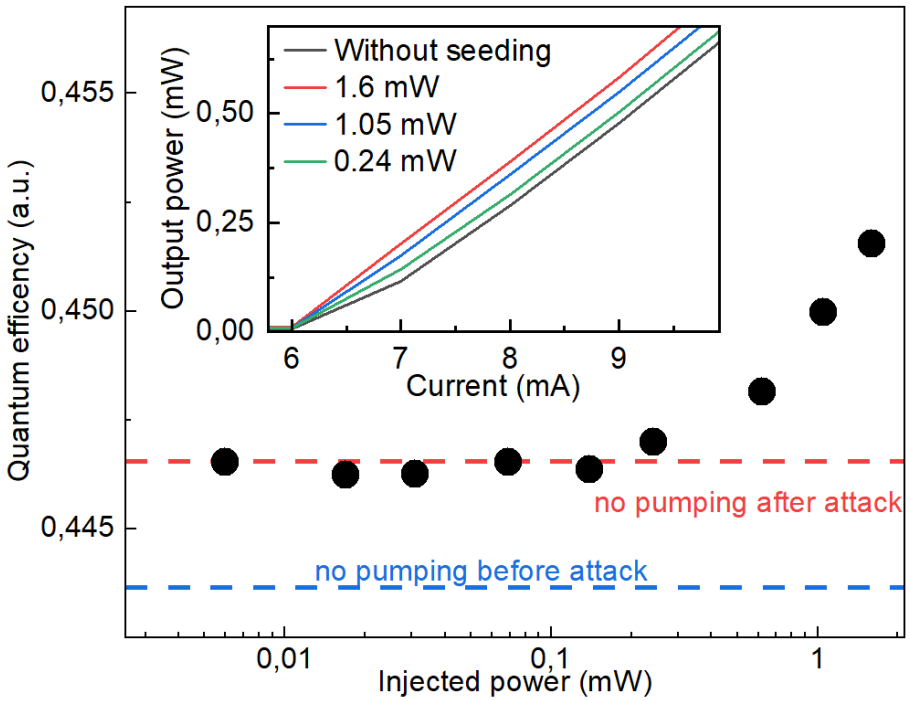

Рисунок 0.11 — Изменение квантовой эффективности под действием внешнего излучения на длине волны 1310 нм. Quantum efficiency - квантовая эффективность в относительных единицах, Output power - выходная мощность в милливаттах, Injected power - введенная мощность в милливаттах, current - ток в миллиамперах, синяя пунктирная линия - значение квантовой эффективности до атаки, красная пунктирная линия - значение квантовой эффективности после атаки.

В рамках данной работы показана реализация атаки оптической накачкой на длине волны 1310 нм, которая приводит к увеличению выходной мощности лазера при неизменных токах накачки, увеличению площади импульса и повышению квантовой эффективности лазера. Данные эффекты создают условия для проведения других типов атак на систему КРК. В случае данной работы было показано, что зондирующей мощности в 200 мкВт достаточно для повышения квантовой эффективнсти на 1%, продемонстрированно на графике 0.11 и увеличения выходной мощности на 4%. Была рассчитана минимально необходимая мощность для эффективной атаки злоумышленника на типичную оптическую схему передатичка, реализующую протокол BB84.

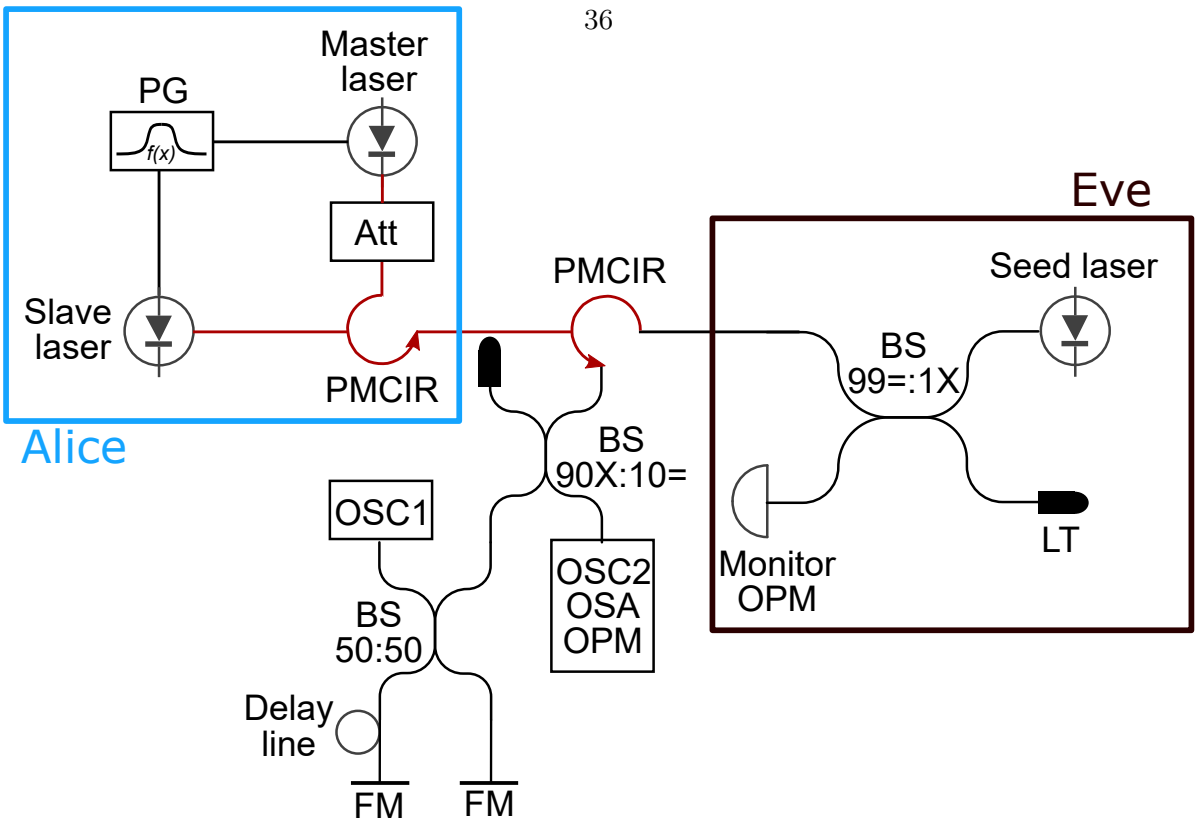

Рисунок 0.12 — Оптическая схема установки лазерного засеивания источника на основе оптической инжекции.

Исследования, проводимые в шестой главе, посвещены изучению влияния мощного когерентного излучения на источник лазерного излучения на основе оптической инжекции. Такие источники активно используются в системах квантовой коммуникации, реализующих протокол с недоверенным приемным узлом. Такие источники обладают улучшенными характеристиками стабильности амплитуды выходного сигнала, временной стабильностью длины волны и уменьшенным чирпом выходных импульсов за счет уменьшения влияния переходных процессов во время генерации. Эти особенности позволяют получать видность интерференции Хонг-Оу-Манделя близкой к теоритическому максимуму в 0.5.

Однако, для таких источников не были исследованы методы воздейсвтия такие как атака "засевом"лазера. Для этого была собрана оптическая схема для проведения исследования влияния мощного лазерного излучения в диапазоне мощностей от 180 до 900 мВт.

В качестве источника были собраны два полупроводниковых лазера с распределенной обратной связью. Первый лазер - Agilecom WSLS-934010C4124-42 со встроенным изолятором, который использовался в качестве ведущего лазера для генерации опорного излучения. Второй же лазер представлял собой лазер Agilecom WSLS-934010C4124-82, аналогичный первому, но уже без встроенного изолятора. Это нужно для того, чтобы максимизировать количество изулчения, вводимого в резонатор ведомого лазера. Эти два лазера подключены друг к другу через оптический циркулятор. Первый порт его подключен в ведущему лазеру, излучение из которого попадает на второй порт циркулятора, куда подключен ведомый лазер. Таким образом изучение из лазера-мастера попадает в резонатор ведомого лазера. Излучение ведомого лазера попадает на второй вход циркулятора и проходит на третий порт циркулятора. В качестве источника мощного лазерного излучения использовался лазер Gooch & Housego AA1406-193300 и волоконный эрбиевый усилитель. Для введения его излучения использовался дополнительный циркулятор, первый порт которого подключается к выходу усилителя, второй к третьему порту первого циркулятора. Для исследования интерференции полученных импульсов был собран волоконный интерферометр Майкельсона.

В ходе работы были исследованы характеристики выходных импульсов под действием внешнего излучения. Исследовались следующие параметры: амплитуда выходных импульсов и их стабильность, выраженная в измерении стандартного отклонения, длительность импульсов и их стандартное отклонение, а так же изучалась корреляция фазы полученных импульсов с помощью волоконного интерферометра Майкельсона. В ходе воздействия изменялось стандартное отклонение энергии выходных импульсов в диапазоне от 2 до 3.5 процентов при мощности лазера атакующего в 900 мВт и при варьировании мощности лазера мастера.Результаты этих имзерений приведены на рисунке 0.13 Данные результаты показывают, что Ева способна увеличивать нестабильность выходной мощности для увеличения среднего числа фотонах в импульсе. Длительность импульса так же изменяется под действием внешнего излучения, изображенном на рисунке 0.14 Под внешним воздействием дрожание импульса возрастает на

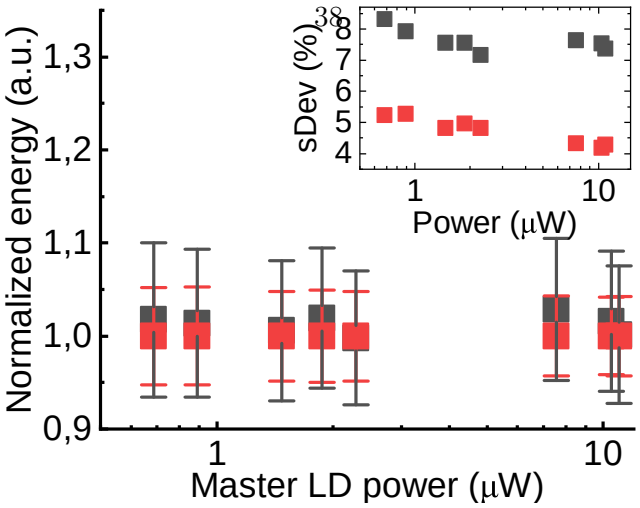

Рисунок 0.13 — Изменение энергии импульса источника под действием внешнего излучения и без него в зависимости от мощности лазера-мастера.

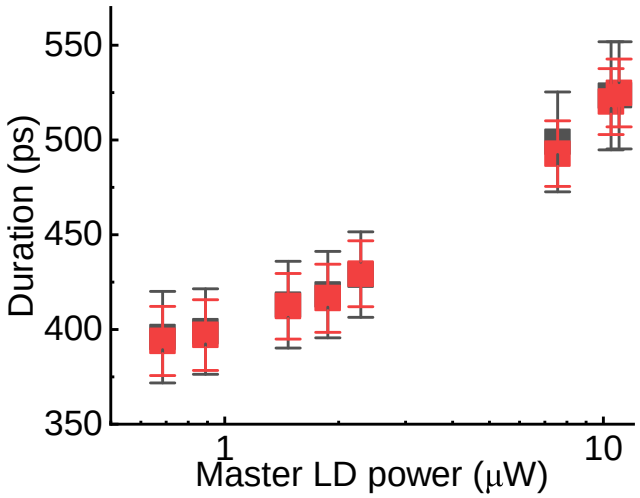

Рисунок 0.14 — Измененение длительности импульса под действием внешнего излучения

2%. Существующие работы показывают, что даже незначительные отклонения в длительности импульса существенно снижают дальность распределения секретного ключа.

Для разработки контрмеры необходимо рассчитать необходимый коэффициент изоляции для нааихудшего сценария, когда злоумышленник использует максимально доступную ему мощность. В непрерывном режиме эта величина составляет 2 Ватта. Эту величину необходимо ослабить до значения меньше -35 дБм. Благодаря использованию в составе схемы волоконно-оптического циркулятора, величина изоляции уже составляет 50 дБ. Для рассчета необходимого

значения аттенюации используется формула

$$\alpha = P_a - P_{req} - \beta \tag{2}$$

, где α - величина изоляции, которую необходимо внести, P_a - величина зондирующей мощности в дБм, P_{req} - мощность, до которой требуется ослабить входное излучение, β - величина изоляции, которая уже реализована в схеме, в дБ. Подставим в 2 значения в 33 дБм мощности, что соответствует 2 Ваттам мощности и 50 дБ изоляции. В результате значение изоляции, необходимое для ослабления 2 Ватт до -35 дБм, равняется 18 дБ. Для обеспечения безопасности данного источника достаточно установить волоконный изолятор, типичная величина изоляции которого равна 30 дБ. Это перекроет весь допустимый диапазон зондирующих мощностей.

Полученные результаты демонстрируют стойкость предложенного источника когерентного излучения ко внешним воздействиям. Для изменения его характеристик злоумышленнику необходимо работать на мощностях, близких к мощностям, запускающих искру в волоконно-оптических линиях связи, что несет для него повышенные риски быть обнаруженным. А протоколы, основанные на протоколе с использованием недоверенного приемного узла обезопашены не только от атак злоумышленника на приемные узлы в виде детекторов одиночных фотонов, но так и от атак на источники одиночных фотонов.

Введение

Актуальность темы.

Квантовое распределения ключа (КРК) - актуальная технология, развившаяся из теории квантовой информатики, позволяющая распределить симметричную битовую последовательность с помощью квантовых методов у двух и более пользователей для использования этой последовательности в качестве ключа для симметричного шифрования данных и одновременным обнаружением несанкционированного доступа со стороны нелегитимных пользователей. Использование квантовых состояний света при распределении ключа позволяет достичь уровня секретности, недоступного для классических протоколов шифрования. Такие квантовые состояния могут быть представлены в виде одиночных фотонов. Их квантовые свойства не позволяют злоумышленнику скопировать их состояния или считать их без изменения и без внесения ошибок. Такие квантовые состояния возможно передавать как по волоконно-оптическим линиям связи (ВОЛС), как по атмосферным каналам, так и в космическом пространстве с помощью спутников. Принцип работы данных систем следующий. На стороне передатчика (Алиса) формируются квантовые состояния. Для этого используется когерентное лазерное излучение, ослабленное до одиночных фотонов с помощью аттенюатора. В подготовленные кванты света вносится изменение в поляризацию или фазовый свдиг фотона. Подготовленное таким образом состояние передается по каналу связи к приемнику (Боб). На приемной стороне происходит независимое от Алисы повторное измерение состояния фотона. В случае корреляции у Боба принятый одиночный фотон регистрируется детектором одиночных фотонов. Благодаря свойствам одиночного фотона в виде невозможности клонирования, невозможности измерения без разрушения и его неделимости возможно отследить воздействие злоумышленника, так как его действия будут приводить к появлению ошибок в полученной битовой последовательности. Так обеспечивается контроль несанкционированного допуска.

Отдельным классом выделяются системы квантового распределения ключа на непрерывных переменных (КРКНП). В таких системах квантовое состояние, подготовленное и переданное Алисой, на приемной стороне взаимодействует с сильным лазерным излучением. И результат этого взаимодействия регистрируется балансным детектором. Основными отличаями данного детектора от детектора одиночных фотонов является использование двух классических фотоприемников, подключенных таким образом, что их фототоки взаимнов вычитаются, что позволяет уменьшить шум системы, и отстуствие охлаждения до температур порядка -40 ° градусов Цельсия. Все это позволяет упростить конечную систему. К преимуществам КРКНП можно отнести большую скорость выработки секретного ключа по сравнению с системами КРК на дискретных переменных, в которых применяются детекторы одиночных фотонов.

Среди сложностей систем КРКНП выделяется способ передачи сильного лазерного излучения или локального осциллятора (ЛО) на приемную сторону и его разделения с квантовым сигналом. В первых системах КРКНП с Гауссовой модуляцией Локальный осциллятор и квантовые состояния генерировались у передатчика, объединялись и передавались совместно в квантовый канал. На приемной стороне локальный осциллятор и квантовый сигнал разделяются, ЛО задерживается специальной линией задержки и снова соединяются на светоделителе для взаимодействия. Результатом этого взаимодействия является интерфереционная картина, распределение интенсивности которой зависит от закодированного Алисой состояния. Полученное поле регистрируется балансным детектором, на выходе такого формируется уровень напряжения, который в дальнейшем подвергается пост-обработке. Передача локального осциллятора через канал ограничивает дальность работы системы такого типа и ограничивает скорость выработки ключа, так как для лучшей работы системы необходим ЛО как можно большей мощности. Второй проблемой является возможности злоумышленника манипулировать локальным осциллятором для создания каналов утечки информации. В качестве альтернативы предлагается использовать локальный осциллятор, сгенерированный на приемной стороне. Такое решение

позволит увеличить дальность передачи ключа, скорость его выработки и закрыть уявзимость к атаке на ЛО.

Одним из перспективных подходов к реализации систем квантовой коммуникации на непрерывных переменных является система квантовой коммуникации на боковых частотах модулированного излучения. В основе данного метода лежит вынесение квантового канала на боковые частоты, которые появляются в результате модуляции оптического излучения переменным электрическим полем. Благодаря этому повышается устойчивость передаваемого сигнала ко внешним воздействиями и обеспечивается высокая спектральная эффективность, а также обеспечивается показатели по отношению скорости выработки ключа к дальности между блоками приемника и передатчика, сравнимые с другими системами квантовой коммуникации. Данный метод подходит и для реализации протоколов на непрерывных переменных с когерентными методами детектирования. В частности, в данной работе рассматривается гетеродинный метод, при котором квантовые состояния, подготовленные Алисой, передаются по волоконной линии связи к приемнику, в нем попадают на светоделитель с формулой 2x2 и коэффициентом деления 50:50 и смешиваются на нем с мощным локальным осциллятором, который отстроен по частоте от передающего лазера на величину, которая превышает частоту смены состояний. Результат интерференции регистрируется балансным детектором. На выходе балансного детектора формируется сигнал на промежуточной частоте от всего спектра сигнала, переданного Алисой. Для извлечения инфорамции требуется провести фильтрацию с помощью фильтра низких частот и демодуляцию полученного сигнала для генерации сырого ключа.

Одной из проблем при реализации гетеродинного метода детектирования для распределения ключа является необходимость компенсации фазовых шумов. Для этого применяют различные методы. Первым из таких методов является передача "пилотного"импульса, при детектировании которого измеряется фазовый шум, внесенный каналом. После этого измеренное значение учитывается в постобработке состояний. Второе - это реализация обратной связи в различных формах. В рамках данной работы предлагается использовать метод

оптической обратной связи для системы квантового распределения ключа на боковых частотах на непрерывных переменных. Суть данного метода заключается в инжекции лазерного излучения от ведущего лазера, который является лазером передатчика, в лазер ведомый, который используется в качестве локального осциллятора в приемнике. Данный метод позволяет стабилизировать длину волны ЛО и уменьшить фазовые шумы из-за того, что оба источника являются генераторами когеретного излучения со случайной фазой.

Метод оптической инжекции требует дополнительного канала для передачи создания обратной связи. Такой канал усложняет систему и повышает требования к волоконно-оптической линии связи (ВОЛС), что особенно критично в городских линиях связи, где выделение дополнительного волокна или канала в сетях с мультиплексированием затруднительно. Решением данной проблемы может являтся система квантового распределения ключа на непрерывных переменных с применением гетеродинного детектирования с независимым ЛО. Суть данной системы заключается в том, что на приемнике и передатичке установленны лазеры со стабилизацией длины волны и со шириной спектральной линии менее 10 кГц. Такой подход позволяет не прибегать к постоянной подстройке длин волн лазеров и уменьшить фазовый шум, связанный с независимостью источников излучения. Однако, фазовый шум при этом не исчезает, поэтому его все еще необходимо компенсировать. В случае реализации такого метода детектирования сигналов для протокола квантового распределения ключа на боковых частотах для этого можно использовать несущую частоту, измеряя ее фазу и внося корректировки в постобработке.

Отличия реальных систем КРК от моделей, используемых для теориетических доказательств, могут быть использованы злоумышленником для проведения различных типов атак на оборудование, входящее в состав системы. В работах ранее было показано, что источники лазерного излучения на основе полупроводниковых кристаллов могут быть уязвимы к "засеву"внешним излучением злоумышленника на длине волны близкой к той, что использует передатчик. В результате этой атаки изменяется форма излучаемого импульса и увеличивается выходная мощность, в отдельных случаях можно наблюдать и

изменение длины волны. Эти эффекты приводят к увеличению среднего числа фотонов, излучаемых передатчиком, что открывает возможность для злоумышленника атаки с ращеплением числа фотонов.

Однако в литературе не рассматривались атака "засевом"лазерным излучением на других длинах волн. Атака такого типа опаснее тем, что для защиты от нее используются пассивные волоконно-оптические элементы, вносящие дополнительное затухание, например изоляторы или DWDM фильтры. Но существуют работы, которые демонстрируют, что величина затухания в таких элементах может уменьшаться при существенном изменении падающей длины волны излучения. Например, изолятор с рабочей длиной волны 1550 нм вносит 50 дБ потерь при обратном прохождении, когда при облучении излучением на длине волны 1310 нм эта величина составляет 20 дБ. А в случае с DWDM фильтром, он практически не вносит затухание на длине волны 1310 нм. Таким образом, злоумышленнику гораздо проще осуществить атаку "засевом"лазерным излучением, так как на данной длине волны вносимое затухание меньше.

Такой тип атаки носит название "атака оптической накачкой". Ее суть заключается в том, что злоумышленник зондирует лазер длиной волны, отличой от рабочей. При этом это излучение поглащается активной средной лазера передатчика так, что поглощенное излучение выступает в роли оптической накачки, которая работает как дополнение к электрической накачки полупроводникового лазера. В этом случае изменяется Ватт-Амперная характеристика лазера и его квантовая эффективность. Это приводит к тому, что изменяется энергия излученных импульсов увеличивается при неизменной величине тока накачки. В рамках данной работы впервые обозначен данный тип атаки, определена нижняя граница необходимой мощности излучения на длние волны 1310 нм для изменения характеристик изучаемого лазера и измерено влияние оптической накачки на характеристики лазера.

Существует решение

Цель работы. Разработать систему гетеродинного приема сигналов в квантовой системе коммуникаций на боковых частотах с локальным осциллятором на

стороне получателя и с применением оптической инжекции.

Задачи работы.

1. Реализовать гетеродинный прием сигналов в системе КРК на боковых частотах с применением метода оптической инжекции для синхронизации длин волн и локальным осциллятором на стороне приемника.
2. Реализовать гетеродинный прием сигналов в системе КРК на боковых частотах с двумя независимыми источниками излучения для приема модулированных сигналов, и сигналов с частотным мультиплексированием. Разработать алгоритм контроля поляризации для систем такого вида
3. Исследовать атаку оптической накачкой на источники излучения, которые могут являться локальным осциллятором для систем квантового распределения ключа на непрерывных переменных
4. Исследовать влияние мощного оптического излучения на источник излучения на основе оптической инжекции и его выходные параметры

Научная новизна работы.

Теоретическая и практическая значимость работы.

Положения выносимые на защиту.

1. Передача фазово-кодированных сигналов в системе квантового распределения ключей на непрерывных переменных с гетеродинным методом детектирования сигналов и локальным осциллятором, реализованным на стороне приемника, становится возможной при стабилизации длин волн используемых источников излучения за счет применения метода оптической инжекции для реализации обратной связи.
2. Алгоритм, заключающийся в контроле поляризации входящего сигнала, основанный на анализе спектрального состава электрического сигнала, полученного после Быстрого Преобразования Фурье, и с поворотом поляризации на основе проведенного анализа, позволяет произвести обмен фазово-кодированными состояниями в системе квантовой коммуникации на боковых частотах с применением непрерывных переменных и гетеродинным методом регистрации сигналов на основе двух независимых источников лазерного излучения телекоммуникационного диапазона длин

волн и с применением частотного мультиплексирования на одной несущей частоте.

3. Поглощение излучения лазера нарушителя активной средой полупроводникового лазера с распределенной обратной связью, используемого в передатчике системы квантового распределения ключей, приводит к увеличению излучаемого им среднего числа фотонов.
4. Засеивание ведомого лазера в источнике излучения, построенного на основе метода оптической инжекции, лазером нарушителя, который работает в непрерывном режиме, мощностью не менее 800 мВт и на длине волны, согласованной с длиной волны ведомого лазера, повышает стандартное отклонение амплитуды выходных импульсов ведомого лазера на 3%, повышает стандартное отклонение их энергии на 3%, увеличивает стандартное отклонение длительности импульсов на 2.5% и увеличивает среднюю излучаемую мощность на 8%, приводящее к снижению дальности передачи секретного ключа на 10%

Апробация работы.

Достоверность научных достижений.

Внедрение результатов работы.

Публикации.

Структура и объем диссертации.

ГЛАВА 1. Обзор литературы

1.1 Протоколы квантовой коммуникации

Технология квантовой коммуникации позволяет распределить последовательность бит между двумя пользователями, которым требуется общий ключ для шифрования данных. В отличии от классических методов шифрования, где ключ передается либо специальными службами в случае протоколов симметричного шифрования, или же где ключ состоит из открытой и закрытой части как в методе шифрования RSA. Однако классические системы криптографии имеют ограничения, связанные с их особенностями работы - на сложности математических вычислений, например факторизации чисел. Однако эта задача может быть решена квантовым компьютером не за полиноминальное время, что представляет угрозу современным способам шифрования. Есть и другой фактор - необходимость передачи ключа для шифрования и дешифрования информации, переданной между абонентами. В качестве решения и было предложено использование технологии квантового распределения ключа. Эта технология позволяет распределять секретный ключ между абонентами с помощью одиночных фотонов. Их использование позволяет перейти к качественно новому уровню передачи ключей, защищенных законами квантовой физики. Из-за этого злоумышленник не может незамеченным считывать квантовые состояния, которыми обмениваются передатичк и приемник, не будучи обнаруженным. Это преимущество вкупе с использованием шифрование методомо одноразового блокнота, для которого доказана абсолютная стойокость, ярко выделяет системы квантового распределения ключа среди классических методов шифрования недостижимым уровнем безопасности.

1.1.1 Протоколы квантовой коммуникации на дискретных переменных

В результате исследований, проводившихся по теме квантового распределения ключей, сформировались несколько подходов к реализации протоколов. Первыми протоколами были протоколы на использовании дискретных переменных, в которых для кодирования используется конечное число дискретных состояний света. Для этого возможно использование одной из двух степеней свободы фотона - фазы или поляризации. Такое подготовленное состояние называется кубитом. Кубит может быть представлен в виде вектора в двхумерном Гильбертовом пространстве как два базовых вектора

$$|0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix} |1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix} \tag{1.1}$$

Любой кубит может быть представлен как линенйная суперпозиция базисов, представленных в выражении 1.1.1

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle \& = cos(\frac{\theta}{2})|0\rangle + e^{i\varphi} * sin(\frac{\theta}{2})|1\rangle, \tag{1.2}$$

где $\theta \in (0, \pi)$, $\varphi \in (0, 2\pi)$, i - мнимая единица. Такое состояние можно изобразить в виде вектора на "Сфере Блоха". В случае $\theta = 0$ или $\theta = \pi$, получаются состояния $|0\rangle$ и $|1\rangle$ соотвественно. Для векторов, соответствующим значениям фазовым набегам 0, $\frac{\pi}{2}$, π, $\frac{3\pi}{2}$ получаются следующие вектора:

$$\varphi = 0 : |+\rangle = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ 1 \end{pmatrix} \tag{1.3}$$

$$\varphi = \pi : |-\rangle = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ -1 \end{pmatrix} \tag{1.4}$$

$$\varphi/2 = 0 : |+i\rangle = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ i \end{pmatrix} \tag{1.5}$$

$$3\varphi/2 = 0 : |-i\rangle = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ -i \end{pmatrix} \tag{1.6}$$

Полученные векторы описывают дискретные состяния, которые приготавливают для передачи в квантовом канале. Протоколы квантовых коммуникаций, использующие такие типы состояний, называют дискретными. В качестве степеней свободы, в которые кодируется информация, используется как фаза, так и поляризация. При необходимости количество состояний и их значения могут варьироваться, но общая черта - дискретность выбранных значений, не изменяется.

1.1.2 Протокол BB84

Самая первая полноценная работа, посвещенная протоколу квантовой коммуникции, была опубликована в 1984 году, ее авторы Чарльз Беннет и Жиль Брассард [1]. По первым буквам их фамилий протокол назван BB84. Эту работу можно считать основополагающей для технологии квантовой коммуникации.
В классической криптографии с открытым ключом ловушечные функции используются для скрытия смысла сообщений между двумя пользователями от пассивного подслушивателя, несмотря на отсутствие какой-либо начальной общей секретной информации между двумя пользователями. В квантовом распределении открытых ключей квантовой канал не используется напрямую для отправки осмысленных сообщений, а используется для передачи запаса случайных битов между двумя пользователями, которые изначально не имеют общей секретной информации, таким образом, что пользователи, путем последующей консультации по обычному классическому каналу, который пассивно подслушивают, могут с большой вероятностью определить, была ли исходная квантовая передача нарушена в пути, как это происходит при подслушивании (преимущество квантового канала в том, что он принуждает подслушивание быть активным). Если передача не была нарушена, они соглашаются использовать эти общие секретные биты известным образом в качестве одноразового блокнота для шифрования смысла последующих осмысленных коммуникаций или для других криптографических приложений (например, аутентификаци-

онных тегов), требующих общей случайной информации. Если передача была нарушена, они отбрасывают ее и пытаются снова, откладывая любые осмысленные коммуникации до тех пор, пока им не удастся передать достаточное количество случайных битов через квантовый канал для использования его в качестве одноразового блокнота. Подробнее, один пользователь ('Алиса') выбирает случайную строку битов и случайную последовательность баз поляризации (прямоугольную или диагональную). Затем она отправляет другому пользователю ('Бобу') поезд фотонов, каждый из которых представляет один бит строки в выбранной для этой позиции бита базе, горизонтальный или 45-градусный фотон означает бинарный ноль, а вертикальный или 135-градусный фотон означает бинарную единицу. По мере того как Боб получает фотоны, он решает, случайным образом для каждого фотона и независимо от Алисы, измерять ли поляризацию фотона в прямоугольной или диагональной базе и интерпретировать результат измерения как бинарный ноль или единицу. При попытке измерить линейную поляризацию диагонального фотона, или наоборот, генерируется случайный ответ, и вся информация теряется. Таким образом, Боб получает осмысленные данные только от половины фотонов, которые он обнаруживает, те, для которых он угадал правильный базис поляризации. Информация Боба дополнительно ухудшается тем, что, в реалистичном случае, некоторые фотоны будут потеряны в пути или не будут засчитаны неполностью эффективными детекторами Боба. Последующие шаги протокола происходят через обычный общественный канал связи, предполагаемый подверженным подслушиванию, но не внедрению или изменению сообщений. Сначала Боб и Алиса определяют, посредством публичного обмена сообщениями, какие фотоны были успешно получены, и из них, какие были получены в правильном базисе. Если квантовая передача не была нарушена, Алиса и Боб должны согласовать биты, закодированных этими фотонами, даже если эти данные никогда не обсуждались по общедоступному каналу. Каждый из этих фотонов, другими словами, предположительно несет один бит случайной информации (например, является ли прямоугольный фотон вертикальным или горизонтальным), известный Алисе и Бобу, но никому другому. Из-за случайной смеси прямоугольных и

диагональных фотонов в квантовой передаче любое подслушивание несет риск изменения передачи таким образом, чтобы вызвать рассогласование между Бобом и Алисой по некоторым битам, о которых они считают, что должны сбыть согласованными . В частности, можно показать, что ни одно измерение фотона в пути, сделанное подслушивателем, который узнал о начальной базе фотона только после того, как сделал свои измерения, не может дать более 1/2 ожидаемых битов информации о ключевом бите, закодированном этим фотоном; и что любое такое измерение, давая n битов ожидаемой информации (n le 1/2), должно вызвать несогласие с вероятностью не меньше n/2, если измеренный фотон или его поддельная копия впоследствии будет снова измерена в его начальной базе. (Этот оптимальный компромисс происходит, например, когда подслушиватель измеряет и повторно передает все перехваченные фотоны в прямоугольной базисе, тем самым узнавая правильные поляризации половины фотонов и вызывая несогласия в 1/4 из них, которые позже будут повторно измерены в начальной базе.) Таким образом, Алиса и Боб могут проверить наличие подслушивания, публично сравнив некоторые биты, по которым они считают, что должны согласиться, хотя, конечно, это пожертвует секретностью этих битов. Позиции битов, использованные в этом сравнении, должны быть случайным подмножеством (скажем, одна треть) правильно полученных битов, чтобы подслушивание более чем нескольких фотонов было маловероятно. Если все сравнения согласуются, Алиса и Боб могут заключить, что квантовая передача была осуществленна без существенного подслушивания, и те из оставшихся битов, которые были отправлены и получены в том же базисе , также согласуются и могут быть безопасно использованы в качестве одноразового блокнота для последующих безопасных коммуникаций по общедоступному каналу. Когда этот одноразовый блокнот будет использован, протокол повторяется для отправки новой порции случайной информации через квантовый канал. Для иллюстрации вышеуказанного протокола далее приводится следующий пример. Необходимость в том, чтобы общественный (не квантовый) канал в этой схеме был защищен от активного подслушивания, может быть смягчена, если Алиса и Боб предварительно договорились о небольшом сек-

ретном ключе, который они используют для создания аутентификационных тегов Вегмана-Картера для своих сообщений по общедоступному каналу. Более подробно схема аутентификации множества сообщений Вегмана-Картера использует небольшой случайный ключ для создания зависящего от сообщения "тега"(подобного контрольной сумме) для произвольно большого сообщения таким образом, что подслушиватель, не знающий ключ, имеет только небольшую вероятность создать другие действительные пары сообщение-тег. Тег таким образом предоставляет доказательство того, что сообщение является законным, и не было сгенерировано или изменено кем-то, не знающим ключа. (Биты ключа постепенно исчерпываются в схеме Вегмана-Картера и не могут быть повторно использованы без компрометации доказуемой безопасности системы; однако в данном приложении эти биты ключа могут быть заменены свежими случайными битами, успешно переданными через квантовый канал.) Подслушиватель все еще может предотвратить связь, подавляя сообщения в общедоступном канале, так же как он может подавить или чрезмерно помешать фотонам, отправленным через квантовый канал. Однако в любом случае Алиса и Боб с большой вероятностью заключат, что их секретные коммуникации подавляются, и не будут обмануты, думая, что их связь защищена, когда на самом деле это не так.

1.1.3 Протокол B92

В 1992 году Чарльзом Беннетом был предложен альтернативный подход к протоколам квантовой коммуникации. В 1.1.2 рассматривался протокол, который использует четыре попарно ортогональных, которые находятся в одном базисе, состояния для кодирования квантовых состаяний. В случае же протокола B92 предлагается использование всего двух неортогональных состояний из двух базисов. Благодаря этому протокол Б92 считается одним из самых простейших в реализации за счет использования необходимого минимума количества состояний для распределения ключа.

Распределение ключей - это термин, применяемый к техникам, позволяющим

двум сторонам получить последовательность случайных бит ("ключ") с высоким уровнем уверенности в том, что никто другой не знает его или имеет значительную частичную информацию о нем. Одна сторона (в дальнейшем "Алиса"), например, может сгенерировать ключ с помощью физического случайного процесса, сделать его копию и лично передать копию другой стороне (в дальнейшем "Боб"). Такие общие секретные биты ключа, хотя и случайные, и бессмысленные по себе, являются ценным ресурсом, поскольку позволяют обменивающимся сторонам достичь, с доказанной безопасностью, двух основных целей криптографии: шифрование последующего значимого сообщения, чтобы сделать его непонятным для третьей стороны, и подтверждение легитимному получателю, что сообщение (обычное или зашифрованное) не было изменено в пути.

Если две стороны изначально не обмениваются секретной информацией и общаются исключительно через классические сообщения, которые мониторятся незаконным прослушивателем, для них невозможно получить сертифицированный секретный ключ. Однако это становится возможным, если они обмениваются как классическими публичными сообщениями (которые могут быть мониторены, но не изменены или подавлены прослушивателем), так и квантовыми передачами, которые имеют свойство того, что их можно подавить или изменить, но не могут в принципе быть мониторены без нарушения. Было показано, что различные типы квантовых передач достаточны: случайная последовательность частиц со спином $1/2$ или одиночных фотонов в четырех некоординированных поляризационных состояниях (например, в линейной или циркулярной поляризациях); аналогичная случайная последовательность низкоинтенсивных поляризованных когерентных или несогласованных импульсов света; последовательность поляризационно-запутанных состояний Эйнштейна-Подольского-Розена (ЭПР) двухфотонных состояний; и аналогичная последовательность пространственно-временно-запутанных двухфотонных состояний, произведенных, например, параметрической конвертацией. Данный протокол работает следующим образом.

1. а) В случае использования ЭПР, Алиса выбирает случайный базис измерений для одного фотона из ЭПР пары: перпендикулярный или циркулярный базис. Другой фотон из пары измеряется Бобом в шаге 3.
2. а) Измерения Алисы определяют случайную последовательность состояний для фотона Боба: горизонтально поляризованный, вертикально, левоциркулярно или правоциркулярно, через ЭПР-корреляции.
   б) В случае использования ослабленных когерентных состояний, Алиса готовит случайную последовательность фотонов с различными состояниями поляризации: горизонтальной, вертикальной, левоциркулярной или правоциркулярной
3. Боб измеряет свой фотон, используя случайную последовательность базисов.
4. Результаты измерений Боба. Некоторые фотоны не получены из-за неполной эффективности детектора. (Реалистичные детекторы также иногда генерируют ошибки из-за темного счета, которые можно обнаружить и исправить, как описано в [5])
5. Боб сообщает Алисе, какие базисы он использовал для каждого полученного им фотона
6. Алиса сообщает ему, какие базисы были правильными.
7. Алиса и Боб оставляют только данные из правильно измеренных фотонов, отбрасывая все остальное
8. Эти данные интерпретируются как двоичная последовательность в соответствии с кодирующей схемой (0 и 1).
9. Боб и Алиса проверяют свой ключ, публично выбирая случайное подмножество позиций бит и проверяя, что это подмножество имеет одинаковую четность в версиях ключа у Боба и Алисы (здесь четность нечетная). Если бы их ключи отличались в одной или нескольких позициях бит, эта проверка должна была бы обнаружить этот факт с вероятностью 0.5.

10. Оставшийся секретный ключ после того, как Алиса и Боб отбросили один бит из выбранного подмножества на шаге 9, чтобы компенсировать информацию, утекшую при раскрытии его четности. Шаги 9 и 10 повторяются k раз, с k независимыми случайными подмножествами, чтобы с вероятностью $1 - 2^{-k}$ удостовериться в том, что ключи Алисы и Боба идентичны, за счет уменьшения длины ключа на k бит. беспокоиться о том, что их ключ был нарушен подслушиванием и должен быть отброшен.

$1 - \langle \mu_1 \,|\, \mu_2 \rangle \neq 0$ Для начала распределения ключа Алиса подготавливает и отправляет Бобу случайную двоичную последовательность квантовых систем, используя состояния ($|u_1\rangle$) и ($|u_2\rangle$), чтобы представлять биты 0 и 1 соответственно. Затем Боб решает, случайным образом и независимо от Алисы для каждой системы, подвергнуть ли ее измерению P_0 или P_1. Затем Боб сообщает Алисе публично, в каких случаях его измерение дало положительный результат (но, конечно же, не сообщает, какое измерение он сделал), и обе стороны соглашаются отбросить все остальные случаи. Если не было подслушивания, оставшиеся случаи, примерно в доле $(1 - \langle \mu_1 \,|\, \mu_2 \rangle)/2$ от исходных испытаний, должны быть идеально скоррелированы, состоящими полностью из случаев, когда Алиса отправила ($|u_1\rangle$) и Боб измерил P_0, или Алиса отправила ($|u_2\rangle$) и Боб измерил P_1. Однако, прежде чем Алиса и Боб смогут доверять этим данным как ключу, они должны, как и в других схемах распределения ключей, пожертвовать некоторую часть для проверки того, что их версии ключа действительно идентичны. Это также удостоверяет отсутствие подслушивания, которое неизбежно нарушило бы состояния ($|u_1\rangle$) или ($|u_2\rangle$) в пути, вызывая иногда положительные результаты при последующих измерениях P_1 или P_0, соответственно. На рисунке 1.1 показана практическая интерферометрическая реализация, в которой два неортогональных состояния ($|\mu_1\rangle$) и ($|\mu_2\rangle$) представлены слабыми когерентными световыми импульсами, различающимися по фазе относительно сопровождающего яркого эталонного импульса (яркие когерентные состояния, обычно почти ортогональные, становятся значительно неортогональными, когда их ослабляют до ожидаемой интенсивности одного фотона, потому что все такие слабые состояния включают значительную компоненту состояния нуле-

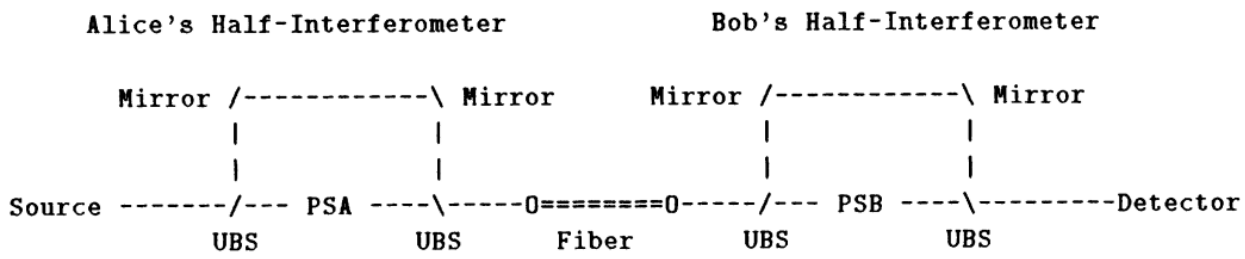

Рисунок 1.1 — Интерферометрическое квантовое распределение ключей с использованием двух неортогональных низкоинтенсивных когерентных состояний. Источник слева поставляет когерентный импульс (волнообразная форма -W-) с интенсивностью ожидаемых фотонов M) 1 в полуинтерферометр Алисы, где несимметричные разделители пучков (UBS), зеркала и фазовый модулятор (PSA 0 или 180 градусов) производят слабый сигнальный импульс (волнообразная форма -w- или, сдвинутый по фазе, -m-), за которым следует яркий опорный импульс -%-. Отправленные к Бобу через одномодовое оптическое волокно, импульсы входят в полуинтерферометр Боба, где в зависимости от того, является ли сумма фазовых сдвигов Алисы и Боба (PSA+PSB) равной 0 или 180 градусов, сигнальный импульс проходит через верхнее или нижнее плечо интерферометра и происходит констурктивная или деструктивно интерференция с ослабленным опорным импульсом перед входом в детектор. Перед этим интерференционным импульсом прибывает очень тусклый импульс (не показан), ослабленный как Алисой, так и Бобом, но ни разу не задержанный. После интерференционного импульса прибывает яркий дважды задержанный опорный импульс (волнообразная форма -W-), который Боб контролирует, чтобы убедиться, что опорные импульсы не подавляются. Также не показаны два неиспользуемых пучка, выходящих из правого делителя пучка каждого полуинтерферометра вниз.

вого количества фотонов). Начиная слева на рисунке, Алиса использует ряд несимметричных делителей пучка и зеркал, чтобы разделить начальный когерентный импульс на два импульса, разделенных во времени: слабый сигнальный импульс интенсивностью p $\neq$ 1 ожидаемый фотон, за которым следует яркий эталонный импульс с M $\neq$ 1 ожидаемым фотоном. Сигнальный импульс сдвигается фазово (PSA) на 0 или 180 градусов для кодирования битов 0 и 1, затем запускается в одномодовое оптическое волокно. Более яркий эталонный импульс не сдвигается по фазе, но задерживается на фиксированное время ht, затем также запускается в то же волокно. На приемном конце аппарата Боб использует полуинтерферометр, аналогичный Алисе, чтобы снова разде-

лить входной пучок, в том же соотношении, что и ранее, на слабую и яркую части. Как и ранее, слабая часть сдвигается по фазе (PSB) на 0 или 180 градусов, случайным образом и независимо от фазовых сдвигов Алисы, в то время как яркая часть задерживается на ht. Наконец, две части приводятся в интерференцию при входе в детектор. Волна, входящая в детектор, состоит из трех импульсов, разделенных временем Δt. Первый импульс, очень слабый импульс, который был ослаблен как Бобом, так и Алисой, но не задержан ни одним из них, далее не рассматривается. Второй импульс, содержащий важную ключевую информацию, представляет собой слабый импульс, состоящий из суперпозиции луча, задержанного Алисой и ослабленного Бобом, и луча, задержанного Бобом и ослабленного Алисой. Если фазовые сдвиги Алисы и Боба равны, произойдет конструктивное интерферирование, и суперпозиционный импульс сгенерирует счет с вероятностью, равной $4T_q$ ожидаемых фотонов, где T - коэффициент передачи волокна, а q - квантовая эффективность детектора. Если фазовые сдвиги Алисы и Боба отличаются, интенсивность суперпозиционного импульса будет намного ниже, идеально - ноль в пределе идеального выравнивания интерферометра (время когерентности источника света здесь не имеет значения, поскольку два интерферирующих импульса точно пропорциональны, будучи ослабленными версиями одного и того же исходного импульса). Наконец, с задержкой δ t после суперпозиционного импульса к детектору Боба приходит яркий импульс, который был задержан как Алисой, так и Бобом, но не был ослаблен ни одним из них. Боб подтверждает его прибытие, с приблизительной ожидаемой интенсивностью MT, что он может сделать надежно, если MT_q) 1. Этот третий импульс не содержит фазовой информации, но служит для подтверждения того, что опорный импульс действительно прибыл. Таким образом, он защищает от атаки, при которой подслушиватель ("Ева") измеряет каждую пару сигнально-опорных импульсов прибором, аналогичным прибору Боба, повторно передает корректно сфабрикованную пару импульсов, когда ей это удается, и подавляет как сигнальный, так и опорный импульсы, когда это не удается, таким образом, подслушивая канал без создания ошибок в последующих результатах измерений Боба. Ива не может подавить опорный импульс

без немедленного обнаружения. Но если она подавит только сигнальный импульс, неподавленный опорный импульс все равно вызовет счет в детекторе Боба с вероятностью pTq, и половина этих счетов приведет к ошибкам в ключе Боба. Кодирование каждого бита в разнице фаз между слабым сигнальным импульсом и сопровождающим его ярким опорным импульсом предоставляет практический способ реализации операторов, аналогичных Po и P , которые дают гарантированный нулевой результат только для двух законных сигналов (μ_i) и (μ_o), соответственно, но не для фальшивых сигналов (например, вакуумного состояния), которые подслушиватель может подменить. Разделение сигнальных и опорных импульсов по времени также позволяет им передаваться через один и тот же оптический волоконный кабель, что автоматически компенсирует фазовые дрейфы окружающей среды в кабеле, которые в противном случае сделали бы такой большой интерферометр невыполнимым.

Поскольку любая пара когерентных или не когерентных оптических сигналов значительно становится некоординированной при низкой интенсивности, кажется, что почти любой источник двух видов слабых световых вспышек, например, очень ослабленный красный по сравнению с зеленым светофором, можно использовать для распределения ключей без сложностей интерферометрии. Алиса случайным образом отправляет красные и зеленые вспышки с интенсивностью 1 фотон, а Боб публично сообщает, какие вспышки он видел, но не их цвета, которые составляют секретный ключ. Из-за низкой интенсивности Боб может быть уверен, что пассивный злоумышленник, стоящий рядом с ним и наблюдающий за тем же источником сигнала, не увидит того же подмножества импульсов, и, следовательно, будет иметь не всю информацию о ключе, который будет согласован Алисой. Однако более вторженческая Ева, стоящая между Алисой и Бобом, может полностью нарушить схему, перехватывая все вспышки Алисы и пересылая вспышку Бобу только тогда, когда сама видит вспышку Алисы, просто останавливая остальные. Чтобы компенсировать их уменьшенное количество, поддельные вспышки Евы должны быть пропорционально ярче, так чтобы вероятность Боба видеть оставалась той же самой (осторожная Ева должна была бы создавать вспышки с не-Пуассонов-

ской статистикой числа фотонов, чтобы имитировать распределение Пуассона с меньшим средним значением). В терминах формализма операторов проекции, обсуждаемого ранее, схема с красным и зеленым не работает, потому что два сигнала, которые Алиса отправляет здесь, не являются чистыми состояниями, а являются статистическими смесями, в которых фаза электрического поля случайна. Поэтому любой оператор Po, который уничтожает все красные вспышки Алисы, также уничтожит вакуумное состояние, поскольку его можно рассматривать как суперпозицию двух красных вспышек с противоположной фазой. Таким образом, Ева может безопасно заменять вакуумное состояние на любую вспышку, которую она не обнаруживает. В отличие от этого, в интерферометрической схеме на рисунке 1.1 нет поддельного сигнала, который могла бы подменить подслушивающая сторона, чтобы скрыть свое неудачное обнаружение первоначального сигнала, и схема остается надежной. Эти соображения можно обобщить, чтобы заключить, что распределение ключей возможно не только с использованием любых двух некоординированных чистых состояний (μ_n) и (u), но и любых двух некоординированных смешанных состояний po и p которые охватывают не пересекающиеся подпространства гильбертова пространства, позволяя Бобу найти два оператора Po и P, таких что Po уничтожает p и P уничтожает P_0, но никакое состояние не уничтожается обоими операторами. Требование охвата не пересекающихся подпространств отсутствует в схемах распределения ключей, использующих более двух смешанных состояний, позволяя таким схемам (например, схеме, которая использует четыре некоординированных не когерентных состояния) быть реализованными с помощью простого квадратичного обнаружения оптических сигналов, а не интерферометрического гомодинного обнаружения, как в рисунке 1.1

1.1.4 Протокол квантовой коммуникации с использованием недоверенного приеммного узла

Существующие протоколы квантовой коммуникации строятся на топологии "точка-точка в которых участвует всего 2 пользователя: приемник и передатчик. Однако у такого подхода есть уязвимости, связанные с возможностью злоумышленника контролировать детектор одиночных фотонов, используемого в блоке приемника. Или же использовать другие каналы утечки информации из-за несовершенства детектора одиночных фотонов: различный временной отклик, наличие обратной вспышки при регистрации фотона. Как решение всех известных уязвимостей детекторов одиночных фотонов был разработан протокол КРК с недоверенным приемным узлом (НПУ-КРК) или же Measurement-Device-Independent Quantum Key Distribution (MDI-QKD).
В данной работе представлена идея квантовой криптографии с измерениями, независимыми от устройства (MDI-QKD), как простое решение для устранения всех (существующих и еще не обнаруженных) каналов утечки информации, связанных с детектором [2], пожалуй, самой критической части реализации, и показываем, что у нее как отличные показатели безопасности, так и производительности. Таким образом, она предлагает огромное преимущество в безопасности по сравнению со стандартными доказательствами безопасности, такими как доказательства Инамори-Люткенхауса-Майерса (ILM) [3] и Готтесмана-Ло-Люткенхауса-Прескилла (GLLP). [4] Более того, данный подход позволяет удвоить дальность передачи, которую могут покрыть те схемы квантовой криптографии, которые используют обычные полупроводниковые лазеры, а ее скорость генерации ключей сравнима со стандартными доказательствами безопасности с использованием запутанных пар. В отличие от квантовой криптографии с прямыми измерениями (DI-QKD), в ее простейшей формулировке MDI-QKD требует дополнительного предположения о том, что у Алисы и Боба почти идеальная подготовка состояний. Однако мы считаем, что это всего лишь небольшое препятствие, потому что источники сигнала Алисы и Боба могут быть ослабленными лазерными импульсами, подготовленными ими самими.

Их состояния могут быть экспериментально проверены в полностью защищенной лабораторной среде за пределами вмешательства Евы через случайную выборку. Более того, как будет обсуждаться позже, недостатки в процессе подготовки Алисы и Боба на самом деле могут быть легко устранены в более точной формулировке протокола.

Простой пример нашего метода следующий. Как Алиса, так и Боб подготавливают слабые когерентные импульсы (СКИ) с фазовым кодированием в четырех возможных поляризационных состояниях BB84 (т. е. вертикальном, горизонтальном, поляризованном под углом 45 и 135 градусов) [5] и отправляют их ненадежному ретранслятору Чарли (или Еве), находящемуся посередине, который выполняет измерение состояния Белла, проецирующее входные сигналы в состояние Белла. Такое измерение может быть реализовано, например, с использованием только линейных оптических элементов с установкой, показанной на рисунке 1.1.4 (На самом деле, такая установка определяет только два из четырех состояний Белла. Но это не проблема, поскольку любое состояние Белла позволяет доказать безопасность.) Кроме того, Алиса и Боб применяют методы фальшивых состояний, чтобы оценить усиление (т. е. вероятность успешного результата ретранслятора) и квантовую погрешность бита (QBER) для различных чисел входных фотонов. После завершения квантовой коммуникационной фазы Чарли использует открытый канал для объявления событий, где он получил успешный результат в ретрансляторе, а также свой результат измерения. Алиса и Боб сохраняют данные, соответствующие этим случаям, и отбрасывают остальные. Кроме того, как и в BB84, они на этапе постобработки выбирают события, где они используют тот же базис в своей передаче с помощью аутентифицированного открытого канала. Наконец, чтобы гарантировать, что их битовые строки правильно коррелируются, Алиса или Боб должны применить инверсию бита к своим данным, за исключением случаев, когда они оба выбирают диагональную базу и Чарльз получает успешный результат измерения, соответствующий тройному состояний. Давайте теперь подробно оценим производительность протокола выше. Для простоты мы рассматриваем улучшенный анализ данных, при котором Алиса и Боб оценивают данные, отправленные в

двух разных базисах [6]. В частности, мы используем прямоугольный базис в качестве базиса генерации ключей, в то время как диагональный базис используется только для тестирования.

Для обзоначений введем $Q^{n,m}_{rect}, Q^{n,m}_{diag}, e^{n,m}_{rect}, e^{n,m}_{diag}$ - обозначают, соответственно, усиление и QBER сигнальных состояний, отправленных Алисой и Бобом, где n и m обозначают количество фотонов, отправленных законными пользователями, a rect или diag представляет их выбор базиса.

(A) Прямоугольный базис.Ошибка соответствует успешному выводу ретранслятора, когда и Алиса, и Боб подготавливают одно и то же поляризационное состояние (т. е. их результаты должны быть антикоррелированы до применения инверсии бита). Предполагая на данный момент идеальные оптические элементы и детекторы, и отсутствие смещения, мы имеем, что каждый раз, когда Алиса и Боб отправляют, соответственно, n и m фотонов, подготовленных в одном и том же поляризационном состоянии, ретранслятор никогда не выдаст успешный результат. Таким образом, мы получаем, что $e^{n,m}_{rect}$ равно нулю для всех n, m. Это означает, что для отфильтрованного ключа не требуется коррекция ошибок. Это замечательно, потому что это подразумевает, что использование источников СКИ (вместо однофотонных источников) не существенно снижает скорость генерации лючей протокола квантовой криптографии (в части коррекции ошибок).

(B) Диагональный базис. Чтобы определить количество необходимой амплификации конфиденциальности, мы рассматриваем диагональный базис. Ошибка соответствует проекции на синглетное состояние в случае, когда Алиса и Боб подготавливают одно и то же поляризационное состояние, или на тройное состояние, когда они подготавливают ортогональные поляризации. Предполагая опять же идеальный сценарий, обсуждаемый в предыдущем абзаце, мы находим, что $e^{1,1}_{diag} = 0$. (Это происходит потому, что когда два идентичных однофотонных входят в 50:50 светоделитель, эффект Хонга-Оу-Манделя [7] гарантирует, что оба фотона всегда выйдут из светоделителя вместе в том же самом выходном режиме. Кроме того, если два фотона подготовлены в ортогональных поляризациях и они выходят из 50:50 светоделителя в том же самом

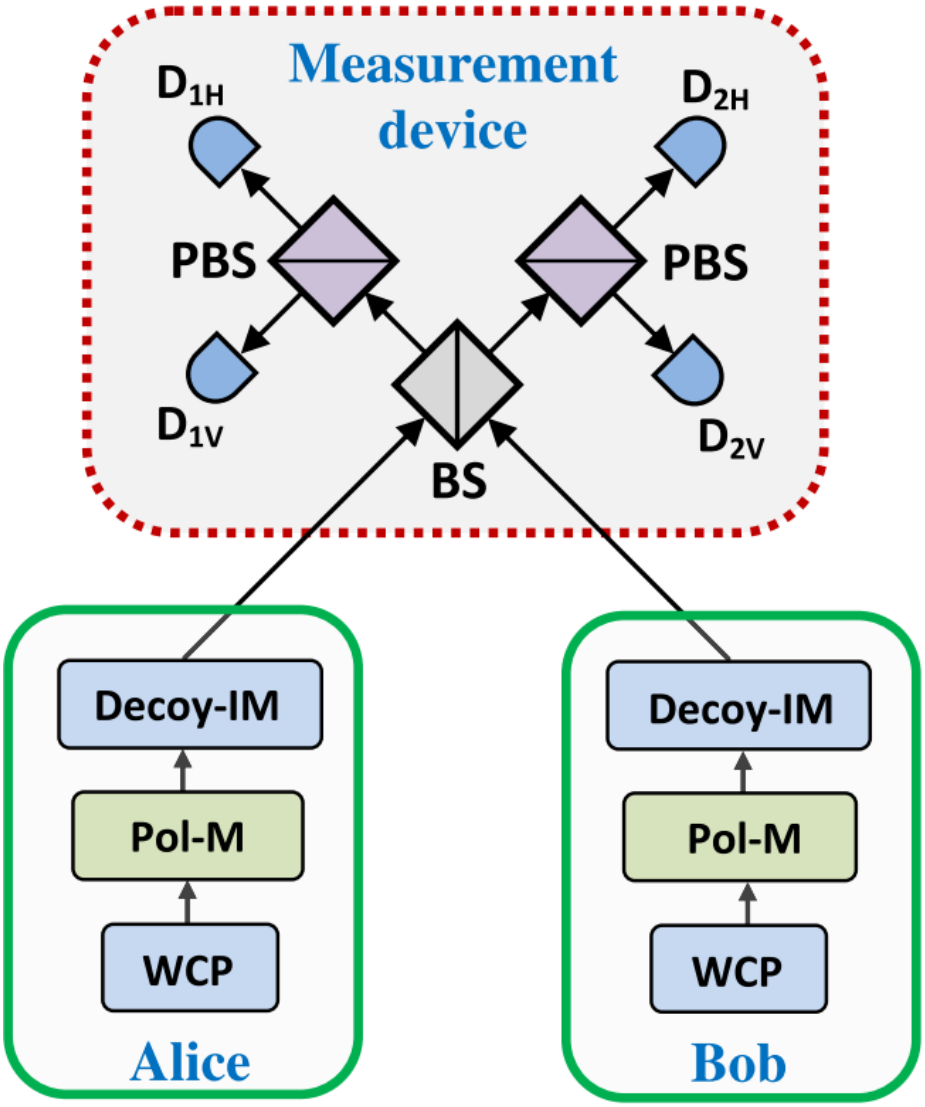

Рисунок 1.2 — Базовая схема протокола MDI-QKD. Алиса и Боб подготавливают фазово случайные слабые когерентные импульсы (СКИ) в разных поляризационных состояниях BB84, которые выбираются независимо и случайным образом для каждого сигнала с помощью модулятора поляризации (Pol-M). Состояния - ловушки генерируются с использованием модулятора интенсивности (Decoy-IM). Внутри измерительного устройства сигналы от Алисы и Боба интерферируют на светоделителе (BS) с коэффициентом деления 50:50, на каждом конце которого находится поляризационный светоделитель (PBS), направляющий входящие фотоны в горизонтальные (H) или вертикальные (V) поляризационные состояния. Четыре фотодетектора используются для обнаружения фотонов, и результаты обнаружения объявляются публично. Успешное измерение состояния Белла соответствует наблюдению активации ровно двух детекторов (связанных с ортогональными поляризациями). Клик в D_{1H} и D_{2V} или в D_{1V} иD_{2H} указывает на проекцию на состояние Белла $|\psi^-\rangle = \frac{1}{\sqrt{2}}(|HV\rangle - |VH\rangle)$, в то время как клик в D_{1H} и D_{1V} или в D_{2H} и D_{2V} показывает проекцию на состояние Белла $|\psi^+\rangle = \frac{1}{\sqrt{2}}(|HV\rangle + |VH\rangle)$. Установки Алисы и Боба надежно защищены от прослушивателя, в то время как измерительное устройство может быть ненадежным.

выходном плече, оба фотона всегда достигнут одного и того же детектора внутри ретранслятора.) Тот факт, что $e_{diag}^{1,1}$ равно нулю, вновь поразителен, так как это означает, что использование источников СЦИ существенно не снижает скорость генерации ключей (также в части усиления секретности).

(C) Скорость генерации ключей. В идеальном сценарии, описанном выше, скорость генерации ключей будет просто определяться как $R = Q_{rect}^{1,1}$ в асимптотическом пределе бесконечно длинного ключа. С другой стороны, если мы учтем недостатки, такие как смещение базиса и темные отсчеты, скорость генерации ключей в реалистичной настройке будет определяться как

$$R = Q_{rect}^{1,1}[1 - H(e_{diag}^{1,1})] - Q_{rect} f(E_{rect}) H(E_{rect}) \tag{1.7}$$

, где Q_{rect} и E_{rect} обозначают, соответственно, усиление и QBER в прямоугольном базисе (то есть $Q_{\text{rect}} = \sum_{n,m} Q_{\text{rect}}^{n,m}$ и $E_{\text{rect}} = \sum_{n,m} \frac{Q_{rect}^{n,m} e_{rect}^{n,m}}{Q_{rect}}$, f($E_{rect}$) > 1 функция неэффективности для процесса коррекции ошибок, а H(x) $= -x\log_2(x) - (1-x)\log_2(1-x)$ функция бинарной энтропии Шеннона. Есть несколько нерешенных вопросов, которые нужно прояснить. Во-первых, мы неявно предположили, что метод фальшивых состояний можно использовать для оценки усиления $Q_{rect}^{1,1}$ и QBER $e_{rect}^{1,1}$. Во-вторых, нам нужно оценить секретную скорость ключа, заданную уравнением 1.1.4, для реалистичного устройства Во-вторых, нам нужно оценить секретную скорость ключа, заданную уравнением 1.1.4, для реалистичной настройки. Давайте уточним эти моменты здесь. Действительно, можно показать, что метод оценки соответствующих параметров в формуле для скорости ключа эквивалентен используемому в стандартных системах квантовой криптографии с фальшивыми состояниями (см. дополнительные материалы для подробностей [15]). Для целей моделирования мы рассматриваем неэффективные и шумные пороговые детекторы и используем экспериментальные параметры из [19] за исключением того, что [19] рассматривает канал свободного пространства, тогда как здесь мы рассматриваем канал на основе оптоволокна с потерей 0,2 дБ/км. Более того, для простоты мы предполагаем, что все детекторы идентичны (т.е. у них одинаковая частота темных отсчетов и эффективность обнаружения), и их темные отсчеты, приблизительно, независимы от входящих сигналов. Кроме того, мы используем протокол

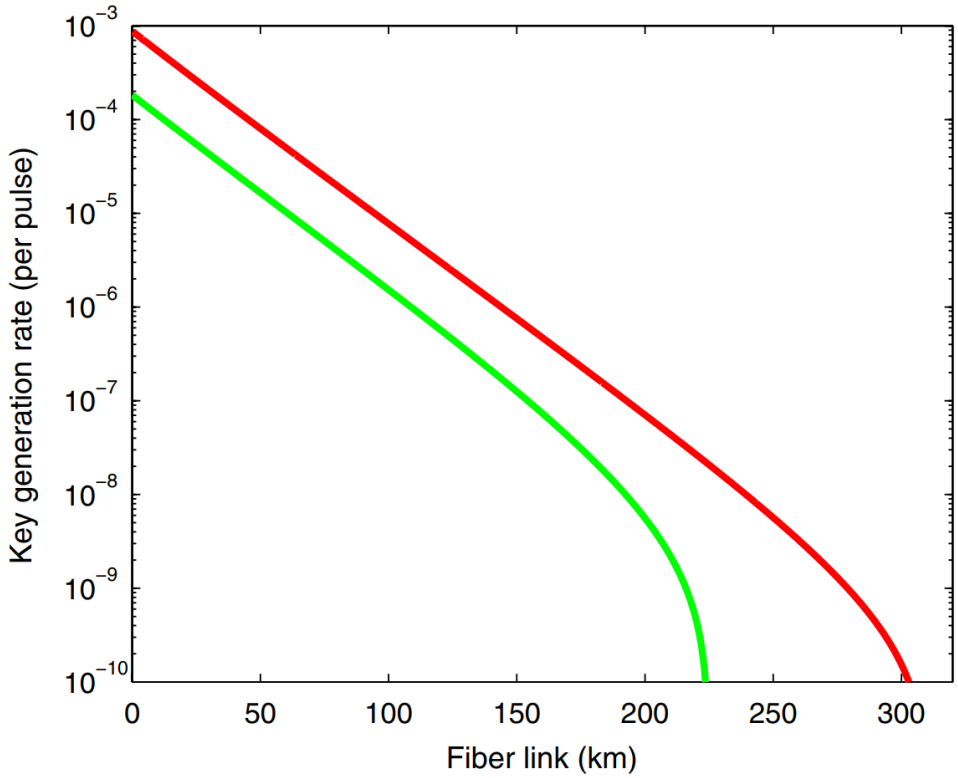

Рисунок 1.3 — Нижняя граница секретной скорости ключа R, заданная уравнением 1.1.4, в логарифмической шкале для установки MDI-QKD с использованием слабых когерентных импульсов, показанной на рисунке 1.1.4 (зеленая кривая). В целях моделирования мы рассматриваем следующие экспериментальные параметры: коэффициент потерь канала составляет 0,2 дБ/км, внутренняя ошибка из-за смещения и нестабильности оптической системы составляет 1,5%, эффективность обнаружения реле (т. е. пропускная способность его оптических компонентов вместе с эффективностью его детекторов) составляет 14,5%, а фоновая частота счета составляет 6,02 × $10^{(} - 6)$. (Для простоты мы рассматриваем упрощенную модель смещения, помещая унитарное вращение в одну из входных ветвей светоделителя с делением пополам 50:50 и также унитарное вращение в одну из его выходных ветвей. Общее значение смещения составляет 1,5%. То есть, мы предполагаем смещение в 0,75% в каждом вращении.) В сравнении красная кривая представляет нижнюю границу R для протокола квантовой криптографии на основе запутанных пар с источником на основе параметирического преобразования с понижением частоты (PDC), расположенным посередине между Алисой и Бобом [8]. На красной кривой мы предполагаем, что используется оптимальная яркость источника PDC. Однако на практике яркость источника PDC ограничена технологией. Поэтому скорость ключа протокола квантовой криптографии на основе запутанных пар будет значительно ниже, чем показано на красной кривой. Это делает наше новое предложение еще более привлекательным по сравнению с существующими данными на рисунке

коррекции ошибок с функцией неэффективности f(E_{rect}) = 1,16 [20]. Полученная нижняя граница секретной скорости ключа проиллюстрирована на рис. 2. Наши расчеты и результаты моделирования показывают, что скорость генерации ключей существенно сравнима с доказательством безопасности [8] для протоколов квантовой криптографии на основе запутанных пар. Наша схема может выдерживать высокие оптические потери более 40 дБ (т. е. 200 км оптоволокон), если ретранслятор размещается посередине между Алисой и Бобом. Другими словами, можно практически удвоить дистанцию передачи по сравнению с установкой, где аппарат измерения состояния Белла находится у Алисы, или установкой с использованием стандартного протокола BB84 с фальшивыми состояниями [22]. Чтобы экспериментально реализовать предложенный протокол MDI-QKD, несколько практических вопросов требуют решения. Среди них, возможно, самый важный - это то, как генерировать неразличимые фотоны из двух независимых лазерных источников и наблюдать стабильное интерференционное явление Хонга-Оу-Манделя [17]. Обратите внимание, что физика, лежащая в основе этого протокола, основана на явлении группировки фотонов в одну группу двух неразличимых фотонов на 50:50 светоделителе. Мы провели простой эксперимент принципиального доказательства, чтобы показать, что высокая видимость интерференции Хонга-Оу-Манделя между двумя независимыми лазерами, которые возможно приобрести, вполне осуществима. Результаты показаны на рис. 3. Согласованность между экспериментальными и теоретическими результатами подтверждает, что высокая видимость интерференционного провала Хонга-Оу-Манделя может быть достигнута даже с двумя независимыми лазерами. Идею MDI-QKD можно обобщить намного дальше. Во-первых, она также применима в случае, когда Алиса и Боб используют запутанные пары фотонов в качестве источников. Во-вторых, она работает даже в том случае, когда процессы подготовки Алисы и Боба неидеальны. Действительно, зависимость от базиса, возникающая из недостатка в процессах подготовки Алисы и Боба, может быть легко устранена с помощью идеи квантовой монетки [11,18], чтобы количественно оценить количество зависимого от базиса недостатка [24]. В-третьих, заметим, что в практических приложениях потре-

буется только конечное количество фальшивых состояний. Это аналогично стандартным протоколам квантовой криптографии с конечными фальшивыми состояниями [9], которые широко используются в экспериментах [10]. В-четвертых, MDI-QKD работает даже без уточненного анализа данных. В-пятых, она также работает для других протоколов квантовой криптографии, включая протокол из шести состояний [11]. Эти вопросы, вместе с учетом эффектов конечного размера, возникающих потому, что Алиса и Боб отправляют только конечное количество сигналов в каждом запуске протокола квантовой криптографии [12].

В заключение, мы предложили идею квантовой криптографии с измерительно-устройствонезависимым подходом (MDI-QKD). По сравнению со стандартными доказательствами безопасности, у него есть ключевое преимущество в удалении всех каналов боковых сигналов детектора, и он может удвоить дистанцию передачи, охватываемую с помощью обычных протоколов квантовой криптографии с использованием слабых когерентных импульсов. Более того, у него довольно высокая скорость генерации ключей, которая сравнима с таковой в стандартных доказательствах безопасности. Действительно, его скорость генерации ключей на порядки выше, чем предыдущий подход полностью измерительно-устройствонезависимой квантовой криптографии. Нашу идею можно реализовать с помощью стандартных пороговых детекторов с низкой эффективностью обнаружения и каналов с высокими потерями. Учитывая его отличную безопасность, производительность и простую реализацию, мы считаем, что MDI-QKD является большим шагом вперед в сокращении разрыва между теорией и практикой квантовой криптографии, и ожидаем, что он будет широко применяться в практических системах квантовой криптографии в будущем.

1.1.5 Протокол квантовой коммуникации с использованием полей близнецов

Значительный теоретический прогресс в достижении практического безопасного QKD на больших расстояниях был достигнут с предложением QKD с двойным полем (TFQKD) [4], которое улучшает масштабирование ключевой скорости в соответствии с квадратным корнем из пропускания канала. Он показывает, что источник когерентного состояния на самом деле может быть преимуществом по сравнению с однофотонным источником, поскольку постселекция фазовой когерентности двойных полей Алисы и Боба может потенциально привести к безопасному QKD с кодирующим состоянием одного фотона и вакуума, а также их линейных суперпозиций. Этот метод способен достичь скорости передачи ключей, зависящей от квадратного корня из коэффициента пропускания канала, и, таким образом, преодолеть известное ограничение по расстоянию для существующих протоколов практического QKD. Теоретически безопасная ключевая скорость может быть даже выше, чем возможности секретных ключей без ретрансляторов, известные как границы Такеока-Гуха-Вильде [19] и Пирандола-Лауренца-Оттавиани-Бьянки (PLOB) [20]. Однако для того, чтобы сделать это реальностью, еще предстоит проделать значительную работу. Во-первых, существует теоретическая проблема объединения постселекции фазовой информации с традиционным методом ложных состояний. Во-вторых, это технически сложная задача точной интерференции одиночных фотонов на большом расстоянии. Для достижения этой цели был предложен протокол "посылать или не посылать"(SNS) [21]. Он предполагает малые вероятности отправки для Алисы и Боба, а затем использует решения об отправке и отказе от отправки для кодирования битовых значений в базисе Z с эффективными событиями-вестниками, объявляемыми Чарли. Таким образом, как было показано в [21], в протоколе можно продолжать использовать модель с метками и обычный метод ложных состояний. Кроме того, поскольку протокол кодирует битовые значения, используя почти безошибочный базис Z, он может терпеть высокую частоту ошибок в базисе X. В этой работе рассматривается

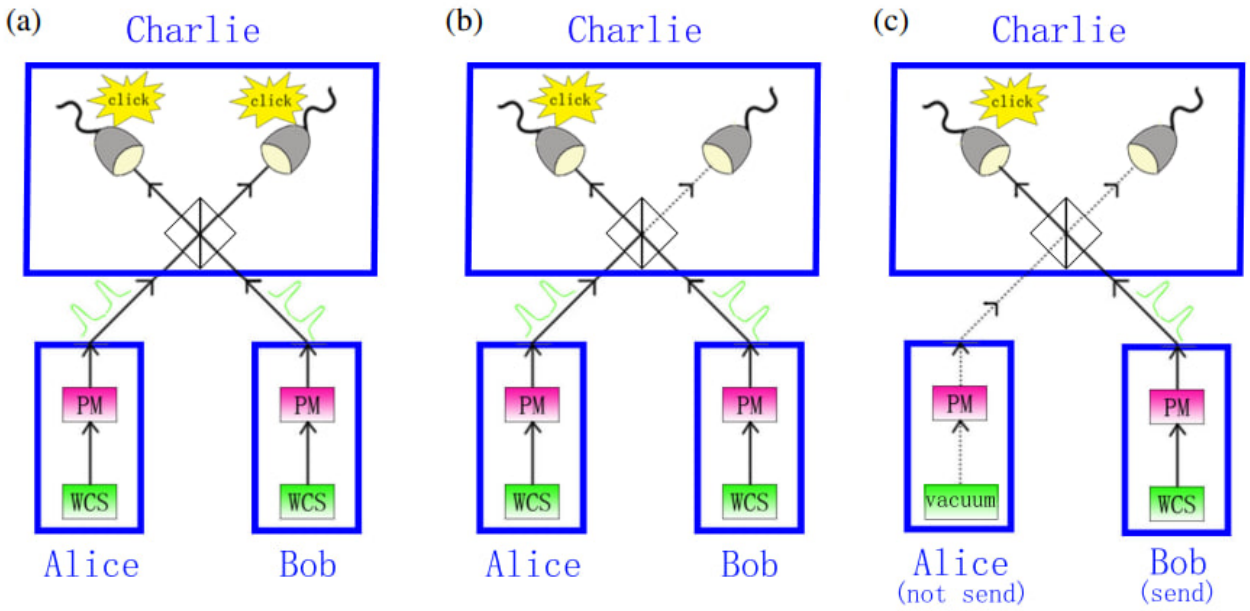

Рисунок 1.4 — Схемы трех различных протоколов. (a) MDIQKD с состояниями-ловушками, где пары импульсов с когерентным состоянием в кодировке BB84 рассылаются, а эффективные события предвещаются двукратным срабатыванием. Скорость передачи ключей линейно зависит от пропускания канала. (b) Оригинальное состояние приманки TFQKD [11], в котором сдвоенные поля когерентных состояний со случайными фазовыми сдвигами посылаются по базам X и Y, а эффективные события возвещаются одиночным щелчком. Скорость передачи ключей зависит от квадратного корня из пропускания канала. Для обоих базисов необходимы однофотонные помехи от удаленных независимых источников. Возможны ошибки рассогласования в обеих базах, и информация о фазовом сдвиге после объявления делает метод "приманка-состояние"недействительным. (c) SNSTFQKD (Sending - not sending TFQKD) с состяниями ловушками [9]. В базисе Z каждая сторона независимо принимает решение об отправке с небольшой вероятностью. События, когда одна сторона решает отправить, другая сторона решает не отправлять, и один и только один детектор щелкает (как показано на рисунке), являются целевыми событиями для генерации защищенных ключей. Он отказоустойчив к большой ошибке смещения в базисе X, так как ошибка смещения в базисе Z отсутствует. Традиционный метод "приманка-состояние"работает, поскольку информация о фазовом сдвиге в базисе Z никогда не объявляется. Объявление одного щелчка делает эффективными события в базисе Z, а ключевая скорость находится в масштабе квадратного корня из пропускания канала. WCS: слабый когерентный источник

экспериментальная демонстрация КРК с полями-близнецами через протокол SNS (SNSTFQKD) по катушкам оптического волокна. Протокол.- Рассмотрим схему протокола SNSTFQKD [8], показанную на рисунке 1.4. Здесь мы реализуем протокол с помощью практического метода четырех интенсивностей [13], где каждая сторона использует четыре различные интенсивности, а именно 0, μ_1, μ_2 и μ_z. Алиса и Боб случайным образом выбирают базис X или Z с вероятностями pX и 1 - pX, соответственно. В базисе X Алиса и Боб готовят и посылают импульсы-обманки. Фазовые сдвиги θ_A и θ_B частным образом накладываются на их импульсы. Событие в базисе Z считается эффективным, если Чарли объявляет, что щелкнул только один детектор. Для того чтобы событие X-базиса было эффективным, нам необходимо дополнительное условие фазового среза, чтобы уменьшить наблюдаемую частоту ошибок в базисе. Без разумного условия фазового среза наблюдаемый коэффициент ошибок в базисе X может быть слишком большим, чем фактический коэффициент ошибок в базисе Z. Обратите внимание, что Чарли не обязан быть честным, и все, что он объявляет, не подрывает безопасность. Но если Чарли хочет сделать хорошую ключевую ставку, ему придется постараться сделать правдивое объявление обо всем. Ошибка в базисе X определяется как объявление Чарли о щелчке правого (левого) детектора, связанном с эффективным событием в базисе X, когда разница фаз между парой импульсов от Алисы и Боба, вероятно, вызвала бы щелчок слева (справа) на измерительной установке Чарли. Эффективное событие в базисе Z, которое Алиса (Боб) решила отправить, а Боб (Алиса) решил не отправлять, соответствует значению бита 1 (0). Значения ε_1^{ph} и s_1, выход однофотонных эффективных событий в базисе Z, могут быть рассчитаны обычным методом ложных состояний. Схема эксперимента показана на рисунке 1.5(a). В установках Алисы и Боба в качестве источников света используются независимые лазеры с непрерывной волной (cw). Свет модулируется на 16 различных фаз с помощью фазового модулятора (ФМ) и кодируется с помощью трех амплитудных модуляторов (АМ). В эксперименте мы устанавливаем базовый период 5 мкс, в течение которого в первые 3 мкс посылается 100 сигнальных импульсов с шириной импульса 2 нс и интервалом

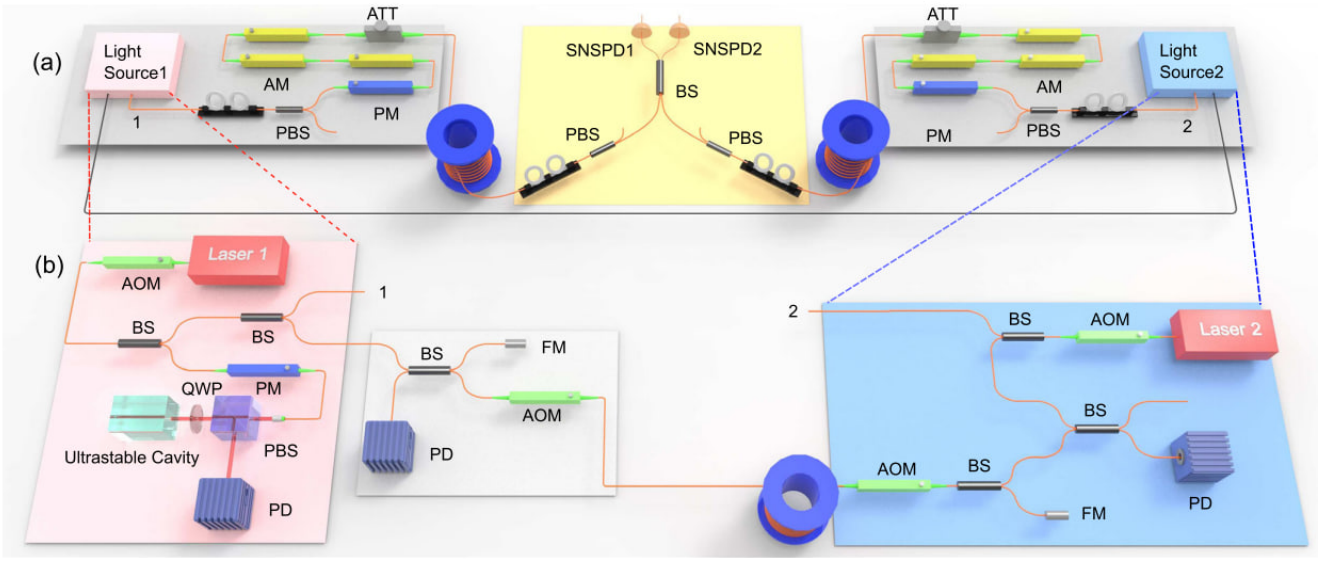

Рисунок 1.5 — (a) Схема нашей экспериментальной установки. В качестве источников Алиса и Боб используют непрерывный лазер с частотной синхронизацией. Эти лазеры затем модулируются фазовым модулятором (ФМ) и тремя амплитудными модуляторами (АМ) для рандомизации фазы, кодирования и модуляции интенсивности обманки. Затем импульсы ослабляются аттенюатором (ATT) и отправляются по оптоволоконным катушкам к Чарли. На измерительной станции Чарли На измерительной станции Чарли импульсы от Алисы и Боба проходят через поляризационные контроллеры (PC) и поляризационные разветвители луча (PBS), затем интерферируют на разветвителе луча (BS). Наконец, свет измеряется сверхпроводящими нанопроволочными однофотонными детекторами (SNSPD). (b) Система частотной синхронизации для лазеров Алисы и Боба. Длина волокна между Алисой и Бобом установлена равной общей длина сигнального волокна. AOM: акустооптический модулятор, FM: зеркало Фарадея, PD: фотодиод. QWP: четвертьволновая пластина.

30 нс, затем в следующие 1,2 мкс - 4 фазовых опорных импульса для оценки относительной фазы между каналами Алисы и Боба, и в заключительные 0,8 мкс - состояние вакуума в качестве времени восстановления сверхпроводящих нанопроволочных однофотонных детекторов (SNSPDs). Интенсивности сигналов устанавливаются в оптимизированные состояния приманки μ_z, ν_1, ν_2 или 0 . Затем сигналы передаются от Алисы и Боба к Чарли, где они интерферируют. Поскольку для интерференции требуются идентичные входные сигналы, для компенсации поляризационного дрейфа канала необходимы поляризационные контроллеры (PC) и поляризационные разветвители луча (PBS) перед поляризационными поддерживающими разветвителями луча (BS). Результаты

интерференции затем обнаруживаются с помощью SNSPD и регистрируются с помощью высокоскоростного устройства регистрации времени. Основной технической проблемой при реализации SNSTFQKD является управление фазовой эволюцией полей-близнецов. Как было указано в, дифференциальное колебание фазы между двумя пользователями может быть записано как

$$\delta_{ba} = \frac{2\pi}{s}(\delta\nu L + \nu\delta L) \tag{1.8}$$

, где ν- оптическая частота света, L - длина волокна, s - скорость света в волокне. Таким образом, необходимо компенсировать два источника, вносящих вклад в разность фаз: первый член в уравнении обозначает разность частот между Алисой и Бобом, а второй - дрейф фазы в волокне. В качестве примера, измеренная скорость дрейфа фазы соответствует гауссову распределению со стандартным отклонением 7,4 рад $^{-1}$ для общего расстояния волокна 150 км. Дрейф немного больше в основном из-за относительно шумной среды в нашей лаборатории . Чтобы справиться с разницей фаз, вызванной разницей длин волн, мы используем метод частотной блокировки, как показано на рисунке 1.5(b). В лаборатории Алисы в качестве начального лазера используется лазер непрерывной волны с центральной длиной волны 1550,12 нм и шириной линии в несколько килогерц. Начальный лазер фиксируется в ультрастабильном резонаторе длиной 10 см с тонкостью около 250 000 с помощью техники Паунда-Древера-Холла, чтобы подавить его ширину линии с нескольких килогерц до примерно десяти герц. Затем свет разделяется на две части, одна из которых используется в качестве источника Алисы, а другая - для блокировки оптической частоты Боба. Этот блокирующий луч далее разделяется на две части, одна из которых отражается от зеркала Фарадея (FM) в качестве локального эталона, а другая частотно-модулируется акустооптическим модулятором (AOM) и отправляется Бобу. Здесь длина волокна установлена равной расстоянию передачи сигнала, чтобы продемонстрировать практичность системы.

Вместо того чтобы активно стабилизировать относительную фазу между Алисой и Бобом, мы компенсируем разницу фаз с помощью постобработки. Определив оценочную относительную фазу между волокнами Алисы и Боба как $\Delta\varphi_T$, мы вычисляем квантовый коэффициент битовых ошибок в базисе X

для обнаружений, лежащих в диапазоне

$$1 - |\cos(\theta_A - \theta_B + \delta\varphi_T| < \Lambda) \tag{1.9}$$

где $\theta_A(\theta_B)$ - случайная фаза, которой Алиса (Боб) модулирует сигнал, а Λ - заданный диапазон. Тогда мы можем вычислить безопасную ключевую скорость с эффектом конечного размера данных по следующей формуле:

$$R = (1-p_x)^2 2p_z(1-p_z)a_1 s_1[1 - H(e_1^{ph})] - fS_z H(E_z) - \frac{1}{N_{total}} log_2 \frac{1}{\varepsilon^5} \tag{1.10}$$

где R - конечная ключевая скорость, $a_1 = \mu_\zeta e^{-\mu_\zeta}$, s_1 - выход эффективных однофотонных событий в базисе Z, ε_1^{ph} - коэффициент фазовой ошибки для событий в базисе Z, S_Z и E_Z - наблюдаемый выход и коэффициент битовой ошибки для базиса Z, N_{total} - общее число посланных сигнальных импульсов, а $\varepsilon = 10^{-10}$, что соответствует общей вероятности отказа $2*10^{-9}$. Скорость передачи ключей была бы еще выше, если бы мы учитывали только статистические флуктуации. Здесь мы предполагаем, что эффективность исправления ошибок составляет f = 1.1. Мы протестировали SNSTFQKD с общим расстоянием между Алисой и Бобом от 0 до 300 км. Во всех экспериментах с различными длинами волокон общее количество импульсов, посылаемых Алисой и Бобом, установлено на уровне $7.2*10^{11}$. Достоверные детектирования составляют $6.5*10^9$, $2.3*10^9$2,3 × 109, $7.6*10^8$ и $2.5*10^9$ для 0, 50, 100 и 150 км в первом эксперименте и $1.7*10^9$, $1.9*10^8$ и $2.4*10^7$ для 100, 200 и 300 км во втором эксперименте. Результаты эксперимента обобщены на рисунке 1.6. Сначала мы экспериментально проверили SNSTFQKD при вероятности темного счета 10-6 (эквивалентно 1000 Гц) и коэффициенте ошибок X-базиса 10 %. Безопасная ключевая скорость на расстоянии 150 км составляет $1.72*10^{-6}$ на импульс, что уже выше, чем смоделированная безопасная ключевая скорость протокола независимого квантового распределения ключей (MDI-QKD), использующего те же параметры, что и в эксперименте, но предполагающего более низкие (2%) оптические ошибки в X-базисе. На самом деле, моделирование показывает, что безопасная скорость передачи ключей уже превышает скорость MDI-QKD на расстоянии 108 км. Далее мы снизили вероятность темного счета примерно до 10^7 (эквивалентно

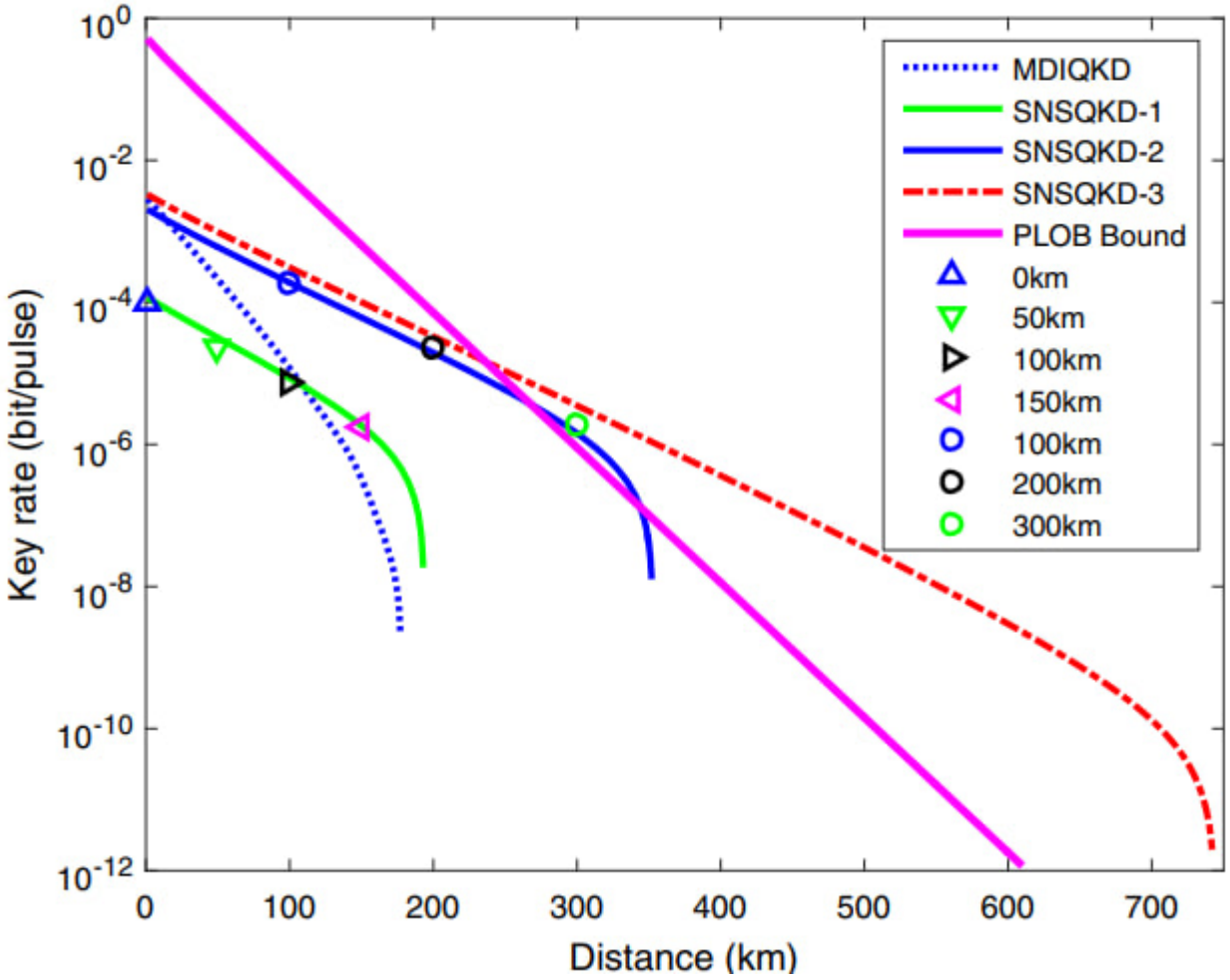

Рисунок 1.6 — Безопасные ключевые скорости и результаты моделирования SNSTFQKD. Треугольники показывают экспериментальные результаты для первого экспериментального теста, а сплошная зеленая кривая - результаты моделирования. эксперимента, а сплошная зеленая кривая представляет результаты моделирования результаты с вероятностью темного счета около 10^{-6} и базовой ошибкой X базиса, которая составляет около 10 %. Для сравнения, пунктирная синяя кривая дает результат моделирования протокола MDI-QKD с четырьмя интенсивными приманками протокола MDI-QKD с теми же параметрами, но с 2% оптических ошибок в базисе X. Кружки показывают экспериментальные экспериментальные результаты для второго теста, а сплошная синяя кривая представляет моделирование с вероятностью темного счета около 10^{-7} и базовой ошибкой X-базиса около 2 процентов импульсов, отправленных Алисой и Бобом для всех экспериментальных тестов, составляет $7.2 * 10^{11}$ Красная пунктирная кривая далее предполагает, что всего 10^{14} импульсов, посланных Алисой и Бобом, с базовой ошибкой X-базиса 2%. Наконец, сплошная пурпурная линия иллюстрирует границу PLOB.

100 Гц), модернизировав SNSPD для интеграции полосового фильтра на кристалле внутри, и снизил уровень ошибки X-базиса примерно до 2%, используя линейный усилитель для управления модуляторами. Безопасная скорость передачи ключей на расстоянии 300 км по оптоволокну составляет $1{,}9610^{-6}$, что выше границы PLOB, равной 8.6410^{-7} на импульс. Моделирование показывает, что SNSTFQKD преодолевает эту границу на расстоянии 267 км, а расстояние передачи может превышать 350 км при экспериментальных параметрах. Наконец, мы моделируем безопасную скорость передачи ключей, предполагая, что всего будет отправлено 10^{14} импульсов (с 2.610^5достоверными срабатываниями, накопленными на расстоянии 720 км), а вероятность темного счета однофотонного детектора уменьшена до 10^{-11} (эквивалентно 0,1 Гц при длительности импульса 100 пс). Все остальные параметры соответствуют параметрам эксперимента на расстоянии 300 км. Моделирование показало, что максимальное расстояние распространения составляет 742 км, а протокол SNSTFQKD достигает скорости передачи ключей выше границы PLOB, когда расстояние между волокнами превышает 236 км. В заключение мы разработали технологии фазовой блокировки и фазовой компенсации, экспериментально протестировали протокол SNSTFQKD и продемонстрировали генерацию защищенных ключей на расстоянии до 300 км по оптоволокну, обеспечив скорость передачи ключей, превышающую емкость секретного ключа без ретранслятора. При расчете ключевой скорости были полностью учтены эффекты конечного размера, что гарантирует безопасность в практической ситуации. Отметим, что и расстояние, и ключевая скорость могут быть значительно улучшены за счет использования двусторонней классической связи. Экспериментальные результаты также показывают, что протокол SNSTFQKD устойчив к фазовому рассогласованию, что является важным преимуществом на практике. Метод фазовой блокировки, использованный в эксперименте, оказался стабильным на расстоянии 1800 км по волокну, а интенсивность опорных фазовых импульсов находилась в пределах нескольких микроватт даже на расстоянии 1000 км. С учетом имеющихся в настоящее время технологий и результатов теоретического моделирования с

практическими параметрами мы ожидаем, что в ближайшем будущем будут достигнуты расстояния распространения более 500 км.

1.1.6 Протокол квантовой коммуникации на боковых частотах модулированного излучения

1.2 Когерентное детектирование

Когерентное детектирование - это метод регистрации сигналов, при котором принимаемый сигнал сбивается с мощным опорным сигналом или излучением, называемым локальным осциллятором (ЛО). Результат этого смешения регистрируется классическим детектором, например, балансным детектором. К преимуществам данного метода регистрации сигналов можно отнести следующее: возможность измерения не только амплитуды входного излучения, но и его фазы. В то время как при некогерентном детектировании информация о фазе принимаемого сигнала теряется, то при когерентном детектировании она сохраняется. Эта особенность позволяет переходить к более сложным типам модуляции, что, в свою очередь, повышает эффективность использования полосы сигналов и повышает скорость передачи данных. В то время когда некогерентный метод детектирования не сохраняет информацию и регистрирует только интенсивность приходящего излучения, что ограничивает скорость передачи информации, которая ограничивается полосой пропускания приемника. Другим преимуществом является большая чувствительность, по сравнению с некогерентным квадратичным детектированием. Это достигается за счет того, что ослабленный информационный сигнал, взаимодействуя с мощным ЛО, усиливается и за счет этого достигается больша чувствительность. Однако у данного подхода есть и минусы: необходимость дополнительных компенсаций фазовых искажений, связанных с прохождением сигнала в среде распространения и нескоррелированность фазовых шумов источником информационного

сигнала и ЛО. Эти недостатки компенсируются либо дополнительными техническими доработками или цифровой обработкой сигналов (ЦОС), что приводит к расширению использования когерентного детектирования в современных системах передачи данных.

Методы когерентного детектирования можно разделить на несколько категорий по используемым частотам или длин волн информационного сигнала и ЛО. В случае если информационный сигнал передается на той же длине волны, что и локальный осциллятор, то такой мето детектирования называют гомодинным. Подробнее данный способ рассматривается в разделе 1.2.1. Если же длины волн информационного сигнала и ЛО разнесены так, что промежуточная их частота больше частоты модулирующего сигнала, то такой способ детектирования называют гетеродинным, подробнее он рассматривается в разделе 1.2.2. Существуют и другие методы дететкирования, позволяющие компенсировать недостатки гомодинного детектирования - двойное гомодинирование или 90-градусный оптических гибрид. Его суть заключается в том, что и информационный сигнал, и ЛО разделяются пополам и каждая из разделенных частей подается на отдельный делитель, где сбиваются друг с другом, однако в одну из частей ЛО вносят дополнительный фазовый сдвиг, за счет которого можно принимать информацию о любой фазе. Подробнее данный способ регистрации рассматривается в разделе 1.2.3.

1.2.1 Гомодинное детектирование

Гомодинное детектирование - один из методов когеретного детектирования, отличительной чертой которого является равенство длин волн информационного сигнала и локального осциллятора. Нашел широкое применение в оптических системах передачи данных благодаря относительной простоте реализации. Структурная схема такого приемника изображена на рисунке 1.7.

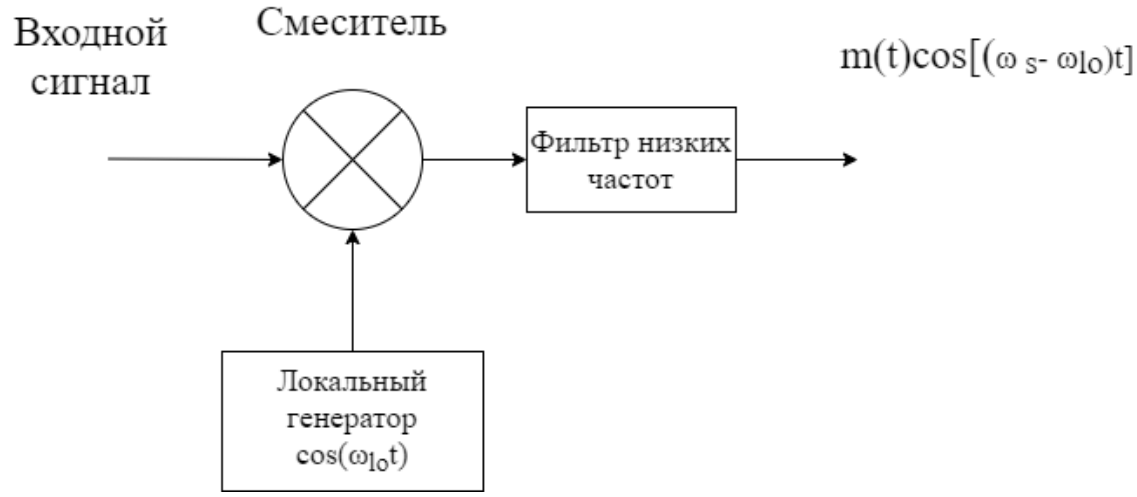

Рисунок 1.7 — Структурая схема гомодинного приема

Интенсивность в случае гомодинного детектирования будет описываться следующим выражением

$$I(t) = |E(t)|^2 = |E_1|^2 + |E_2|^2 + 2|E_1|\cos[(\omega_1 - \omega_2)t + \varphi_1 - \varphi_2] \qquad (1.11)$$

, где E_1, E_2 - комплексные амплитуды сигналов информационного и локального осциллятора, ω_1, ω_2 - частоты информационного сигнала и ЛО, φ_1, φ_2 - фазы информационного сигнала и ЛО. Но так как в случае гомодинного детектирования частоты излучения равны, то результат детектирования приводится к виду

$$S(t) = S_0 + S_m \cos(\Delta\varphi) \qquad (1.12)$$

Таким образом результат интерференции при гомодинном детектировании пропорционален разности фаз между локальным осциллятором и исследуемым сигналом. Однако при $\Delta\varphi = 90$ градусов невозможно однозначно различить фазу информационного сигнала и требуется дополнительные технические средства.

1.2.2 Гетеродинное детектирование

Другой разновидностью когеретного детектирования является гетеродинное детектирование. Данный метод нашел свое широкое распространение в радио-

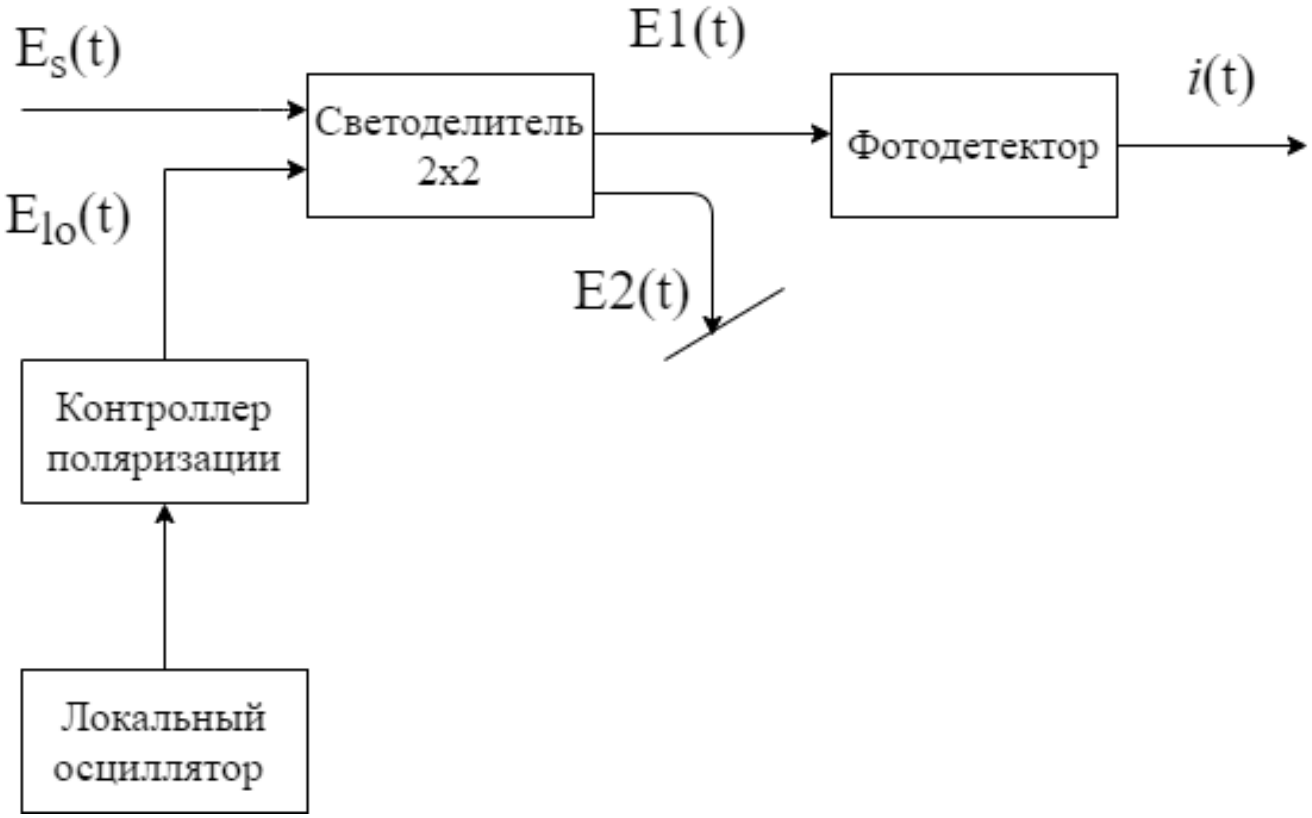

Рисунок 1.8 — Стурктурная схема гетеродинного оптического приемника

технике с 1917 года под названием супергетеродинный приемник. Суть данного метода заключается в следующем. Входной сигнал, несущий информацию подается на один из входов смесителя. На второй же вход смесителя подается сигнал локального осциллятора. При этом частоты входного сигнала и ЛО отличаются. В результате эти два сигнала интерферируют и на выходе смесителя образуется новая частота - промежуточная частота, которая равна разности частот ЛО и входного сигнала. Данный метод описывается следующим образом:

$$I(t) = |E(t)|^2 = |E_1|^2 + |E_2|^2 + 2|E_1|\cos[(\omega_1 - \omega_2)t + \varphi_1 - \varphi_2] \qquad (1.13)$$

, где E_1, E_2 - комплексные амплитуды сигналов информационного и локального осциллятора, ω_1, ω_2 - частоты информационного сигнала и ЛО, φ_1, φ_2 - фазы информационного сигнала и ЛО. В результате на выходе фотоприемника формируется сигнал

$$S(t) = S_0 + S_m\cos((\omega_1 - \omega_2)t + \Delta\varphi) \qquad (1.14)$$

В выражении 1.2.2 присутствует разностная частота $\omega_1 - \omega_2$, которая содержит себе информацию от входного сигнала о его амлпитуде и фазе. Благодаря

этому, возможно излвекать информацию из сложных типов модуляции, таких как квадртатурно-амплитудная, при этом не прибегая к дополнительным техническим приспособлениям. Данный метод детектирования сигналов является самым гибким для регистрации любых типов модуялции, однако требует точной подстройки частоты и ее стабилизации и фазовой синхронизации между входным сигналом и ЛО для проведения измерений фазы входного сигнала.

1.2.3 90-градусный оптический гибрид

Одним из главных недостатков гомодинного детектирования, описанного в разделе 1.2.1 - является невозможность измерения сигнала с фазой в неортогональном состоянии относительно локального осциллятора. В результате этого при использовании 4 фазовых состояний для кодирования информации, 50 процентов из них будут утеряны из-за невозможности однозначно различить. Для устранения этого существенного недостатка был разработан метод когерентного детектирования с использованием 90-градусного оптического гибрида или двойного гомодинирования. Данный метод развивает схему гомодинного детектирования из раздела 1.2.1. Входной сигнал и сигнал ЛО разделяются пополам на двух разных делителях. После этого части входного сигнала смешиваются с частями ЛО. Но в одном из плеч локального осциллятора установлен дополнительный фазовый сдвиг на $\frac{\pi}{2}$. За счет этой модификации возможно измерение фазы принятого сигнала во всех используемых состояниях. Результат измерения попадает на 2 балансный приемника или класических фотодиода. В результате в том плече, где базисы фаз совпали, сигнал на выходе балансного детектора будет изменяться в зависимости от разности фаз. В другом же плече будет наблюдаться средний уровен сигнала, который невозможно интерпретировать как одно из измеренных фазовых значений. Данный метод приема лишен недостатка гомодинного приемника, однако он вносит дополнительные 3 дБ потерь по входному сигналу, что ухудшает его соотношение сигнал - шум, а также удваивает оптическую схему, что негативно сказывается на цене данного

метода. Однако такой метод является более предпочтительным, чем одиночный гомодинный приемник.

1.3 Протоколы квантового распределения ключа на непрерывных переменных

В качестве альтернативы КРК-ДП протоколам, которые в идеале основаны на однофотонном детектировании, КРК-НП протоколы кодируют ключи в непрерывных переменных (НП) наблюдаемых световых полях [8], которые могут быть измерены с помощью гомодинного детектирования с ограниченным уровнем дробового шума. В гомодинном детекторе оптический сигнал подключается к сильному излучению локального осциллятора (ЛО) с ограниченным уровнем шума на сбалансированном делителе луча, и измеряется интенсивность света на выходных портах. В зависимости от разности оптических фаз между сигналом и ЛО, разность фототоков, возникающих в каждом из двух детекторов, будет пропорциональна одной из двух квадратур поля. Таким образом, ЛО несет в себе опорную фазу, которая позволяет переключаться между измерением q- и p-квадратур (или, в более общем случае, выполнять томографию состояния путем измерения функции Вигнера, связанной с состоянием). Первое предложение об использовании квадратур бозонического поля для реализации КРК появилось в 1999 году, когда Ральф [455] рассмотрел кодирование ключевых битов с помощью четырех фиксированных квадратурных смещений ярких когерентных или двухмодовых запутанных пучков. Позже Ральф обсудил безопасность двухмодовой схемы на основе запутанности более подробно [456], рассматривая не только атаки перехвата-передачи, но и телепортацию НП. Последняя была определена как оптимальная атака на протокол, накладывающая требования высокого сжатия сигнала и низких потерь в канале [456]. Независимо от этого Хиллери [457] предложил протокол КРК-НП, основанный на квадратурном кодировании одномодового луча, случайным образом сжатого в одном из квадратурных направлений. Безопасность от атак перехвата-передачи

и расщепления луча оценивалась на основе принципа неопределенности. Другая ранняя схема КРК-НП была предложена Ридом [458] и основывалась на проверке корреляций типа ЭПР для обнаружения подслушивающего устройства. В 2000 году Серф и другие [459] предложили первый полностью непрерывный протокол КРК, в котором квадратуры сжатого луча использовались для кодирования безопасного ключа с гауссовским распределением. Безопасность протокола была показана против индивидуальных атак на основе соотношения неопределенностей и оптимальности квантового клонирования. Позже были введены процедуры согласования для гауссовски распределенных данных, что позволило реализовать исправление ошибок (ИО) и усиление секртености (УС) близко к теоретическим границам [460]. Другой протокол КРК-НП, основанный на гауссовой модуляции сжатых пучков, был предложен Готтесманом и Прескиллом [461]. Было показано, что этот протокол защищен от произвольных атак при возможных уровнях сжатия, благодаря использованию квантовых кодов с коррекцией ошибок. В 2001 году Гроссханс и Гранжье представили основополагающий протокол с когерентным состоянием и гауссовской квадратурной модуляцией и показали его защищенность от индивидуальных атак [462], прибегнув к НП-версии теоремы об отсутствии клонирования [463]. Стандартный протокол, основанный на прямой сверке (ПС), где Алиса является опорной стороной для постобработки информации, был, однако, ограничен 50-процентным пропусканием канала, то есть 3 дБ. В качестве попытки преодолеть ограничение в 3 дБ Зильберхорн и др. предложили использовать постселекцию в КРК-НП [464]. В качестве альтернативы было показано, что использование обратной сверки (ОС), где опорной стороной является Боб, позволяет протоколу с когерентным состоянием быть защищенным от индивидуальных атак вплоть до произвольно низких коэффициентов пропускания канала [465]. В 2004 году для протоколов с когерентным состоянием было предложено использование гетеродинного обнаружения [466]; преимущество этого протокола без переключения заключается в том, что измеряются обе квадратуры, что увеличивает скорость передачи ключа. Безопасность КРК-НП от коллективных гауссовых атак была продемонстрирована независимо друг от друга Навас-

куэсом и другими [467] и Гарсией-Патроном и Серфом [468]. Коллективные гауссовские атаки были полностью охарактеризованы Пирандолой и другими [469], которые позже вывели мощности секретных ключей для КРК-НП [43,44]. Безопасность от коллективных атак была расширена на общие атаки Реннером и Цираком [86] с помощью квантовой теоремы де Финетти, примененной к бесконечно-мерным системам. Это позволило завершить доказательства безопасности основных односторонних протоколов КРК-НП в асимптотическом пределе бесконечно больших наборов данных [470], в том числе с доверенным шумом [124,471,472]. Следующим развитием стало изучение эффектов конечного размера и полностью композитных доказательств (например, см. работы [92,95]). Стоит также упомянуть о существовании других направлений исследований, в которых при вычислении скорости секретного ключа учитываются ограничения реалистичного подслушивающего устройства [473,474]. Помимо разработки односторонних гауссовских протоколов и доказательств их безопасности, сообщество квантовой информации разработало ряд других типов протоколов, гауссовских или нет, которые основаны на использовании систем КВ. В следующих разделах, помимо стандартных односторонних гауссовских протоколов (основанных на когерентных или сжатых состояниях), мы рассмотрим двусторонние протоколы, протоколы тепловых состояний, одномерные протоколы, протоколы с дискретной модуляцией и протоколы с ретрансляцией, такие как КРК-НП НПУ. Понятно, что это не охватывает все современные разработки в широкой области КРК-НП. Например, мы не будем явно обсуждать протоколы, основанные на использовании негауссовых операций, таких как вычитание фотонов [475], квантовый катализ [476] или квантовые ножницы [477].

1.3.1 Протокол квантового распределения ключа с использованием модуялции Гаусса

Протокол квантового распределения ключа на непрерывных переменных с применением Гауссовой модуляции является одним из первых протоколов, для

которого существует доказательство секретности с учетом эффектов конечного ключа и против оптимальной атаки злоумышленника. С учетом этого факта и того, что его реализация может быть достаточно простой, данный протокол стал одним из первых реализованных на практике протколом на непрерывных переменных.

Этапы протокола с использованием модуляции Гаусса

Данный протокол состоит из 4 шагов - 1. подготовка и распределение состояний, 2. - сверка ошибок, 3. определение параметров и 4. усиление секретности.

1. Подготовка и распределение состояний: Алиса готовит большое количество когерентных состояний $|\alpha_1\rangle \dots |\alpha_N\rangle$, где α_i независимые и тождественно распределенные комплексные гауссовские переменные распределением V_0. В зависимости от протокола (гомодинный или гетеродинный) Боб измеряет либо случайную квадратуру (x или p) для каждого состояния и сообщает Алисе о своем выборе, либо обе квадратуры. Затем Боб получает список из N или 2N вещественных чисел, соответствующих результатам его измерений. Алиса также имеет доступ к своему собственному списку данных (она хранит только соответствующие значения квадратур, если Боб выполнил обнаружение гомодина). Обозначим соответствующие списки Алисы и Боба через $x = x_1 \dots x_n$ и $y = y_1 \dots y_n$, (где n - N или 2N).
2. Исправление ошибок: Протокол в целом достигает лучшей производительности при обратном согласовании : это означает, что строка Боба соответствует необработанному ключу, а Алиса пытается угадать его значение. Для достижения этой цели Алиса и Боб используют классические методы исправления ошибок. Точнее, Алиса и Боб договариваются о линейном коде с коррекцией ошибок до начала протокола, и Боб отправляет Алисе значение синдрома y для этого кода. Чтобы восстановить y, Алисе

нужно просто исправить x, то есть декодировать в косетевой код, определяемый полученным синдромом.

3. Оценка параметров: Этот шаг полезен для получения верхней границы информации, доступной Еве. Для протоколов КРК-НП это обычно требует оценки ковариационной матрицы двухстороннего состояния, разделяемого Алисой и Бобом. Получив эту оценку, Алиса и Боб могут вычислить размер ℓ безопасного ключа, который они могут извлечь из своего состояния.
4. Усиление конфиденциальности: Алиса и Боб применяют случайную универсальную хэш-функцию к своим соответствующим (исправленным) строкам и получают две строки S_A и S_B длины ℓ.

Варианты этого протокола могут отличаться типом подготавливаемых состояний (когерентные, сжатые или даже тепловые) и способом детектирования (гомодинный или гетеродинный), но основные этапы протокола остаются в основном идентичными

Экспериментальная реализация протокола с модуялцией Гаусса

Как и в случае КРК на дискретных переменных, протоколы КРК-НП "приго в целом проще реализовать на практике. Далее мы подробно описываем реализацию протокола GG02, принцип и безопасность которого были рассмотрены в разделах 2 и 3 соответственно, с помощью волоконной оптики PM. Этот протокол особенно интересен с практической точки зрения, поскольку он требует всего лишь генерации когерентных состояний, их модуляции в фазовом пространстве и обнаружения квадратур полученных состояний с помощью гомодинных (или гетеродинных) методов. Компоненты, необходимые для достижения этих функциональных возможностей, легко доступны на телекоммуникационной длине волны, которая подходит для работы с волоконно-оптическими системами. Оптическая конфигурация для выполнения этого протокола показана на рисунке 1.9. В этой схеме сигнал и опорная фаза

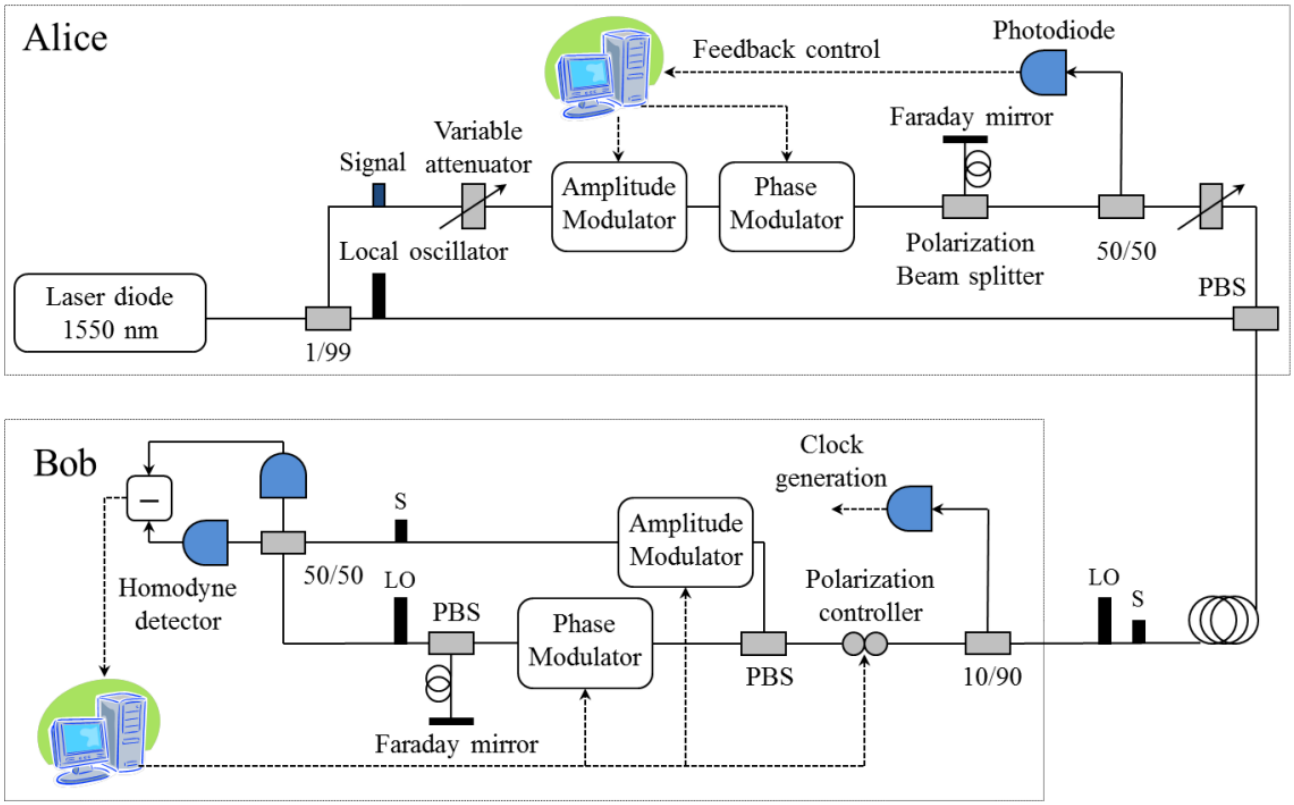

Рисунок 1.9 — Оптическая схема волоконной системы КРК-НП с гомодинным детектированием. Laser diode - лазерный диод, signal - сигнал, Local oscillator - локальный осциллятор, Variable attenuator - переменный аттенюатор, Amplitude modulator - амплитудный модулятор, Phase modulator - фазовый модулятор, Polarization beam splitter (PBS) - поляризационный делитель луча, Faraday mirror - Зеркало Фарадея, Photodiode - Фотодиод, Feedback control - управление обратной связью, Polarization controller - контроллер поляризации, Clock generation - генерация опорной частоты, Homodyne detector - гомодинный приемник.

(или локальный генератор), необходимые для выполнения когерентного обнаружения, генерируются источником лазерного диода в месте нахождения Алисы. Сигнал модулируется по амплитуде и фазе в соответствии с гауссовским распределением, как того требует протокол, а затем ослабляется на подходящем уровне дисперсии модуляции. Он также мультиплексируется по времени и по поляризации с локальным осциллятором перед входом в квантовый канал. На месте Боба два сигнала демультиплексируются с помощью линии задержки и поляризационного делителя луча и накладываются во времени для интерференции на ограниченный шумами сбалансированный импульсный гомодинный

детектор. Квадратурная селекция, требуемая протоколом GG02, выполняется фазовым модулятором, помещенным в тракт локального генератора. Установка дополнена несколькими активными элементами обратной связи и управления, которые обеспечивают необходимые условия синхронизации и стабильности для выполнения квантового распределения ключей. Описанная система реализует первую часть, а именно (1) распределение и измерение состояния, полного протокола GG02, описанного в разделе 1.3.1; остальные части постобработки, а именно 2 согласование ошибок, 3 оценка параметров и 4 усиление конфиденциальности, и, в частности, первые две, требуют сложных вычислительных алгоритмов. Первоначальная реализация оптической установки на рисунке 1.9 использовалась в европейской сети SECOQC QKD [4], которая была развернута по проложенным оптическим волокнам и объединяла различные технологии КРК [4,54]. Она также использовалась в полевых испытаниях линии связи точка-точка с классическим симметричным шифрованием и быстрым обновлением ключей, обеспечиваемым квантовым слоем, которые продемонстрировали надежность работы системы КРК-НП в течение длительного периода времени в условиях серверной [55]. Эти реализации, а также некоторые другие [56-59], были пригодны для защиты коммуникаций в сетях городского масштаба (с расстоянием до 25 км) с высокими требованиями к скорости передачи данных. Хотя существует несколько интересных применений экспериментов на коротких расстояниях, с точки зрения квантовых информационных сетей важно иметь возможность увеличить расстояние связи за этот предел. В реализациях дискретно-переменного КРК ограничение по расстоянию в основном определяется характеристиками однофотонных детекторов, в частности, их темновыми отсчетами. В КРК-НП ограничение дальности было связано с эффективностью сложных методов постобработки. Хотя это уже не так, полезно понять причину этого ограничения: эффективное согласование коррелированных гауссовских переменных на самом деле затруднено, особенно при низких отношениях сигнал/шум (SNR), которые присущи экспериментам на больших расстояниях, что снижает коэффициент эффективность сверки. Помимо исправления ошибок, процедура оценки параметров также имеет решающее значение для извлече-

ния секретного ключа на практике. Для оптической установки на рисунке 1.9 соответствующими экспериментальными параметрами являются дисперсия модуляции Алисы V_A, коэффициент пропускания канала T и избыточный шум ξ, который представляет собой шум, добавляемый каналом сверх основного шума выстрела, и соответствует обычному коэффициенту ошибок квантового бита, встречающемуся в дискретно-переменных реализациях КРК. Как V_A, так и ξ обычно выражаются в единицах дробового шума. Параметр V_A подстраивается в реальном времени, чтобы в любой момент времени быть как можно ближе к SNR, соответствующему порогу доступного кода с исправлением ошибок, в то время как параметры T и ξ должны оцениваться в реальном времени путем случайного раскрытия части ключа. Два дополнительных экспериментальных параметра, которые используются для вычисления оценки секретной информации, которая может быть извлечена из общих данных, - это скорость электронного шума и эффективность η обнаружения гомодина. В так называемом реалистичном сценарии КРК-НП предполагается, что эти параметры недоступны для Евы и измеряются в ходе безопасной процедуры калибровки, которая проводится перед развертыванием системы. Однако в общем случае эти параметры могут быть доступны Еве. Процедура оценки параметров позволяет вычислить границы для информации подслушивающего лица, принимая во внимание неопределенность калиброванных значений.

1.3.2 Протокол квантового распределения ключа с использованием модуялции Гаусса и локальным осциллятором, сгенерированным на приемной стороне

Generatingthelocaloscillatorlocallyincontinuous−variablequantumkeydistributio

Как протоколы КРК на дискретных переменных (КРК-ДП) , основанные на обнаружении одиночных фотонов [1, 2], так и протоколы КРК на непрерывных переменных (КРК-НП), основанные на когерентном детектировании [9-11] были продемонстрированы как жизнеспособные решения на практике. Одним

из известных протоколов КРК-НП является протокол когерентного состояния с гауссовской модуляцией (ГМКС) [11], который был продемонстрирован на 80-километровой оптоволоконной линии связи [12]. Одним из важных преимуществ ГМКС КРК является его устойчивость к некогерентному фоновому шуму. Сильный локальный осциллятор (ЛО), используемый в когерентном обнаружении, также действует как естественный и чрезвычайно селективный фильтр, который может эффективно подавлять шумовые фотоны. Эта внутренняя функция фильтрации делает КРК-НП привлекательным решением для безопасного распределения ключей по зашумленному каналу, таком как освещенное волокно в обычной оптоволоконной оптической сети [13-15] или оптической линии связи в свободном пространстве [16]. Однако все существующие реализации КРК-НП основанные на когерентном детектировании, имеют серьезный недостаток: для уменьшения фазового шума как сигнал, так и ЛО генерируются одним и тем же лазером и распространяются по небезопасному квантовому каналу [11, 12, 16, 17] 1. Такая схема имеет несколько ограничений. Во-первых, она позволяет Еве получить доступ как к квантовому сигналу, так и к ЛО. Ева может проводить сложные атаки, манипулируя ЛО, что было продемонстрировано в недавних исследованиях [18-21]. Во-вторых, Передача сильного ЛО по каналу с потерями может резко снизить эффективность КРК в некоторых приложениях. Например, для достижения когерентного обнаружения с ограничением по дробовому шуму необходимое число фотонов в ЛО обычно превышает 10^8 фотонов на импульс на стороне приемника [11, 12, 17]. При частоте повторения импульсов 1 ГГц и потерях в канале 20 дБ, требуемая мощность ЛО на входе квантового канала составляет около 1,2 Вт (на длине волны 1550 нм). Если оптическое волокно используется в качестве квантового канала, шумовые фотоны, генерируемые сильным ЛО внутри оптического волокна, могут значительно снизить эффективность КРК и пропускную способность мультиплексирования. В-третьих, ЛО обычно на 7 или 8 порядков ярче, чем квантовый сигнал, поэтому требуются сложные схемы мультиплексирования и демультиплексирования для эффективного отделения ЛО от квантового сигнала на стороне приемника для эффективного

отделения ЛО от квантового сигнала на стороне приемника. Короче говоря, в КРК-НП желательно генерировать ЛО "локально используя независимый лазерный источник на стороне приемника. К сожалению, такая схема никогда не была реализована на практике. Основная проблема заключается в том, как эффективно установить надежную фазовую привязку между Алисой и Бобом. Хотя в классической когерентной связи были разработаны различные методы, такие как восстановление несущей [22], оптическая фазовая автоподстройка частоты [23], и оптическая инжекционная фазовая подстройка частоты [24], были разработаны для классической когерентной связи, но эти методы не подходят для КРК, где квантовый сигнал крайне слаб, а допустимый фазовый шум мал. Кроме того, чтобы предотвратить манипуляции Евы с ЛО, лазер ЛО должен быть изолирован от внешнего мира как оптически, так и электрически. В этой статье мы решаем вышеупомянутую давно нерешенную проблему, предложив и продемонстрировав схему восстановления данных с помощью пилота схема восстановления данных с обратной связью, которая обеспечивает надежное когерентное обнаружение с использованием "локально"генерируемого ЛО. Эта схема основана на наблюдении, что в ГМКС КРК, Бобу не нужно выполнять измерение в "правильном базисе". Фактически, Боб может выполнить измерение в произвольно повернутом базисе, поскольку при условии, что информация о базисе (фазовый эталон) если информация о базисе (фазовый эталон) доступна после измерения. Имея эту информацию после измерения, Алиса или Боб могут вращать имеющиеся данные и генерировать коррелированные данные с другими.

Экспериментальная реализация протокола КРК на непрерывных переменных с модуляцией Гаусса.

На рисунке 1.10 показана оптическая схема системы КРК-НП с "локальным"локальным осциллятором (ЛЛО), основанной на протоколе когерентного состояния с гауссовской модуляцией. У отправителя, Алисы, в качестве опти-

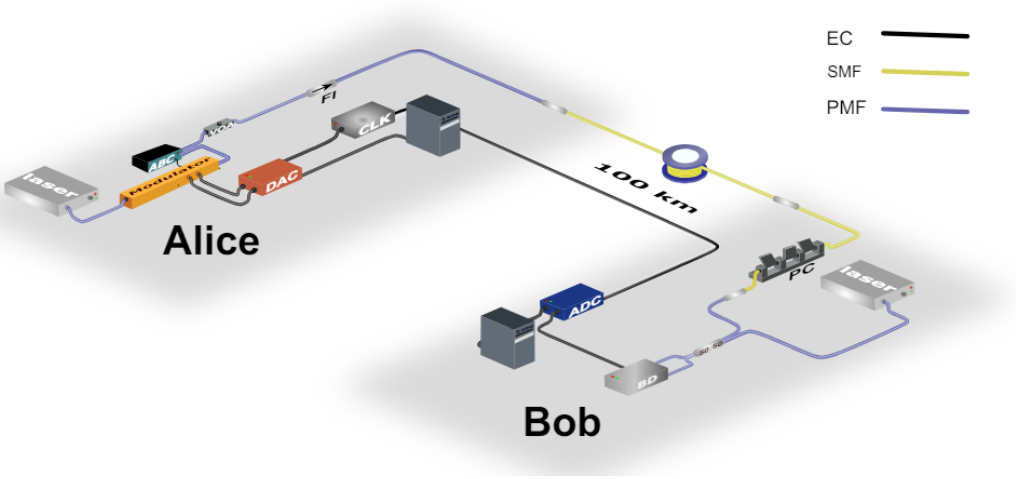

Рисунок 1.10 — Станция Алисы состоит из непрерывного (CW) лазера, работающего на длине волны 1550 нм, синфазного и квадратурного (IQ) модулятора с автоматическим регулятором смещения (ABC) для получения когерентных состояний на боковых частотах. А Для управления IQ-модулятором использовался цифро-аналоговый преобразователь (ЦАП) с разрешением 16 бит и частотой дискретизации 1 Гвыб/с. Переменный оптический аттенюатор (VOA) использовался после IQ-модулятора для регулировки дисперсии модуляции квантового сигнала. Изолятор Фарадея (ФИ), направление которого указано стрелкой, используется перед 100-километровым оптоволоконным каналом со сверхнизкими потерями, который представляет собой квантовый канал. Станция Боба состоит из поляризационного контроллера (ПК) для настройки поляризации входящего сигнала и сбалансированного светоделителя для наложения этого сигнала на локальный осциллятор, генерируемый другим CW-лазером (разблокированным/свободно работающим по отношению к лазеру Алисы). Сигнал был обнаружен и оцифрован с помощью сбалансированного детектора (BD), а затем аналого-цифрового преобразователя (АЦП) с частотой дискретизации 1 Гсэмпл/с.

ческого носителя использовался непрерывный лазер (CW) с узкой шириной линии ≈ 100 Гц, работающий на длине волны 1550 нм. Когерентные состояния готовились путем модуляции КВ-лазера с помощью синфазно-амплитудного (IQ) модулятора, управляемого 16-битным цифро-аналоговым преобразователем (ЦАП) с двумя каналами, работающими с частотой дискретизации 1 ГС/с. IQ-модулятор работал в однополосном режиме, управляя напряжениями смещения постоянного тока (DC) с помощью автоматического регулятора смещения (ABC). После IQ-модулятора был установлен переменный оптический аттеню-

атор (VOA) для регулировки дисперсии модуляции теплового состояния. На выходе отправителя был добавлен изолятор Фарадея, чтобы избежать обратных отражений от канала и атак "троянского коня". Сигнал передавался по квантовому каналу, изготовленному из коммерческого волокна с ультранизкими потерями (TeraWave SCUBA 150 Ocean Optical Fiber). Затухание волокна составляет 0,146 дБ/км на длине волны 1550 нм. Общие потери в нашем 100-километровом оптоволоконном канале составили 15,4 дБ из-за разницы диаметров модового поля между соединением волокна SMF-28 и SCUBA 150. В приемнике Боба для измерения квантового состояния использовалось радиочастотное (РЧ) гетеродинное детектирование. Для этого в качестве ЛЛО использовался другой CW-лазер, свободно работающий по отношению к лазеру Алисы. Разница частот между лазерами Алисы и Боба составляла ≈ 230 МГц. Затем поляризация квантового сигнала была настроена так, чтобы соответствовать поляризации ЛЛО с помощью регулятора поляризации. Затем квантовый сигнал и ЛЛО были объединены на сбалансированном светоделителе, затем самодельный сбалансированный детектор с полосой пропускания ≈ 365 МГц для обнаружения интерференционной картины. Наконец, обнаруженный сигнал оцифровывался с помощью 16-битного аналого-цифрового преобразователя (АЦП) с частотой дискретизации 1 ГС/с и записывался для автономной цифровой обработки сигнала. АЦП и ЦАП были синхронизированы с помощью опорного генератора (CLK) с частотой 10 МГц. Время измерения делилось на кадры, каждый из которых содержал 10^7 выборок АЦП. Три измерения проводились автономно: измерение квантового сигнала, измерение вакуумного шума (лазер Алисы выключен, лазер Боба включен) и измерение электронного шума (лазер Алисы выключен, лазер Боба выключен). Выигрыш вакуумного шума по сравнению с электронным составил ≈ 15 дБ в полосе частот квантового сигнала. Чтобы откалибровать V_{mod} теплового состояния, мы провели измерения "спина к спине"(B2B), в которых Алиса и Боб были соединены через короткий волоконный патч-корд, а VOA был тонко настроена для установки различных значений V_{mod}.

Передача данных на большие расстояния является ключевым требованием для

широкомасштабного развертывания и интеграции КРК в существующие телекоммуникационные сети. КРК-НП естественным образом подходит для такой интеграции. Однако безопасная и практичная конфигурация системы (ЛЛО КРК-НП) сталкивается с ограничениями по дальности передачи из-за фазового фазового шума лазеров. В данной работе мы продемонстрировали возможность передачи данных на большие расстояния ЛЛО КРК-НП по оптоволоконному каналу длиной 100 км . Этот рекордный эксперимент стал возможен благодаря использованию машинного обучения для компенсации фазового шума и оптимизации модуляции для согласования информации и избыточного шума одновременно.

1.4 Фазовый шум в системах квантового распределения ключа

Фазовый шум в системах квантового распределения ключа является одним из факторов, которые ограничивают скорость выработки секретного ключа. В то время, как этот эффект практически не влияет на протоколы, построенных на дискретных переменных, но этот эффект является критическим для протоколов на непрерывных переменных, как и для протоколов, основанных на "полях близнецах"и с недоверенным приемным узлом. В случае этих протоколов происходит интерференция либо нескольких когерентных состояний между собой, либо между когерентным состоянием и локальным осциллятором. В обоих случаях происходит измерение, которое будет зависеть от разности фаз между взаимодействующими компонентами излучения. И в случае наличия дополнительного фазового шума, результат этой интерференции будет абсолютно случайным, независимым от закодированных состояний Алисой и Бобом. В этом случае ключ не будет сгенерирован. Поэтому данный шум необходимо компенсировать различными методами.

Избыточный шум в системах КРК может быть обусловлен различными источниками: дискретизация, модуляция, относительный шум интенсивности (RIN), рассеяние Рамана и остаточный фазовый шум (RPN). Предполагается, что эти

источники шума статистически независимы и поэтому общий избыточный фазовый шум может быть представлен в виде суммы независимых величин

$$\zeta = \zeta_{RIN} + \zeta_{mod} + \zeta_{quant} + \zeta_{Ramman} + \zeta_{RPN} + K \tag{1.15}$$

Среди этих источников шума, остаточный фазовый шум (ОФШ), определяется как распределение разности между реальной фазой квантового сигнала и измеренной фазой принятого сигнала, является главным источником избыточного шума в системах КРК-НП ЛЛО. В случае гауссово-модулированного протокого на когерентных состояния, избытычный шум, связанный с ОФШ на приемной стороне определяется как

$$\zeta = 2TV_{mod}(1 - e^{\frac{-V_{RPN}}{2}}) \tag{1.16}$$

, где T - пропускание, включающее в себя квантовый канал и эффективность детектора, V_{mod} - распределение модуляции, т.е. распределение ансамбля когерентных состояний и V - распределение остаточного фазового шума. Исходя из выражения 1.4, доступно два варианта уменьшение фазового шума в КРК-НП с ЛЛО: работа системы при низкой дисперсии модуляции или минимизация ОФШ. Хотя первый вариант практичен и прост в реализации, он требует тщательной оптимизации V_{mod} из-за зависимости СКР от дисперсии модуляции. В частности, от дисперсии модуляции зависят как взаимная информация, так и эффективность согласования информации. Для уменьшения ОФШ требуется эффективная оценка фазы. В настоящее время стандартный подход заключается в использовании пилотных методов для оценки относительной фазы между непрерывно излучающими лазерами передатчика и приемника. Качество оценки фазы сильно зависит от отношения сигнал/шум (SNR) пилотных сигналов, реализуемых с помощью одночастотных тонов или обучающих символов, передаваемых вместе с квантовым сигналом. Однако эти методы ограничены потерями в канале, которые увеличиваются с расстоянием, и необходимостью в маломощном пилотном сигнале для уменьшения перекрестных помех квантовому сигналу.

1.4.1 Методы борьбы с фазовым шумом в системах квантового распределения ключа

В ходе развития технологии квантового распределения ключа были разработаны несколько методов компенсации фазовых искажений с целью улучшения характеристик конечных систем. Существует несколько способов реализации компенсаций фазовых искажений: восстановление фазы несущей частоты, пилотные импульсы и реализация обратной связи в виде оптической инжекции или оптической фазовой автоподстройки частоты. Данные методы обладают как своими преимуществами, так и недостатками. Данный раздел посвящен рассмотрению принципов работы данных методов компенсации фазовых искажений.

Пилотные импульсы

Первым из методов восстановления стали так называемые пилотные импульсы. Их суть заключается в том, что к квантовым состояниям мультиплексируется дополнительный классический сигнал, который является опорным для измерения фазового шума при прохождении квантового канала. Просле прохождения этими сигналов квантового канала, они попадают на схему демультиплексирования и разделяются.На балансном детекторе происходит измерение фазы и пилотного импульса, и квантового сигнала. Так как эти оба сигнала распространялись по одному и тому же каналу, а также были излучены одним и тем же источником, то их фазовые шумы являются скоррелированными. В результате измерения фазы пилотного импульса, можно вносить корректировки измеренного фазового набега в квантовом сигнале на этапе постобработки.
Однако данный метод усложняет приемный модуль за счет необходимости дополнительной системы демультиплексирования, а также увеличивает шум,

связанный с рассеянием, так как передаваемый пилотный импульс должен быть достаточно мощным для точных измерений.

Оптическая фазовая автоподстройка частоты

Другим же методом подстройки фазы двух источников излучения является оптическая фазовая автоподстройка частоты или ОФАПЧ (OPLL). В этом случае, два лазера сбиваются на фотоприемнике. Их разностная частота подстраивается так, чтобы она сравнялась с опорной частотой генератора, относительно которой будет подстраиваться фаза излучения. В качестве источника опорной частоты может выступать термостатированный кварцевый генератор. Эти частоты сбиваются на смесителе для формирования сигнала ошибки. Этот сигнал ошибки передается на PID контроллер температуры лазера для управления его длиной волны до тех пор, пока этот сигнал ошибки не станет меньше заданного значения. Из плюсов данной реализации можно выделить ее точность и скорость работы. К недостаткам можно отнести сложность исполнения и необходимость точной подстройки и стабилизации температур и токов лазеров.

1.5 Известные атаки злоумышленника на источники лазерного излучения

Секретность распределенного ключа в системах квантового распределения базируется на теоретических доказательствах секретности, в которых допускается, что злоумышленник (Ева) может сделать все, что не запрещено законами квантовой физики. Однако, несовершенства технической реализации систем КРК позволяют Еве их использовать для доступа к части секретного ключа. Среди таких атак выделяется атаки на источник лазерного излучения в системе КРК. Этот тип атак позволяет увеличить мощность, излучаемую лазером,

установленным в Алисе, и таким образом увеличить среднее число фотонов. Этот эффект позволяет применять атаку с расщеплением числа фотонов эффективнее и получать доступ к части секретного ключа.
Другой же тип атаки направлен непосредственно на Локальный осциллятор в системе КРК-НП для изменения времени начала синхронизации

1.5.1 Атака "засевом"лазерным излучением

Первоначально атаки злоумышленника были нацелены на приемную часть, а именно на детектор одиночных фотонов. В результате этой атаки злоумышленник имеет возможность "навязывать"секретный ключ легитимным пользователям. В дальнейшем появились атаки на модуляторы - атака "троянским конем". Такое воздействие позволяет узнать о выборе базиса легитимными пользователями и иметь доступ к секретному ключу за счет зондирования фазового модулятора излучением, сильно отличающимся по длине волны от той, что используют Алиса и Боб. Но существует и атака на источник излучения из состава системы квантового распределения ключей - атака "засевом"лазерным излучением. Одним из главных условий секретности распределенного ключа в системах КРК является предположение, что интенсивность квантоввых состояний, передаваемых Алисой, в среднем меньше 1 фотона на импульс. Однако атака "засевом"позволяет нарушить это предположение. Стратегия этой атаки заключается в следующем. Злоумышленник использует свое мощное излучение на близкой длине волны и посылает его в оптическую схему Алисы. В результате мощность, претерпевшая затухание из-за прохождения оптических элементов, попадает в резонатор лазера Алисы. Впрыснутые таким образом носители увеличивают выходную мощность вынужденного излучения Алисы. Под действием излучения увеличивается и энергия импульса, и непрерывная мощность. В результате этого увелчивается излучаемое число фотонов Алисой. Этот эффект позволяет злоумышленнику либо производить различение состояний-ловушек в протоколах с их реализацией или же проводить успешнее атаку

с разделением числа фотонов, тем самым получая доступ к секретному ключу. Еще одним эффектом, который негативно сказывается на секретности распределяемого ключа, является возможность злоумышленника вносить корреляции в излучение Алисы. Это происходит также с помощью атаки "засевом"лазерным излучением. Однако создание корреляций происходит с помощью зондирования импульсным излучением, а не непрерывным как в других работах. Интреференционная картина импульсов злоумышленника и Алисы будут скоррелированны и для внесения этой корреляции не требуется большой мощности - достаточно 1 нВт средней мощности. С ростом зондирующей мощности корреляции будут только возрастать, что позволит получить Еве также доступ к части секретного ключа.

Таким образом, атака "засевом"лазерным излучения является серьезной угрозой стойкости систем КРК, которую необходимо учитывать и разрабатывать контрмеры для ее предовтращения.

1.5.2 Атака на мощность локального осциллятора в системах квантового распределения ключа на непрерывных переменных

Существующие системы квантового распределения ключей на непрерывных переменнных используют один лазер для генерации квантовых состояний и локального осцциллятора. Такой подход позволяет упростить конечную систему. Однако, у генерации ЛО на стороне передатчика есть несколько недостатков: снижение уровня сигнала ЛО при передаче по волокну в виду есетественного затухания. Другой же недостаток данного подхода - уязвимость ЛО ко внешнему воздействию злоумышленника. В работе [14] описывается атака на ЛО в системе КРКНП. В доказательствах секретности не учитывается ЛО, хотя он, как классический сигнал, может быть без проблем перехвачен, измерен, усилен и отправлен снова в канал. Локальный же осциллятор используется для оценки пропускания канала и оценки распределения шума детектора - дробового шума. Эта величина является критической для оценки секретности ключа.

Стратегия злоумышленника заключается в следующем. Злоумышленник вносит затухание в начало локального осциллятор. Так как ЛО используется для генерации опорной частоты, то внесение затухания в ЛО вызывает задержку во времени при формировании опорной частоты. Для выполнения успешной атаки Ева производит следующие действия

1. Нарушитель, Ева, вводит аттенюатор, не разрушающий фазу излучения, в квантовый канал и применяет некоторое затухание α $(0 \leqslant \alpha \leqslant 1)$ на часть $\nu(0 \leqslant \nu \leqslant 1)$ импульсов локального осциллятора для изменения их формы. Тактовая частота, формируемая для гомодинного детектирования, зависящая от этих импульсов, сдивагется на величину δ.
2. Ева вводит светоделитель в квантовый канал и для части $\mu(0 \leqslant \mu \leqslant 1)$ входящих импульсов выполняет измерение обеих квадратур и подготавливает подходящие квантовые состояния, когда как для части $1 - \mu$ сигнальных импульсов, применяется функция светоделителя. Это называется частичной атакой "перехват - пересылка".

Когда Ева увеличивает часть μ сигнальных импульсов, для которых она выполняет атаку "перехват-пересылка то она вносит больше шума, который снижает количество секретных бит ключа, которые Алиса и Боб могут извлечь из квантовой передачи. Часть ν локального осциллятора, в которую вносится затухание, и само затухание α - это два параметра, которые выполняют одну и ту же функцию - масштабируют распределение измерений, выполненых Бобом, не изменяя границу его дробового шума. Это приводит к тому, что Алиса и Боб приходят к выводу о том, что в квантовый канал не было внесено дополнительного шума, зеленый график на рисунке 1.11 и поэтому распределяют ключ без обнаружения Евы.

1.5.3 Выводы по главе

В данной главе рассматриваются основы технологии квантового распределения ключей. Подходы

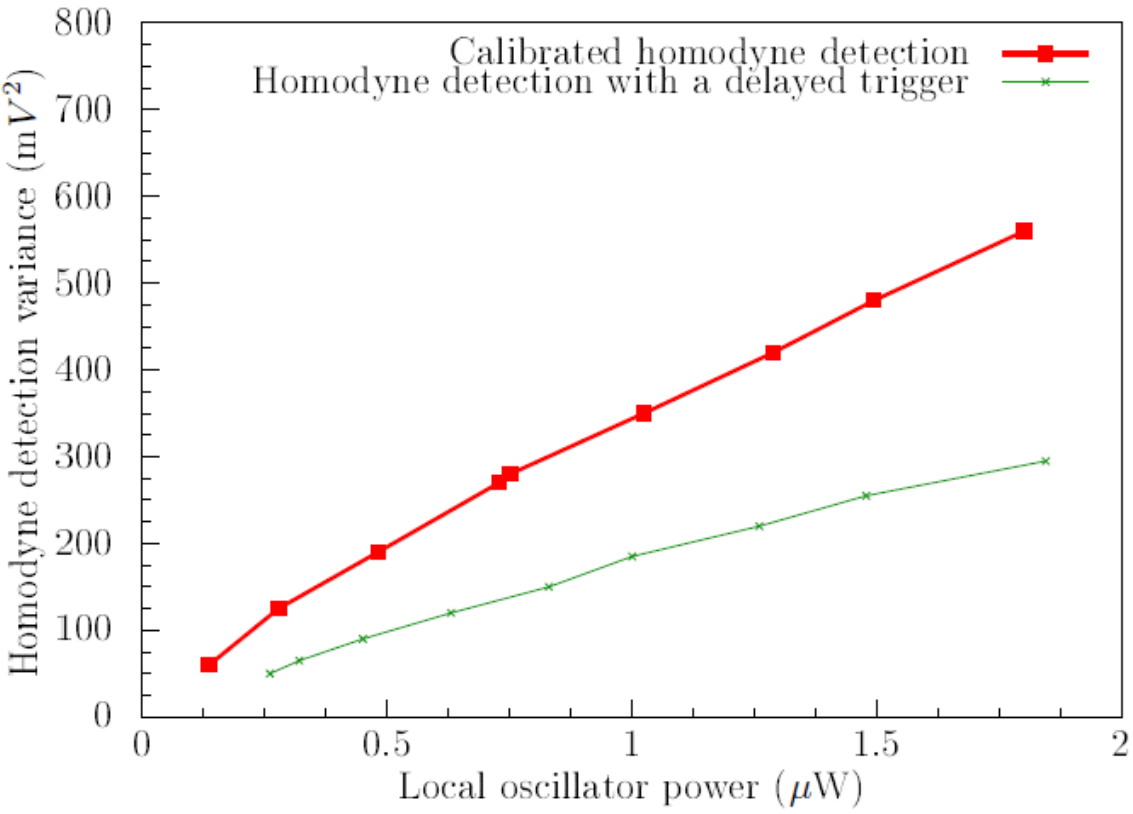

Рисунок 1.11 — График распределения шума гомодинного детектора без атаки (красный цвет) и под действием атаки (зеленый) на ЛО.

ГЛАВА 2. Система квантового распределения ключа на боковых частотах с применением обратной связи

Система квантового распределения ключа на боковых частотах

Одной из существующих реализаций систем квантового распределения ключа является реализация на боковых частотах, предложенная Юрием Тарасовичем Мазуренко. В отличии от других систем квантового распределения ключа, где лазерное излучение ослабляется до уровня мощности менее 1 фотона в импульсе, в системе квантового распределения ключа на боковых частотах (КРКБЧ) генерируются квантовые состояния на дополнительных оптических каналах, которые получаются в результате модулирования оптического лазерного излучения переменным электрическим сигналом с помощью электро-оптического модулятора на основе кристалла ниобата лития. Такая реализация системы квантового распределения ключа дает преимущества в виде

1. Устойчиовсть ко внешним воздействиям в виде колебаний волоконно-оптического тракта, которые изменяют поляризацию квантовых состояний случайным образом.
2. Возможность реализации частотного мультиплексирования на одной оптической несущей частоте для повышения инфомрационной емкости канала или для повышения его секретности за счет случайного выбора частоты для измерений квантовых состояний.
3. Совместимость с текущими волоконно-оптическими линиями связи за счет применения стандартной элементной-компонентной базы.

Эти преимущества выделяют систему квантового распределения ключа на поднесущих частотах среди остальных.

Принцип работы системы КРКБЧ

Установка КРКБЧ работает следующим образом. Полупроводниковый лазер с рабочей длиной волны генерирует излучение на длине волны 1550 нм. Это излучение прередается по волоконно-оптическому тракту с сохранением поляризации на фазовый модулятор. На электрический же вход электо-оптического модулятора подается радиосигнал, сформированный генератором. В качестве генератора выступает I/Q генератор, который на выходе выдает частоту 4.8 ГГц с фазовым кодированием. Эти фазовые сдвиги определяют какое квантовое состояние кодирует Алиса в свои состояния. Значения данных фазовых свдигов соответствуют значениям 0, 90, 180, 270 градусов. В результате взаимодействия электрического и оптического сигнала внутри кристалла, на выходе модулятора в оптическом сигнале появляются дополнительные гармоники. Их частота будет равна $\omega - \Omega$ и $\omega + \Omega$, где ω - частота излучения лазера, Ω - частота модуляции. Полученный в результате сигнал попадает на модулятор интенсивности на основе кристалла ниобата лития. Данно устройство создает импульсы из непрерывного излучения, сгенерированного лазером. Это необходимо для того, чтобы было возможно регулировать время прихода одиночного фотона на детектор одиночных фотонов, режим работы которого будет описан далее. Приготовленные импульсы попадают на аттенюатор оптической мощности (ПОА), который вносит затухание в пришедший сигнал до такого уровня, что на поднесущих частотах должна быть мощность, равная средней мощности, которая соответствует среднему числу фотонов меньше единицы. При этом на несущей частоте допускается использование мощности больше 1 фотона в среднем, так как сигнал на этой частоте не используется для распределения секретного ключа. Сгенерированные квантовые состояния передаются в блок приемника по стандартной волоконно-оптической линии связи, построенной с помощью одномодового волокна. Пройдя ВОЛС сигнал попадает на блок приемника. При прохождении сигнала по такой линии связи, поляризация прошедшего состояния изменяется на случайную, что приводит к негативным последствиям.

2.1 Метод оптической инжекции

Для систем квантового распределения ключа необходимы стабильные источники излучение с фиксированной длиной волны и без нелинейных эффектов в виде чирпа. Некачественные источники лазерного излучения привдоят к нарушению интерфереционной картины в случае протоколов MDI или же снижению скорости генерации секретного ключа и уменьшения дальности его передачи в протоколах BB84 с применением состояний ловушек. Одним из активно развивающихся решений этой проблемы является метод фазовой синхронизации с помощью оптической инжекции.

Полупроводниковые лазеры на основе кристалла InGaAs имеют выходное зеркало, которое пропускает больше 50% излучения. Благодаря такому коэффициенту пропускания, такие лазеры подвержены внешнему оптическому воздействию, которое зачастую является нежелательным из-за возможного образования паразитной обратной связи. Однако эту прозрачность можно использовать во благо для реализации оптической инжекции. Этот метод предлагает использование второго лазера, излучение которого попадает в резонатор другого лазера, образуя пару ведущий - ведомый. В результат этого выходное излучение ведомого лазера меняется под действием излучения ведущего источника. К плюсам метода оптической инжекции можно отнести следующее

1. Применение оптической инжекции улучшает форму спектра выходного излучения, уменьшая дополнительные гармоники.
2. Уменьшает возникающие в кристалле нелинейные процессы, негативно влияющие на частотный составл выходного излучения
3. Улучшает форму выходных импульсов за счет подавления релаксационных колебаний и стабилизации выходной частоты
4. Стабилизация амплитуды и длительности импульсов

Данные эффекты положительно сказываются на качестве выходного излучения и, как следствие, положительно влияют на характеристики систем квантвого распределения ключа, в которых они используются.

2.1.1 Математическая модель оптической инжекции

Система уравнений описывающих излучение ведомого лазера:

$$\begin{aligned}
\dot{Q}^{\text{м}} &= (G^{\text{м}} - 1)\frac{Q^{\text{м}}}{\tau_{\text{ф}}^{\text{м}}} + C_{\text{сп}}^{\text{м}} R_{\text{сп}}^{\text{м}} + F_Q^{\text{м}}, \\
\dot{\varphi}^{\text{м}} &= \frac{\alpha^{\text{м}}}{2\tau_{\text{ф}}^{\text{м}}}(G_{\text{лин}}^{\text{м}} - 1) + F_\varphi^{\text{м}}, \\
\dot{N}^{\text{м}} &= \frac{I^{\text{м}}}{e} - \frac{N^{\text{м}}}{\tau_e^{\text{м}}} - \frac{G^{\text{м}} Q^{\text{м}}}{\Gamma^{\text{м}} \tau_{\text{ф}}^{\text{м}}} + F_N^{\text{м}},
\end{aligned} \tag{2.1}$$

и связанную систему для ведомого лазера:

$$\begin{aligned}
\dot{Q} &= (G-1)\frac{Q}{\tau_{\text{ф}}} + C_{\text{сп}} R_{\text{сп}} + \\
&\quad + 2\kappa_{\text{и}}\sqrt{Q^{\text{м}} Q}\cos(\Delta\omega_{\text{и}} t + \varphi^{\text{м}} - \varphi) + F_Q, \\
\dot{\varphi} &= \frac{\alpha}{2\tau_{\text{ф}}}(G_{\text{лин}} - 1) + \\
&\quad + \kappa_{\text{и}}\sqrt{\frac{Q^{\text{м}}}{Q}}\sin(\Delta\omega_{\text{и}} t + \varphi^{\text{м}} - \varphi) + F_\varphi, \\
\dot{N} &= \frac{I}{e} - \frac{N}{\tau_e} - \frac{GQ}{\Gamma\tau_{\text{ф}}} + F_N,
\end{aligned} \tag{2.2}$$

где члены $C_{\text{сп}}^{\text{м}} R_{\text{сп}}^{\text{м}}$ и $C_{\text{сп}} R_{\text{сп}}$ описывают вклад спонтанного излучения, а $F_Q^{\text{м}}$, $F_\varphi^{\text{м}}$, $F_N^{\text{м}}$ и F_Q, F_φ, F_N – ланжевеновские силы для ведущего и ведомого лазеров соответственно.

2.2 Измерение диапазона фазовой синхронизации двух когерентных источников излучения

При методе оптической инжекции необходимо учитывать то, что два лазера необходимо настроить таким образом, чтобы их излучение синхронизировалось

по фазе. Для этого необходимо учитывать то, что существует полоса синхронизации, которая определяется как

$$\Delta\Omega = \Delta\omega_{\text{синх}} \sin(\varphi_{\text{синх}} - \psi), \tag{2.3}$$

где $\Delta\omega_{\text{синх}}$ определяется как

$$\Delta\omega_{\text{синх}} = z\sqrt{1 + \alpha^2(1 + 2\gamma_Q Q_{\text{с}})}, \tag{2.4}$$

и где мы ввели обозначение

$$z = \kappa_{\text{и}}\sqrt{Q_{\text{с}}^{\text{м}}/Q_{\text{с}}}. \tag{2.5}$$

Уравнение (2.3) накладывает первое ограничение на полосу синхронизации, которое можно записать следующим образом:

$$|\Delta\Omega| \leqslant \Delta\omega_{\text{синх}}. \tag{2.6}$$

выражение 2.6 показывает, что необходимо подбирать частоты и мощности ведущего и ведомого лазера для их синхронизации.

Для этого используются исследуемые лазеры и оптичесский анализатор спектра. У ведущего лазера изменяется длина волны за счет изменения температуры кристалла, контролируемой управляющей электроникой через элемент Пельтье. Излучение лазера ведомого подключается через оптический циркулятор с сохранением поляризации для минимизиации потерь в волокне. Второй вход циркулятора же подключен к волоконному выводу лазера-ведомого, чтобы излучение из лазера-ведущего входило внутрь резонатора. Выходное излучение лазера-ведомого подается на второй выход циркулятора и проходит в третий его порт, где устанавливается оптический анализатор спектра, который измеряет характеристики пришедшего излучения. В случае синхронизации, на анализаторе спектра возникает только одна длина волны лазера без изменений. Однако в случае разницы длин волн слишком большой, то будет наблюдаться несколько гармоник излучения, которые соответствуют длинам волн лазера-ведомого и лазера-ведущего. При некоторой комбинации длин волн, может также наблюдаться генерация нелинейных гармоник сигнала, сигнализирующих о том,

что лазеры находятся в зоне нестабильной синхронизации. Таким образом подбирается оптимальное соотношение длин волн лазеров. Для дальнейшего изучения диапазона возможно использование перестараиваемого аттенюатора в волокнонном тракте лазера-ведущего для изменения соотношения мощностей лазера-ведущего и лазера-ведомого.

2.3 Изменение длины волны излучения локального осциллятора под действием внешнего излучения.

Для измерения влияния оптической инжекции на длину волны лазера локального осциллятора, установленного на приемной стороне, необходимо измерить длину волны под действием оптической инжекции и без нее. Для этого была собрана оптическая схема состоящая из

1. Лазер-ведущий, установленный в передатичке
2. Лазер-ведомый, установленный в приемнике
3. Оптический анализатор спектра Yokogawam AQ6370D
4. Оптический циркулятор с сохранением поляризации

Излучение лазера-ведущего подается на первый порт оптического циркулятора, оно проходит во второй порт циркулятора, где подключен лазер-ведомый. Его же излучение проходит в 3 порт циркулятора и попадает на спектроанализатор. Производится измренение длин волн лазеров ведущего и ведомого без воздействия внешнего излучения. Результаты этих измерений отображены на рисунке 2.1 Измеренные длины волн лазеров - длина волны лазера-ведущего 1549.964 нм, длина волны лазера-ведомого без действия внешнего излучения - 1549.808 нм. Под действием же излучения от лазера-ведущего длина волны лазера-ведомого становится 1549.949 нм. То есть практически идеально совпадает с длиной волны лазера-ведущего. Данный эффект позволяет убрать промежуточные частоты, которые бы возникали при использовании двух разных источников излучения, что упрощает постобработку, а также снижает фазовый шум, т.к. фазы лазеров будут скоррелированы и будет требоваться корректи-

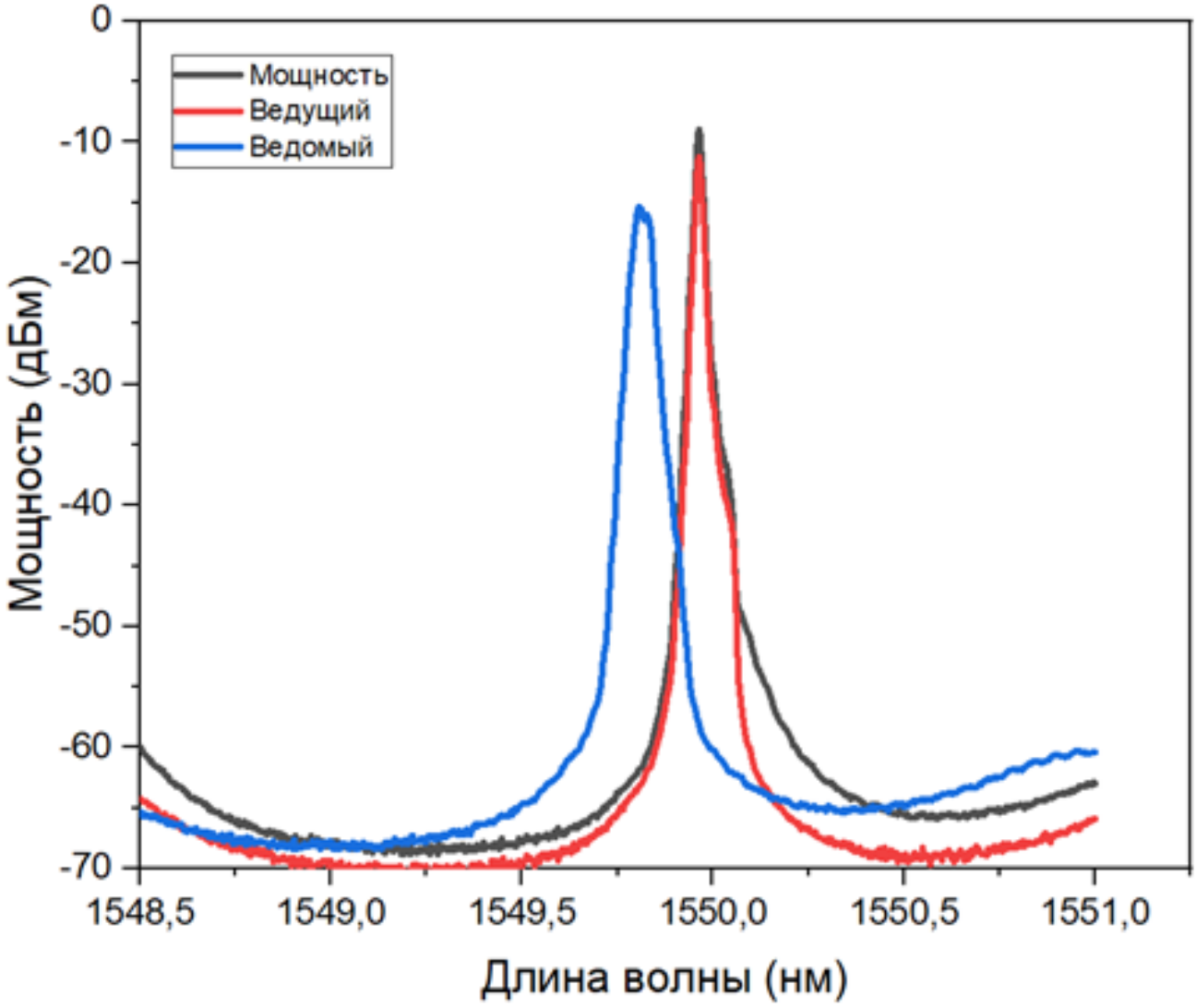

Рисунок 2.1 — *
Спектры лазерного излучения. Красным цветом отображен спектр излучения лазера-ведущего, синим - лазера-ведомого, а черным - лазера-ведомого под действием лазера-ведущего

ровка только из-за прохождения квантовыми состояния волоконно-оптической линии связи.

2.4 Математическая модель гетеродинного детектирования для системы КРК на боковых частотах с применением обратной связи.

Излучение лазера может быть представлено следующим образом:

$$F(t) = A_0 * \sin(\omega_0 t + \varphi_0), \tag{2.7}$$

где A_0 – амплитуда сигнала, ω_0 – частота лазерного излучения, φ_0 – начальная фаза излучения. Модулирующий сигнал:

$$S(t) = (1 + m \sin(\Omega t + \varphi(t))), \tag{2.8}$$

где m – индекс модуляции, Ω – частота модуляции, $\varphi(t)$ – вносимая модуляция.

Лазерное излучение после модуляции выглядит следующим образом:

$$F_s(t) = F(t) * S(t) = A_0 * \sin(\omega_0 t + \varphi_0) + \frac{A_0 * m}{2} * (\cos((\omega_0 + \Omega)t + (\varphi_0 + \varphi(t))) - \\ - \frac{A_0 * m}{2} * (\cos((\omega_0 - \Omega)t + (\varphi_0 - \varphi(t))), \tag{2.9}$$

Результат квадратичного детектирования сигнала, полученного в выражении (2.9) будет выглядеть следующим образом:

$$F_d(t) = F(t)^2 * S(t)^2 = (A_0 * \sin(\omega_0 t + \varphi_0))^2 * (1 + m * \sin(\Omega t + \varphi_0 + \varphi(t))^2 = \\ = \frac{1}{8}\Big\{ 4A_0^2 + 2A_0^2 * m^2 - 4A_0^2 \cos(2\omega t + 2\varphi_0) - 2A_0^2 * m^2 \cos(2\omega t + 2\varphi_0) - \\ - 2A_0^2 * m^2 \cos(2\Omega t + 2\varphi(t)) + A_0^2 * m^2 \cos(2\omega t - 2\Omega t + 2\varphi_0 - 2\varphi(t)) + \\ + A_0^2 * m^2 \cos(2\omega t + 2\Omega t + 2\varphi_0 + 2\varphi(t)) + 8A_0^2 m \sin(\Omega t + 2\varphi(t)) - \\ + 4A_0^2 m \sin(2\omega t - \Omega t + 2\varphi_0 - \varphi(t)) - 4A_0^2 m \sin(2\omega t + \Omega t + 2\varphi_0 + \varphi(t)) \Big\}, \tag{2.10}$$

В результате ток, протекающий через фотодиод, будет определяться выражением:

$$I = R(\lambda) G C F_d, \tag{2.11}$$

где $R(\lambda)$ – спектральная чувствительность фотодиода, G – электрическое усиление балансного детектора, C – отношение апертуры волокна к размеру чувствительной площадки фотодетектора.

В случае проводимого эксперимента единственная гармоника, которая лежит в полосе пропускания балансного детектора – это $A_0^2 m * \sin(\Omega t + \varphi(t))$. Остальные же гармоники не попадают в полосу пропускания и будут проявляться в виде постоянной составляющей, которая отфильтровывается перед первым усилителем.

2.5 Оптическая схема эксперимента для системы квантового распределения ключа на боковых частотах с применением метода оптической инжекции

Для системы кватового распределения ключей на боковых частотах на непрерывных переменных с когерентным методом детектирования вопрос создания обратной связи и использования локального осциллятора на стороне приемника не изучался. В рамках данного раздела предлагается оптическая схема эксперимента по передаче фазово-кодированных сигналов по волоконно-оптической линии связи. Для регистрации фазово-кодированных сигналах на поднесущих гармониках применяется метод гетеродинного детектирования сигналов. Его суть заключается в том, чтобы закодированный сигнал на симметричном светоделителе проинтерферировал с опорным излучением локального осциллятора. Также излучение локального осциллятора, установленного в блоке получателя, выступает в роли лазера-ведущего для источника излучения, установленного в блоке отправителя. За счет этого достигается синхронизация длин волн излучения лазера-ведущего и лазера-ведомого, локального осциллятора и информационного лазера соответственно. Эта особенность позволяет не применять частотную подстройку источников излучения и упростить конечную систему.

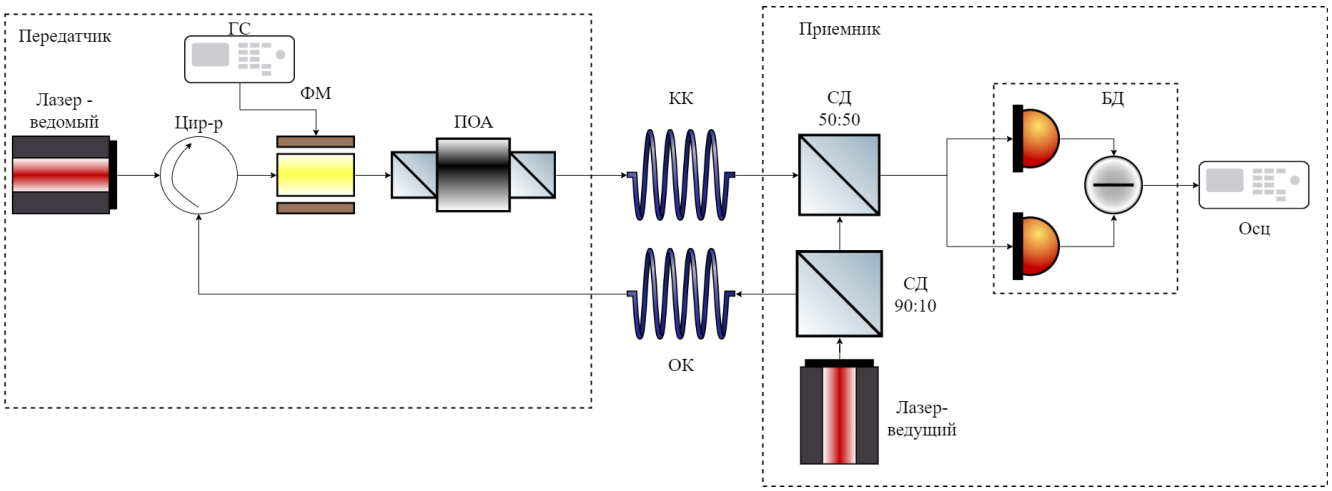

Рисунок 2.2 — Оптическая схема установки системы КРК на поднесущих гармониках с оптической инжекцией, где СД - светоделитель, ГС - генератор сигналов, ФМ - фазовый модулятор, ПОА - переменный оптический аттенюатор, КК - квантовый канал, ОК - открытый канал, Цир-р - циркулятор, БД - балансный детектор, Осц - осциллограф

2.6 Описание экспериментальной установки

Оптическая схема установки по экспериментальной передаче фазово-кодированных сигналов и применением гетеродинного метода детектирования и оптической инжекции на рисунке Данная схема работаетследующим образом. Лазер-ведущий генерирует оптическое излучение, которое разделяется на 2 части светоделителем 90:10, 10 процентов которого по открытому каналу передаются на сторону передатчика в 1 порт оптического циркулятора. Во второй порт циркулятора подключен лазер передатчика. Такая схема подключения как раз создает оптическую инжекцию и частоты лазера передатчика и лазера локального осциллятора совпадают. Полученное излучение на стороне передатчика проходит фазовую модуляцию с помощью связки фазового модулятора и генератора сигналов произвольной формы на частоте 100 МГц. После этого подготовленный сигнал ослабляется с помощью переменного оптического аттенюатора. После этого излучение передается по квантовому каналу на сторону приемника. В приемнике принятный сигнал попадает на симметричный светоделитель с 2 входами и 2 выходами с коэффициентом деления 50:50. На второй же вход этого делителя попадает излучени ЛО, его 90 процентов после светоде-

лителя. В итоге эти сигналы интерферируют и результат этой интерференции регистрируется балансным детектором. Так как длины волн информационного лазера и ЛО совпадают, то в результате интерференции они регистрируются как постоянный уровень напряжения, однако благодрая выносу фазово-кодированных состояний на поднесущие гармоники, то их интерференция с ЛО и дает результат в виде промежуточной частоты, которая равна частоте модуляции, примененой в Алисе. Эта частота на выходе балансного детектора осцифровывается с помощью осциллографа и в дальнейшем обрабатывается.

2.7 Полученные экспериментальные результаты

В результате интерференции на выходе балансного детектора регистрируется промежуточная частота равная $\omega + \Omega - F$, где ω - частота лазера Алисы, Ω - частота модуляции, F - частота ЛО. Благодаря применению оптической инжекции частоты ЛО и лазера Алисы совпадают, поэтому на выходе балансного детектора остается только гармоника на частоте модуляции, в которую и вносится фазовый свдиг для передачи информации. Этот сигнал изображен на рисунке 2.3 На этом графике видна один гармонический сигнал в 100 МГц, в котором содержится информация о фазе, которую необходимо извлечь методами цифровой обработки сигналов. Для более точного измерения фазы сигнала, необходимо эту частоту отфильтровать от шума, который появлятеся из-за прохождения канала и собственных шумов балансоного детектора. Результат цифровой фильтрации сигнала с рисунка 2.3 отображается ниже. После применения к сигналу с рисунка 2.4 алгоритма Быстрого Преобразования Фурье для изучения спектрального состава. Результат изображен на рисунке ниже. На рисунке 2.5 изображен результат БПФ примененноного к сигналу после фильтрации. Единсвтенная гармоника находится на частоте 100 МГц, что согласуется с тем, что частоты лазеров-ведущего и лазера-ведомого совпадают. Для получения информации о фазе принятого сигнала необходимо цифровыми методами обработки информации извлечь ее оттуда. Для этого также возможно

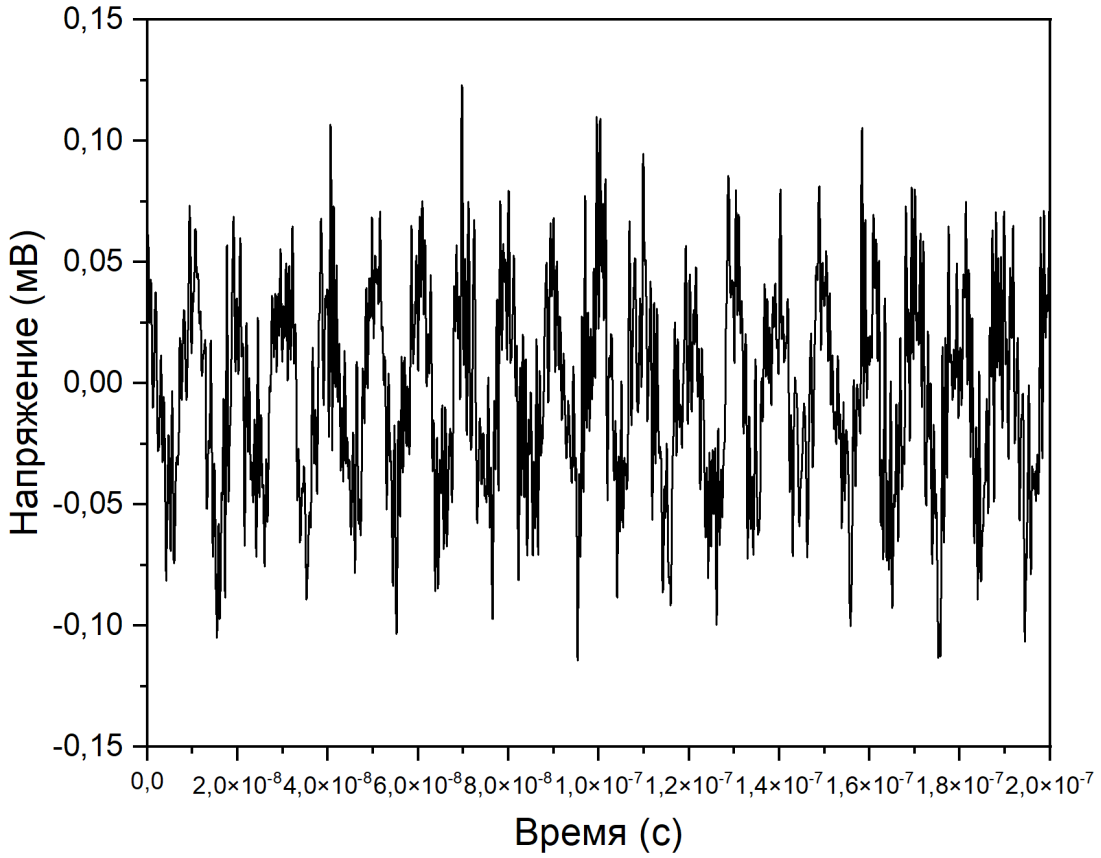

Рисунок 2.3 — Выходной зашумленный сигнал на выходе балансного детектора.

использование быстрого преобразования Фурье. Результат этого преобразования отображен на рисунке 2.6 В результате работы алгоритма по извлечению информации из принятого сигнала, на выходе формируется последовательность фазовых сдвигов, которым сопоставляется определенному значению бита. Такая последовательность будет являтся сырым ключом. На рисунке 2.6 изображены как раз фазовые сдвиги, которые соответствуют виду модуляции QPSK, которые широко распространена в классических системах передачи данных. Благодаря этому можно передавать 2 бита информации за один такт передачи данных.

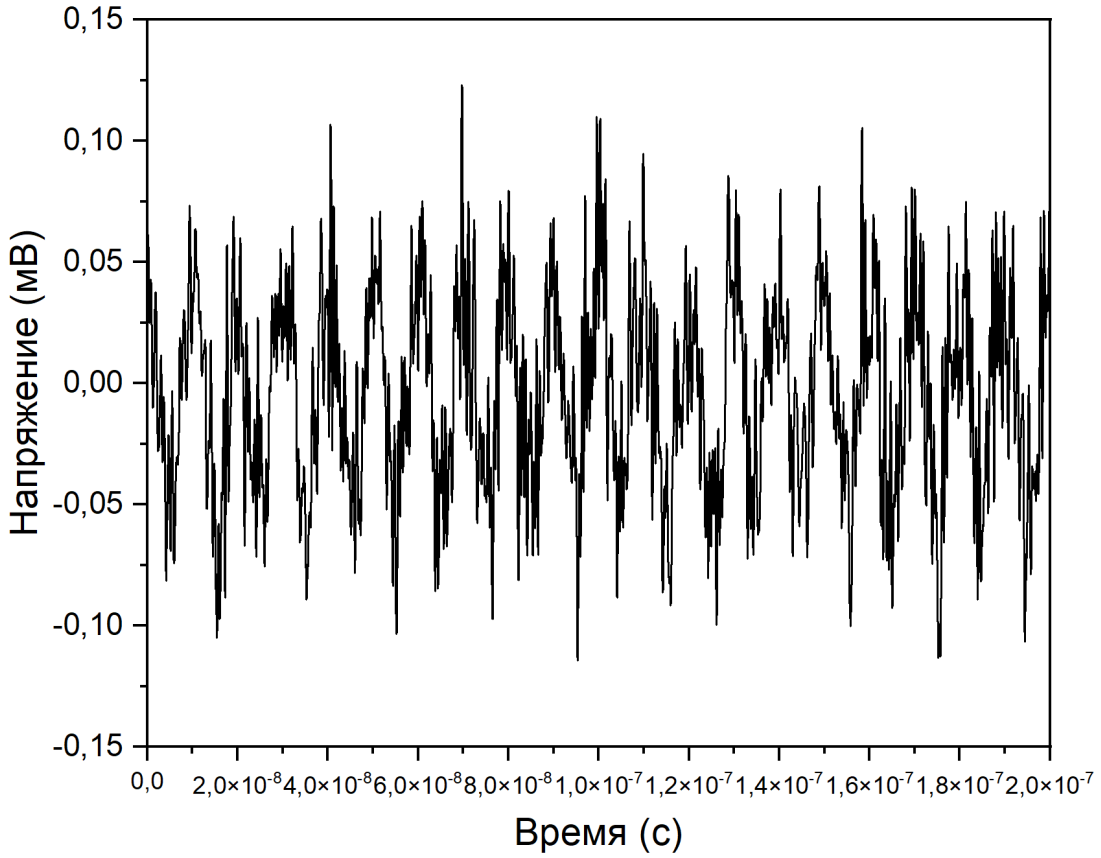

Рисунок 2.4 — Выходной сигнал балансного детектора после фильтрации.

2.8 Выводы по главе

В данной главе впервые рассматривается применение обратной связи для системы квантового распределения ключей на боковых частотах на непрерывных переменных в виде оптической инжекции. Такая обратная связь, применяемая к гетеродинному методу детектирования, позволяет стабилизировать частоты лазеров-отправитель и лазер Локального Осциллятора с точностью до нескольких мегагерц. Такая точность позволяет не выполнять подстройку частоты, как в системах с двумя независимыми источниками излучения. В рамках главы также рассмотрен схема оптического эксперимента по распределению последовательности сырых бит, в рамках которой проведена фильтрация сигнала на промежуточной частоте и его постобработка для извлечения фазы сигнала и,

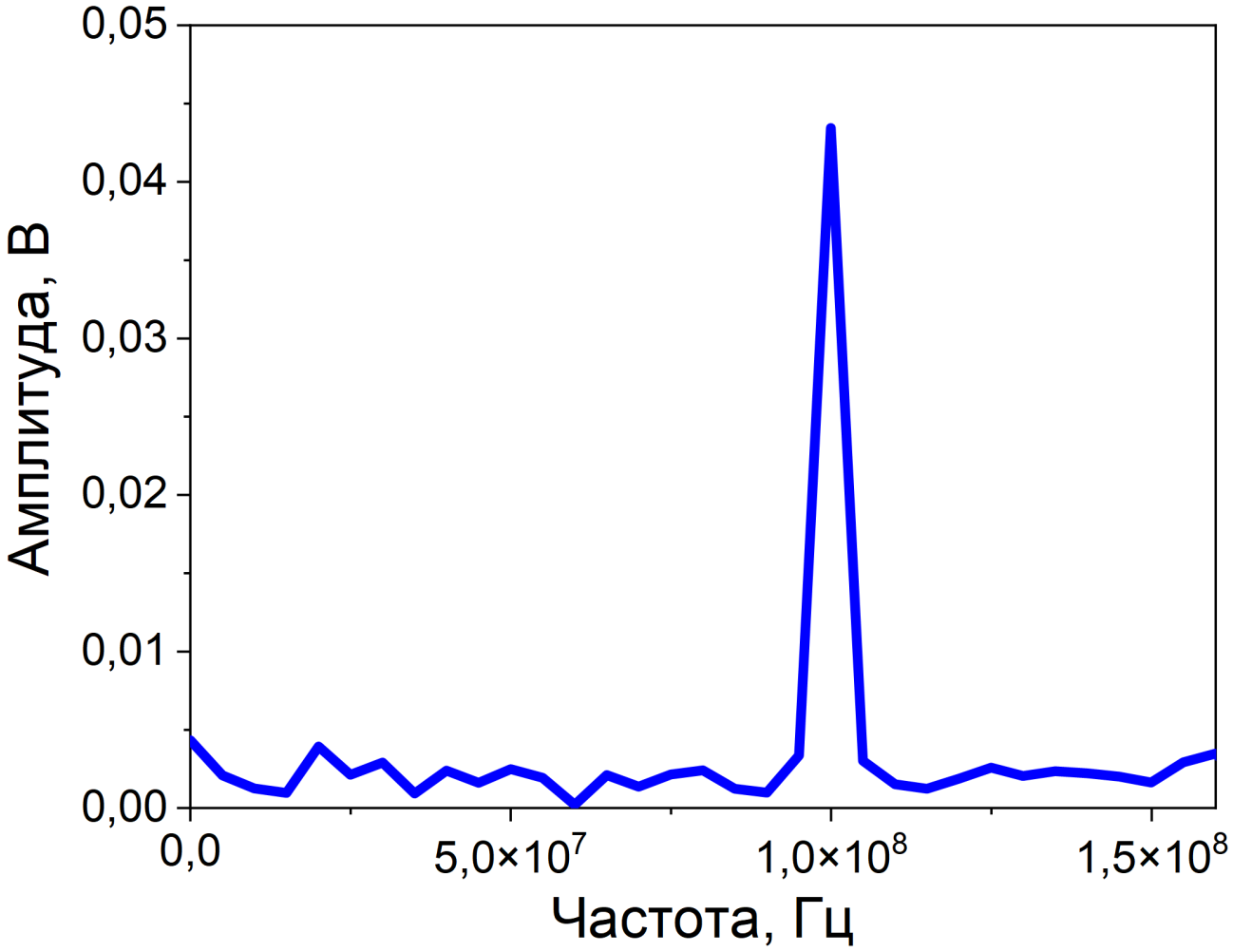

Рисунок 2.5 — Спектр полученного сигнала

соответсвенно, бит информации. Данный метод требует наличия дополнительного оптического канала для создания обратной связи и более тщательного исследования на уязвимость технической реализациии для дальнейшего внедрения в реальные системы КРК.

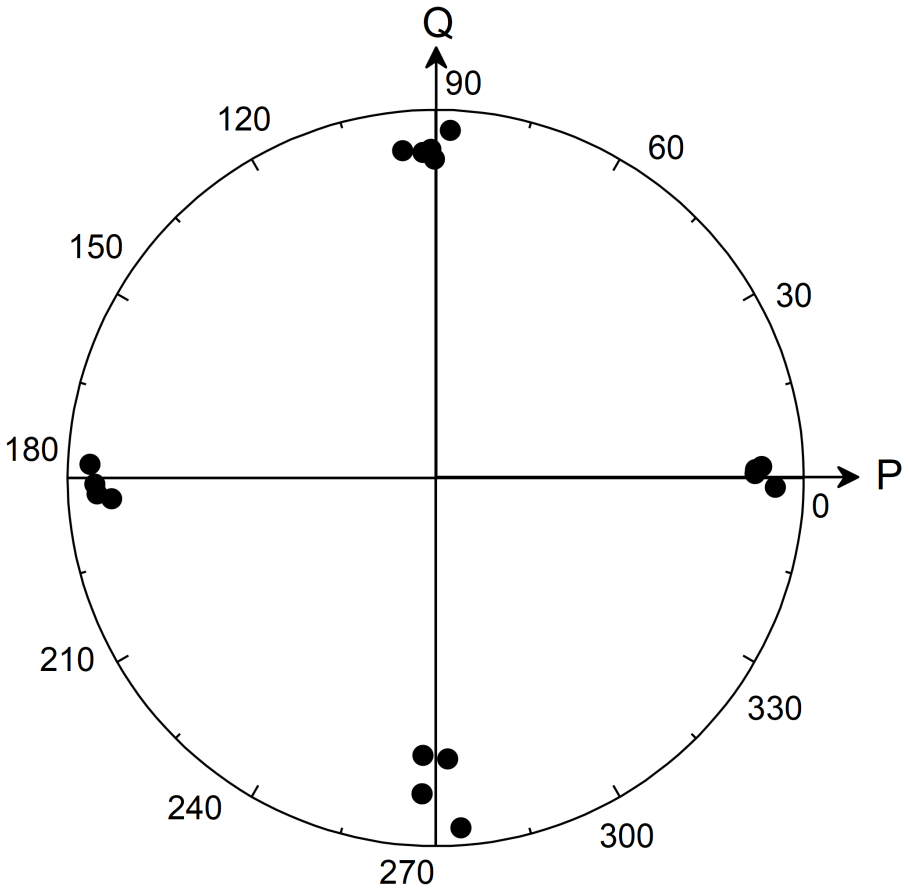

Рисунок 2.6 — Измеренные значения фазовых свдигов в выходном сигнале балансного детектора

ГЛАВА 3. Система квантового распределения ключа на поднесущих гармониках с применением двух независимых источников когерентного излучения на непрерывных переменных

Первые системы квантового распределения ключа на непрерывных переменных основывались на генерации и локального осциллятора, и квантовых состояний, одним лазером. Это позволяло избегать проблем с рассогласованием фаз ЛО и квантовых состояний. Однако, это несло и существенные недостатки. Была необходима система мультиплексирования на стороне передатчика и демультиплексирования на стороне приемника для того, чтобы была возможность передавать локальный осциллятор в одном же волокне с квантовыми состояниями без нежелательной интерференции ЛО с ними. Другим недостатком являлась ограниченная мощность передаваемого локального осциллятора. Это связано с несколькими причинами. Первая причина - при передаче по ВОЛС локальный осциллятор затухает как и все сигналы, проходящие по волокну, что ограничивает его мощность на этапе интерференции в приемном модуле. Вторая причина ограничения мощности локального осциллятора - нелинейные эффекты, возникающие во время прохода мощного сигнала по волоконно-оптическому тракту, связанный с рассеянием Релея и прочими. Соответственно, передача мощного ЛО может перекрыть все преищмуества его мощности дополнительными шумамами. И самая главная проблема - это возможные атаки на ЛО от злоумышленника. Итогом всех этих проблем стало использование "локального"локального осциллятора на стороне приемника, сгенерированного отдельным независимым лазером.

3.1 Метод гетеродинного детектирования сигналов для системы квантового распределения ключа на боковых частотах

В данной главе предлагается использование гетеродинного метода детектирования сигнала с применением двух независимых источников когерентного излучения на непрерывных переменных. Данный способ обладает следующими достоинствами

1. Использование источника ЛО на стороне приемника решает проблемы передачи ЛО в канале, связанные с шумом и недостаточной мощностью
2. Оптическая схема с ЛО на стороне приемника защищает этот источник от атак злоумышленника, что существенно повышает устойчивость данной системы к воздействию злоумышленника
3. При гетеродинном приеме сигнала, информация о принятом сигнале переносится в полосу радиочастот на промежуточную частоту, что позволяет анализировать и усиливать гармоническое колебание, что существенно расширяет возможность по применяемым видам модуляции
4. Применение гетеродинного метода детектирования сигналов также позволяет разделять частотно-мультиплексированные сигналы на одну несущую оптическую частоту для повышения скорости выработки секретного ключа или повышения секретности за счет случайного выбора рабочей частоты.

Современные работы по созданию систем КРК на непрерывных переменных переходят к использованию ЛО, сгенерированного на стороне приемника. В данной работе рассматривается применение двух независимых источников излучения для системы квантового распределения ключа на поднесущих гармониках и с частотным мультиплексированнием на одной несущей частоте.

3.2 Протокол квантового распределения ключа на поднесущих гармониках с гетеродинном методом детектирования сигналов

Протокол работает следующим образом:

1. Алиса готовит квантовые состояния, кодируя информацию в фазовый свиг излучения на боковых частотах ослабленного лазерного излучения, и передает их.
2. Боб измеряет пришедшие квантовые состояния с помощью гетеродинного детектирования.
3. Выходной сигнал балансного детектора оцифровывается и обрабатывается с помощью алгоритма Быстрого Преобразования Фурье.
4. Измеряется частота и фаза нужной гармоники из полученного мгновенного спектра.
5. Оценивается соотношение сигнал/шум.
6. Проводится процедура исправления ошибок с помощью соответствующих кодов.

3.3 Оптическая схема системы квантового распределения ключа на боковых частотах с применением гетеродинного детектирования

Данная схема устроена следующим образом. Лазер на стороне передатчика генерирует непрерывное лазерное излучение. Это излучение проходит по оптическому волокну с сохранением поляризации и попадает на фазовый модулятор. На фазовый модулятор попадает сигнал от генератора сигналов свободной формы. Этот генератор подготавливает модулирующий сигнал. В нем содержаться фазовые сдвиги, которые соответствуют кодировке QPSK с фазами 45, 135, 215 и 305 градусов. Этот сигнал модулирует оптическое излучение и на выходе получаются дополнительные поднесущие гармоники сигнала в выходном спектре фазового модулятора. После этого сигнал попадает на волоконно-оптический

перестраиваемый аттенюатор для снижения уровня мощности на поднесущих гармониках до однофотонного уровня. После этого сигнал проходит квантовый канал и попадает на схему контроля поляризации, которая рассматривается в секции 3.5. После прохождения этой схемы, сигнал попадает на светоделитель с 2 входами и 2 выходами с коэффициентом деления 50:50, на входы которого попадает и сигнал локального осциллятора. В результате происходит интерференция этих сигналов. Но частоты ЛО и информационного сигнала отличаются так, что частота ЛО больше частоты лазера передатчика. В итоге этот результат интерференции регистрируется балансным детектором. Разностные частоты от всех сигналов, которые проинтерферировали, находятся в полосе пропускания балансного детектора благодаря подбору частот. При необходимости частота лазера ЛО может быть подстроена для переноса спектра сигнала вверх или вниз по частоте. По итогу на выходе БД формируется несколько гармонических колебаний. Для анализа необходимо отфильровать синусоидальное колебание на частоте модуляции, так как оно несет информацию о фазе, закодированной передатчиком. После этого его можно обрабатывать уже методами цифровой обработки сигналов (ЦОС). Для компенсации же фазовых искажений можно обрабатывать промежуточную частоту между лазерами передатчика и приемника. Ее фазовые колебания будут содержать фазовый шум и передатчика с квантовым каналом, и фазовый шум ЛО. Это измеренное значение необходимо учитывать на этапе постобработки. Оптическая схема гетеродинного метода детектирования для системы КРК приведена на рисунке 3.1

3.4 Математическая модель системы квантового распределения ключа на боковых частотах с применением гетеродинного детектирования

Излучение лазера может быть представлено следующим образом:

$$F(t) = A_0 * \sin(\omega_0 t + \varphi_0), \tag{3.1}$$

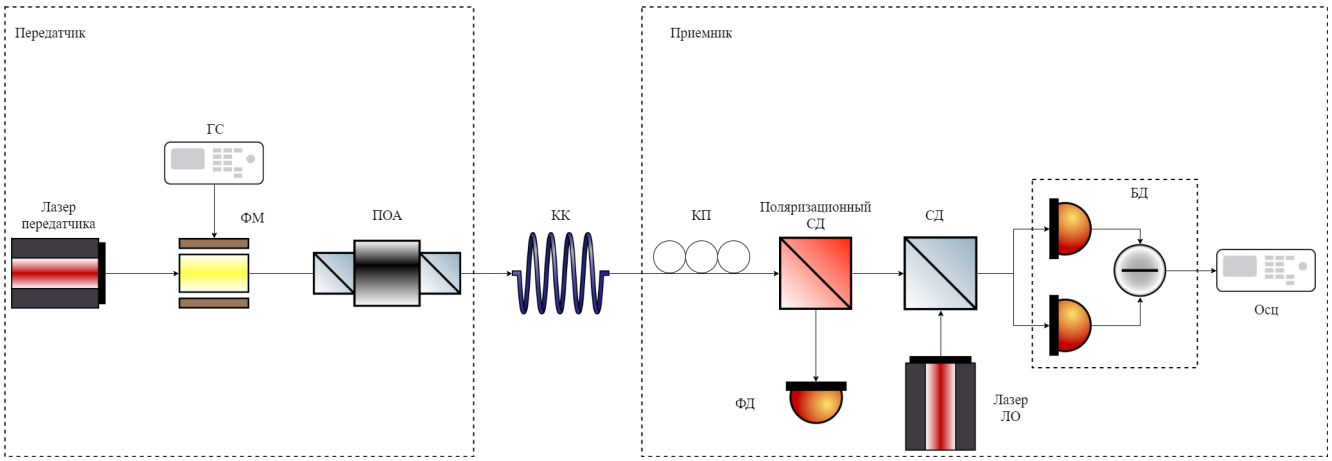

Рисунок 3.1 — Схема эксперимента по реализации гетеродинного метода приема сигналов для КРК, где ГС - генератор сигналов, ФМ - фазовый модулятор, ПОА - перестраиваемый оптический аттенюатор, КК - квантовый канал, КП - контроллер поляризации, СД - светоделитель, ФД - фотодиод, ЛО - локальный осциллятор, БД - балансный детектор, ОСЦ - осциллограф

где A_0 – амплитуда сигнала, ω_0 – частота лазерного излучения, φ_0 – начальная фаза излучения. Модулирующий сигнал:

$$S(t) = (1 + m\sin(\Omega t + \varphi(t))), \tag{3.2}$$

где m – индекс модуляции, Ω – частота модуляции, $\varphi(t)$ – вносимая модуляция.

Лазерное излучение после модуляции выглядит следующим образом:

$$F_s(t) = F(t) * S(t) = A_0 * \sin(\omega_0 t + \varphi_0) + \frac{A_0 * m}{2} * (\cos((\omega_0 + \Omega)t + (\varphi_0 + \varphi(t))) - \\ - \frac{A_0 * m}{2} * (\cos((\omega_0 - \Omega)t + (\varphi_0 - \varphi(t))), \tag{3.3}$$

Результат квадратичного детектирования сигнала, полученного в выражении (2.9) будет выглядеть следующим образом:

$$
\begin{aligned}
&F_d(t) = (F(t) * S(t) * F_{het}(t))^2 = \\
&+ \frac{A_{sig}^2 * A_{het}^2}{8} * \cos(2ft - 2\omega t) + \frac{A_{sig}^2 * A_{het}^2}{16} * \cos(2ft - 2\omega t) + \\
&+ \frac{A_{sig}^2 * A_{het}^2}{4} * \cos(2\omega * t + 2\varphi) + \frac{A_{sig}^2 * A_{het}^2 * m^2}{8} * \cos(2\omega * t + 2\varphi) + \\
&+ \frac{A_{sig}^2 * A_{het}^2}{8} + \cos(2ft + 2\omega t + 2\varphi) + \frac{A_{sig}^2 * A_{het}^2 * m^2}{16} * \cos(2ft + 2\omega t + 4\varphi) - \\
&- \frac{A_{sig}^2 * A_{het}^2 * m^2}{8} * \cos(2\Omega t) - \frac{A_{sig}^2 * A_{het}^2 * m^2}{16} * \cos(2ft - 2\Omega t + 2\varphi) - \\
&- \frac{A_{sig}^2 * A_{het}^2 * m^2}{32} * \cos(2ft - 2\omega t - 2\Omega t) - \frac{A_{sig}^2 * A_{het}^2 * m^2}{16} * \cos(2\omega t - 2\Omega t) - \\
&- \frac{A_{sig}^2 * A_{het}^2 * m^2}{32} * \cos(2ft + 2\omega t - 2\Omega t + 4\varphi) - \\
&- \frac{A_{sig}^2 * A_{het}^2 * m^2}{16} * \cos(2ft + 2\Omega t + 2\varphi) - \frac{A_{sig}^2 * A_{het}^2 * m^2}{32} * \cos(2ft - 2\omega t + 2\Omega t) - \\
&- \frac{A_{sig}^2 * A_{het}^2 * m^2}{16} * \cos(2\omega t + 2\Omega t + 2\varphi) -, \frac{A_{sig}^2 * A_{het}^2 * m^2}{32} * \cos(2ft - 2\omega t + 2\Omega t) - \\
&- \frac{A_{sig}^2 * A_{het}^2 * m^2}{16} * \cos(2\omega t + 2\Omega t + 2\varphi) - \frac{A_{sig}^2 * A_{het}^2 * m^2}{32} * \cos(2ft + 2\omega t + 2\Omega t + \\
&+ \frac{A_{sig}^2 * A_{het}^2 * m}{2} * \sin(\Omega t) - \frac{A_{sig}^2 * A_{het}^2 * m}{4} * \sin(2ft - \omega t + 2\varphi) - \\
&- \frac{A_{sig}^2 * A_{het}^2 * m}{8} * \sin(2ft - 2\omega t - \Omega t) - \frac{A_{sig}^2 * A_{het}^2 * m}{4} * \sin(2\omega t - \Omega t + 2\varphi) - \\
&- \frac{A_{sig}^2 * A_{het}^2 * m}{8} * \sin(2ft + 2\omega t - \Omega t + 4\varphi) + \frac{A_{sig}^2 * A_{het}^2 * m}{2ft + \Omega t + 2\varphi} + \\
&+ \frac{A_{sig}^2 * A_{het}^2 * m}{8} * \sin(2ft - 2\omega t + \Omega t) + \frac{A_{sig}^2 * A_{het}^2 * m}{4} * \sin(2\omega t + \Omega t + 2\varphi) + \\
&+ \frac{A_{sig}^2 * A_{het}^2 * m}{8} * sin(2ft + 2\omega t + \Omega t + 4\varphi)
\end{aligned}
\tag{3.4}
$$

В результате ток, протекающий через фотодиод, будет определяться выражением:

$$I = R(\lambda)GCF_d, \tag{3.5}$$

где $R(\lambda)$ – спектральная чувствительность фотодиода, G – электрическое усиление балансного детектора, C – отношение апертуры волокна к размеру чувствительной площадки фотодетектора.

В случае проводимого эксперимента единственная гармоника, которая лежит в полосе пропускания балансного детектора – это $A_0^2 m * \sin(\Omega t + \varphi(t))$. Остальные же гармоники не попадают в полосу пропускания и будут проявляться в виде постоянной составляющей, которая отфильтровывается перед первым усилителем.

3.5 Алгоритм подстройки поляризационных искажений для системы квантового распределения ключа на боковых частотах с применением гетеродинного детектирования

Существенной проблемой для интерференции сигналов является их поляризация. Как известно, сигналы в ортогональный поляризациях не взаимодействуют. Что существенно снижает эффективность передачи данных в системах КРК на непрерывных переменных. В рамках данного раздела предалаегся реализация алгоритма подстройки поляризации пришедшего сигнала. При использовании связки поляризационного светоделителя и контроллера поляризации можно подстраивать поляризацию за счет анализа спектрального состава принятного сигнала с помощью быстрого преобразования Фурье. В случае неправильной поляризации, на выходе поляризационного светоделителя сигнал разделяется на две поляризации по осям: быструю и медленную. В итоге получается так, что на балансный детектор приходят два сигнала, а не один. Это приводит к тому, что в спектре полученного сигнала появляется не только гармоника на частоте модуляции, но и ее удвоение. Что можно отслеживать и использовать контроллер поляризации для контроля входной поляризации. На рисунке 3.2 В спектре этого сигнала наблюдается гармоники на частоте 20 МГц, что соответствует частоте модулирующего излучения и 40 МГц, что является удвоенной частотой модуляции. На основе этой информации система обратной

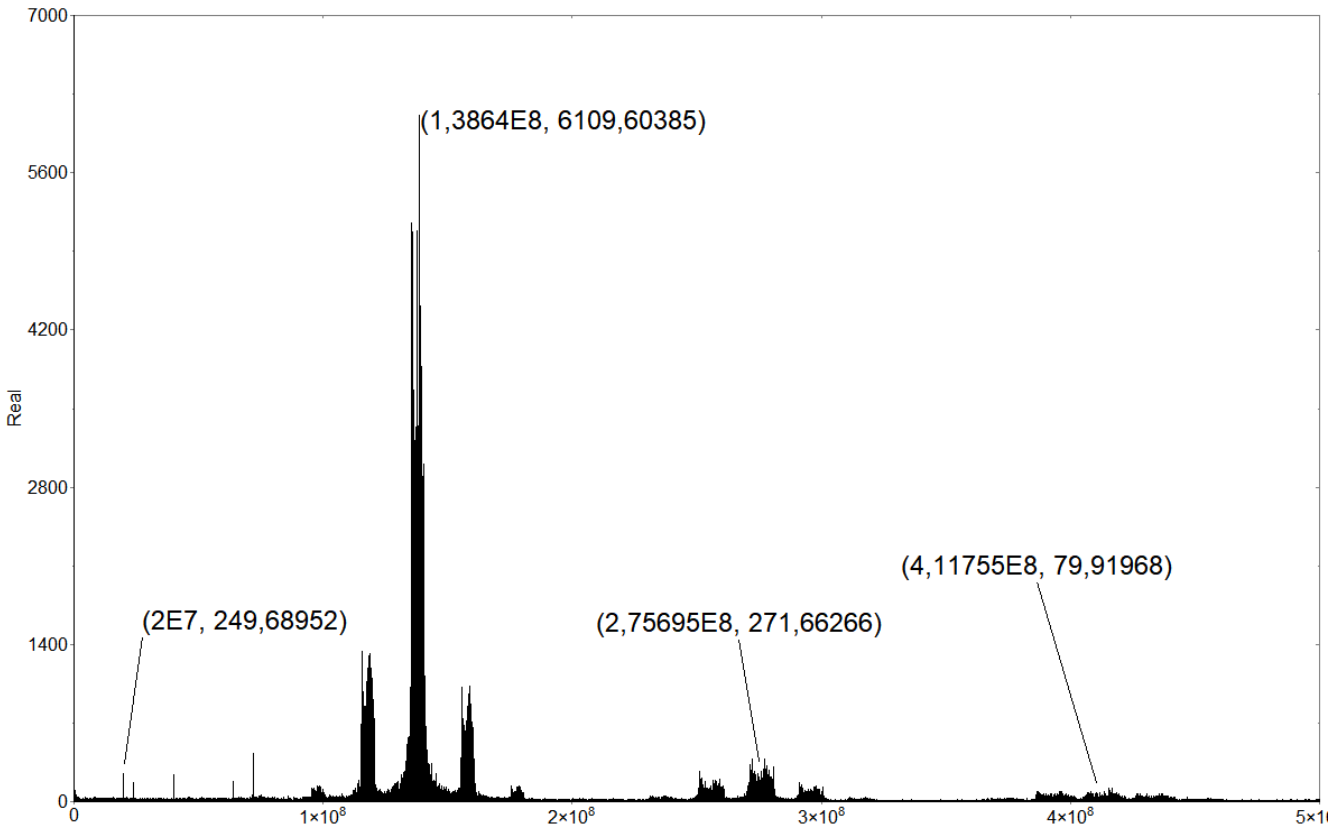

Рисунок 3.2 — Спектр выходного сигнала с неправильной поляризацией

связи должна дать команду на контроллер поляризации для ее контроля. В результате действий КП должен приветси сигнал к виду, отображенному на рисунке 3.3 На графике 3.3 видно, что присутствует только спектральная линия от частоты модуляции и по амплитуде она существенно больше, чем на графике 3.2. В общем виде алгоритм можно записать следующим образом

1. Применение БПФ к принятому сигналу
2. Анализ спектрального состава сигнала
3. Поворот поляризации сигнала до уничтожения гармоники на удвоенной частоте модуляции
4. Дальнейший поворот поляризации сигнала до максимума гармоники на частоте модуляции

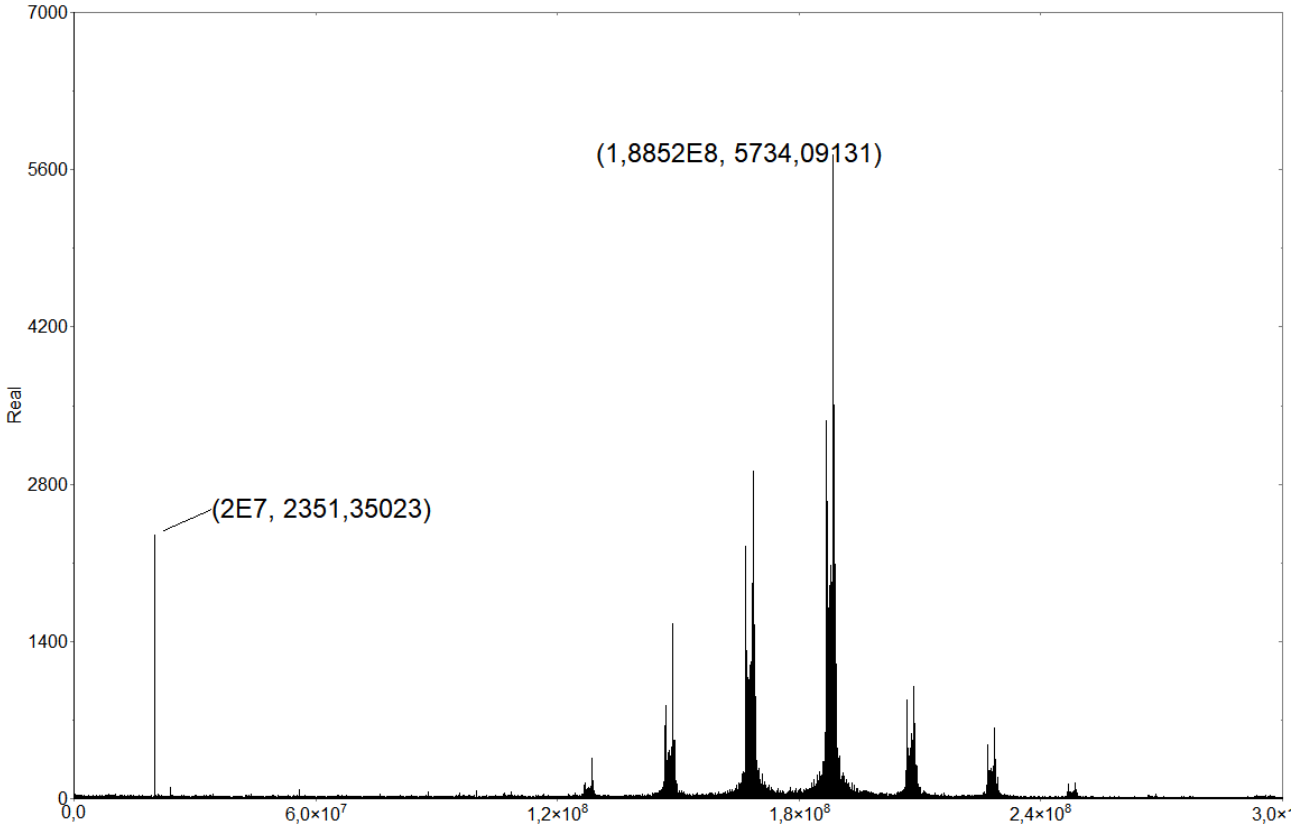

Рисунок 3.3 — Спектр выходного сигнала с балансного детектора с правильной поляризацией

3.6 Математическая модель гетеродинного детектирования с двумя независимыми источниками излучения

3.7 Описание экспериментальной установки

Для реализации системы квантового распределения ключей на поднесущих гармониках с применением двух независимых источников излучения на непрерывных переменных была собрана экспериментальная схема изображенная на рисунке 3.1 Данная схема работает следующим образом. Лазерное излучение, сгенерированное лазером NeoPhotonics μITLa с шириной линии менее 100 кГц и выходной мощностью 1 мВт и длиной волны 1550.0026 нм. В качестве лазера локального осциллятора использовался лазер Hewlett and Packard 8168C с излучением на длине волны 1550.0018 нм и выходной мощностью 1 мВт. В качестве

фазового модулятора использовался фазовый модулятор производства EOSpace с полосой пропускания 40 ГГц и вносимыми потерями 4 дБ. В качестве балансного детектора использовался детектор фирмы General Photonics BDP-003 с чувствительностью 0.8 А/Вт на длине волны 1550 нм, полосой пропускания 200 МГц и коэффициентом усиления 10^5. Для измерений и выполнения Быстрого Преобразования Фурье использовался осциллограф Rohde and Schwarz RTM 3000 с полосой пропускания 1 ГГц и количеством выбором 5 ГВ/с. На электрический же вход фазового модулятора подается гармонический синусоидальный сигнал с частотой 20 МГц и амплитудой 1 В и дополнительным смещением в 0.8 В. В результате взаимодействия лазерного излучения и электрического сигнала на фазовом модуляторе в спектре излучения образуются 2 дополнительные гармоники - боковые частоты. Полученный сигнал попадает на переменный оптический аттенюатор, который вносит затухание таким образом, чтобы на боковых частотах был уровень сигнала, мощность которого в среднем меньше мощности одного фотона. После этого полученный сигнал передается по одномодовому оптическому волокну на сторону приемника. Попав на сторону приемника, сигнал попадает на блок контроля поляризации, о принципе работы которого будет рассказано позже. Прошедший сигнал попадает на один из входов светоделителя с 2 входами и 2 выходами и коэффициентом деления 50:50. На другой же вход светоделителя попадает излучение лазера - локального осциллятора (ЛО). В результате на светоделителе квантовые состояния от Алисы интерферируют с локальным осциллятором. За счет этой интерференции с мощным ЛО, квантовые состояния усиливаются и регистрируются балансным детектором, который основан на двух классических фотодиодах.

3.8 Описание полученных результатов

При интерференции локального осциллятора и квантовых состояний, посланных Алисой, на светоделителе на стороне Боба, формируются комбинационные частоты от всех спектральных составляющих. Их модели описаны в разделе

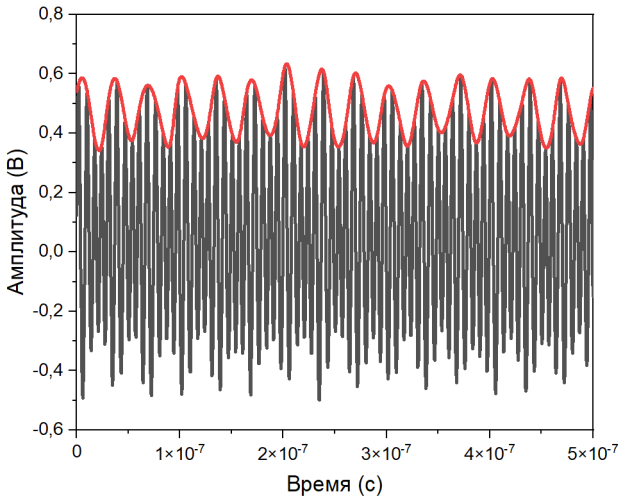

Рисунок 3.4 — *
Выходной сигнал с балансного детектора во временной области

3.6. В полученной модели интерес представляют только разностные частоты по причине того, что только они попадают в полосу пропускания балансного детектора. На выходе балансного детектора формируется гармонический сигнал состоящий из двух огибающих и несущей. Форма этого сигнала изображена на рисунке 3.4 Информацию несут только огибающие данного сигнала. Для их анализа их предварительно необходимо отфильтровать. Это можно сделать как программными методами, так и с помощью физических фильтров, установленных после балансного детектора. В рамках данной работы предлагается программно фильтровать огибающую, которая соответствует частоте $(\omega_{LO} - (\omega_{car} - \Omega_{mod})$, так как она попадает в полосу пропускания балансного детектора.

В результате работы данной системы на выходе балансного детектора формируются сигналы на промежуточных частотах, которые соответствуют разности частот локального осциллятора и частот сигналов, пришедших от Алисы. Спектр сигнала изображен на рисунке **??**

3.9 Определение фазового шума

3.10 Выводы по главе

В данной главе впервые изучено применение двух независимых источников излучения для передачи квантовых состояний света в системе квантового распределения ключей на непрерывных переменных на боковых частотах. Данный подход позволяет распределять сырую последовательность бит в системе КРКБЧ-НП с гетеродинным методом детектирования. Благодаря которому информация об измеренных квантовых состояниях перенеосится на промежуточную частоту, которая лежит в полосе балансного детектора, что значительно упрощает фильтрацию и усиление, так как эта частота находится в радиодиапазоне, где эти операции известны и отработаны. Другим преимуществом является то, что благодаря переносу на промежуточную частоту возможно применять любой вид модуляции будь то фазовая или амлпитудно-фазовая без дополнительных элементов, что существенно улучшает гибкость и характеристики системы относительно гомодинного метода детектирования. Также в этой главе решается проблема контроля поляризации в системах с двумя независимыми источниками излучения и гетеродинным методом детектирования. Данный метод основывается на Быстром Преобразовании Фурье и использовании активного контроллера поляризации для быстрой ее подстройки, что позволит контролировать поляризацию на лету, не ограничивая скорость выработки сырой последовательности.

ГЛАВА 4. Атака оптической накачкой на источник когеретного излучения

Использование технологии квантового распределения ключа дают абсолютную защиту информации от доступа злоумышленника за счет использования метода одноразовых блокнотов для шифрования данных и за счет использования одиночных фотонов в качестве носителей ключа для его передачи через оптические линии связи, применение которых обеспечивает безопастность за счет фундаментальных законов квантовой физики. Однако несовершенство технических компонентов, применяемых в практических реализациях систем КРК, может дать злоумышленнику доступ к секретному ключу за счет внесения изменений в функционирование элементов или, что хуже, полностью контролировать их работу. Поэтому критически необходимо исследовать потенциальное влияние злоумышленника на элементы в составе систем квантового распределения ключа. В данной главе рассматривается новый тип атаки на источник когерентного излучения - атака оптической накачкой.

4.1 Атака оптической накачкой на лазер с распределенной обратной связью

Существующие источники когерентного излучения в системах квантового распределения ключа могут подвергаться воздействию злоумышленника по изменению его характеристик. На это нацелена атака лазерным засеиванием. Суть которого заключается в том, что Злоумышленник (Ева) вводит свое излучение в резонатор лазера с распределенной обратной связью, используемый Алисой для передачи квантовых состояний. В результате этого воздействия, изменяется выходная мощность излучения, форма и площадь импульса. При этом воздействие возможно даже изменение длины волны. Эти эффекты могут быть использованы Евой для получения информации о ключе. Данная атака задей-

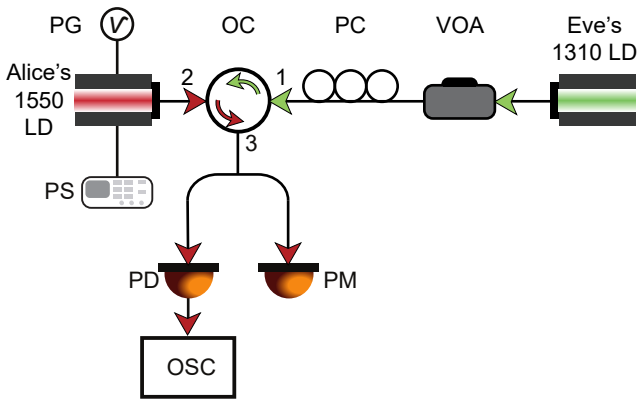

Рисунок 4.1 — Экспериментальная установка по проведению атаки оптической накачкой на источник когерентного излучения из состава системы кванотового распределения ключа. Alice's LD - лазерный диод Алисы, PG - генератор импульсов, PS - источник напряжения, OC - оптический циркулятор, PC - контроллер поляризации, VOA - перестраиваемый оптический аттенюатор, Eve's LD - лазер Евы, PM - измеритель мощности, PD - фотодиод, Osc - осциллограф.

ствует механизм оптической инжекции, рассмотренный ранее, используя длину волны лазера, близкую к рабочей длине волны лазера Алисы.

Однако существующие уявзимости в пассивных оптических компонентах, используемых для защиты от других типов атак, позволяют Еве использовать другие длины волн для проведения своих манипуляций по изменению характеристик излучения. Для этих целей может быть использовано излучение на длине волны 1310 нм. Данная глава посвещена проведению атаки оптической накачкой на полупроводниковый лазер с распределенной обратной связью, работающим в режиме переключения усиления. Измерялись параметры выходного излучения, его мощность, ватт-амперная характеристика. Изучается влияение оптической накачки на длине волны 1310 нм на форму и площадь импульсов. Схема эксперимента представлена на 4.1. Данная схема работает следующим образом. На лазер Алисы (LD1550, Agilecom WSLS-934010C4124-82) подается ток смещения с помощью лабораторного блока питания. Величина тока накачки должна не превышать порогового значения. После этого подаются импульсы с генератора импульсов для работы лазерного диода в режиме переключения генерации. Выход лазерного диода подключен ко 2 выходу оптического циркулятора с сохранением поляризации. В первый же вход циркулятора подается

излучение от лазера Евы. Ее лазер также основан на полупроводниковом кристалле с распределенной обратной связью, однако его рабочая длина волны составляет 1310 нм, когда лазер Алисы работает на длине волны 1550 нм. Непрерывное излучение от лазера Евы попадает на переменный оптический аттенюатор (OZ Optics, BB-100) для изменения выходной мощности лазера без изменения тока накачки, увеличение или уменьшение которого приводит к изменению длины волны лазера, что является критичным изменением для воспроизводимости эксперимента. После этого излучения попадает на механический контроллер поляризации для согласования оси поляризации выходного излучения с осью поляризации оптического циркулятора и лазера соответственно для максимальной эффективности ввода оптического излучения в резонатор лазера Алисы. Попадая на 1 вход оптического циркулятора, излучение Евы проходит его без изменений и с небольшим затуханием попадает в волоконный вывод лазера Алисы. Распространясь по нему, оно попадает на зеркало кристалла, от которого оно частично отражается, а частично проходит внутрь. Для очистки данных была измерена мощность излучения, отраженного от всех элементов лазера и вычтена из полученных результатов. В результате прошедшее излучение поглощается кристаллом InGaAs и благодаря этому создается дополнительная инверсия населенностей в кристалле, которая повышает выходную мощность лазерного излучения на длине волны 1550 нм. Влияние этого эффекта и рассматривается в данной главе.

4.2 Изменение Ватт-Амперной характеристики лазера с распределенной обратной связью при атаке на других длинах волн

Одной из основных характеристик лазера является его ватт-амперная характеристика. Эта кривая показывает зависимость прироста мощности выходного излучения в зависимости от тока накачки, пропускаемого через кристалл. В рамках данного раздела описывается изменение этой характеристики в зависимости от мощности лазера Евы. Для этого лазер Алисы работал в непрерывном

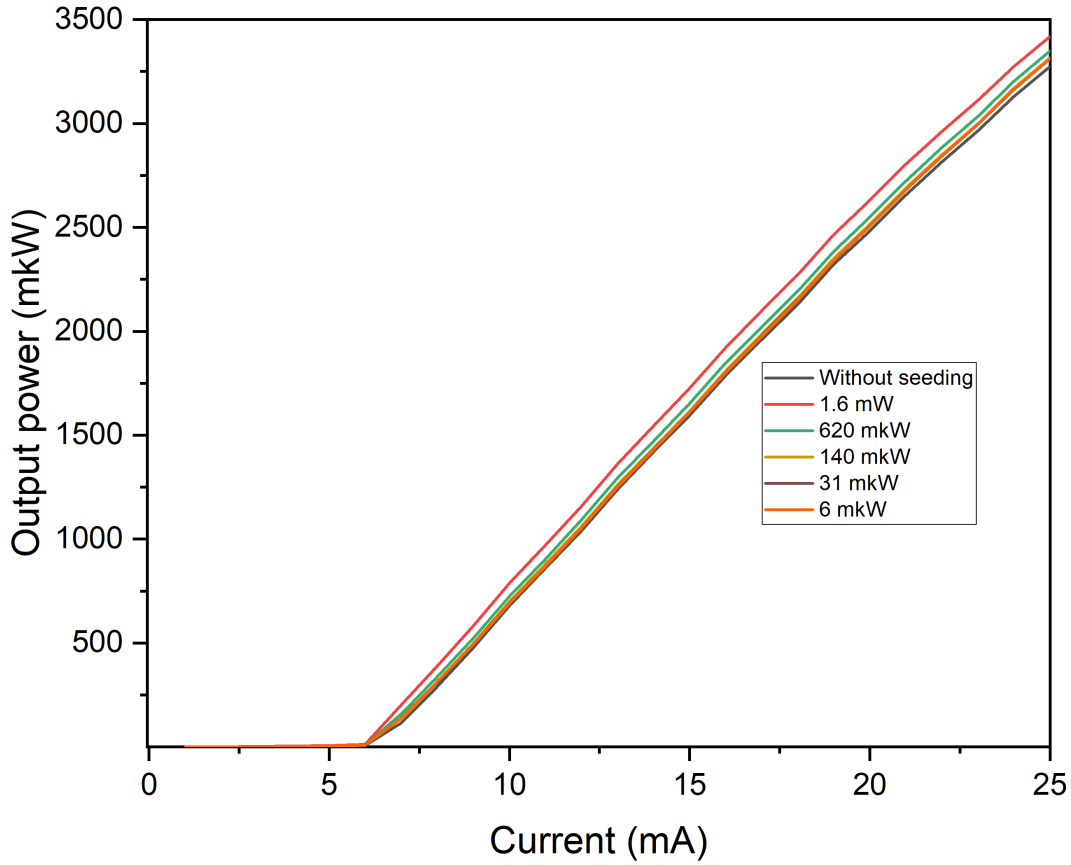

Рисунок 4.2 — Ватт-Амперные характеристики лазера Алисы под действием внешней оптической накачки от Евы.

режиме только с накачкой током от лабороторного блока питания. Мощность контролировалась оптическим измерителем мощности (Thorlabs, PM400). А ток накачки лазера варьировался от 0 до 25 мА. Результат измерения данных характеристик представлен на рисунке 4.2. Данные графики демонстрируют, что дополнительная накачка от Евы в диапазоне мощностей от 1.6 мВт до 31 мкВт сдвигает исходную Ватт-Амперную кривую, что показывает возможность Евы манипулировать мощностью Алисы. Для численной оценки этого влияния необходимо перейти к дифференциальной квантовой эффективностью. Эта величина показывает эффективность преобразования электронного тока в фотоны, излучаемые лазером. Формула расчета величины дифференциальной квантовой эффективности ниже

$$\eta = \frac{2e}{\hbar\omega}\frac{dP}{dI} \tag{4.1}$$

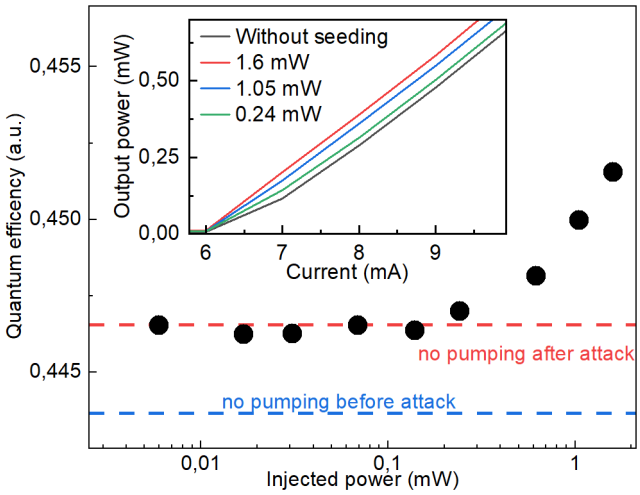

Рисунок 4.3 — График зависимости дифференциальной квантовой эффективности в зависимости от мощности накачки Евы. Красная пунктирная линия обозначает значение дифференциальной квантовой эффективности после проведенной атаки, а синяя пунктирная линия обозначает значение дифференциальной квантовой эффективности до атаки.

, где η - дифференциальная квантовая эффективность, e - заряд электрона, $\hbar$ - приведенная постоянная Планка, ω - частота лазера, dP/dI - аппроксимированное значение производной измеренных Ватт-Амперных характеристик. В результате этих вычислений показано на рисунке 4.3, что Ева, используя оптическую накачку на 1310 нм, изменяет дифференциальную квантовую характеристику лазера Алисы. В результате аппроксимации наклона ватт-амперных характерстик и рассчета дифференциальной квантовой эффективности (ДКЭ) по формуле 4.1 было показано, что Ева может увеличивать ДКЭ на несколько процентов, что негативно сказывается на скорости выработки секретного ключа и этот эффект должен быть учтен.

4.3 Изменение формы импульса при атаке на лазер с распределенной обратной связью, работающем в режиме переключения усиления

Для измерения влияния оптической накачки на форму и энергию импульсов, сгенерированных Алисой, необходимо использовать лазер Алисы в импульсном режиме. Для этого атакуемый лазер был переведен в режим работы

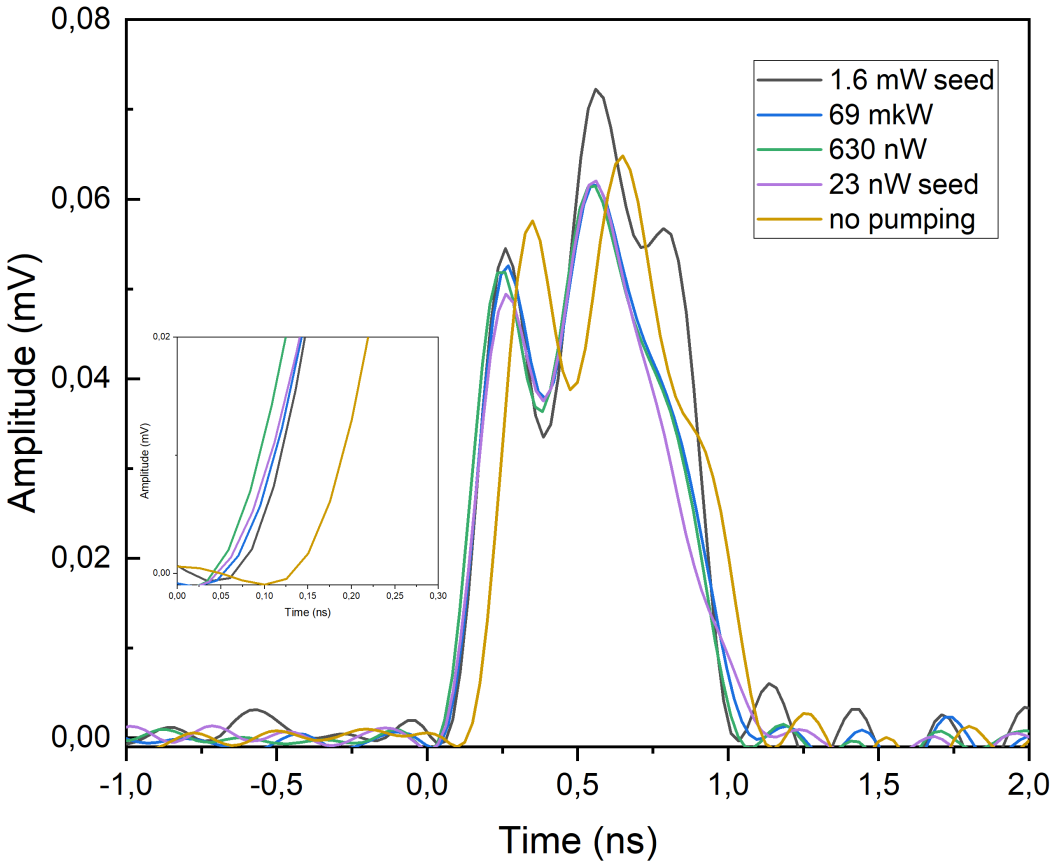

Рисунок 4.4 — Формы импульсов, сгенерированных Алисой, под действием оптической накачки и без нее.

переключения усиления для генерации импульсов. Ток накачки составил 3 мА. Импульсы же генерировались генератором импульсов (P400, Highland Technology). Полученные импульсы регистрировались опто-электронным конвертором (PDI35-10G, Laserscom) и оцифровывалось осциллографом 735Zi, Lecroy, с полосой пропускания 3.5 GHz, скорость оцифровки 40 GS/s. Для синхронизации на осциллограф был дополнительно выведен электрический сигнал с генератора импульсов для запуска развертки и точного измерения времени прихода импульсов. Частота повторения этих импульсов составляла 10 MHz и длительность импульса составляла 700 ps. Результат измерения этих импульсов представлен на рисунке 4.4. Как видно из рисунка 4.4, дополнительная накачка Евы не только увеличивает выходную энергию импульсов, а также сдвигает их время генерации на величину приблизительно равной 100 пс. Для

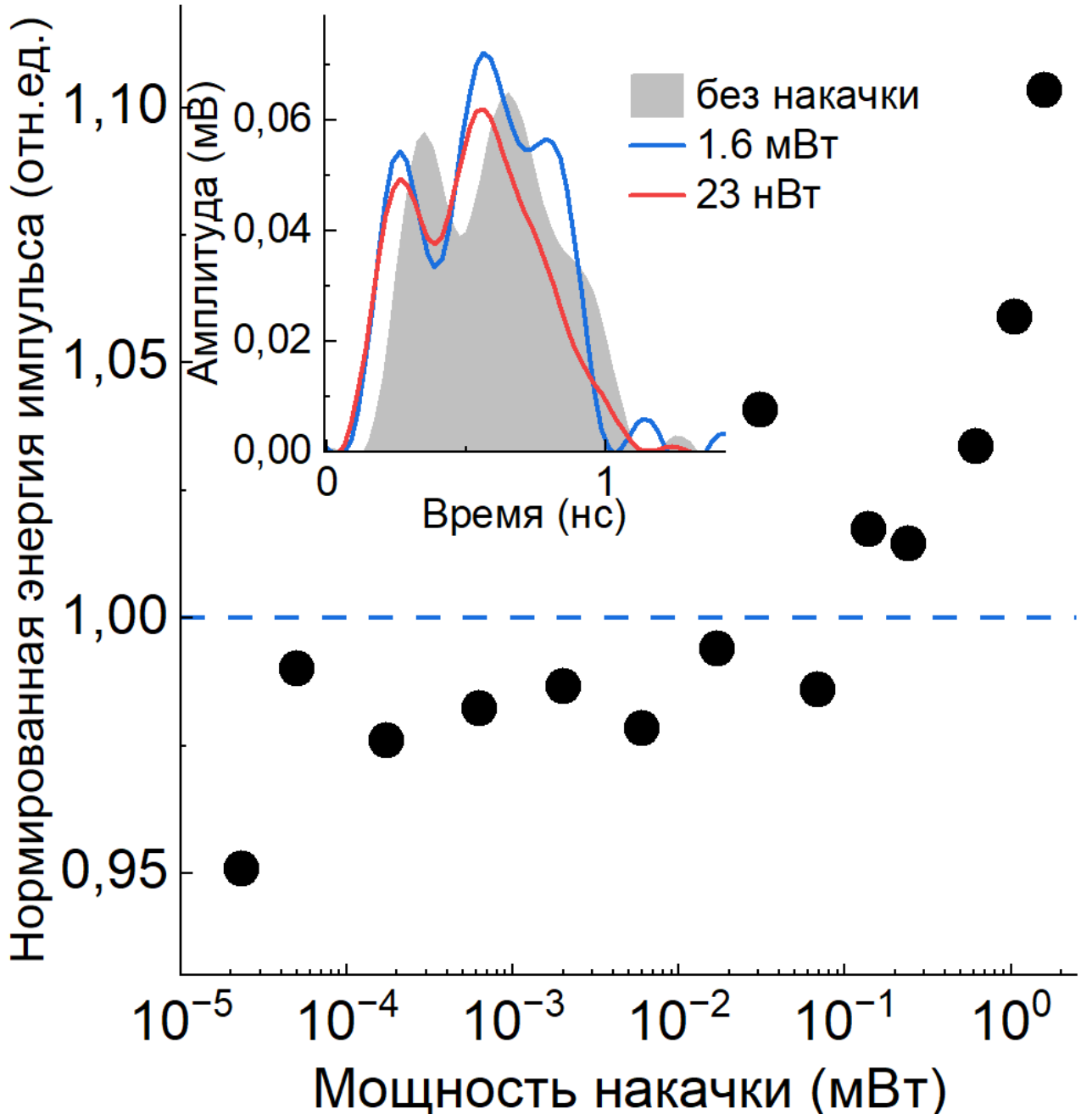

Рисунок 4.5 — Caption

оценки влияния оптической накачки на площадь импульсов, исследуемые импульсы были оцифрованы и их площадь была проинтегрирована в программной среде Origin. Результаты этого интегрирования представлены на рисунке 4.5. Проведенные измерения показывают, что воздействие Евы изменяет не только дифференциальную квантовую эффективность, но и энергию импульсов, излучаемой Алисой, что позволяет также снижать дальность и скорость выработки секретного ключа. В результате воздействия энергия импульсов не только может увеличиться на 10 процентов, но даже может уменьшится при некоторых

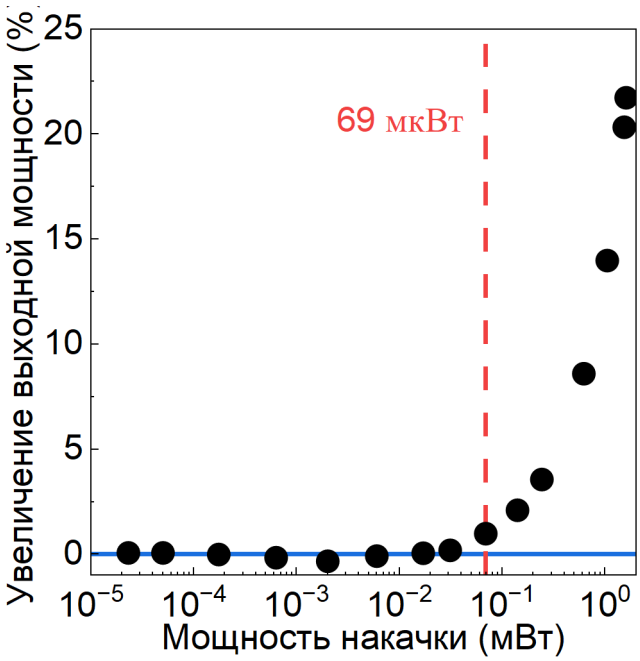

Рисунок 4.6 — Изменение средней мощности лазера Алисы под действием оптической накачки Евы.

мощностях оптического излучения накачки.

Для полной картины изменения мощности, излучаемой Алисой под действием оптической накачки злоумышленника, необходимо оценить еще и средний уровень мощности. Для этого используется лазер, работающий в импульсном режиме, как и описано выше, однако мощность измеряется с помощью измерителя оптической мощности (ИОМ). Скорость работы данного ИОМ не позволяет измерить мощность каждого импульса, поэтому он интегрирует всю мощность и импульсную, и непрерывную. Результат измерения показан на рисунке 4.6 В результате воздействия Евы, мощность лазера с распределенной обратной связью увеличивается на 20%, когда как значение энергии импульсов повышается только на 10%. Что объясняется тем, что Ева также повышает и непрерывное излучение из лазера Алисы.

4.4 Определение минимально необходимой изоляции лазерного источника для предотвращения атаки оптической накачкой

В качестве исходной мощности, которая необходима для создания заметного эффекта, определенная ранее в этом разлеле составляет 70 мкВт или -11.6 дБм. Существующие на рынке решения предлагают лазеры, способные выдавать 14 Вт или 41.46 дБм мощности на длине волны 1310 нм. Для определения изоляции необходимо вычесть из мощности лазера минимально необходимую мощность для создания эффекта по формуле 4.2.

$$\alpha_{iso} = P_{laser} - P_{req} \tag{4.2}$$

В результате вычислений величина изоляции, необходимая для предотвращения атаки оптической накачкой составляет 53 дБ.

4.5 Оценка возможности проведения атаки на существующие системы квантового распределения ключей

Современные системы квантового распределения ключей содержат в себе элементы, предназначенные для защиты от различных атак на техническую реализацию. К таким элементам относятся различные пассивные фильтры и изоляторы. Однако некоторые защитные элементы могут вести себя непредсказуемо для разных длин волн. Эти особенности позволюят злоумышленнику их использовать для получения информации о ключе. Ярким примером могут служить DWDM (Dense Wavelength Division Multiplexion) фильтры и оптические изоляторы. Их заявленные характеристики соблюдаются только в относительно небольшом диапазоне длин волн. С изменением зондирующей длиной волны изменяется и величина изоляции, вносимой элементом. Пример этого эффекта отображен на рисунке 4.7 Как видно из рисунка 4.7, представленные элементы не вносят существенной изоляции как на рабочей длине волны. К прмиеру,

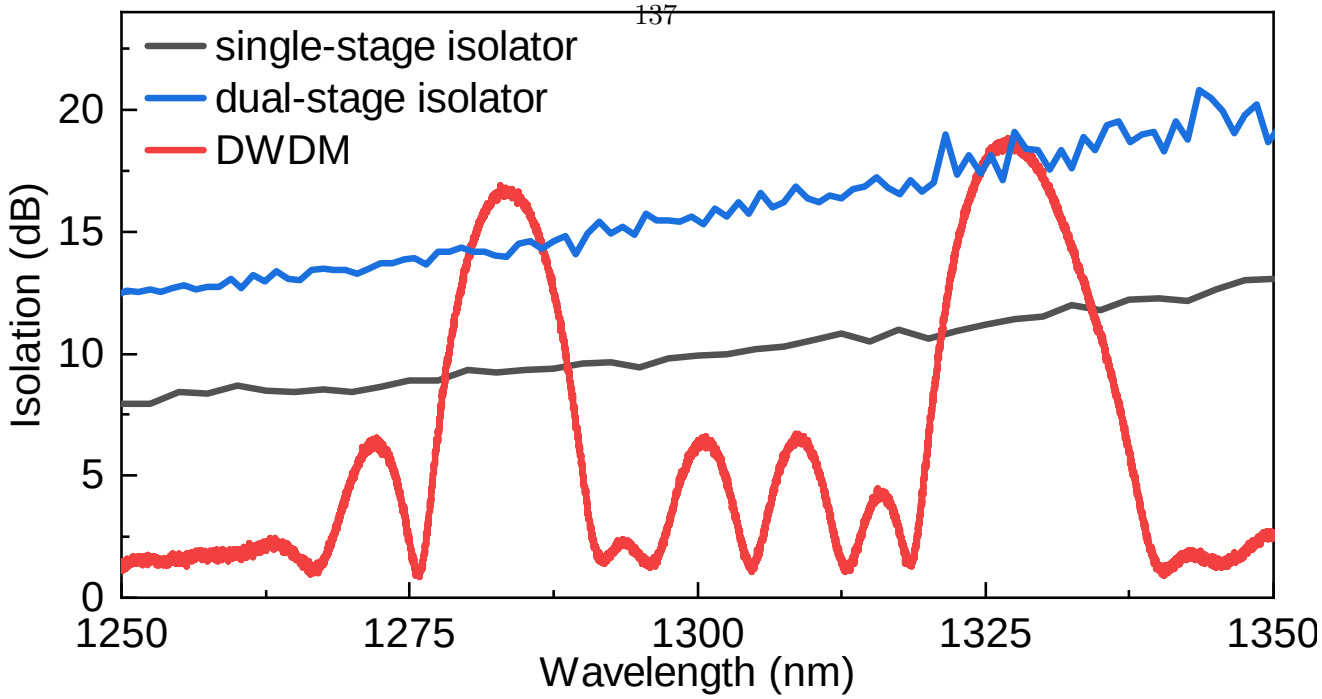

Рисунок 4.7 — Величина изоляции пассивных элементов, используемых в системах КРК. Красным цветом обозначен спектр изоляции DWDM фильра, серым - одностадийного изолятора, синим - двухстадийного изолятора

изоляция одностадийного изолятора на длине волны 1550 нм составляет 30 дБ, а двухстадийного - 40 дБ. Однако на длине волне 1310 нм эти величины составляют 8 и 12.5 дБ соответственно. Когда DWDM фильтр на длине волны 1310 нм вносит 5 дБ, в то время как на длине волны 1550 нм вносит 30 дБ потерь. Таким образом видно, что пассивные элементы не вносят заявленной изоляции и эта лазейка может быть использован злоумышленником. В качестве схемы КРК будет использоваться схема из работы [15]. Для расчета необходимой минимальной зондирующей мощности необходимо просуммировать все потери, вносимые элементами на длине волны 1310 нм. Измеренные значения потерь элементов продемонстрировано в таблице 4.5

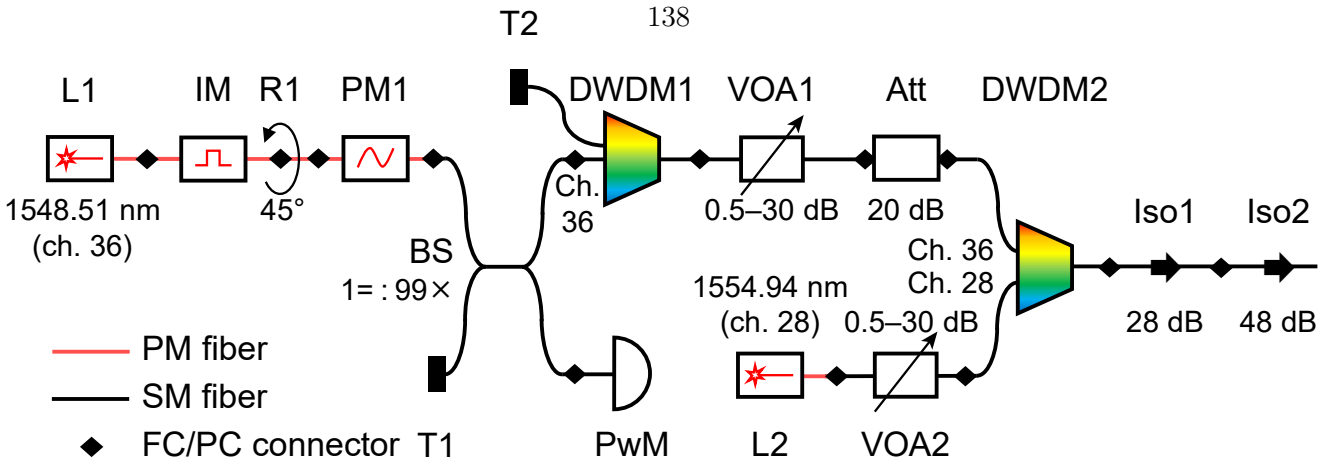

Рисунок 4.8 — *
Оптическая схема блока Алиса

Вычисления производятся по формуле

Элемент	Потери, дБ
Встроенный изолятор в лазере	10.5
Изолятор 1	10.56
Изолятор 2	16.24
Фиксированный аттенюатор	19.6
Переменный аттенюатор	0.5
Светоделитель	23.98
DWDM1	4.08
DWDM2	3.03
Фазовый модулятор	4.5
Модулятор интенсивности	4.5

$$\alpha_{1310} = \alpha_{\text{Iso1}} + \alpha_{\text{Iso2}} + \alpha_{\text{Att}} + \alpha_{\text{VOA1}} + 2\alpha_{\text{DWDM}} + \alpha_{\text{PM}} + \alpha_{\text{IM}} + \alpha_{\text{LD}}, \tag{4.3}$$

где α_{Iso} вносимые потери изолятором на длине волны 1310 нанометров, α_{att}, α_{VOA} , α_{DWMD}, α_{PM}, α_{IM}, и α_{LD} вносимые потери компонентов 4.8. Для определения потерь использовались схожие компоненты как в работе [15]. Раскрывать модели всех элементов не представляется возможным по соображениям конфедициальности. Но эти элементы представляют собой стандартные телекоммуникационные элементы доступные для заказа. Потери на длине вол-

ны 1310 нм фиксированного аттенюатора (Thorlabs FA20T) и светоделителя 99:1 (Thorlabs TW1550R1A2) определены в даташите производителем. Потери фазового модулятора на основе кристалла Ниобата Лития, легированного Титаном, измерялись с помощью лазера, который используется в эксперименте, и измерителем мощности. Потери в модуляторе интенсивности считаем аналогичными. Остальные же элементы измерялись с помощью источника суперконтиниума и оптического анализатора спектра (HP Hewlett Packard 70004A) по методологии, описанной в [15]. Потери на изоляторе, встроенном в лазерный диод, считаем аналогичными одностадийному изолятору в 10 дБ. В итоге изоляция всей системы, изобраденной на рис. 4.8 составляет 97.55 дБ, что существенно превышает минимальное определенное значение в 53 дБ. Поэтому данная система устойчива к атаке оптической накачкой.

4.6 Экспериментальное подтверждение контрмеры против атаки оптической накачкой

4.7 Выводы по главе

В данной главе рассматривается новый тип атаки на источники лазерного излучения - атака оптической накачкой, на примере накачки на длине волны 1310 нм. Однако, данный эффект наблюдается в широком диапазоне длин волн, обусловленном шириной полосы поглощения полупроводникового кристалла, на котором построен DFB лазер. Изучено влияние на интенсивность излучаемой мощности, определена минимально необходимая мощность для создания заметного эффекта в 70 мкВт. Определена минимально необходимая изоляция для предотвращения атаки оптической накачкой на длине волны 1310 нм и зондирующей мощностью 500 мВт в 53 дБ. Определена стойкость существующей системы квантового распределения ключей к атаке оптической накачкой. Ее суммарная изоляция составлиа 97.55 дБ, что превышает минимальное порого-

вое значение в 53 дБ, что делает данную систему устойчивой к атаке оптической накачкой.

ГЛАВА 5. Исследование источника когерентного излучения на основе оптической инжекции на устойчивость к лазерному засеиванию мощным излучением

5.1 Введение

На данный момент в практических системах квантового распределения ключей в качестве источника одиночных фотонов используется ослабленный лазерный источник. Это открывает для подслушивающего устройства множество возможностей атаковать источник КРК и получить информацию о секретном ключе. Обычно в качестве контрмеры против атак на источник света КРК рекомендуется использовать некоторую степень изоляции. Однако практические оптические компоненты также могут изменять значение изоляции при внешнем воздействии или под влиянием условий окружающей среды. В данной работе продемонстрировано, что источник лазерного излучения на основе лазерной инжекции обладает очень высокой устойчивостью к атакам внешним засевом, и рекомендуется использовать эту схему в качестве безопасного источника фотонов для систем КРК. Квантовое распределение ключей (КРК) позволяет двум сторонам распределять секретный ключ по ненадежному каналу, используя квантово-механические свойства одиночных фотонов. Протоколы КРК в принципе не поддаются взлому. Однако их практическая реализация демонстрирует длинный список побочных каналов, которые могут предоставить подслушивающему лицу дополнительную информацию о секретном ключе и сделать систему, использующую его, небезопасной [15; 16]. Такие побочные каналы почти всегда являются результатом отличия аппаратного обеспечения от его идеальной модели.

Одним из наиболее ярких примеров несовершенных устройств являются практические источники фотонов. На сегодняшний день в практических системах КРК используются сильно ослабленные лазерные импульсы от полупроводниковых лазерных диодов (ЛД), а не истинные однофотонные источ-

ники, поскольку последние пока не позволяют достичь практической скорости передачи ключей [17]. Однако, поскольку полупроводниковые лазеры очень чувствительны ко внешним воздействиям, существует несколько атак с лазерной заливкой, которые открывают лазейки для подслушивающих [18–20]. Например, предыдущие экспериментальные исследования показали, что мощности инжекции в диапазоне 100 - 160 нВт может быть достаточно для управления интенсивностью импульсов Алисы [18;19], а мощности даже около 1 нВт может быть достаточно для частичного управления фазой импульсов Алисы [20].

В этой работе обращается внимание на то, что описанные выше атаки с лазерным засевом относятся к источнику света, основанному на одном лазерном диоде с усилением. В то же время, ЛД источники с оптической инжекцией стали широко использоваться в квантовой криптографии, особенно в реализациях квантового распределения ключей, не зависящих от измерительных приборов (MDI КРК) [21; 22].

Схема с оптической инжекцией незаменима для приложений, требующих высокой видности интерференции между независимыми лазерными источниками. Техника инжекции света значительно улучшает интерференцию за счет низкого джиттера времени импульса и синхронизации частотных чирпов при сохранении случайности фазы излучаемых лазерных импульсов [23]. Более того, последние исследования показывают, что лазерный источник с оптической инжекцией позволяет уменьшить флуктуации интенсивности и тем самым увеличить безопасную скорость передачи ключей при реализации техники состояний-ловушек [24].

К сожалению, конфигурация источника с инжекционной блокировкой ранее не тестировалась на устойчивость к атакам с лазерным посевом. В этой работе мы впервые исследуем ее оптические характеристики при внешней лазерной атаке и проводим анализ защищенности при наличии изменений выходного сигнала. В работе показано, что конфигурация источника фотонов с внутренним засевом является эффективной контрмерой против известных атак на источник фотонов КРК. Между тем, наше исследование демонстрирует и другие эффекты, которые могут иметь место только в исследуемой конфигурации ис-

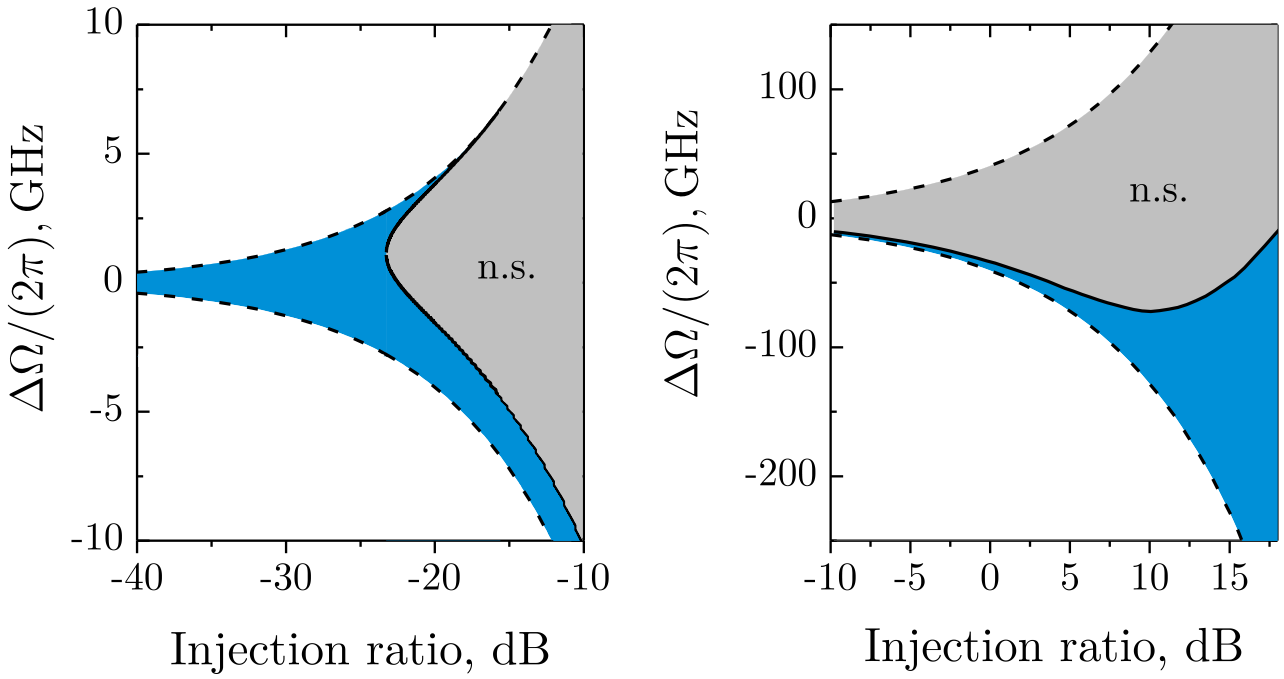

Рисунок 5.1 — Карта фазовой синхронизации двух лазеров(область стабильной синхронизации обозначена синим).

точника. В частности, ведомый лазер действует как ненасыщенный оптический усилитель. Это приводит к независимому усилению сигналов ведущего и Евы и позволяет злоумышленнику извлечь дополнительную информацию о секретном ключе

5.2 Теоретическое описание метода оптической синхронизации

5.2.1 Полупроводниковые источники света с инжекционной синхронизацией

Фазовая синхронизация с помощью оптической инжекции - это метод оптической частотной и фазовой синхронизации, основанный на освещении лазерного резонатора внешним светом. Источник с оптической инжекцией содержит "ве-

Таблица 1 — Параметры лазера для создания оптической инжекции

Параметр	Значение	Параметр	Значение
N_{th}	5.5×10^7	N_{tr}	5.0×10^7
τ_e	$1\ ns$	τ_{ph}	$1\ ps$
C_{sp}	10^{-5}	Γ	0.12
α	5	κ_{inj}	$5.0 \times 10^{10} ns^{-1}$
I	$22\ mA$	γ_Q	0

дущий"лазер, который обеспечивает внешнее излучение для воздействия на "ведомый"лазер [25].

В зависимости от интенсивностей и спектральных показателей ведущего и ведомого ЛД, источник может обеспечивать режим свободной генерации, стабильной или нестабильной синхронизации [26]. Эти режимы определяются как области диаграммы с коэффициентом инжекции и частотной подстройкой в виде координат, как показано на рис. 5.1. Частота перестройки - это разность между частотами ведущего и свободно работающего ведомого каналов. Коэффициент инжекции R_I определяется как

$$R_I = -10 \times \lg\left(\frac{Q_c^M}{Q_c}\right), \tag{5.1}$$

где Q_c^M и Q_c значения интенсивности ведущего и ведомого лазеров в режиме свободной генерации в установившемся режиме, соответственно. Отметим также, что в импульсном режиме работы ЛД интенсивности Q_c^M и Q_c определяются пиковыми мощностями импульсов как

$$Q = \frac{< P >}{f_R \times \tau_P}, \tag{5.2}$$

где $< P >$ - средняя мощность в Ваттах, f_R - частота повторения импульсов, Гц, и τ_P - длительность импульса, с. Когда источник работает в режиме стабильной синхронизации, ведомый лазер будет вынужден синхронизироваться с ведущим, то есть излучать на той же частоте. В целом, согласно карте синхронизации на рисунке 5.1, диапазон синхронизации частоты становится больше с увеличением коэффициента инжекции [27]. Между тем, в практических источниках света для систем КРК коэффициент инжекции отрицательный. Низкий

коэффициент инжекции обусловлен двумя факторами. Во-первых, излучение ведущего не полностью заходит в резонатор ведомого. А второй фактор связан с длительностью импульса в соответствии с ф-л. 5.2. Широко используемый случай реализации оптической схемы предполагает длительность импульса ведомого лазера в несколько раз меньше, чем у ведущего ЛД (в два раза и больше). Это позволяет избежать высокоамплитудных релаксационных осцилляций в выходных импульсах за счет засева ведомого лазера только частью импульса без частотного чирпа по интенсивности ведущего. В итоге, для получения высокой стабильности интенсивности исследуемых источников ведущий и свободно работающий ведомый ЛД должны иметь как можно более близкую рабочую длину волны.

5.2.2 Статистика интерференции фазово-рандомизированного классического света

Статистические свойства интерференционного сигнала фазово-рандомизированного классического света хорошо изучены и имеют строгие модели, учитывающие все характеристики импульсов [28; 29]. Недавно они были разработаны для реализации высококачественных квантовых генераторов случайных сигналов, основанных на интерференции фазово-рандомизированных импульсов. Благодаря этому, используя функцию плотности вероятности интерференционного сигнала, можно дать оценку видимости интерференции, объяснить влияние на нее свойств импульса и, наконец, что очень важно, настроить источник света так, чтобы получить наибольшую видимость интерференции. Поэтому в наших экспериментах мы не измеряем двухфотонную интерференцию, а измеряем и анализируем функцию плотности вероятности интерференции классического света.

Процедура состоит в следующем. Она включает в себя реализацию несимметричного интерферометра с линией задержки, обеспечивающей время задержки, кратное периоду повторения импульсов. Это приводит к интерференции меж-

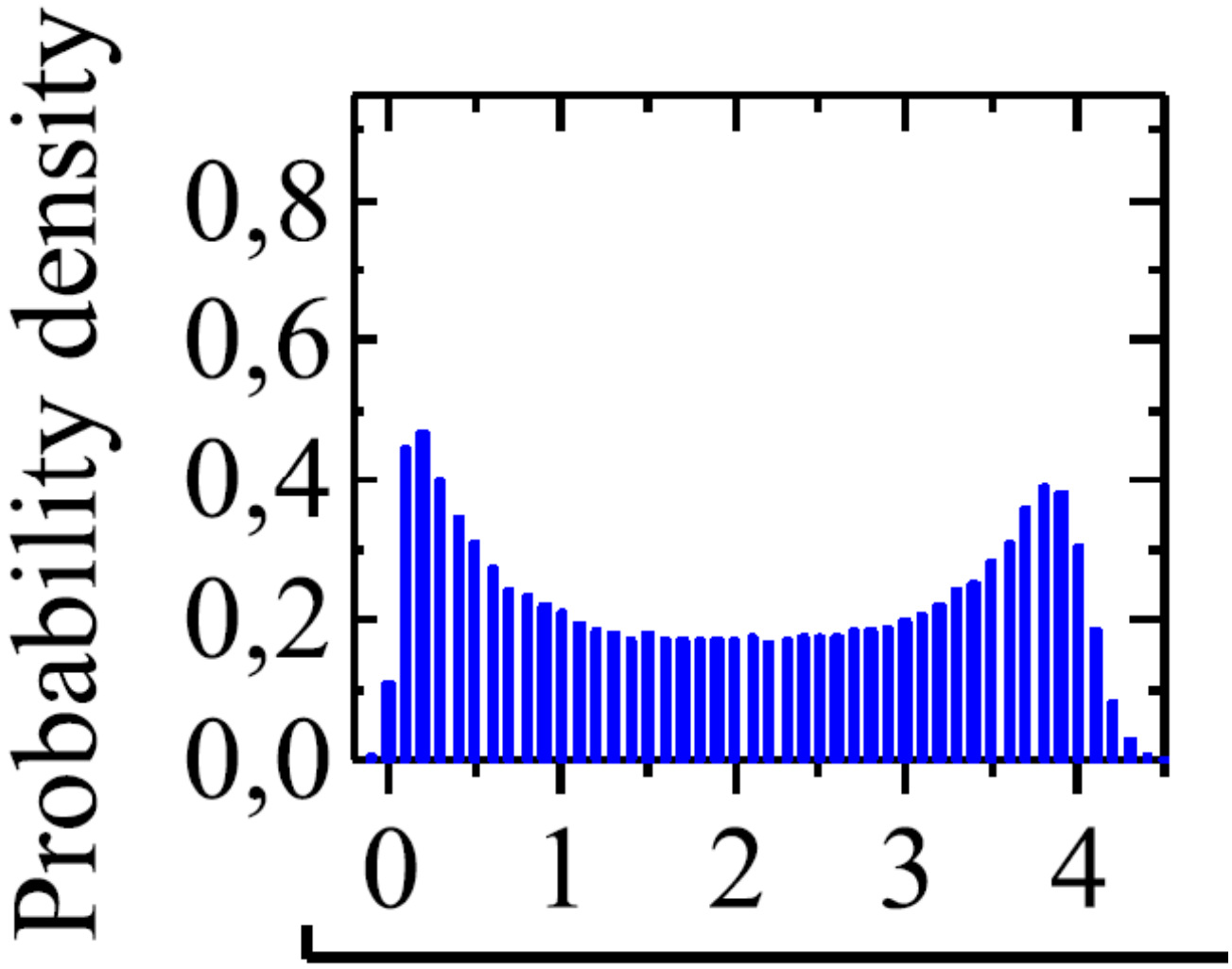

Рисунок 5.2 — Нормализованная функция плотности распределения интерференции колоколообразных импульсов без чирпа [29].

ду импульсами, испускаемыми в разное время. Далее с помощью осциллографа накапливается большая выборка измерений площади интерференционного сигнала и строится гистограмма зависимости числа импульсов от их площади.

В работе [29], авторы показали, что безщелевой колоколообразный лазерный импульс будет иметь двухпиковую форму PDF, где пики будут располагаться на интенсивности конструктивной и деструктивной интерференции, как показано на рис. 5.2. Чтобы сравнить функции плотности распределения (ФПР) друг с другом, введем экспериментальную видимость интерференции

$$\eta = \frac{S_{max} - S_{min}}{4\sqrt{s_1 s_2}}, \tag{5.3}$$

где S_{max} и S_{min} - нормированные интенсивности конструктивной и деструктивной интерференции, определяемые по максимальным экспериментальным вероятностям, s_1 и s_2 - интенсивности начальных импульсов, которые принимаются равными 1.

5.3 Проведение эксперимента

На риснуке Рисунок 5.3 показана экспериментальная установка. Она включает в себя три основные части. Это источник света Алисы, атакующий лазер злоумышленника и измерительное оборудование.

5.3.1 Источник света на испытаниях

В этой работе реализован оптический источник излучения с оптической инжекцией. Его оптическая схема обозначена как Alice в рис. 5.3. Ведущий лазер излучает импульсы со случайной фазой. Они поступают в ведомый лазер через волоконно-оптический циркулятор PMCIR1 (PMCIR-3-A-1550-900-5-08-FA, Optel) из порта 1 в порт 2 и “засевают” ведомый лазер. Далее импульсы от ведомого ЛД передаются из порта 2 циркулятора на выход Алисы - порт 3 циркулятора.

В качестве источника мы использовали пару идентичных волоконно-оптических DFB лазерных диодов с выходным волокном сохраняющим поляризацию (Agilecom, WSLS-934010C4124). Они отличаются только наличием встроенного изолятора. У ведущего лазера он есть, а у ведомого - нет. Чтобы избежать нежелательной обратной связи в ведущем лазере с ведомым, ведущий ЛД дополнительно защищен с помощью внешнего волоконно-оптического изолятора (с изоляцией около 60 дБ, не показан в рис. 5.3). Отметим, что PMCIR1 также обеспечивает изоляцию порта 2 от порта 1 более чем на 40 дБ. В сумме, с

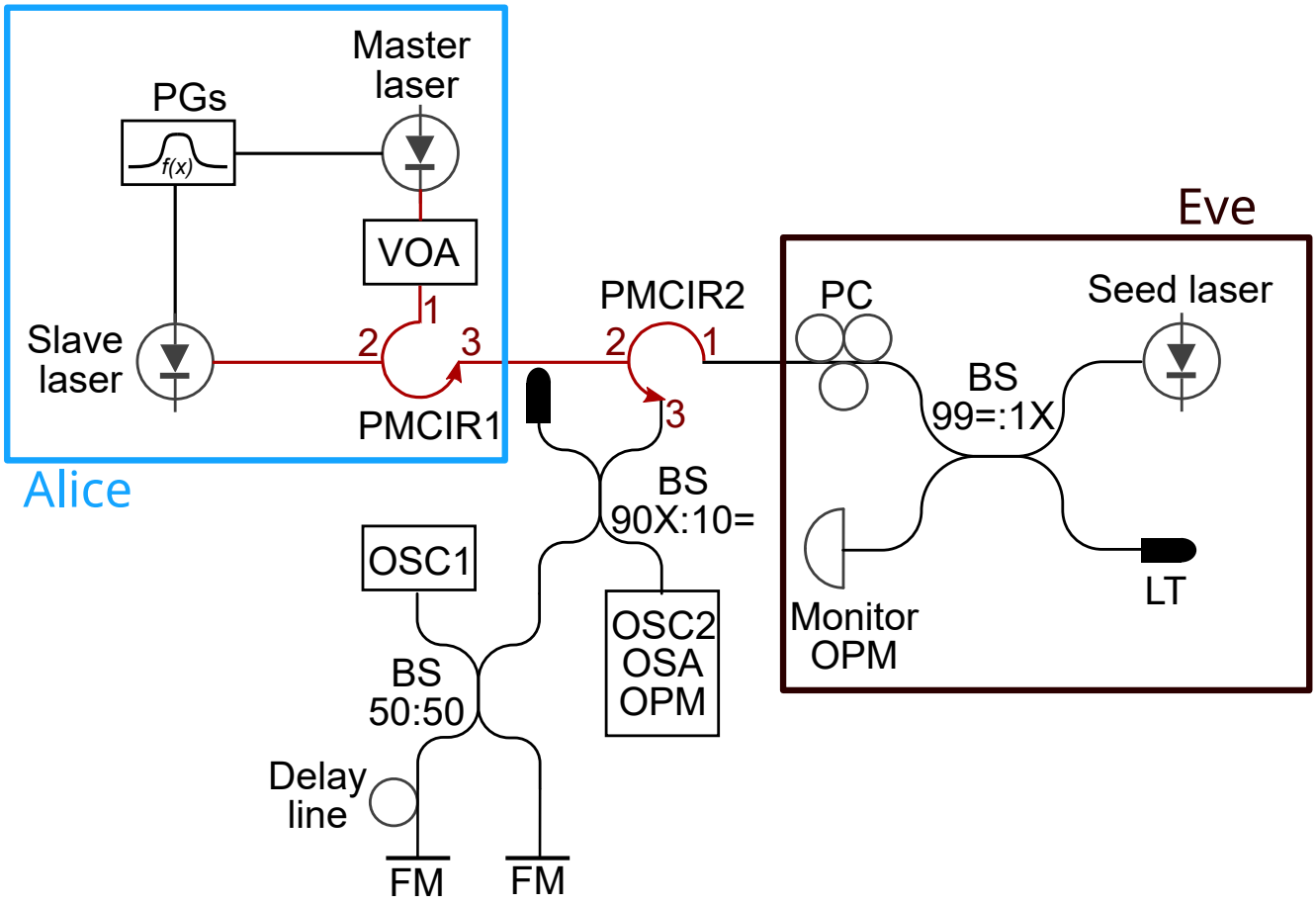

Рисунок 5.3 — Экспериментальная установка (PM-волокна выделены красным цветом): VOA - перестраиваемый оптический аттенюатор, BS - светоделитель, PMCIR - циркулятор с сохранением поляризации, PMBS - светоделитель с сохранением поляризации, PG - генератор импульсов, OPM - измеритель оптической мощности, OSC - осциллограф, OSA - оптический анализатор спектра, BS - светоделитель, LT - световая ловушка, FM - зеркало Фарадея. Коэффициент связи светоделителя (BS) обозначается 99 =: 1× означает, что 99% света проходит в порт, горизонтально противоположный графическому обозначению СД, в то время как 1% света свет попадает в другой порт

.

учетом типичной изоляции встроенного изолятора около 30 дБ, ведущий лазер изолирован от ведомого лазера более чем на 130 дБ.

На лазерные диоды подается ток смещения от лабораторного источника питания (E3648A, Keysight) с напряжением смещения около 1.2-1.4 В и током 2-4 мА. Для получения оптических импульсов с частотой повторения 10.035 МГц ведущий и ведомый лазерные диоды управляются по отдельности двумя цифровыми генераторами задержки и импульсов (P400, Highland Technology). Электрические импульсы подаются в виде прямоугольников с амплитудой - 5 В и длительностью 2.7 нс и 1.9 нс для управления ведущим и ведомым лазерами, соответственно. Для идеальной формы импульса время прихода ведущего импульса на ведомый диод должно быть немного раньше, чем электрический импульс привода ведомого. Такое согласование времени было достигнуто точной настройкой времени задержки между ГС с разрешением задержки 1 пс. Время задержки для ведомого лазера составило 7.6 нс

Согласование спектральных характеристик ведущего и ведомого лазеров достигается путем температурной подстройки ЛД с помощью встроенных термоэлектрических элементов. Фактическая частота отстройки, определяемая как разница между пиковыми частотами ведущего и свободно работающего ведомого, составляет менее 6 ГГц. На рисунках 5.3.1 и 5.3.1 показаны спектральные характеристики и огибающую импульса ведущего ЛД, свободно работающего ведомого ЛД (без сигнала от ведущего ЛД) и всего источника света (ведомый ЛД, засеянный ведущим ЛД) после настройки.

Максимальная средняя мощность ведущего лазера на входе в ведомый ЛД составляет 11 мкВт. Чтобы избежать изменения спектральных характеристик при изменении мощности ведущего лазера, она изменяется с помощью микроэлектромеханического переменного оптического аттенюатора VOA (V1550PA, Thorlabs). Управляющее напряжение VOA от 0 до 5 В контролирует затухание, которое может быть увеличено до 25 дБ с помощью напряжения.

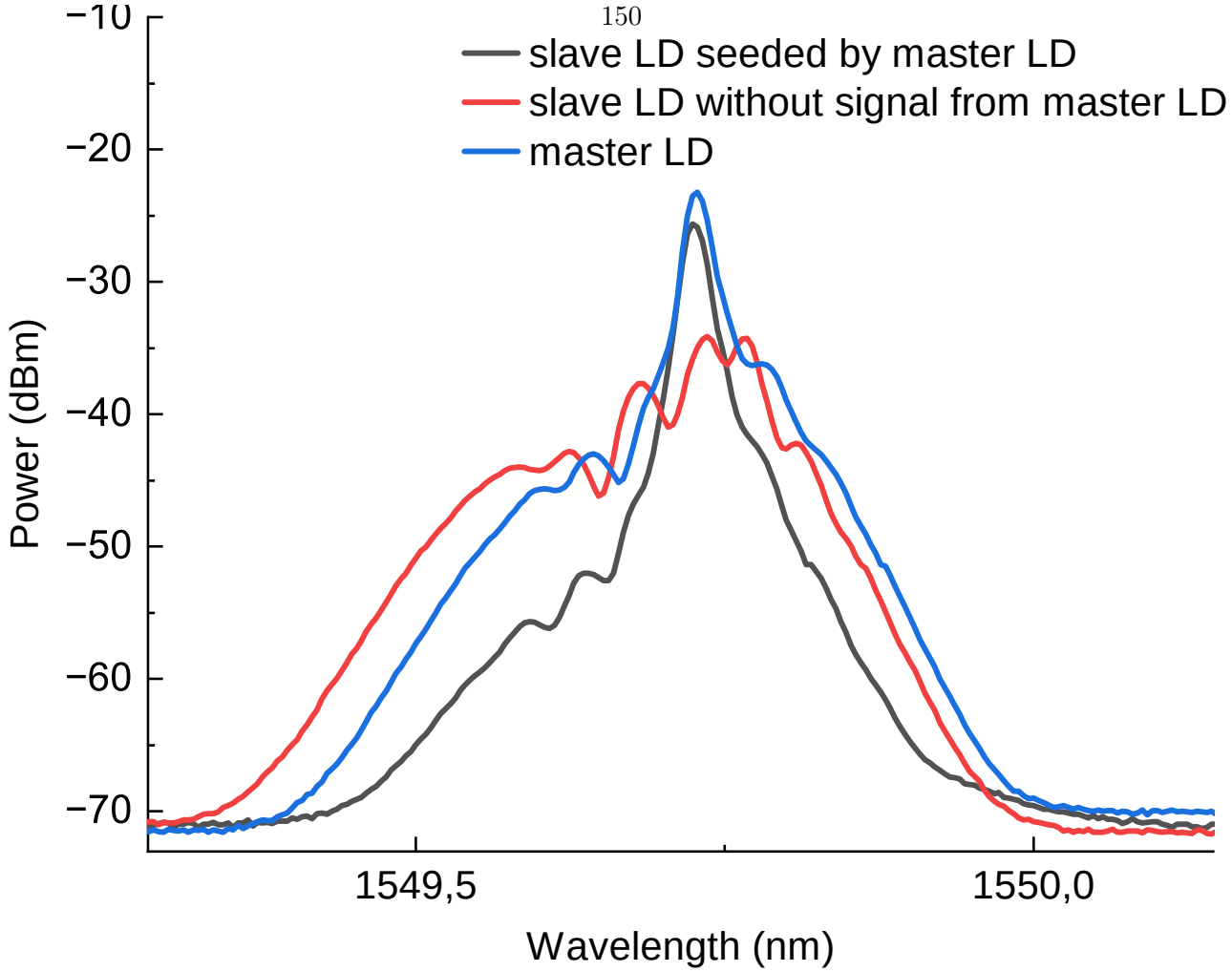

Рисунок 5.4 — Спектры лазерных диодов ведущего, ведомого и источника излучения для КРК

5.3.2 Экспериментальная установка

Наша экспериментальная установка моделирует сценарий, в котором Ева атакует источник QKD из квантового канала. Из-за наличия волоконно-оптического циркулятора в схеме источника Алисы, свет злоумышленника может воздействовать только на ведомый лазер; типичная конструкция волоконно-оптического циркулятора не позволяет свету передаваться от порта 3 циркулятора к порту 1.

В качестве начального лазера злоумышленника мы использовали лазерный диод с распределенной обратной связью (Gooch and Housego AA1406), усиленный волоконным усилителем на основе легированного эрбием и иттер-

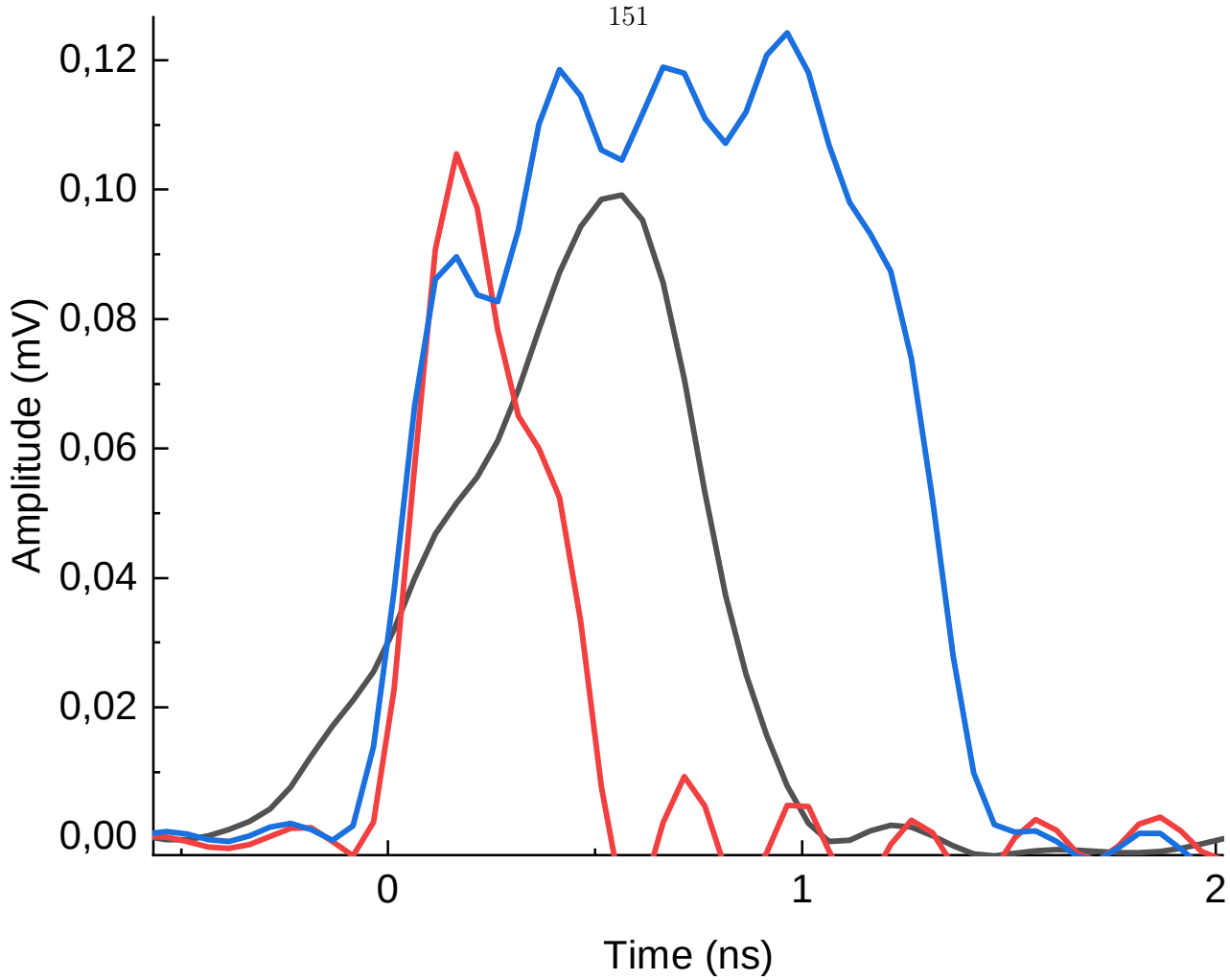

Рисунок 5.5 — Формы импульсов лазеров мастера, слейва и источника излучения КРК

бием волокна (EDFA, заказной блок QGLex) [30]. Он работает в непрерывной генерации на рабочей длине волны в диапазоне от 1548.6 до 1550.6 нм. Применяемая в экспериментах мощность составляет около 500 мВт, поскольку дальнейшее увеличение мощности приводит к изменению вносимых потерь и изоляции циркулятора Алисы PMCIR1. Установка Евы также оснащена делителем луча 99:1 и мониторным измерителем оптической мощности, позволяющим измерять мощность Eve в режиме онлайн. Механический регулятор поляризации установлен для достижения минимальных потерь для света злоумышленника в установке. Свет злоумышленника поступает в источник Алисы через сохраняющий поляризацию волоконно-оптический циркулятор PMCIR2 (PMCIR-3-A-1550-900-5-08-FA, Optel). Далее, прежде чем попасть на целевой ведомый лазер, он проходит в обратном направлении циркулятора Алисы

PMCIR1, что обеспечивает изоляцию для света злоумышленника примерно в 46-51 дБ . В результате мощность атакующего лазера, достигающая ведомого лазера Алисы, составляет около 1.8 мкВт .

Конфигурация измерений позволяет контролировать среднюю мощность, спектральные, амплитудно-временные характеристики импульсов и интерференцию следующих друг за другом импульсов. Средняя мощность измеряется с помощью оптического измерителя мощности OPM (S154C, Thorlabs). Выходные спектры измеряются оптическим анализатором спектра OSA (AQ6370D, Yokogawa) со спектральным разрешением 0.02 нм. Амплитуда, длительность импульсов, их стабильность и интерференционные сигналы измеряются осциллографами OSC1 и OSC2 (735Zi, Lecroy, полоса пропускания 3.5 ГГц) и p-i-n фотодиодами (PDI35-10G, Thorlabs) с полосой пропускания 10 ГГц. Для анализа статистических распределений амплитуды и длительности оптических импульсов для каждого измерения накапливается 30 тыс. выборок и строится стандартное отклонение. Затем из средних значений амплитуды и длительности и их стандартных отклонений рассчитываются энергия импульса и его стабильность соответственно.

В наших экспериментах мы анализируем качество импульсов, основываясь на форме функции плотности вероятности интерференционного сигнала, как это описано в разд. 5.2. Чтобы обеспечить интерференцию между следующими друг за другом импульсами, мы реализуем полностью волоконный интерферометр Майкельсона на зеркалах Фарадея и с линией задержки длиной около 10 метров. Затем, 20 тысяч измерений площади интерференционного сигнала накапливаются в фиксированном временном интервале (синхронизированном с электрическими импульсами ЛД) для построения гистограммы с помощью встроенного осциллографа.

Во-первых, мы полностью охарактеризовали источник КРК для различных мощностей ведущего ЛД и экспериментально определили границы мощности ведущего ЛД, необходимые для стабильной оптической инжекции. Далее мы провели серию экспериментов по внешней лазерной атаке на Алису и получили зависимости всех характеристик КРК-источника от средней мощности ведуще-

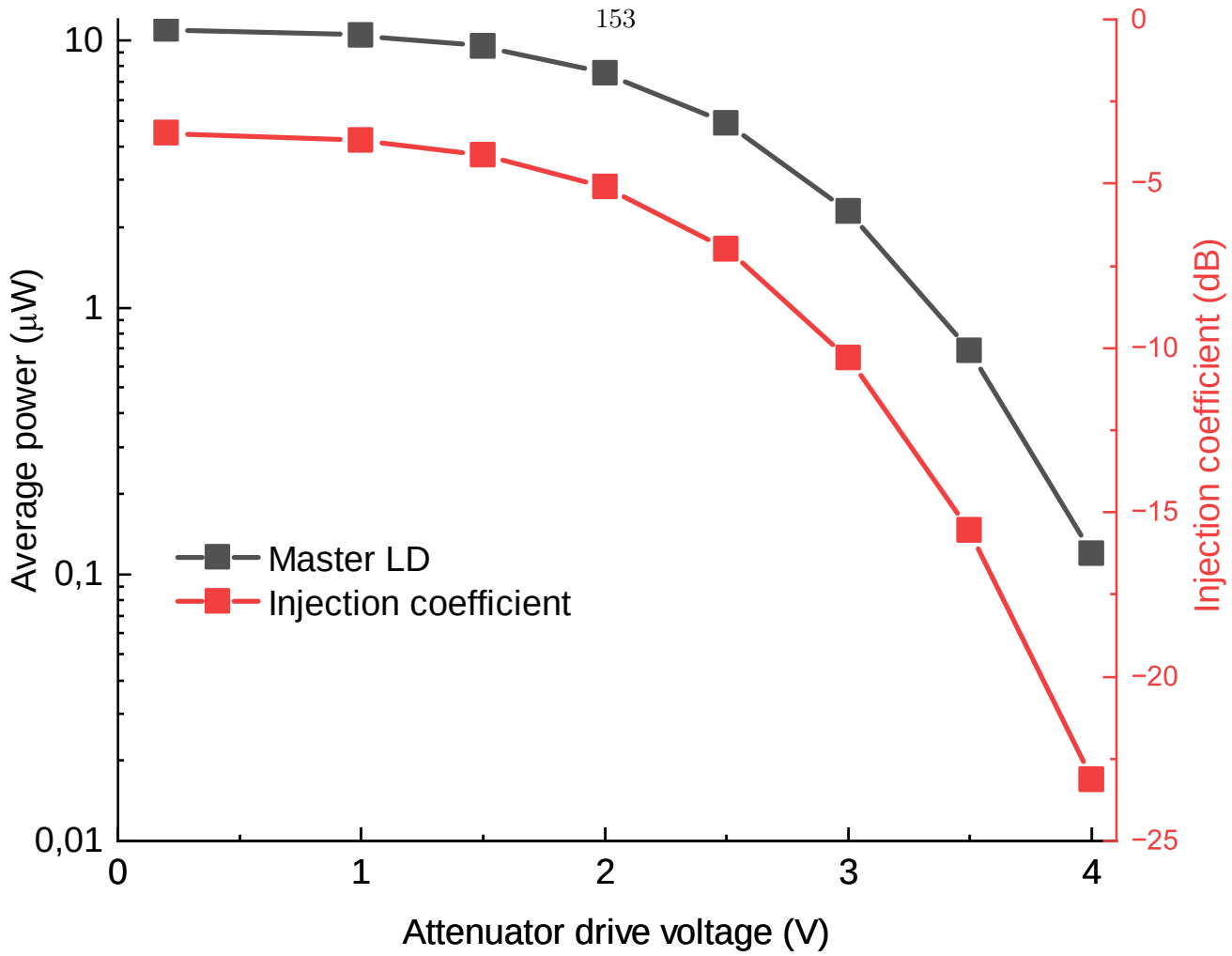

Рисунок 5.6 — Зависимость мощности ведущего лазера (черный) и коэффициента инжекции(красный) от напряжения на аттенюаторе.

го ЛД. И, наконец, мы исследовали выходные спектры КРК под воздействием внешнего излучения с различной рабочей длиной волны.

5.4 Результаты экспериментов

5.4.1 Характеристики источника КРК

Средняя мощность ведущего ЛД на втором порту PMCIR1 изменяется от 11 до 0.12 мкВт при увеличении напряжения VOA до 4 вольт. Рисунок Раздел 5.3.2

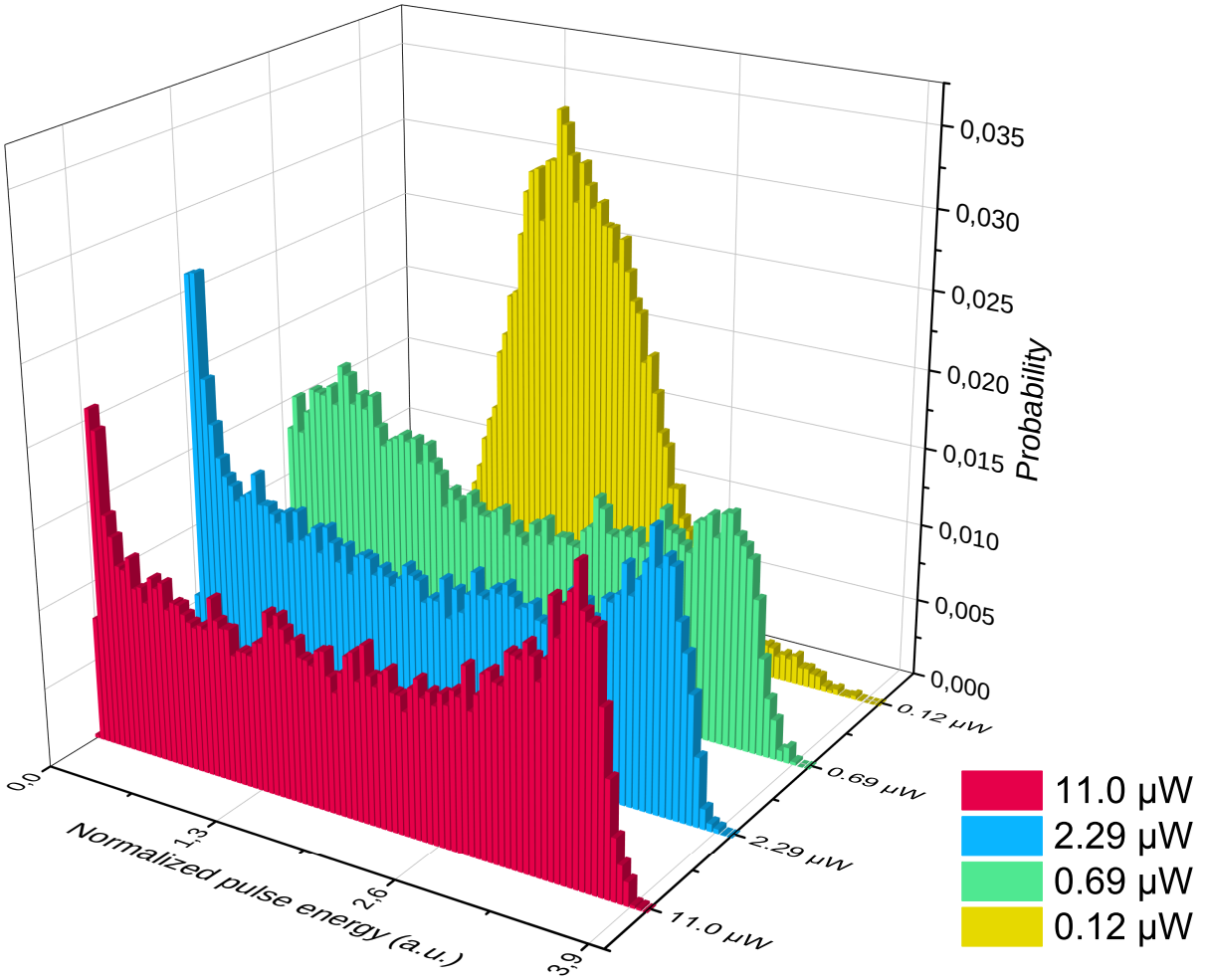

Рисунок 5.7 — Функции плотности вероятности интерференции импульсов источника КРК под действием различной мощности лазера-ведущего

демонстрирует эту зависимость и соответствующий расчетный коэффициент инжекции без учета потерь на сопряжении полупроводникового материала с оптическим волокном внутри ведомого лазера (в зависимости от внутренней конструкции ЛД, он может находиться в диапазоне от 1 до 10 дБ).

Чтобы определить диапазон, в котором ведомый ЛД синхронизируется с излучением ведущего, мы измерили и проанализировали функцию плотности распределения интерференции следующих друг за другом импульсов, спектральные и время-амплитудные характеристики выходных импульсов для каждой мощности ведущего ЛД, построенные на рисунке разд. 5.3.2. ФПР, измеренные для различных мощностей ведущего ЛД на рисункеразд. 5.3.2, показывают, что синхронизация происходит, когда мощность ведущего ЛД находится в диапазоне от 2.29 до 11 мкВт. Форма ФПР имеет два пика, соот-

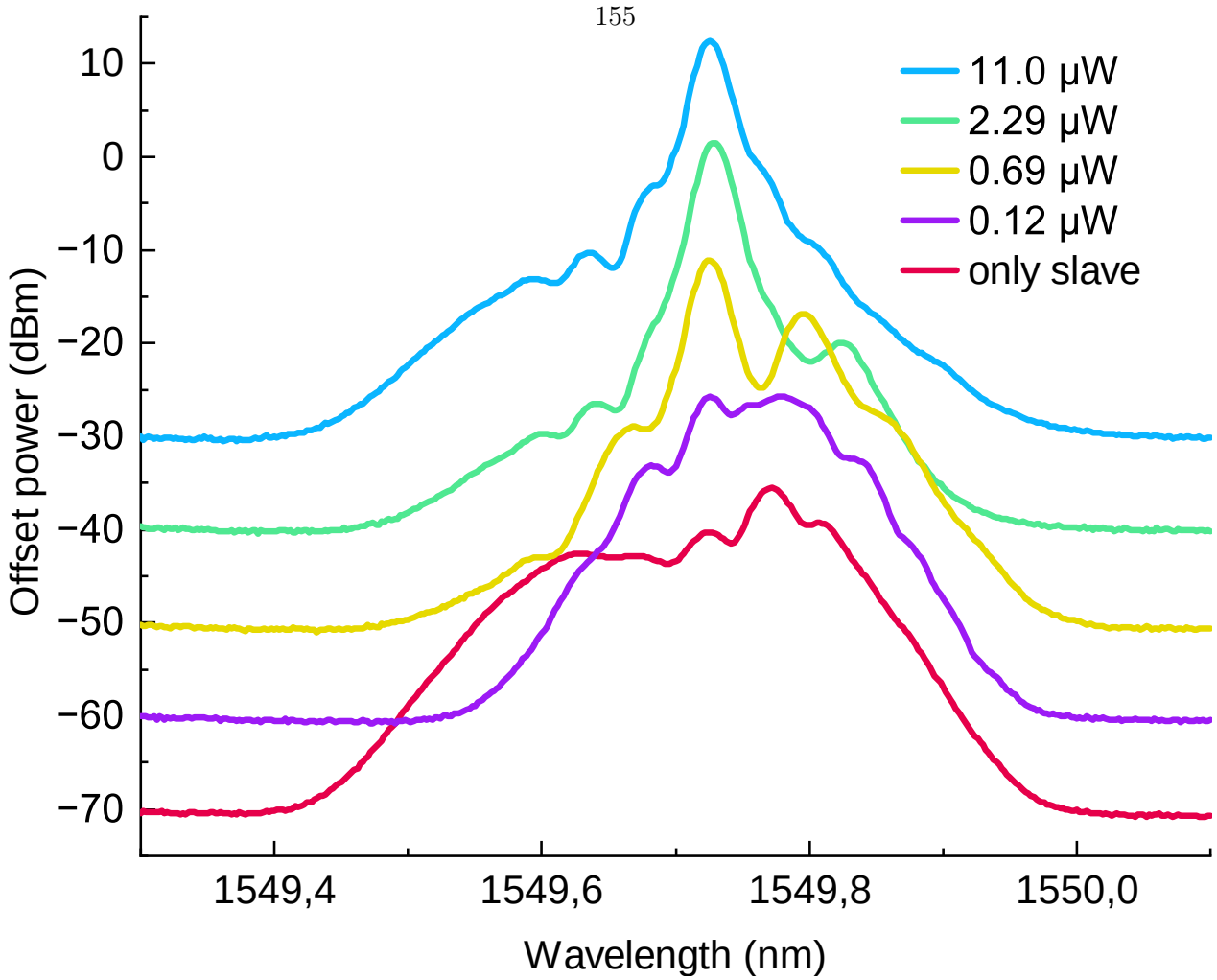

Рисунок 5.8 — Спектры излучения лазера-ведомого под действием переменных мощностей лазера-ведущего

ветствующих идеальной конструктивной и деструктивной интерференции. При мощности основного ЛД 0.69 мкВт видность интерференции ухудшается. И, наконец, при минимальной мощности ведущего 0.12 мкВт, ФПР имеет только один высокий пик в центре. Это означает, что ведомый не имеет оптической синхронизации с ведущим. Без синхронизации временной джиттер импульсов увеличивается, что приводит к увеличению вероятности отсутствия помех.

Из спектров Раздел 5.3.2 и измерений огибающей импульсов разд. 5.3.2 также видно, что ведомый ЛД не синхронизируется с излучением ведущего на 0.12 мкВт. В этом случае длина волны выходного сигнала отличается от длины волны ведущего, а также форма выходного импульса далека от идеальной колоколообразной формы, на нее влияют релаксационные осцилляции. В “граничном” состоянии при мощности ведущего излучения 0.69 мкВт релаксаци-

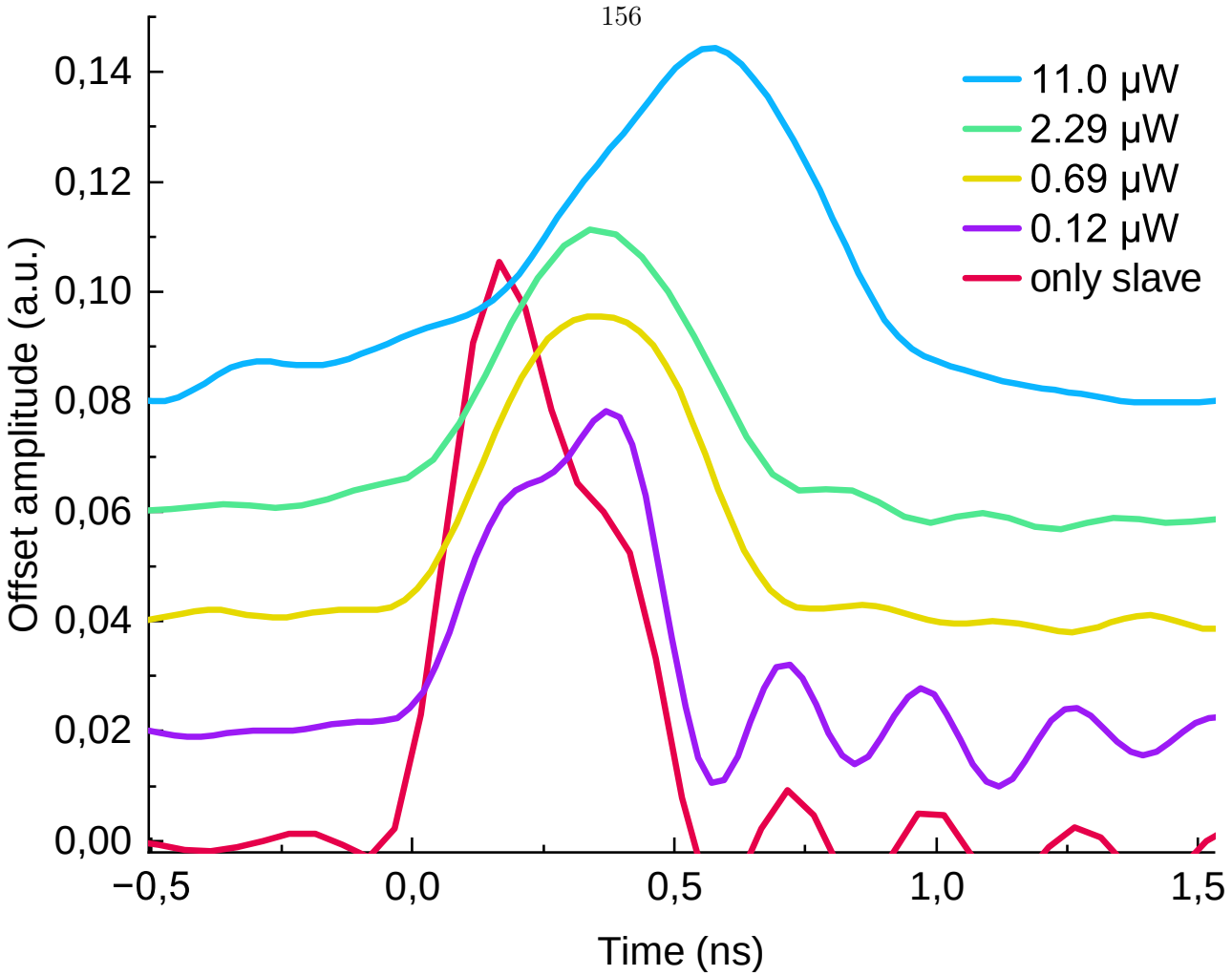

Рисунок 5.9 — Формы импульсов лазера-ведомого под действием различных мощностей лазера-ведущего

онные колебания в форме импульса отсутствуют, в то же время его спектр имеет второй интенсивный пик, по частоте отличающийся от частоты ведущего ЛД.

5.4.2 Длина волны источника равна длине волны источника

Как описано в разд. 5.3, в эксперименте злоумышленником излучается постоянная мощность излучение, а мы изменяется мощность ведущего. Рисунок 5.10 демонстрирует зависимость средней мощности источника КРК от мощности ведущего ЛД для двух случаев: в присутствии света Евы и без него. Для оценки средней оптической мощности атакуемого источника КРК мы сначала измеряем

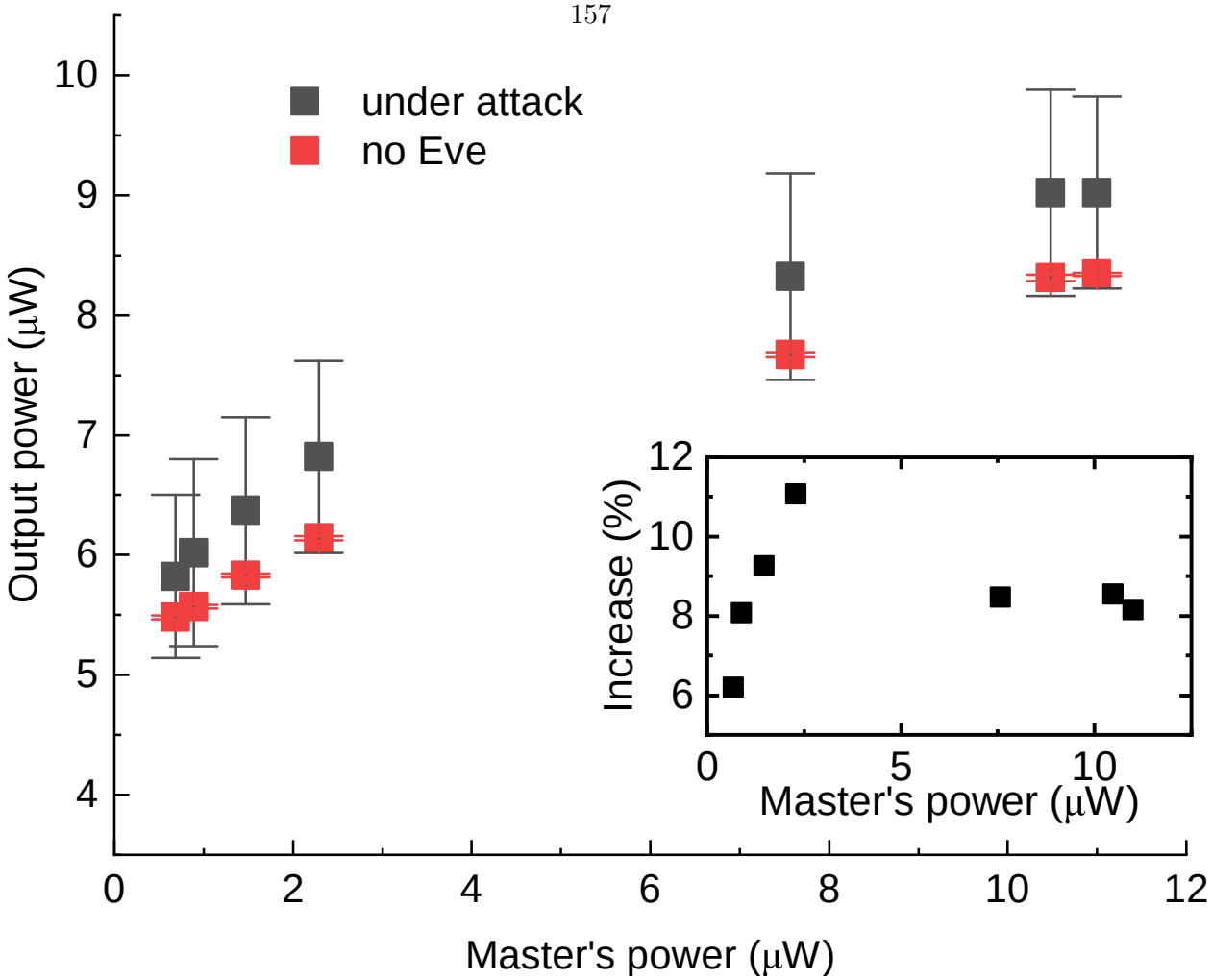

Рисунок 5.10 — Средняя выходная мощность источника КРК без Евы и в присутствии атаки с лазерным засевом.

общую среднюю мощность, а затем вычитаем отраженную мощность Евы, измеренную при выключенном источнике КРК. Мы обнаружили увеличение средней выходной мощности на 6-11%. Как видно из приведенного графика, монотонной зависимости увеличения мощности от мощности ведущего ЛД не наблюдается. Увеличение мощности значительно варьируется при малом сигнале ведущего устройства и становится постоянным около 8% 8 %, когда мощность ведущего устройства составляет от 7.57 до 11 мкВт. Однако более важным является вопрос о том, насколько сильно изменяется энергия импульса. Чтобы ответить на этот вопрос, сначала измерилась среднюю амплитуда и длительность импульса, а также их стандартное отклонение, рассчитанное на основе выборки размером 30 тысяч. Раздел 5.4.2 показывает измеренные амплитуду и длительность, а также рассчитанную нормализованную энергию импульса с атакой и без нее.

Из Раздел 5.4.2(a) и (b) видно, что средняя амплитуда импульса увеличивается при атаке, в то время как длительность импульса почти такая же, как и без атаки. Отклонения обеих измеренных величин увеличиваются при атаке. Энергия импульса рассчитывается как умножение измеренной средней амплитуды на среднюю длительность, а стандартное отклонение энергии импульса (СО) - как квадратный корень из суммы квадратов СО измеренных амплитуды и длительности. (Следует отметить, что примененный метод расчета корректен в случае наших экспериментальных данных, поскольку все измеренные формы импульсов имеют однопиковую форму, близкую к колоколообразной, в то время как в общем случае, когда импульсы имеют сложную форму, энергия может перераспределяться между пиками, и, таким образом, площадь импульса должна быть получена из прямых измерений, а не из отдельных измерений амплитуды и длительности импульса). Раздел 5.4.2c показывает энергию импульса с атакой и без атаки, нормированную на энергию без атаки при каждой мощности ведущего ЛД. Вставленный график демонстрирует стандартное отклонение энергии импульса для обоих случаев. Изменение энергии импульса при атаке не показывает зависимости от мощности ведущего ЛД, она распределяется хаотично. Максимальное увеличение средней энергии импульса составляет 2.8%2,8%, когда мощность ведущего ЛД равна 7.57 мкВт. В то же время, колебания энергии импульса увеличиваются во всех исследованных случаях. Стандартное отклонение стало выше примерно на 3% при атаке по сравнению с результатами без атаки.

В рамках работы также проведена оценка временного джиттера в присутствии и без атаки. Он определяется как стандартное отклонение измерения периода при 30 тыс. отсчетов. Оно составляет 125-128 пс без света Евы и почти такое же 126-130 пс в присутствии атаки.

Мы предполагаем, что разница между увеличением средней мощности и энергии импульса означает, что наибольший вклад в увеличение средней мощности вносит усиление излучения Евы в ведомом лазере, а не изменение выходных импульсов. Слабое увеличение энергии импульса и стабильное повышение его стабильности обусловлены слабыми изменениями числа электронов в валент-

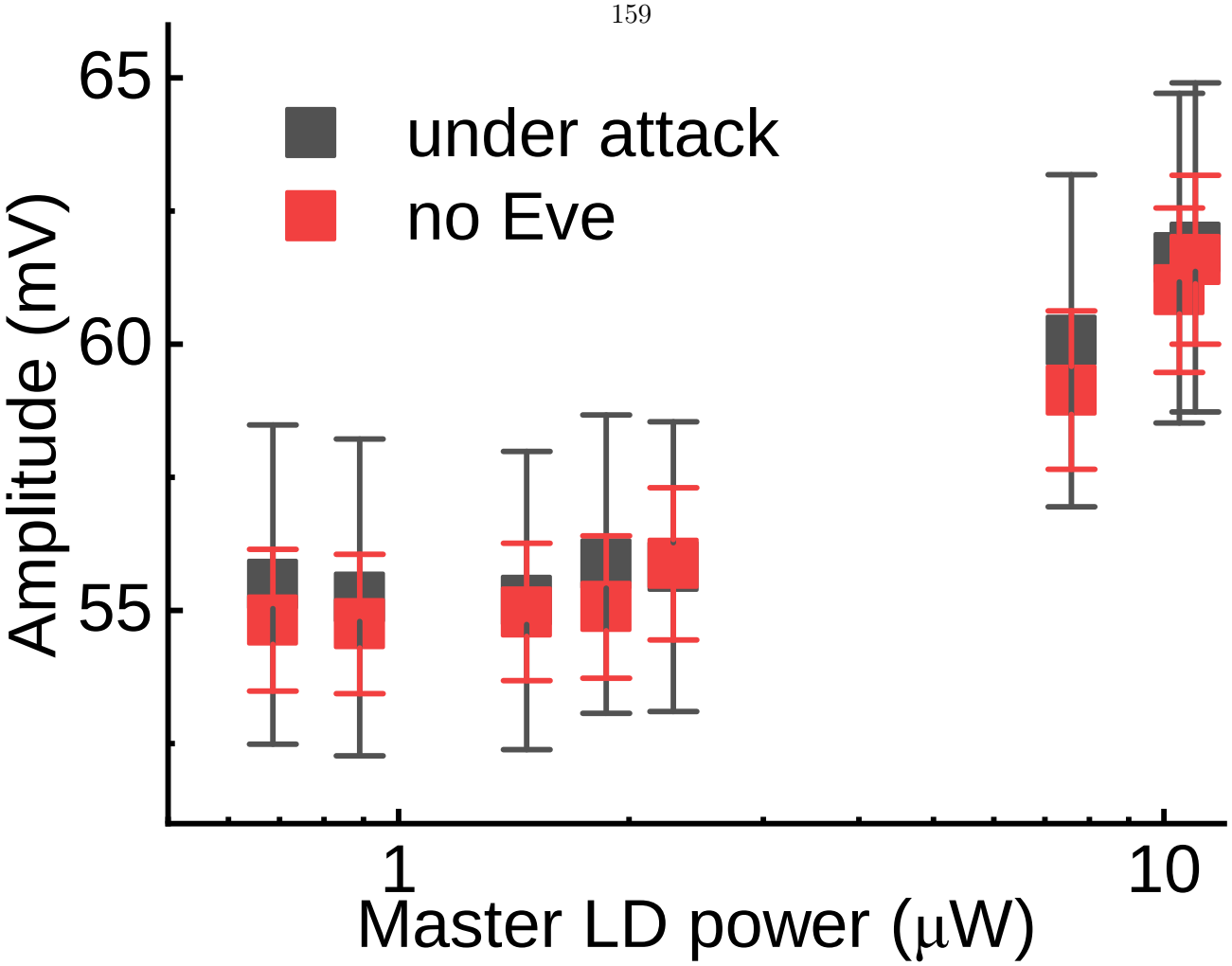

Рисунок 5.11 — Изменение средней амплитуды импульсов. Черным цветом обозначены амплитуды импульсов под действием атаки, а красным без нее.

ной зоне, вызванными стимулированным поглощением инжектированного света Евы.

В наших экспериментах мы также количественно оценили влияние инжектированного света на статистику интерференции. Раздел 5.4.2 и Раздел 5.4.2 позволяет сравнить функции плотности вероятности интерференционного сигнала со светом Евы и без него для двух граничных случаев - когда ведущий лазер принимает максимальное и минимальное значения для обеспечения синхронизации. В обоих случаях мы наблюдаем изменения в ФПР из-за атаки внешнего света.

Чтобы количественно оценить влияние света Евы на интерференцию, видимость интерференции оценивается по ф-л. 5.3, где ожидаемые интенсивности конструктивной и деструктивной интерференции берутся по пиковым значени-

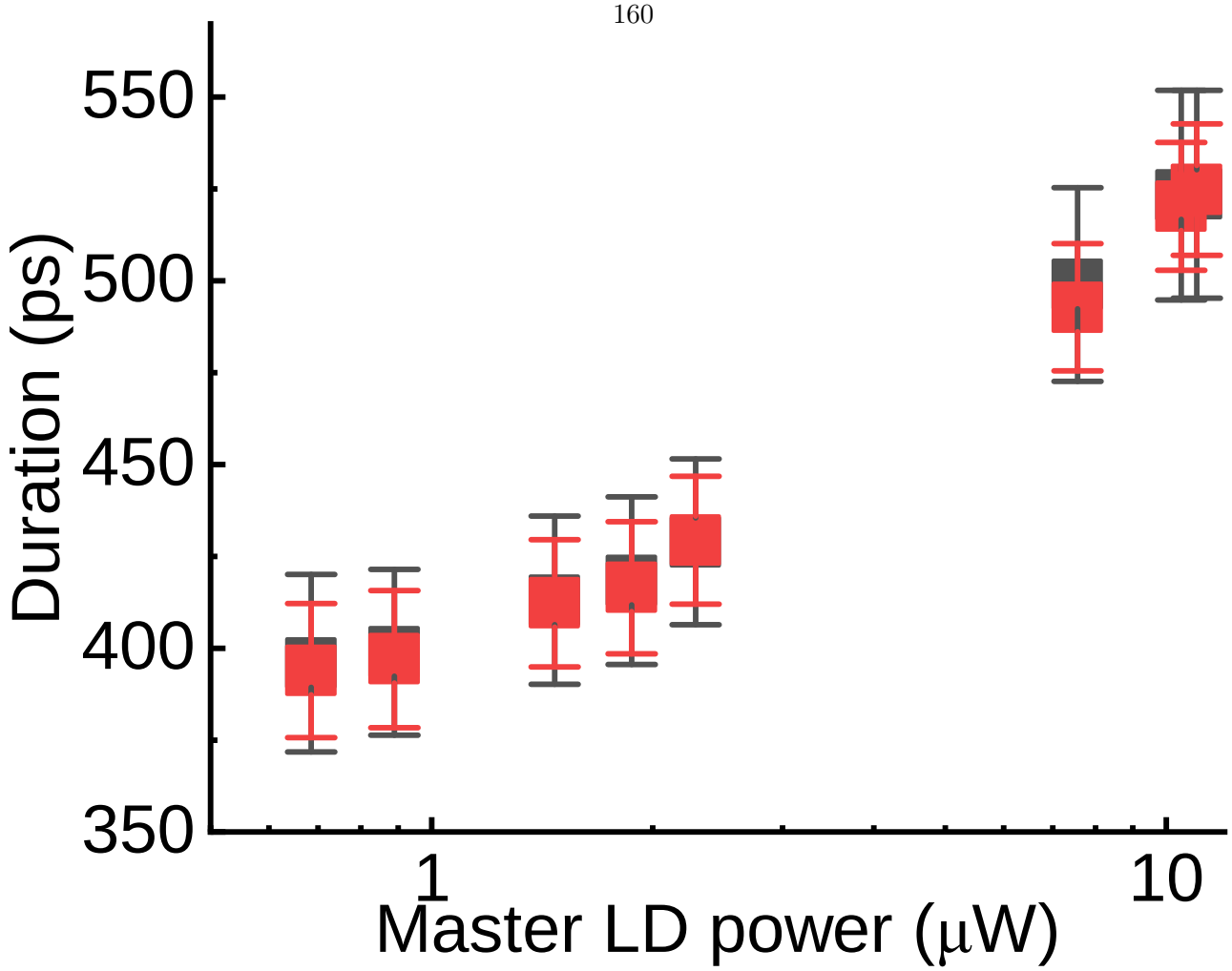

Рисунок 5.12 — Изменение средней длительности импульсов. Черным цветом обозначены длительности импульсов под действием атаки, а красным без нее.

ям вероятности экспериментальных ФПВ. Видность уменьшается примерно с 86.4 до 80.1 , когда мощность ведущего устройства принимает максимальное значение в 11 мкВт, примерно с 71.5 до 52.5, когда мощность ведущего устройства составляет 0.69 мкВт . Таким образом, влияние света злоумышленника на интерференционный сигнал усиливается с уменьшением соотношения мощностей хозяина и Евы. Мы предполагаем, что этот эффект вызван смешением усиленного света Евы с мешающими импульсами Алисы и, как было показано в начале текста, увеличением колебаний энергии импульсов, а не фазовой перестройкой между светом ведущего и Евы при его усилении в ведомом ЛД.

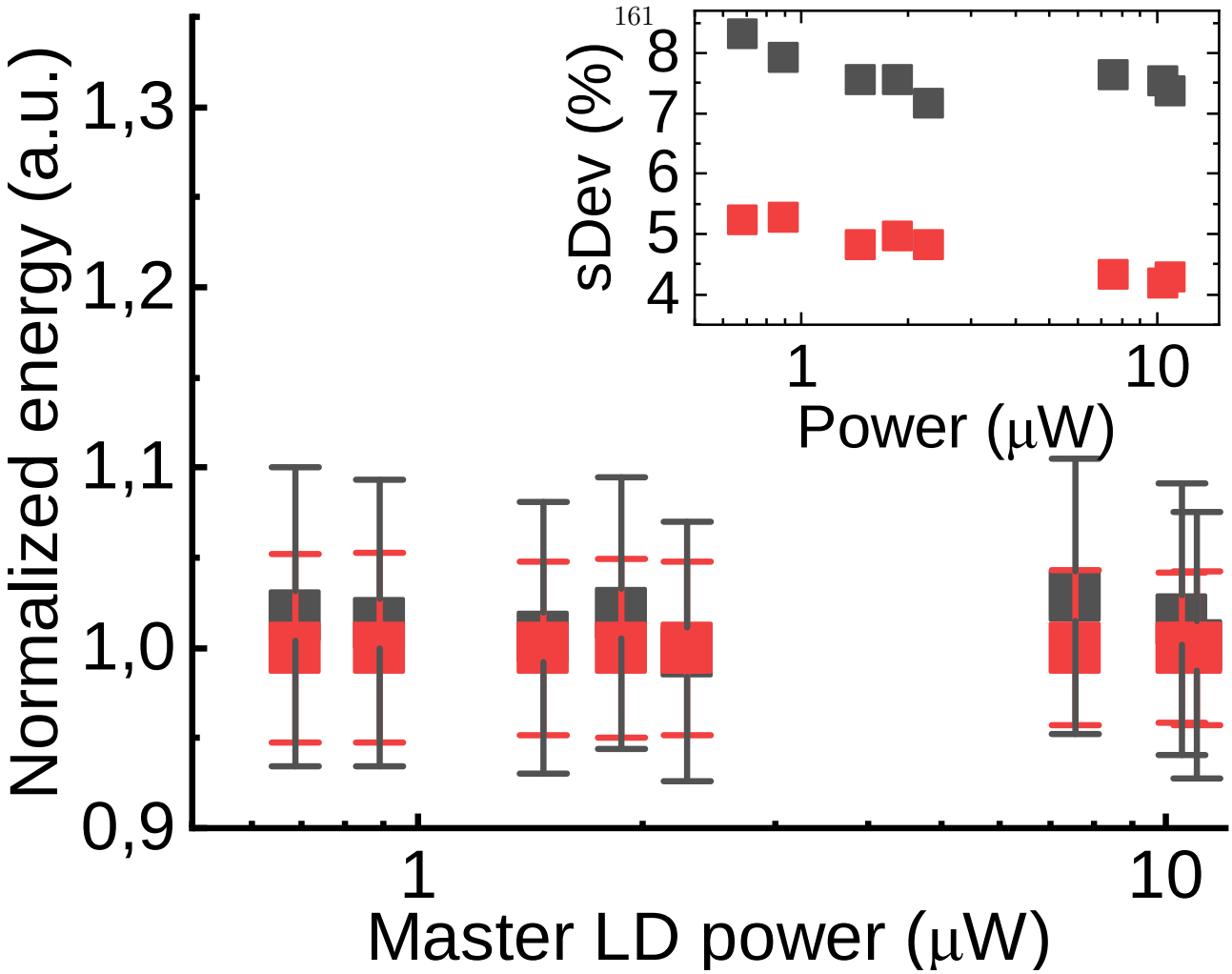

Рисунок 5.13 — Изменение средней площади импульсов. Черным цветом обозначены площади импульсов под действием атаки, а красным без нее.

5.4.3 Атака в зависимости от длины волны

. В этом разделе исследуется влияние лазера Евы, работающего на разных длинах волн, на выходной спектр источника КРК. Длина волны атакующего лазера изменялась в зависимости от температуры диода его затравочного лазера, а мощность инжектируемого света Евы была одинаковой во всех измерениях.

Рисунок 5.16 показывает выходные спектры для различных длин волн затравочного лазера. Спектры атакуемого КРК источника и отраженного излучения Евы с выключенным QKD-источником измеряются отдельно. Далее, чтобы оценить, усиливает ли ведомый лазер излучение Евы или нет, отраженные спектры вычитаются из спектров атакуемого источника QKD.

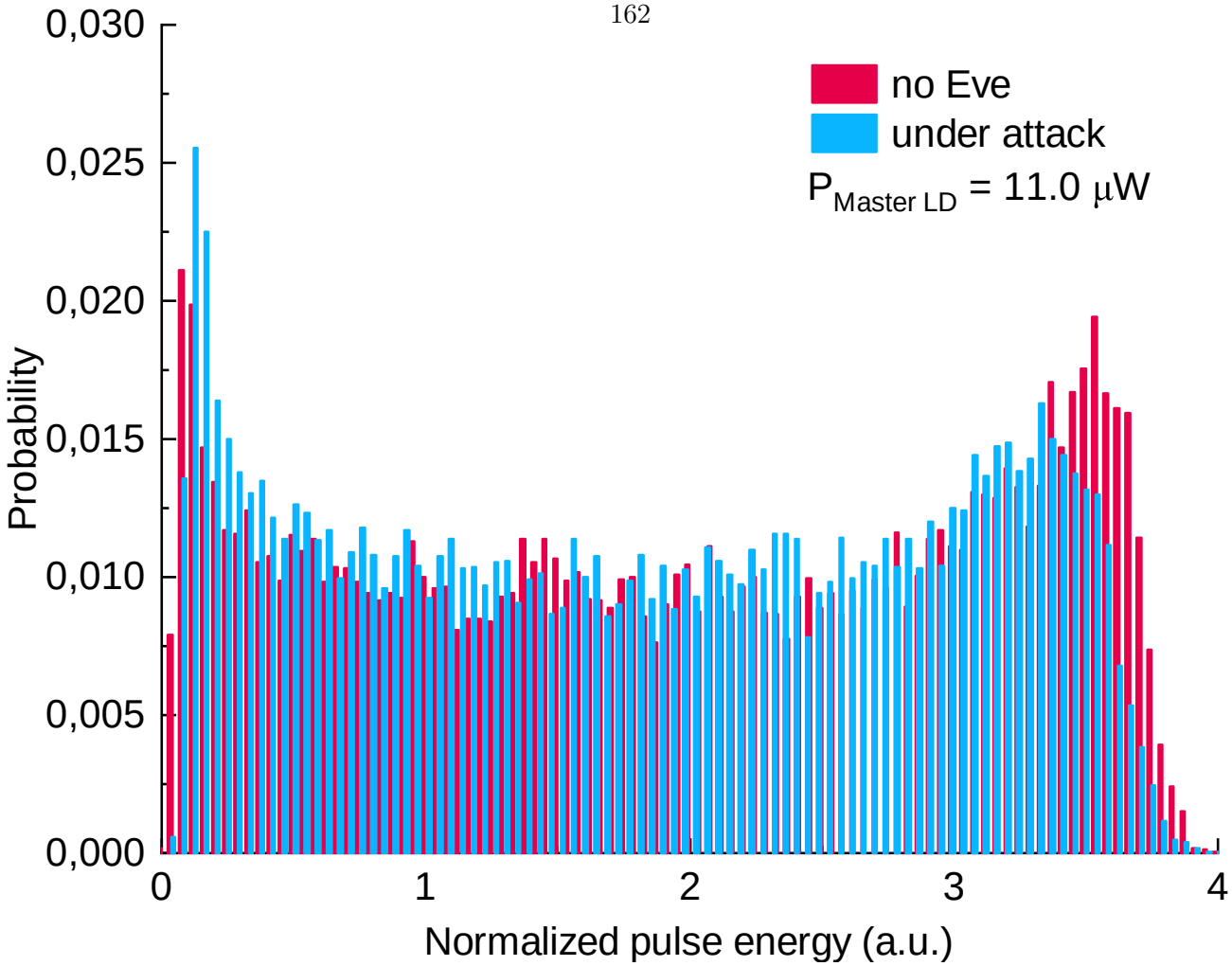

Рисунок 5.14 — Функция плотности вероятности интерференции при мощности лазера-ведущего 11 мкВт. Красным обозначена ФПВ без атаки, синим цветом обозначена ФПВ под действием атаки.

Отметим, что реализованная процедура измерения не является точной для получения коэффициентов усиления, более того, спектральное разрешение в 0.02 нм дает лишь грубую оценку спектральных характеристик при определении характеристик DFB-лазеров. Однако этого достаточно, чтобы показать, что излучение Евы усиливается ведомым лазером в широком спектральном диапазоне.

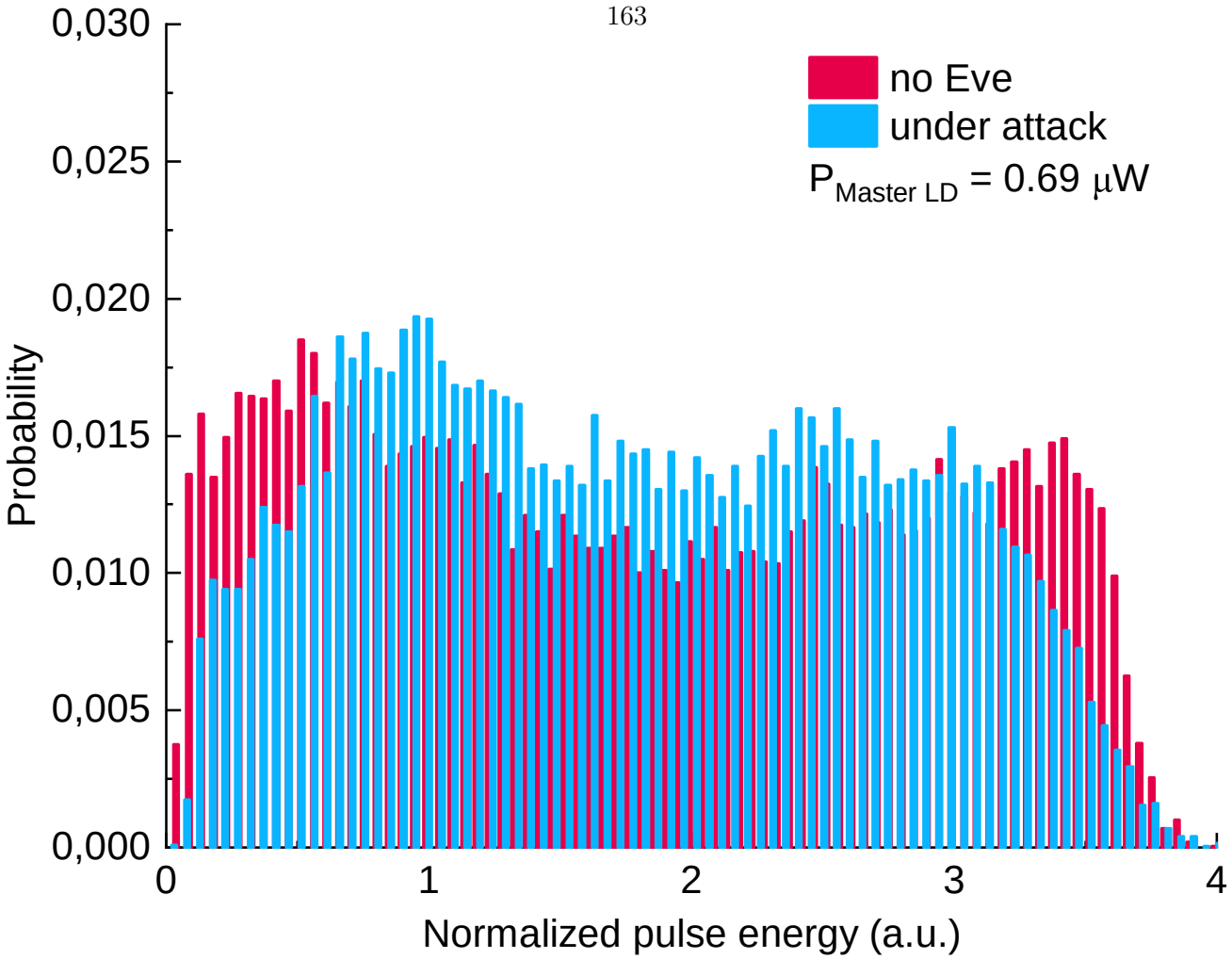

Рисунок 5.15 — Функция плотности вероятности интерференции при мощности лазера-ведущего 0.69 мкВт. Красным обозначена ФПВ без атаки, синим цветом обозначена ФПВ под действием атаки.

5.5 Выводы по главе

В рамках данной главы впервые рассматривалась атака "засевом"лазерным излучением источника на основе оптической инжекции для систем квантового распределения ключей. В результате работы было оценено влияние атаки злоумышленника с помощью лазера мощностью в 500 мВт. Эта атака приводит к увеличению средней мощности излучения до 11%, увеличивает энергию импульсов на 2.8% и стандартное отклонение их амплитуды на 3%. При этом длительность импульсов не изменяется. Также был рассмотрен вопрос усиления других длин волн излучения злоумышленника. Источник излуче-

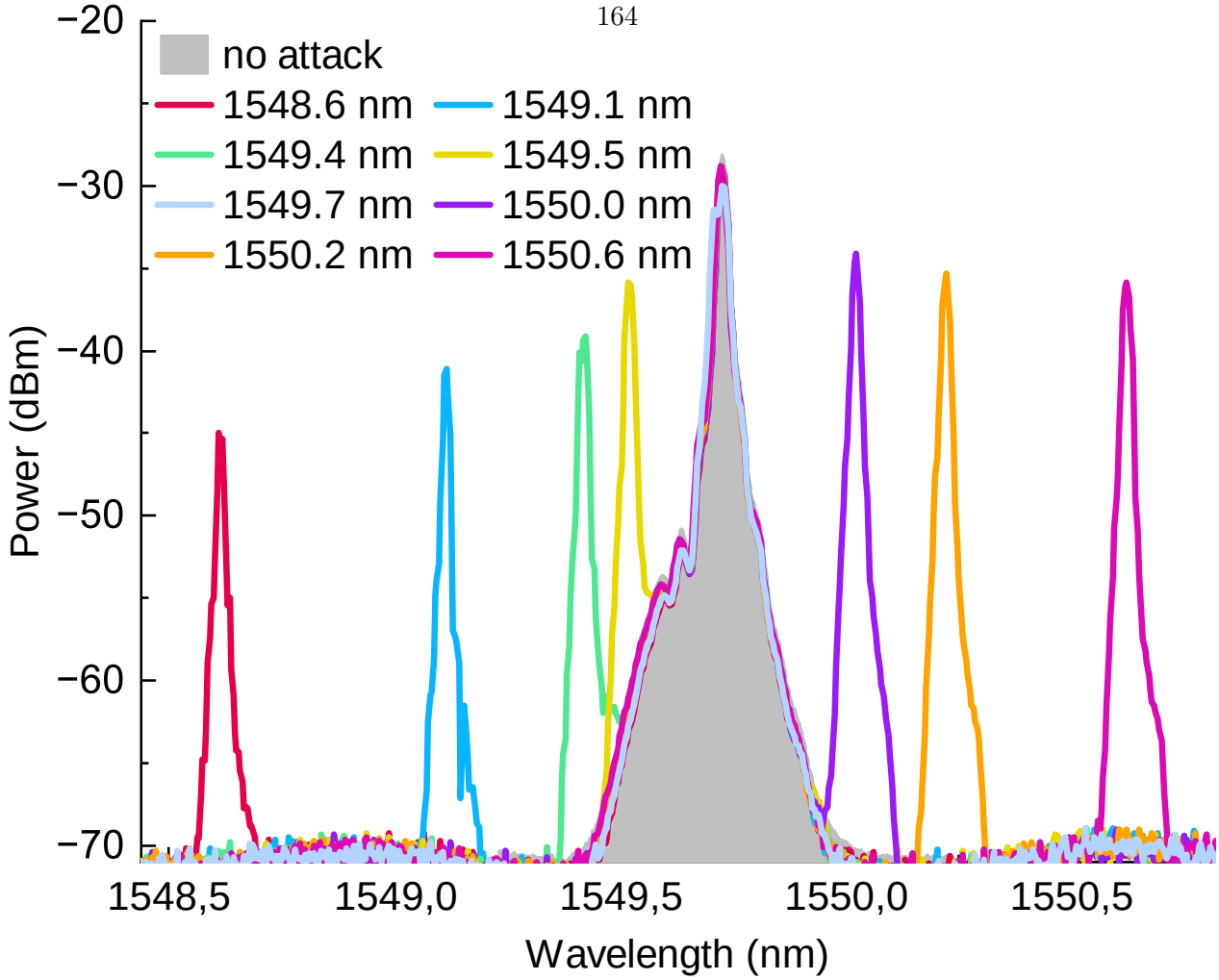

Рисунок 5.16 — Спектры выходного сигнала источника QKD для разных длин волн лазера Евы. (Спектры отраженного излучения Евы исключены из измеренных выходных спектров)

.

ния, построенный на основе оптчиеской инжекции, является устойчивым к атаке лазерным "засеовм"благодаря наличию оптического циркулятора и дополнительного внешнего излучения от лазера-ведущего. В результате чего злоумышленнику необходимо как пройти изоляцию этого циркулятора, так и превзойти лазер-ведущий, чтобы осуществить атаку. Это возможно только с помощью высокомощного излучения, которое смогут обнаружить легитимные пользователи.

Заключение

Список литературы

1. Eavesdrop-detecting quantum communications channel / C. H. Bennett, G. Brassard, S. Breidbart, S. Wiesner // *IBM Tech. Discl. Bull.* — 1984. — Vol. 26. — Pp. 4363–4366.

2. Quantum hacking: Experimental demonstration of time-shift attack against practical quantum-key-distribution systems / Yi Zhao, Chi-Hang Fred Fung, Bing Qi et al. // *Phys. Rev. A.* — 2008. — Vol. 78, no. 4. — P. 042333.

3. *Inamori H., Lütkenhaus N., Mayers D.* Unconditional security of practical quantum key distribution // *Eur. Phys. J. D.* — 2007. — Vol. 41. — Pp. 599–627.

4. Security of quantum key distribution with imperfect devices / D. Gottesman, H.-K. Lo, N. Lütkenhaus, J. Preskill // *Quantum Inf. Comput.* — 2004. — Vol. 4. — Pp. 325–360.

5. *Bennett Charles H., Brassard Gilles.* Quantum cryptography: public key distribution and coin tossing // Proc. International Conference on Computers, Systems, and Signal Processing. — Bangalore, India: IEEE Press, New York, 1984. — Pp. 175–179.

6. *Lo Hoi-Kwong, Ma Xiongfeng, Chen Kai.* Decoy state quantum key distribution // *Phys. Rev. Lett.* — 2005. — Vol. 94, no. 23. — P. 230504.

7. *Hong C. K., Ou Z. Y., Mandel L.* Measurement of subpicosecond time intervals between two photons by interference // *Phys. Rev. Lett.* — 1987. — Nov. — Vol. 59. — Pp. 2044–2046. — URL: https://link.aps.org/doi/10.1103/PhysRevLett.59.2044.

8. *Ma Xiongfeng, Fung Chi-Hang Fred, Lo Hoi-Kwong.* Quantum key distribution with entangled photon sources // *Phys. Rev. A.* — 2007. — Jul. — Vol. 76. — P. 012307. — URL: https://link.aps.org/doi/10.1103/PhysRevA.76.012307.

9. Practical decoy state for quantum key distribution / Xiongfeng Ma, Bing Qi, Yi Zhao, Hoi-Kwong Lo // *Phys. Rev. A.* — 2005. — Vol. 72. — P. 012326.

10. Practical long-distance quantum key distribution system using decoy levels / D. Rosenberg, C. G. Peterson, J. W. Harrington et al. // *New J. Phys.* — 2009. — Vol. 11. — P. 045009.

11. Optimal eavesdropping in quantum cryptography. 1. Information bound and optimal strategy / C. A. Fuchs, N. Gisin, R. B. Griffiths et al. // *Phys. Rev. A.* — 1997. — Vol. 56, no. 2. — Pp. 1163–1172.

12. Phase encoding schemes for measurement-device-independent quantum key distribution with basis-dependent flaw / Kiyoshi Tamaki, Hoi-Kwong Lo, Chi-Hang Fred Fung, Bing Qi // *Physical Review A.* — 2012. — Apr. — Vol. 85, no. 4. — URL: http://dx.doi.org/10.1103/PhysRevA.85.042307.

13. *Gobby C., Yuan Z. L., Shields A. J.* Quantum key distribution over 122 km of standard telecom fiber // *Appl. Phys. Lett.* — 2004. — Vol. 84, no. 19. — Pp. 3762–3764.

14. *Jouguet Paul, Kunz-Jacques Sébastien, Diamanti Eleni.* Preventing calibration attacks on the local oscillator in continuous-variable quantum key distribution // *Phys. Rev. A.* — 2013. — Vol. 87. — P. 062313.

15. Preparing a commercial quantum key distribution system for certification against implementation loopholes / Vadim Makarov, Alexey Abrikosov, Poompong Chaiwongkhot et al. // *arXiv.* — 2023.

16. *Sun Shihai, Huang Anqi.* A review of security evaluation of practical quantum key distribution system // *Entropy.* — 2022. — Vol. 24, no. 2. — P. 260.

17. Quantum key distribution using deterministic single-photon sources over a field--installed fibre link / Mujtaba Zahidy, Mikkel T. Mikkelsen, Ronny Müller et al. // *Npj Quantum Inf.* — 2024. — Vol. 10. — P. 2.

18. Laser-seeding attack in quantum key distribution / Anqi Huang, Álvaro Navarrete, Shi-Hai Sun et al. // *Phys. Rev. Appl.* — 2019. — Vol. 12. — P. 064043.

19. Hacking quantum key distribution via injection locking / Xiao-Ling Pang, Ai-Lin Yang, Chao-Ni Zhang et al. // *Phys. Rev. Appl.* — 2020. — Vol. 13. — P. 034008.

20. Quantified effects of the laser-seeding attack in quantum key distribution / V. Lovic, D.G. Marangon, P.R. Smith et al. // *Phys. Rev. Appl.* — 2023. — Vol. 20. — P. 044005.

21. High-Speed Measurement-Device-Independent Quantum Key Distribution with Integrated Silicon Photonics / Kejin Wei, Wei Li, Hao Tan et al. // *Phys.Rev.X.* — 2020. — Vol. 10. — P. 031030.

22. Gigahertz measurement-device-independent quantum key distribution using directly modulated lasers / R. I. Woodward, Y. S. Lo, M. Pittaluga et al. // *npj Quantum Inf.* — 2021. — Vol. 7. — P. 58.

23. Quantum cryptography without detector vulnerabilities using optically-seeded lasers / L C Comandar, M Lucamarini, B Fröhlich et al. // *Nat. Photonics.* — 2016. — Vol. 10. — Pp. 312–315.

24. Optically injected intensity-stable pulse source for secure quantum key distribution / Hong-Bo Xie, Yang Li, Cong Jiang et al. // *Opt. Express.* — 2019. — Vol. 27, no. 9. — Pp. 12231–12240.

25. *Liu Zhixin, Slavík Radan.* Optical Injection Locking: from Principle to Applications // *J. Light. Technol.* — 2020. — Vol. 38, no. 1. — Pp. 43–59.

26. *Lau Erwin K., Sung Hyuk-Kee, Wu Ming C.* Frequency Response Enhancement of Optical Injection-Locked Lasers // *IEEE J. Quantum Electron.* — 2008. — Vol. 44, no. 1. — Pp. 90–99.

27. Rate equation analysis of injection-locked quantum cascade lasers / Cheng Wang, Frédéric Grillot, Vassilios Kovanis, Jacky Even // *J. Appl. Phys.* — 2013. — Vol. 113, no. 6. — P. 063104.

28. Quantum noise extraction from the interference of laser pulses in an optical quantum random number generator / Roman Shakhovoy, Denis Sych, Violetta Sharoglazova et al. // *Opt. Express.* — 2020. — Vol. 28, no. 5. — Pp. 6209–6224.

29. Influence of Chirp, Jitter, and Relaxation Oscillations on Probabilistic Properties of Laser Pulse Interference / Roman Shakhovoy, Violetta Sharoglazova, Alexander Udaltsov et al. // *IEEE J. Quantum Electron.* — 2021. — Vol. 57, no. 2. — P. 2000307.

30. Laser-damage attack against optical attenuators in quantum key distribution / Anqi Huang, Ruoping Li, Vladimir Egorov et al. // *Phys. Rev. Appl.* — 2020. — Vol. 13. — P. 034017.